Wspólna opinia EROD i EIOD 2/2022 na temat wniosku Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (akt w sprawie danych)

Przyjęta 4 maja 2022 r.

Streszczenie

W niniejszej wspólnej opinii EROD i EIOD pragną zwrócić uwagę na szereg nadrzędnych obaw związanych z wnioskiem dotyczącym aktu w sprawie danych i wezwać współprawodawców do podjęcia zdecydowanych działań.

EROD i EIOD zauważają, że wniosek będzie miał zastosowanie do szerokiej gamy produktów i usług, w tym do produktów skomunikowanych („internet rzeczy"), wyrobów medycznych lub zdrowotnych oraz wirtualnych asystentów. Niektóre produkty i usługi mogą nawet przetwarzać szczególne kategorie danych osobowych, takie jak dane dotyczące zdrowia lub dane biometryczne. Zważywszy że niektórych rodzajów danych nie wykluczono wyraźnie z zakresu stosowania wniosku, dane ujawniające szczególnie chronione informacje o osobach fizycznych mogłyby stać się przedmiotem udostępniania i wykorzystywania danych zgodnie z zasadami określonymi we wniosku.

EROD i EIOD z zadowoleniem przyjmują starania służące zapewnieniu, aby wniosek nie miał wpływu na obecne ramy ochrony danych, uważają jednak, że konieczne są dodatkowe zabezpieczenia, aby uniknąć obniżenia w praktyce poziomu ochrony podstawowych praw do prywatności i do ochrony danych osobowych. Po pierwsze, dodatkowe zabezpieczenia są szczególnie konieczne, ponieważ wynikające z wniosku prawa do dostępu do danych oraz ich wykorzystywania i udostępniania prawdopodobnie rozciągałyby się na podmioty inne niż osoby, których dane dotyczą, w tym przedsiębiorstwa, w zależności od tytułu prawnego, na podstawie którego urządzenie jest używane. Po drugie, EROD i EIOD są głęboko zaniepokojeni przepisami wniosku dotyczącymi obowiązku udostępniania danych organom sektora publicznego oraz instytucjom, agencjom lub organom Unii w przypadku „wyjątkowej potrzeby". Ponadto EROD i EIOD obawiają się, że mechanizm nadzoru ustanowiony we wniosku może prowadzić do rozdrobnionego i niespójnego nadzoru.

1. Prawa do dostępu do danych, ich wykorzystywania i udostępniania

Aby ograniczyć ryzyko związane z interpretacją lub wdrożeniem wniosku w sposób, który mógłby mieć wpływ na stosowanie obowiązujących przepisów o ochronie danych lub je podważać, EROD i EIOD wzywają współprawodawcę do wyraźnego sprecyzowania, że w zakresie przetwarzania danych osobowych przepisy o ochronie danych mają pierwszeństwo w przypadku sprzeczności z przepisami wniosku.

Aby promować minimalizację danych, produkty należy projektować w taki sposób, by osoby, których dane dotyczą, miały możliwość korzystania z urządzeń anonimowo lub w sposób jak najmniej naruszający prywatność, niezależnie od ich tytułu prawnego do urządzenia. Posiadacze danych powinni również w jak największym stopniu ograniczyć ilość danych opuszczających urządzenie (np. przez anonimizację danych).

Ponadto rozszerzenie prawa do przenoszenia danych, o którym mowa w motywie 31, jako jeden z celów wniosku, wymagałoby – w zakresie, w jakim dotyczy to danych osobowych – skutecznego wzmocnienia pozycji osób, których dane dotyczą, aby zapewnić tym osobom większą kontrolę nad ich danymi osobowymi. Ponieważ definicja „użytkownika" obejmuje osoby prawne, w przypadku korzystania z tego prawa przez przedsiębiorstwo przybiera ono formę zobowiązania handlowego producenta / posiadacza danych do zapewnienia przedsiębiorstwom dostępu do danych i umożliwienia ich wykorzystywania, a nie „prawa" osób fizycznych do dostępu do swoich danych osobowych i ich przenoszenia. Tak naprawdę zgodnie z pojęciem „użytkownika" przyjętym we wniosku osoby fizyczne stają się uprawnione do rozszerzonego prawa do przenoszenia danych tylko przypadkowo, w zależności od tytułu prawnego, na podstawie którego korzystają z produktu lub powiązanej usługi (własność, najem lub leasing), a nie od ich związku z informacjami dotyczącymi prywatnego korzystania przez te osoby z produktu lub usługi.

W związku z tym, aby zapewnić skuteczne wzmocnienie pozycji osób fizycznych w odniesieniu do ich danych osobowych, pojęcie użytkownika wspomniane w art. 2 pkt 5 wniosku i w całym tekście należy uwzględnić i doprecyzować w następujący sposób: a) dodać do definicji użytkowników „i osoby, których dane dotyczą", b) wyraźne rozróżnić sytuacje, w których użytkownik jest osobą, której dane dotyczą, od sytuacji, w której użytkownik nie jest osobą, której dane dotyczą.

Ponadto EROD i EIOD zalecają doprecyzowanie, że w przypadku gdy użytkownik nie jest osobą, której dane dotyczą, wszelkie dane osobowe wygenerowane w wyniku korzystania z produktu lub powiązanej usługi udostępnia się użytkownikowi wyłącznie zgodnie z szczególnie art. 6 i 9 RODO oraz pod warunkiem spełnienia wymogów określonych w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Podobne zastrzeżenia dotyczą udostępniania danych osobom trzecim na wniosek użytkownika biznesowego.

EROD i EIOD podkreślają potrzebę zapewnienia, aby dostęp do danych osobowych oraz ich wykorzystywanie i udostępnianie przez użytkowników innych niż osoby, których dane dotyczą, a także przez osoby trzecie i posiadaczy danych odbywało się w pełnej zgodności z wszystkimi przepisami RODO, rozporządzenia (UE) 2018/1725 oraz dyrektywy o prywatności i łączności elektronicznej, włącznie z informowaniem osób, których dane dotyczą, o dostępie administratorów do ich danych osobowych i ułatwianiem administratorom wykonywanie praw osób, których dane dotyczą. EROD i EIOD przypominają również, że ważne jest zapewnienie, aby wszelkie dalsze przetwarzanie danych osobowych było zgodne w szczególności z art. 6 ust. 4 RODO oraz, w głównej mierze ze względu na możliwość zautomatyzowanego podejmowania decyzji, w tym profilowania, z odpowiednimi obowiązkami przewidzianymi w art. 22 RODO.

EROD i EIOD zalecają również ujęcie we wniosku wyraźnych ograniczeń lub obostrzeń co do wykorzystywania danych osobowych generowanych w wyniku korzystania z produktu lub usługi przez dowolny podmiot inny niż osoby, których dane dotyczą, zwłaszcza w przypadkach gdy dane te mogą pozwolić na wyciągnięcie precyzyjnych wniosków dotyczących życia prywatnego tych osób lub w inny sposób wiązałyby się z dużym ryzykiem dla praw i wolności zainteresowanych osób. EIOD i EROD zalecają w szczególności wprowadzenie wyraźnych ograniczeń dotyczących wykorzystywania danych osobowych generowanych w wyniku korzystania z produktu lub powiązanych usług do celów marketingu bezpośredniego lub reklamy bezpośredniej, monitorowania pracowników, punktowej oceny kredytowej lub określania kwalifikowalności do ubezpieczenia zdrowotnego, obliczania lub zmiany składek ubezpieczeniowych. To zalecenie pozostaje bez uszczerbku dla wszelkich dalszych ograniczeń, które mogą być stosowne, na przykład w celu ochrony osób wymagających szczególnego traktowania, zwłaszcza małoletnich, lub ze względu na szczególnie wrażliwy charakter niektórych kategorii danych (np. danych dotyczących korzystania z wyrobu medycznego lub danych biometrycznych) oraz ochrony zapewnianej przez unijne przepisy o ochronie danych.

2. Obowiązek udostępniania danych w przypadku „wyjątkowej potrzeby"

W odniesieniu do rozdziału V wniosku EROD i EIOD mają poważne obawy co do zgodności z prawem, konieczności i proporcjonalności obowiązku udostępniania danych organom sektora publicznego oraz instytucjom, agencjom lub organom Unii w przypadku „wyjątkowej potrzeby".

EROD i EIOD przypominają, że wszelkie ograniczenia prawa do danych osobowych muszą opierać się na podstawie prawnej, która jest odpowiednio dostępna i przewidywalna oraz sformułowana na tyle precyzyjnie, by osoby fizyczne mogły zrozumieć jej zakres stosowania. Zgodnie z zasadami konieczności i proporcjonalności podstawa prawna musi również określać zakres i sposób wykonywania uprawnień przez właściwe organy oraz muszą jej towarzyszyć wystarczające zabezpieczenia chroniące osoby fizyczne przed arbitralną ingerencją.

EROD i EIOD zauważają, że okoliczności uzasadniające dostęp nie są ściśle sprecyzowane, i uważają, że prawodawca powinien znacznie skrupulatniej określić założenia dotyczące niebezpieczeństwa lub wyjątkowej potrzeby. Ponadto EROD i EIOD uważają, że niektóre organy sektora publicznego oraz instytucje, agencje i organy Unii powinny być jako takie wyłączone z zakresu stosowania rozdziału V i powinny mieć wyłącznie możliwość zobowiązania posiadaczy danych do udostępniania danych zgodnie z uprawnieniami przewidzianymi w przepisach sektorowych.

3. Wdrożenie i egzekwowanie

EROD i EIOD zwracają uwagę na ryzyko trudności operacyjnych, które mogą wynikać z wyznaczenia więcej niż jednego właściwego organu odpowiedzialnego za stosowanie i egzekwowanie wniosku. EROD i EIOD mają poważne obawy, że ta struktura zarządzania doprowadzi do złożoności i nieporozumień zarówno dla organizacji, jak i osób, których dane dotyczą, oraz do rozbieżności w podejściu regulacyjnym w całej Unii, a tym samym wpłynie na spójność monitorowania i egzekwowania.

EROD i EIOD z zadowoleniem przyjmują wyznaczenie organów nadzorczych odpowiedzialnych za ochronę danych jako właściwych organów zajmujących się monitorowaniem stosowania przepisów wniosku w zakresie ochrony danych osobowych, co jest ważne dla uniknięcia niespójności i ewentualnych konfliktów między przepisami wniosku a przepisami o ochronie danych oraz dla zachowania podstawowego prawa do ochrony danych osobowych określonego w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) i art. 8 Karty praw podstawowych Unii Europejskiej.

EROD i EIOD zwracają się do współprawodawców o wyznaczenie w przedmiotowym wniosku również krajowych organów nadzorczych odpowiedzialnych za ochronę danych jako właściwych organów koordynujących. Organy nadzorcze odpowiedzialne za ochronę danych dysponują wyjątkową wiedzą fachową, zarówno prawną, jak i techniczną, w zakresie monitorowania zgodności przetwarzania danych. Ponadto EROD i EIOD są zdania, że ze względu na to, iż RODO ma zastosowanie, gdy w zbiorze danych dane osobowe i nieosobowe są nierozerwalnie związane, rola organów ochrony danych powinna przeważać w strukturze zarządzania określonej we wniosku.

Biorąc pod uwagę nadzorczą rolę EIOD jako organu ochrony danych w instytucjach, organach i agencjach Unii Europejskiej oraz fakt, że niektóre unijne instytucje, organy i agencje mogą również działać jako użytkownik lub posiadacz danych w rozumieniu omawianego wniosku, EROD i EIOD zalecają dodanie odniesienia do EIOD jako organu właściwego do nadzorowania całego wniosku w zakresie, w jakim dotyczy on instytucji, organów, urzędów i agencji Unii.

Spis treści

Europejska Rada Ochrony Danych i Europejski Inspektor Ochrony Danych

uwzględniając art. 42 ust. 2 rozporządzenia 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,

uwzględniając Porozumienie EOG, a w szczególności jego załącznik XI i protokół 37, w brzmieniu zmienionym decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

PRZYJMUJĄ NINIEJSZĄ WSPÓLNĄ OPINIĘ

1 INFORMACJE OGÓLNE

1. Wniosek dotyczący aktu w sprawie danych („wniosek”) opracowano zgodnie z komunikatem „Europejska strategia w zakresie danych” („strategia w zakresie danych”)[1].

2. Europejska Rada Ochrony Danych („EROD”) i Europejski Inspektor Ochrony Danych („EIOD”) zauważają, że według Komisji „[o]bywatele będą obdarzać zaufaniem i akceptować innowacje wykorzystujące potencjał danych tylko wtedy, gdy będą mieli pewność, że udostępnianie danych osobowych w UE będzie zawsze przebiegało zgodnie z rygorystycznymi unijnymi przepisami o ochronie danych”[2].

3. Jak określono w uzasadnieniu wniosku, „jest [on] kluczowym filarem i drugą ważną inicjatywą zapowiedzianą w strategii w zakresie danych. W szczególności akt ten przyczynia się do stworzenia międzysektorowych ram zarządzania dostępem do danych i ich wykorzystaniem przez ustanawianie przepisów dotyczących kwestii, które mają wpływ na relacje między podmiotami gospodarki opartej na danych, w celu zapewnienia zachęt do horyzontalnego udostępniania danych między sektorami”. Cele szczegółowe wniosku są następujące:

– *„Ułatwianie dostępu do danych i ich wykorzystania przez konsumentów i przedsiębiorstwa, przy jednoczesnym zachowaniu czynników zachęcających do inwestowania w sposoby generowania wartości za pomocą danych.*

– *Zapewnienie możliwości korzystania przez organy sektora publicznego oraz instytucje, agencje lub organy Unii z danych znajdujących się w posiadaniu przedsiębiorstw w określonych przypadkach wystąpienia wyjątkowej potrzeby uzyskania dostępu do danych.*

– *Ułatwianie przechodzenia od jednych do drugich usług w chmurze i usług przetwarzania brzegowego.*

[1] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Europejska strategia w zakresie danych”, 19 lutego 2020 r., COM(2020) 66 final.
[2] Europejska strategia w zakresie danych, wprowadzenie, s. 1.

– *Wdrożenie środków zabezpieczających przed bezprawnym przekazywaniem danych bez powiadomienia przez dostawców usług w chmurze.*

– *Zapewnienie opracowania norm w zakresie interoperacyjności w odniesieniu do danych, które mają być ponownie wykorzystywane między sektorami”*[3].

2 ZAKRES OPINII

4. 23 lutego 2022 r. Komisja opublikowała wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania („akt w sprawie danych” lub „wniosek”).

5. 23 lutego 2022 r. Komisja zwróciła się do EROD i EIOD o wydanie wspólnej opinii („opinia”) na temat wniosku na podstawie art. 42 ust. 2 rozporządzenia (UE) 2018/1725.

6. **Wniosek ma szczególne znaczenie dla ochrony podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania ich danych osobowych. Zakres opinii ogranicza się do aspektów wniosku związanych z danymi osobowymi, które to aspekty stanowią jeden z głównych filarów wniosku.**

7. EROD i EIOD z zadowoleniem przyjmują motyw 7 wniosku, w którym wyraźnie wspomniano, że wniosek uzupełnia prawo Unii w zakresie ochrony danych i prywatności, w szczególności RODO i dyrektywę o prywatności i łączności elektronicznej, oraz pozostaje bez uszczerbku dla tego prawa.

8. EROD i EIOD podkreślają, że **koniecznie należy zapewnić i utrzymać przestrzeganie i stosowanie dorobku UE w dziedzinie ochrony danych osobowych**. **Jeżeli w kontekście wniosku mowa jest o danych osobowych, istotne jest, aby wyraźnie uniknąć w tekście prawnym wniosku wszelkich niespójności i ewentualnych konfliktów z RODO, dyrektywą o prywatności i łączności elektronicznej lub rozporządzeniem (UE) 2018/1725**. Chodzi nie tylko o pewność prawa, lecz także uniknięcie sytuacji, w której wniosek skutkowałby bezpośrednim lub pośrednim zagrożeniem podstawowych praw do prywatności i ochrony danych osobowych, ustanowionych w art. 7 i 8 Karty praw podstawowych Unii Europejskiej („Karta”) oraz art. 16 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”).

9. Zważywszy że wniosek, jak wyjaśniono bardziej szczegółowo w niniejszej opinii, budzi szereg obaw dotyczących ochrony podstawowych praw do prywatności i ochrony danych osobowych, **opinia ta nie służy przedstawieniu wyczerpującego wykazu wszystkich problemów ani zaproponowaniu innego brzmienia przepisów w każdym przypadku**. **Celem niniejszej opinii jest natomiast odniesienie się do głównych krytycznych aspektów wniosku dotyczących prywatności i ochrony danych**.

[3] Uzasadnienie, s. 3.

3 OCENA

3.1 Uwagi ogólne

10. EROD i EIOD uznają cel, jakim jest uwolnienie potencjału informacji, które można wydobyć z danych, aby uzyskać cenną wiedzę na temat ważnych wspólnych wartości oraz na potrzeby działań w dziedzinie zdrowia, nauki, badań naukowych i klimatu. Ponadto podkreślają, że RODO już dopuszcza taką możliwość w odniesieniu do danych osobowych.

11. EROD i EIOD uznają również wagę skuteczniejszego prawa do przenoszenia danych, z myślą o sprzyjaniu innowacyjności i promowaniu konkurencji oraz zapewnieniu konsumentom korzystającym z produktów lub powiązanych usług możliwości rzeczywistego kontrolowania sposobu wykorzystywania danych generowanych w rezultacie korzystania przez nich z danego produktu lub powiązanej z nim usługi, i z zadowoleniem przyjmują ten cel[4].

12. Wniosek służy ustanowieniu zharmonizowanych przepisów dotyczących udostępniania danych generowanych w wyniku korzystania z produktu lub powiązanej usługi użytkownikom tego produktu lub tej usługi oraz udostępniania danych przez posiadaczy danych odbiorcom danych[5]. EROD i EIOD uznają zatem, że przewidywany zakres stosowania wniosku nie dotyczy wyłącznie danych osobowych, lecz miałby zastosowanie zarówno do danych osobowych, jak i nieosobowych, które są generowane w wyniku korzystania z produktów lub usług w rozumieniu wniosku.

13. EROD i EIOD zauważają jednak, że rozszerzone prawo do przenoszenia danych rozciągałoby się na **szeroki zakres produktów i usług, które mogą ujawniać szczególnie chronione dane** dotyczące osób fizycznych, w tym dzieci i innych wymagających szczególnego traktowania kategorii osób, których dane dotyczą. Wniosek jest wyraźnie ukierunkowany na dane generowane przez internet rzeczy i internet ciał, w tym pojazdy, sprzęt gospodarstwa domowego, wyroby konsumpcyjne oraz wyroby medyczne i zdrowotne[6]. Dane generowane przez te produkty skomunikowane staną się przedmiotem wprowadzonych wnioskiem praw i obowiązków w zakresie dostępu do danych. W rezultacie przetwarzane mogą być dane z najbardziej prywatnych miejsc i otoczenia osoby, której dane dotyczą, a także szczególnie chronione dane dotyczące zdrowia.

14. We wniosku nie dokonano rozróżnienia między danymi osobowymi zdefiniowanymi w art. 4 ust. 1 RODO a innymi danymi nieosobowymi, jeżeli chodzi o określenie zakresu praw dostępu do danych oraz do ich udostępniania i wykorzystywania. Ponadto **wynikające z wniosku prawa do dostępu do danych oraz do ich wykorzystywania i udostępniania prawdopodobnie rozciągałyby się w praktyce na podmioty inne niż osoba, której dane dotyczą**, w tym na przedsiębiorstwa, w zależności od tytułu prawnego, na podstawie którego produkt jest używany. Prawa i obowiązki w zakresie udostępniania danych, które mają zostać ustanowione we wniosku, stwarzają zatem **znaczne ryzyko gromadzenia, udostępniania i wykorzystywania danych osobowych bez wiedzy osoby, której dane dotyczą**, zwłaszcza jeżeli te prawa i obowiązki nie zostaną określone zgodnie z zaleceniami zawartymi w niniejszej opinii, w szczególności w przypadku korzystania z prawa do przenoszenia danych przez użytkownika innego niż osoba, której dane dotyczą. Przykłady problematycznych przypadków

[4] Uzasadnienie, s. 13.
[5] Artykuł 1 ust. 1 wniosku.
[6] Motyw 14 wniosku.

wykorzystywania danych obejmują m.in. urządzenia do śledzenia lokalizacji produktów noszonych lub usług używanych przez osoby, których dane dotyczą, niebędących „użytkownikami" w rozumieniu wniosku.

15. EROD i EIOD są zaniepokojeni faktem, że wniosek w obecnym brzmieniu w znacznym stopniu przyczyniłby się do utowarowienia danych osobowych, tj. postrzegania danych osobowych jako zwykły towar, którym można handlować. Nie tylko podważyłoby to samą koncepcję godności ludzkiej i podejście ukierunkowane na człowieka, które UE chce utrzymać w swojej strategii w zakresie danych, lecz także groziłoby naruszeniem praw do prywatności i ochrony danych jako praw podstawowych[7].

16. EROD i EIOD uznają i z zadowoleniem przyjmują starania służące zapewnieniu, aby wniosek nie miał wpływu na obecny system ochrony danych przewidziany w RODO i dyrektywie o prywatności i łączności elektronicznej. EROD i EIOD uważają jednak, że **konieczne są dodatkowe zabezpieczenia**, aby uniknąć obniżenia w praktyce poziomu ochrony podstawowych praw do prywatności i do ochrony danych osobowych.

17. W dalszej części niniejszej opinii EROD i EIOD przedstawiają zalecenia dotyczące sposobu zwiększenia skuteczności we wniosku odpowiednich zasad, zabezpieczeń i obowiązków w zakresie ochrony danych. Biorąc pod uwagę szeroki zakres praw i obowiązków określonych we wniosku w odniesieniu do dostępu do danych oraz do ich wykorzystywania i udostępniania, ogólne odniesienia do RODO nie są wystarczające. EROD i EIOD uważają, że konieczne jest dalsze doprecyzowanie, zwłaszcza w przypadku gdy brzmienie wniosku może prowadzić do błędnej interpretacji, jeżeli bardziej szczegółowe odniesienie do prawa o ochronie danych (zarówno RODO, jak i dyrektywy o prywatności i łączności elektronicznej) nie jest wyraźnie zaznaczone. EROD i EIOD uważają, że w przypadku braku takich uściśleń istnieje ryzyko, że wbrew deklarowanym celom Komisji wniosek skutkowałby obniżeniem poziomu ochrony osób, których dane dotyczą.

18. Zalecenia te wynikają również z niejasnego zakresu (w odniesieniu do danych nieosobowych lub danych osobowych) określonych we wniosku praw i obowiązków w zakresie dostępu do danych oraz ich udostępniania i wykorzystywania przez posiadaczy danych, użytkowników (jako osoby niebędące osobami, których dane dotyczą) oraz osób trzecich lub odbiorców.

19. W związku z tym EROD i EIOD zauważają, że biorąc pod uwagę, iż rozszerzone prawo do przenoszenia danych rozciągałoby się na szeroki zakres produktów i usług, które mogą ujawniać szczególnie chronione dane dotyczące osób fizycznych, aby nie obniżać stopnia ochrony danych osobowych, należy we wniosku wyraźnie i jasno określić, że przetwarzanie danych osobowych przez posiadaczy danych, użytkowników (jako osoby niebędące osobami, których dane dotyczą) oraz osoby trzecie lub odbiorców podlega wszystkim warunkom i zasadom przewidzianym w przepisach o ochronie danych[8].

3.2 Wzajemna zależność między wnioskiem a unijnymi przepisami o ochronie danych

20. EROD i EIOD zauważają, że art. 1 ust. 3 wniosku stanowi, iż „[d]o danych osobowych przetwarzanych w związku z prawami i obowiązkami określonymi w niniejszym rozporządzeniu zastosowanie ma

[7] W tym względzie zob. również https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf s 4.
[8] Zob. w szczególności pkt 22 i przypis 8 opinii.

prawo Unii dotyczące ochrony danych osobowych, prywatności i poufności komunikacji oraz integralności urządzeń końcowych" oraz że wniosek „nie ma wpływu na stosowanie prawa Unii dotyczącego ochrony danych osobowych, w szczególności rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE, w tym na uprawnienia i kompetencje organów nadzorczych". Ponadto ten sam przepis stanowi, że „[w] zakresie, w jakim dotyczy to praw określonych w rozdziale II niniejszego rozporządzenia, oraz w przypadku gdy użytkownicy są osobami, których dane osobowe dotyczą, podlegającymi prawom i obowiązkom wynikającym z tego rozdziału, przepisy niniejszego rozporządzenia uzupełniają prawo do przenoszenia danych określone w art. 20 rozporządzenia (UE) 2016/679".

21. EROD i EIOD z dużym zadowoleniem przyjmują cel art. 1 ust. 3 wniosku, którym jest zapewnienie, aby stosowanie obowiązujących przepisów i zasad w zakresie ochrony danych nie zostało naruszone ani podważone. W oświadczeniu w sprawie pakietu usług cyfrowych i strategii w zakresie danych[9] EROD wezwała Komisję do zagwarantowania pewności prawa i spójności z istniejącymi ramami ochrony danych. EROD zachęciła Komisję w szczególności do zapewnienia, aby przepisy i zasady w zakresie ochrony danych miały pierwszeństwo w każdym przypadku przetwarzania danych osobowych.

22. EROD i EIOD z zadowoleniem odnotowują, że w kompromisowym tekście aktu w sprawie zarządzania danymi – zarówno w motywach, jak i w części normatywnej – wyraźnie stwierdzono, że w przypadku konfliktu między przepisami tego aktu a prawem Unii lub prawem krajowym w dziedzinie ochrony danych osobowych przyjętym zgodnie z prawem Unii pierwszeństwo powinno mieć to drugie[10].

23. EROD i EIOD zdecydowanie zalecają zmianę art. 1 ust. 3 wniosku polegającą na dostosowaniu tego przepisu do brzmienia aktu w sprawie zarządzania danymi, aby zwiększyć spójność między wnioskiem, aktem w sprawie zarządzania danymi i obowiązującymi przepisami o ochronie danych osobowych. EROD i EIOD uważają, że w art. 1 ust. 3 i w motywie 30[11] należy dodać odniesienie do rozporządzenia (UE) 2018/1725.

24. EROD i EIOD uważają takie wyraźne stwierdzenie za konieczne w świetle podmiotów, które mogą korzystać z prawa do dostępu do danych generowanych w wyniku korzystania z produktów lub powiązanych usług oraz do wykorzystywania i udostępniania tych danych. We wniosku przyznaje się te prawa „użytkownikowi" zdefiniowanemu jako „osoba fizyczna lub prawna, która posiada lub wynajmuje produkt, korzysta z produktu na zasadzie leasingu lub otrzymuje [usługę]"[12]. W motywie 18 wyjaśniono, że użytkownik może być „przedsiębiorstwem lub konsumentem", który zakupił albo wziął w najem lub w leasing dany produkt. W związku z tym w praktyce prawo do dostępu do danych oraz do ich wykorzystywania i udostępniania prawdopodobnie obejmie podmioty inne niż osoba,

[9] Oświadczenie EROD w sprawie pakietu usług cyfrowych i strategii w zakresie danych, 18 listopada 2021 r.

[10] Artykuł 1 ust. 2 lit. a) i motyw 3a projektu rozporządzenia w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi) – tekst podlegający przeglądowi, grudzień 2021 r., dostępny pod adresem https://www.consilium.europa.eu/en/press/press-releases/2021/11/30/promoting-data-sharing-presidency-reaches-deal-with-parliament-on-data-governance-act/

[11] Chociaż w art. 1 ust. 2 lit. d) wniosku wskazano, że rozporządzenie to ma zastosowanie do „organów sektora publicznego oraz instytucji, agencji lub organów Unii, które w przypadku wystąpienia wyjątkowej potrzeby zwracają się do posiadaczy danych z wnioskiem o udostępnienie tych danych do celów wykonania zadania realizowanego w interesie publicznym, oraz posiadaczy danych, którzy przekazują te dane w odpowiedzi na taki wniosek" (tj. instytucji UE występujących z wnioskiem na podstawie rozdziału V), nie wykluczono instytucji UE z zakresu pojęcia „użytkownik" ani pojęcia „odbiorca". W każdym przypadku wszelkie wnioski składane przez instytucje UE powinny być również zgodne z rozporządzeniem (UE) 2018/1725 (oprócz spełniania wymogów określonych w rozdziale V).

[12] W art. 2 ust. 5 wniosku mowa jest o „usługach", ale należy go sprostować tak, aby odnosił się do pojedynczej „usługi".

której dane dotyczą, w tym przedsiębiorstwa, w zależności od tytułu prawnego, na podstawie którego produkt jest używany[13].

25. EROD i EIOD uznają, że podmioty inne niż osoba, której dane dotyczą, mogą mieć uzasadniony powód, aby uzyskiwać dostęp do danych generowanych w wyniku korzystania z produktu lub powiązanej usługi. Jednocześnie EROD i EIOD uważają, że istnieje również istotne ryzyko, że z praw do dostępu do danych wygenerowanych w wyniku korzystania z produktu lub powiązanej usługi, do udostępniania tych danych lub do ich wykorzystywania można by korzystać w celu nieuzasadnionej ingerencji w prawa i wolności osób, których dane dotyczą. Na przykład pracodawca, który zakupił wirtualnych asystentów głosowych i udostępnił te rozwiązania swoim pracownikom, mógłby korzystać z prawa do dostępu, aby uzyskać dostęp do ich historii wyszukiwania.

26. Aby ograniczyć ryzyko związane z interpretacją lub wdrożeniem wniosku w sposób, który mógłby mieć wpływ na stosowanie obowiązujących przepisów o ochronie danych lub je podważać, EROD i EIOD wzywają prawodawcę do nadania art. 1 ust. 3 bardziej kategorycznego brzmienia poprzez wyraźne sprecyzowanie, że przepisy o ochronie danych „**mają pierwszeństwo”** w przypadku sprzeczności z przepisami wniosku w zakresie przetwarzania danych osobowych.

27. Ponadto EROD i EROD zalecają również **wyraźne rozróżnienie** w art. 3, 4, 5, 6 i 8 wniosku między prawami osób, których dane dotyczą, do dostępu do danych generowanych przez te osoby w wyniku ich własnego korzystania z produktów lub powiązanych usług i do wykorzystywania tych danych a ewentualnymi prawami lub obowiązkami innych podmiotów. Dostęp do danych osobowych i udostępnianie ich **przez użytkowników innych niż osoba, której dane dotyczą**, powinny być **możliwe jedynie** w zakresie, w jakim wszystkie mające zastosowanie zasady i przepisy dotyczące ochrony danych pozwalają na takie przetwarzanie danych osobowych[14].

28. EROD i EIOD z zadowoleniem przyjęliby na przykład motyw stanowiący, że zgodnie z RODO wykonanie umowy może być podstawą prawną przetwarzania danych osobowych tylko wtedy, gdy osoba, której dane dotyczą, jest stroną lub gdy podejmowane są działania na wniosek osoby, której dane dotyczą, przed zawarciem umowy. Ponadto w motywie tym należy również wspomnieć, że wymogu „konieczności” nie spełnia samo ujęcie w umowie klauzuli przewidującej przetwarzanie. Administrator danych powinien być w stanie wykazać, w jaki sposób główny przedmiot konkretnej umowy zawartej z osobą, której dane dotyczą, nie będzie mógł zostać faktycznie zrealizowany bez przetwarzania danych osobowych[15].

[13] Zob. również motyw 18 wniosku.

[14] W zakresie, w jakim dotyczy to danych osobowych, należy doprecyzować charakter rozszerzonego prawa do przenoszenia danych:
w przypadku korzystania z tego prawa przez przedsiębiorstwo chodziłoby raczej o zobowiązanie handlowe producenta / posiadacza danych do zapewnienia przedsiębiorstwom dostępu do danych z zastrzeżeniem wszystkich warunków i ograniczeń określonych w RODO, a nie o „prawo” do przenoszenia i zlecania przetwarzania danych osobowych.

[15] Wytyczne EROD 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) RODO w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, wersja 2.0, przyjęte 8 października 2019 r.

3.3 Wzajemna zależność między wnioskiem a aktem o rynkach cyfrowych i aktem w sprawie zarządzania danymi

29. EROD i EIOD zauważają, że wniosek ma na celu **uzupełnienie**[16] wniosku dotyczącego **aktu o rynkach cyfrowych**[17] i aktu w sprawie zarządzania danymi[18].

30. EROD i EIOD zauważają, że **przedsiębiorstwa wyznaczone jako strażnicy dostępu na podstawie aktu o rynkach cyfrowych** nie są kwalifikującymi się **osobami trzecimi** do udostępniania danych na podstawie wniosku[19].

31. EROD i EIOD zauważają, że we wniosku **nie wyjaśniono współzależności z niektórymi kluczowymi przepisami aktu o rynkach cyfrowych** dotyczącymi udostępniania danych, w szczególności z art. 6 ust. 1 lit. h)[20] oraz i)[21] aktu o rynkach cyfrowych. W związku z tym EROD i EIOD zalecają dostosowanie brzmienia wniosku do ostatecznego tekstu aktu o rynkach cyfrowych uzgodnionego przez współprawodawców.

32. EROD i EIOD uważają w szczególności, że pewne ograniczenia dotyczące **rodzajów danych, które mają być udostępniane**, np. wspomniane w art. 6 ust. 1 lit. j) aktu o rynkach cyfrowych dane dotyczące zapytań, kliknięć i wyświetleń (z wyszukiwania w internecie), i które mają być udostępniane w formie zanonimizowanej[22], powinny mieć również zastosowanie odpowiednio w kontekście udostępniania danych związanych z zapytaniami kierowanymi do wirtualnych asystentów.

33. Biorąc pod uwagę akt w sprawie zarządzania danymi, EROD i EIOD zauważają, że wniosek zawiera **definicję inną** niż definicja terminu „posiadacz danych”[23] zawarta w tym akcie, co może prowadzić do braku pewności prawa. Ponadto definicję „posiadacza danych” zawartą we wniosku należy doprecyzować[24].

---

[16] Uzasadnienie wniosku, s. 4 i 5.
[17] COM(2020) 842 final.
[18] COM(2020) 767 final.
[19] Artykuł 5 ust. 2 wniosku.
EROD i EIOD odnotowują również, że zgodnie z art. 7 ust. 1 z zakresu rozszerzonego prawa do przenoszenia danych wyłączone są dane generowane w wyniku korzystania z produktów lub powiązanych usług dostarczonych przez mikroprzedsiębiorstwa lub małe przedsiębiorstwa.
[20] Artykuł 6 ust. 1 lit. h) wniosku dotyczącego aktu o rynkach cyfrowych, który to przepis nakłada na strażników dostępu wymóg m.in. dostarczenia użytkownikom końcowym narzędzi ułatwiających im przenoszenie danych zgodnie z RODO, w tym poprzez zapewnianie im stałej możliwości uzyskania dostępu do danych w czasie rzeczywistym. Uwaga: na dzień 1 kwietnia 2022 r. nie ma jeszcze publicznie dostępnej wersji tekstu kompromisowego (w przeciwieństwie do aktu w sprawie zarządzania danymi).
[21] Artykuł 6 ust. 1 lit. i) wniosku dotyczącego aktu o rynkach cyfrowych, który to przepis nakłada na strażników dostępu wymóg zapewnienia możliwości stałego dostępu w czasie rzeczywistym do danych zagregowanych lub niezagregowanych i możliwości korzystania z nich wyłącznie wówczas, gdy dane te są bezpośrednio powiązane z faktem korzystania przez użytkownika końcowego z produktów lub usług oferowanych przez odpowiedniego użytkownika biznesowego za pośrednictwem stosownej podstawowej usługi platformowej oraz gdy użytkownik końcowy zdecyduje się udostępnić takie dane, wyrażając zgodę w rozumieniu RODO.
[22] Zob. również opinia EIOD 2/2021 na temat wniosku dotyczącego aktu o rynkach cyfrowych, 10 lutego 2021 r., pkt 32, s. 12, „strażnik dostępu musi być w stanie wykazać, że zanonimizowane dane dotyczące zapytań, kliknięć i wyświetleń zostały odpowiednio zbadane pod kątem ryzyka ewentualnej ponownej identyfikacji”.
[23] Definicja „posiadacza danych” znajduje się w art. 2 ust. 6 przedmiotowego wniosku oraz w art. 2 ust. 5 wniosku dotyczącego aktu w sprawie zarządzania danymi.
[24] Konieczne może być doprecyzowanie znaczenia sformułowania „poprzez kontrolę technicznego projektu produktu i powiązanych usług”.

34. EROD i EIOD uważają, że w części normatywnej wniosku należy doprecyzować, czy i na jakich warunkach „odbiorca danych”[25] może być „**dostawcą usług udostępniania danych**”[26] (lub „dostawcą usługi pośrednictwa w zakresie danych”[27]), o którym mowa w akcie w sprawie zarządzania danymi. W motywie 35 przywołano przypadek, w którym osoba trzecia *jest* dostawcą usługi pośrednictwa w zakresie danych w rozumieniu aktu w sprawie zarządzania danymi, i doprecyzowano, że **w tym przypadku zastosowanie mają zabezpieczenia przewidziane w tym akcie z myślą o osobie, której dane dotyczą**. Istota motywu 35 wniosku nie znajduje jednak odzwierciedlenia w przepisach w części normatywnej wniosku. EROD i EIOD zalecają **określenie konkretnych zabezpieczeń** dla osób, których dane dotyczą, zawartych w akcie w sprawie zarządzania danymi, które to zabezpieczenia miałyby zastosowanie do udostępniania danych na podstawie wniosku przez posiadaczy danych osobom trzecim jako pośrednikom. Ponadto zgodnie z uwagami poczynionymi w sekcji 3.2 we wniosku należy sprecyzować, że zabezpieczenia te **uzupełniają** zabezpieczenia ustanowione w RODO, a także w dyrektywie o prywatności i łączności elektronicznej [28], w szczególności przewidziany w tej dyrektywie wymóg zgody użytkownika końcowego na przetwarzanie danych przez osobę trzecią.

3.4 Przepisy ogólne (rozdział I wniosku)

3.4.1 Art. 1: Przedmiot i zakres stosowania

35. EROD i EIOD zauważają, że ze względu na użycie w art. 1 ust. 1 wniosku bardzo szerokich pojęć, takich jak „produkt” i „powiązane usługi”, zakres stosowania jest również bardzo szeroki i mógłby zyskać na doprecyzowaniu[29].

36. Artykuł 1 ust. 4 wniosku stanowi, że nie ma on wpływu na unijne i krajowe akty prawne przewidujące wymianę danych, dostęp do nich i ich wykorzystywanie do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar, w tym rozporządzenie (UE) 2021/784 i wnioski dotyczące elektronicznego materiału dowodowego [COM(2018) 225 i COM(2018) 226], ani na odpowiednie przepisy dyrektywy (UE) 2015/849 i rozporządzenia (UE) 2015/847. Ponadto wniosek nie ma też wpływu na kompetencje państw członkowskich w odniesieniu do działań związanych z bezpieczeństwem publicznym, obroną, bezpieczeństwem narodowym, administracją celną i podatkową oraz zdrowiem i bezpieczeństwem obywateli zgodnie z prawem Unii.

37. Nie jest jednak jasne, czy art. 1 ust. 4 wniosku ma jakiekolwiek istotne współzależności ze wspomnianymi rozporządzeniami i dyrektywą. Stwierdzenie, że wniosek nie ma wpływu na te przepisy, nie oznacza, że operacje przetwarzania danych na podstawie wniosku nie mogą być wykorzystywane do celów tych przepisów. EROD i EIOD zalecają doprecyzowanie możliwych współzależności z wyżej wspomnianymi ramami prawnymi[30].

---

[25] Zdefiniowany w art. 2 pkt 7 wniosku.
[26] „Dostawcy usług pośrednictwa danych” w kompromisowym tekście Rady, LIMITE, 10 grudnia 2021 r. [należy sprawdzić, zaktualizować, kiedy/jeżeli dostępna będzie wersja publiczna].
[27] Zob. art. 9 wniosku dotyczącego aktu w sprawie zarządzania danymi.
[28] Dyrektywa o prywatności i łączności elektronicznej: art. 5 ust. 3.
[29] Zob. opinię Grupy Roboczej Art. 29 8/2014 w sprawie najnowszych osiągnięć w zakresie internetu przedmiotów, przyjęta 16 września 2014 r.
[30] Zob. również sekcja 3.7 opinii w kwestii dostępu do danych i ich wykorzystywania przez organy sektora publicznego oraz instytucje, agencje lub organy Unii zgodnie z rozdziałem V wniosku.

3.4.2 Artykuł 2: Definicje

38. Definicja „danych” zawarta w art. 2 pkt 1 wniosku mogłaby, w zależności od charakteru danych, obejmować również dane osobowe, co oznacza, że przepisy zawarte we wniosku mogą mieć zastosowanie obok RODO. Termin „dane” jest stosowany we wniosku bez rozróżnienia na dane osobowe i nieosobowe, co może prowadzić do zamętu. Na przykład w motywie 24 w odniesieniu do możliwości wykorzystywania przez posiadaczy danych – na podstawie ustaleń umownych – danych wygenerowanych przez użytkownika nie wyjaśniono, jakiego rodzaju danych to dotyczy. Jeżeli przykład ten odnosi się również do danych osobowych, to jest on niekompletny pod względem obowiązków spoczywających na administratorach na mocy RODO i w związku z tym z łatwością mógłby zostać błędnie zinterpretowany.

39. EROD i EIOD zalecają zatem, aby współprawodawca uzupełnił art. 2 wniosku o definicję „danych osobowych” (zgodną z definicją w RODO) i „danych nieosobowych”. Podobnie EROD i EIOD zalecają dodanie do art. 2 wniosku definicji „osoby, której dane dotyczą” i „zgody”, ponieważ terminy te są często używane we wniosku i w motywach. W art. 2 ust. 5 wniosku „użytkownika” zdefiniowano jako osobę fizyczną lub prawną, która posiada lub wynajmuje produkt, korzysta z produktu na zasadzie leasingu lub otrzymuje usługi. W celu zapewnienia jasności i skutecznego wzmocnienia pozycji osób fizycznych w odniesieniu do ich danych osobowych EROD i EIOD zalecają dodanie do tej definicji sformułowania „oraz osobę, której dane dotyczą” (oraz włączenie definicji osoby, której dane dotyczą, jako mającej takie samo znaczenie jak w RODO), a także wyraźne odróżnienie sytuacji, w których użytkownik jest osobą, której dane dotyczą, od sytuacji, w której użytkownik nie jest taką osobą.

3.5 Udostępnianie danych przez przedsiębiorstwa konsumentom i między przedsiębiorstwami (rozdział II wniosku)

40. Rozdział II wniosku dotyczy danych generowanych w wyniku korzystania z produktów lub powiązanych usług. We wniosku zdefiniowano „produkt” jako „materialną rzecz ruchomą, [...] która pozyskuje, generuje lub gromadzi dane dotyczące jej wykorzystania lub środowiska, która jest w stanie przekazywać dane za pośrednictwem publicznie dostępnych usług łączności elektronicznej i której podstawową funkcją nie jest przechowywanie ani przetwarzanie danych”. „Powiązaną usługę” zdefiniowano z kolei jako „usługę cyfrową, w tym oprogramowanie, która jest zawarta w produkcie lub wzajemnie z nim połączona w taki sposób, że jej brak uniemożliwiłby produktowi wykonywanie jednej z jego funkcji”. Ponadto w art. 7 ust. 2 wniosku doprecyzowano, że w przypadku gdy we wniosku mowa jest o produktach lub powiązanych usługach, takie odniesienie rozumie się jako obejmujące również wirtualnych asystentów[31], o ile są oni wykorzystywani do uzyskiwania dostępu do produktu lub powiązanej usługi lub sterowania nimi.

41. EROD i EIOD uważają, że definicja produktu pokrywa się częściowo z **pojęciem „urządzenia końcowego”[32] w rozumieniu art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej**. W

[31] Definicja wirtualnego asystenta znajduje się w art. 2 pkt 4.

[32] Zgodnie z art. 1 ust. 1 lit. a) dyrektywy Komisji 2008/63/WE z dnia 20 czerwca 2008 r. w sprawie konkurencji na rynkach końcowych urządzeń telekomunikacyjnych „końcowe urządzenie” oznacza „urządzenie bezpośrednio lub pośrednio podłączone do interfejsu publicznej sieci telekomunikacyjnej w celu przesyłania, przetwarzania lub odbierania informacji”. Zob. również wytyczne EROD 02/2021 w sprawie wirtualnych asystentów głosowych, wersja 2.0, przyjęta 7 lipca 2021 r., pkt 25: *„[z]godnie z definicją „urządzenia końcowego”, smartfony,* ***inteligentne telewizory*** *i* ***podobne urządzenia internetu***

art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej wymaga się uzyskania zgody abonenta lub użytkownika przed przechowywaniem informacji lub uzyskaniem dostępu do informacji już przechowywanych w urządzeniu końcowym abonenta lub użytkownika końcowego, chyba że takie przechowywanie lub dostęp są ściśle niezbędne w celu świadczenia usługi przez dostawcę usługi społeczeństwa informacyjnego, wyraźnie zażądanej przez abonenta lub użytkownika. Ponadto wszelkie operacje przetwarzania danych osobowych po tych operacjach przetwarzania, w tym przetwarzanie danych osobowych uzyskanych dzięki dostępowi do informacji w urządzeniu końcowym, muszą również mieć podstawę prawną na mocy art. 6 RODO, aby były zgodne z prawem[33].

42. EROD i EIOD z zadowoleniem przyjmują wyjaśnienie zawarte w motywie 15 wniosku, w którym wyraźnie wskazano, że produkty takie jak: komputery osobiste, serwery, tablety i smartfony, kamery, kamery internetowe, systemy do nagrywania dźwięku i skanery tekstu nie będą objęte zakresem stosowania wniosku. EROD i EIOD uważają jednak, że w art. 2 pkt 2 wniosku zdefiniowano „produkt" przy użyciu takich (ogólnych) pojęć, że urządzenia te mogą w rzeczywistości wchodzić w zakres definicji zawartej w części normatywnej wniosku. EROD i EIOD uważają zatem, że konieczna jest zmiana definicji „produktu", tak aby wyraźnie wyłączyć takie produkty, jak: komputery osobiste, serwery, tablety i smartfony, kamery, kamery internetowe, systemy do nagrywania dźwięku i skanery tekstu, również w części normatywnej wniosku[34].

43. EROD i EIOD z zadowoleniem odnotowują, że art. 4 ust. 5 wniosku stanowi, że jeżeli użytkownik nie jest osobą, której dane dotyczą, wszelkie dane osobowe wygenerowane w wyniku korzystania z produktu lub powiązanej usługi są udostępniane użytkownikowi przez posiadacza danych wyłącznie wtedy, gdy istnieje ważna podstawa prawna zgodnie z art. 6 ust. 1 rozporządzenia (UE) 2016/679 oraz, w stosownych przypadkach, spełnione są warunki określone w art. 9 rozporządzenia (UE) 2016/679. Ponieważ we wniosku przyznaje się prawo do dostępu do danych generowanych w wyniku korzystania z produktów lub powiązanych usług oraz do korzystania z tych danych „użytkownikom" (co obejmuje podmioty inne niż osoby, których dane dotyczą), EROD i EIOD uważają, że takie doprecyzowanie stanowi ważne zabezpieczenie. Jako że zgodność przetwarzania danych osobowych z prawem jest uregulowana w całym art. 6 RODO, **EROD i EIOD zalecają jednak zastąpienie odniesienia do art. 6 ust. 1 RODO w art. 4 ust. 5 wniosku odniesieniem do całego art. 6 RODO, a bardziej ogólnie do wszystkich zasad i warunków przewidzianych w przepisach o ochronie danych**. Ponadto ponieważ dostęp do danych generowanych w wyniku korzystania z produktów lub powiązanych usług może również obejmować dostęp do informacji przechowywanych na urządzeniu końcowym abonenta lub użytkownika, EROD i EIOD zalecają doprecyzowanie, że posiadacz danych udostępnia dane

---

rzeczy *są* ***przykładami urządzeń końcowych****. Nawet jeśli VVA sami w sobie są usługami programowymi, zawsze działają za pośrednictwem urządzenia fizycznego, takiego jak inteligentny głośnik lub inteligentny telewizor.* ***VVA*** *korzystają z sieci łączności elektronicznej, aby uzyskać dostęp do tych urządzeń fizycznych, które stanowią „urządzenia końcowe" w rozumieniu dyrektywy o e-prywatności. W związku z tym przepisy art. 5 ust. 3 dyrektywy o e-prywatności mają zastosowanie zawsze, gdy VVA przechowuje informacje lub uzyskuje do nich dostęp w podłączonym do niego urządzeniu fizycznym*".

[33] Zob. wytyczne EROD 1/2020 dotyczące przetwarzania danych osobowych w kontekście pojazdów podłączonych do internetu i aplikacji związanych z mobilnością („wytyczne EROD 1/2020"), pkt 41, w którym przedstawiono podobne rozumowanie dotyczące takich pojazdów. Zob. również opinię EROD 5/2019 w sprawie wzajemnej zależności między dyrektywą o prywatności i łączności elektronicznej a RODO, w szczególności w zakresie właściwości, zadań i uprawnień organów ochrony danych.

[34] EROD i EIOD pragną podkreślić, że ustalenia, iż definicja „produktu" zawarta we wniosku pokrywa się częściowo z definicją „urządzenia końcowego" w rozumieniu art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, nie należy rozumieć jako zalecenia zmiany definicji „produktu" w celu dostosowania jej do definicji „urządzenia końcowego".

użytkownikowi wyłącznie wtedy, gdy – w stosownych przypadkach – spełnione są warunki określone w **art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej**.

44. EROD i EIOD przypominają, że w przypadku gdy zgodnie z art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej wymagana jest zgoda, zgoda na podstawie art. 6 RODO byłaby najprawdopodobniej właściwą podstawą prawną w odniesieniu do przetwarzania danych osobowych po przechowywaniu informacji lub uzyskaniu dostępu do informacji już przechowywanych na urządzeniu końcowym abonenta lub użytkownika[35].

45. Podobne względy mają zastosowanie do udostępniania danych osobom trzecim na wniosek użytkownika biznesowego zgodnie z art. 5 ust. 6 wniosku. Ponadto EROD i EIOD zalecają dalsze dostosowanie brzmienia art. 5 ust. 6 do art. 4 ust. 5 wniosku poprzez doprecyzowanie, że dane generowane w wyniku korzystania z produktu lub powiązanej usługi są udostępniane „przez posiadacza danych osobie trzeciej" wyłącznie wtedy, gdy spełnione są wszystkie warunki i zasady przewidziane w przepisach o ochronie danych, w szczególności gdy istnieje ważna podstawa prawna na mocy art. 6 oraz, w stosownych przypadkach, spełnione są warunki określone w art. 9 RODO i art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej.

46. W związku z tym EROD i EIOD podkreślają potrzebę zapewnienia, aby **dostęp do danych osobowych oraz ich wykorzystywanie i udostępnianie przez użytkowników innych niż osoby, których dane dotyczą, odbywały się w pełnej zgodności z wszystkimi przepisami RODO oraz dyrektywy o prywatności i łączności elektronicznej**, włącznie z informowaniem osób, których dane dotyczą, o dostępie administratorów do ich danych osobowych i ułatwianiem administratorom realizowania praw osób, których dane dotyczą.

47. Mając na uwadze w szczególności **art. 3 ust. 1** i art. 4 ust. 1 wniosku, EROD i EIOD uważają, że w celu propagowania **minimalizacji danych** produkty powinny być zaprojektowane w taki sposób, aby osoby, **których dane dotyczą** (niezależnie od ich tytułu prawnego do urządzenia) miały możliwość **używania produktów objętych wnioskiem, w szczególności urządzeń wchodzących w zakres internetu ciał lub internetu rzeczy anonimowo** lub w sposób jak najmniej naruszający prywatność. Posiadacze danych powinni również w jak największym stopniu ograniczyć ilość danych opuszczających urządzenie (np. przez anonimizację danych)[36]. We wniosku należy jasno określić ten aspekt, aby osoby, których dane dotyczą, miały większą kontrolę nad swoimi danymi osobowymi. **Artykuł 3 ust. 2 lit. a)** wniosku, odnoszący się do obowiązku informowania użytkownika o charakterze i ilości danych, które mogą być generowane w wyniku korzystania z produktu, nie powinien być interpretowany jako niekorzystnie wpływający na zasadę minimalizacji danych określoną w RODO. Ponadto EROD i EIOD zauważają, że w art. 3 należy wyraźnie wskazać, które podmioty są zobowiązane do wypełniania obowiązków wymienionych w art. 3 ust. 1 i 2 wniosku. W trosce o pewność prawa EROD i EIOD zalecają wyraźne wskazanie, które podmioty są odpowiedzialne za każdy z wymienionych obowiązków.

48. EROD i EIOD zauważają, że **ograniczenia prowadzenia rejestrów** dotyczących dostępu przedsiębiorstw do danych na podstawie **art. 4 ust. 2** oraz dostępu osób trzecich do danych na podstawie **art. 5 ust. 3** wniosku nie należy interpretować jako mającego niekorzystny wpływ na wynikające z RODO obowiązki

[35] Zob. wytyczne EROD 1/2020 dotyczące przetwarzania danych osobowych w kontekście pojazdów podłączonych do internetu i aplikacji związanych z mobilnością, pkt 27.
[36] Zob. opinię Grupy Roboczej Art. 29 8/2014 w sprawie najnowszych osiągnięć w zakresie internetu przedmiotów, przyjętą 16 września 2014 r.

w zakresie bezpieczeństwa danych osobowych i rozliczalności. Ten ważny aspekt należy jasno określić w przepisach.

49. EROD i EIOD zauważają również, że zgodnie z **art. 5 ust. 9** [37] wniosku prawo użytkownika do udostępniania danych osobom trzecim „**nie może niekorzystnie wpływać na prawa *innych osób* do ochrony danych**". W tym względzie EROD i EIOD podkreślają potrzebę doprecyzowania **zakresu** i znaczenia tego przepisu. Ponadto aby zapewnić **spójność** z prawem osób, których dane dotyczą, wynikającym z art. 20 RODO i uzupełnianym przez wniosek, EROD i EIOD zalecają zawarcie w motywie odniesienia do kryteriów **zapewniania równowagi** między prawem do przenoszenia danych a **kwestiami ochrony danych dotyczącymi innych osób**, określonymi w wytycznych EROD dotyczących przenoszenia danych[38].

50. **Artykuł 6** wniosku stanowi, że osoba trzecia przetwarza dane udostępnione jej na podstawie art. 5 wyłącznie do celów i na warunkach uzgodnionych z użytkownikiem i z zastrzeżeniem praw osoby, której dane dotyczą, w odniesieniu do danych osobowych, oraz usuwa dane, gdy nie są już one niezbędne do uzgodnionego celu. Ponadto art. 6 ust. 2 lit. b) stanowi, że osoba trzecia nie może wykorzystywać danych do profilowania osób fizycznych, chyba że jest to konieczne do świadczenia usługi zażądanej przez użytkownika. Biorąc pod uwagę scenariusz, w którym użytkownik jest podmiotem innym niż osoba, której dane dotyczą, EROD i EIOD przypominają, że ważne jest zapewnienie, aby **wszelkie dalsze przetwarzanie danych osobowych było zgodne, w stosownych przypadkach, z art. 6 ust. 4 RODO oraz – ze szczególnym uwzględnieniem scenariusza profilowania – z odpowiednimi obowiązkami przewidzianymi w art. 22 RODO**. W przypadku przetwarzania szczególnych kategorii danych osobowych (np. danych dotyczących zdrowia lub seksualności) co do zasady wymagana będzie wyraźna zgoda osoby, której dane dotyczą, chyba że można powołać się na inny wyjątek od zakazu zawartego w art. 9 RODO. W przypadku gdy zastosowanie ma art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, dane powinny być przetwarzane wyłącznie za zgodą abonenta lub użytkownika, chyba że jest to ściśle niezbędne do świadczenia usługi społeczeństwa informacyjnego wyraźnie zażądanej przez abonenta lub użytkownika[39].

51. Ze względu na pewność prawa oraz w celu uniknięcia takiej możliwej interpretacji, że odpowiednie przepisy o ochronie danych w kontekście obowiązku przetwarzania danych osobowych przez osoby trzecie zgodnie z art. 6 ust. 1 wniosku to wyłącznie przepisy odnoszące się do praw osób, których dane dotyczą (rozdział III RODO), jak zalecono również w pkt 43 i 45 opinii, EROD i EIOD zalecają uzupełnienie brzmienia art. 6 ust. 1 odnoszącego się do RODO „i z zastrzeżeniem praw osoby, której dane dotyczą, w odniesieniu do danych osobowych" przez zastąpienie tego sformułowania następującym tekstem: „oraz jeżeli spełnione są wszystkie warunki i zasady przewidziane w przepisach o ochronie danych, w szczególności gdy istnieje ważna podstawa prawna zgodnie z art. 6 oraz, w stosownych przypadkach, spełnione są warunki określone w art. 9 RODO i art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, i z zastrzeżeniem praw osoby, której dane dotyczą, w odniesieniu do danych osobowych".

[37] Z uwagi na art. 4 ust. 1 podobny przepis należy zawrzeć w art. 4 wniosku.
[38] Zob. wytyczne Grupy Roboczej Art. 29 (zatwierdzone przez EROD) dotyczące prawa do przenoszenia danych, s. 11–12.
[39] Zob. również wytyczne EROD dotyczące przetwarzania danych osobowych w kontekście pojazdów podłączonych do internetu i aplikacji związanych z mobilnością, wersja 2.0, przyjęte 9 marca 2021 r., pkt 15.

52. W odniesieniu do art. 6 ust. 2 lit. a) EROD i EIOD z zadowoleniem przyjmują zakaz zmuszania i oszukiwania w jakikolwiek sposób użytkownika przez osobę trzecią lub manipulowania nim[40]. EROD i EIOD z zadowoleniem przyjmują także odniesienie w motywie 34 wniosku do tzw. zwodniczych interfejsów. EROD i EIOD zauważają jednak, że czynniki, które mogą mieć wpływ na proces decyzyjny, mogą różnić się w zależności od tego, czy użytkownik jest również osobą, której dane dotyczą. **EROD i EIOD zalecają zatem wyraźne doprecyzowanie, że w art. 6 ust. 2 lit. a) wniosku zakazuje się wszelkich form zmuszania lub oszukiwania osób, których dane dotyczą, lub manipulowania tymi osobami** (niezależnie od tego, czy użytkownik jest również osobą, której dane dotyczą).

53. Podobne względy dotyczą art. 6 ust. 2 lit. b) wniosku: osoba trzecia nie powinna mieć możliwości wykorzystywania otrzymanych danych do profilowania osób fizycznych, chyba że jest to konieczne do świadczenia usługi zażądanej przez użytkownika. Ponadto EROD i EIOD uważają, że we wniosku nie zdefiniowano „usługi", która ma być świadczona przez osobę trzecią na żądanie użytkownika (który może być podmiotem innym niż osoba, której dane dotyczą). Możliwe jest zatem, że takie „usługi" mogą pociągać za sobą poważną ingerencję w prawa i wolności osób fizycznych lub w inny sposób wywierać istotny wpływ na zainteresowane osoby.

54. W związku z tym EROD i EIOD zalecają ujęcie we wniosku wyraźnych ograniczeń lub obostrzeń co do wykorzystywania danych osobowych generowanych w wyniku korzystania z produktu lub usługi przez dowolny podmiot inny niż osoba, której dane dotyczą (jako „użytkownik", „posiadacz danych" lub „osoba trzecia"), zwłaszcza w przypadkach, gdy dane te mogą umożliwić wyciągnięcie precyzyjnych wniosków dotyczących życia prywatnego tej osoby lub w inny sposób wiązałyby się z dużym ryzykiem dla praw i wolności zainteresowanych osób.

55. EIOD i EROD zalecają w szczególności wprowadzenie ograniczeń dotyczących wykorzystywania danych osobowych generowanych w wyniku korzystania z produktu lub powiązanych usług do celów marketingu bezpośredniego lub reklamy bezpośredniej, monitorowania pracowników, punktowej oceny kredytowej lub określania kwalifikowalności do ubezpieczenia zdrowotnego, obliczania lub zmiany składek ubezpieczeniowych. To zalecenie pozostaje bez uszczerbku dla wszelkich dalszych ograniczeń, które mogą być stosowne, na przykład w celu ochrony osób wymagających szczególnego traktowania, zwłaszcza małoletnich, lub ze względu na szczególnie wrażliwy charakter niektórych kategorii danych (np. danych dotyczących korzystania z wyrobu medycznego) oraz ochrony zapewnianej przez unijne przepisy o ochronie danych.

56. Ponadto EROD i EIOD przypominają ogólną zasadę, że również osoba trzecia jako administrator danych podlega zasadzie minimalizacji danych oraz że w miarę możliwości należy stosować techniki anonimizacji. Przestrzeganie zasady minimalizacji danych ma szczególne znaczenie w przypadku danych mogących ujawnić intymne aspekty życia prywatnego osoby fizycznej[41].

[40] Jak określono w motywie 34, przywołując tzw. zwodnicze interfejsy.

[41] Zob. oświadczenie EROD w sprawie pakietu usług cyfrowych i strategii w zakresie danych, przyjęte 18 listopada 2021 r., w którym podkreślono „znaczenie obowiązku uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych, który jest szczególnie istotny w kontekście »przedmiotów podłączonych do internetu« (np. internetu rzeczy i internetu ciał), ze względu na poważne zagrożenia dla podstawowych praw i wolności zainteresowanych osób.

3.6 Obowiązki posiadaczy danych prawnie zobowiązanych do udostępniania danych oraz postanowienia w umowach między przedsiębiorstwami dotyczące dostępu do danych i korzystania z nich (rozdziały III i IV wniosku)

57. Rozdział III dotyczy warunków, w tym wynagrodzenia, na podstawie których dane są udostępniane, w przypadku gdy posiadacz danych jest zobowiązany do udostępniania danych odbiorcy danych zgodnie z rozdziałem II lub innymi przepisami prawa Unii lub państwa członkowskiego.

58. W tym względzie w art. 8 wniosku nie przewidziano żadnej roli osoby, której dane dotyczą, ani nie wspomniano o tej osobie, ponieważ warunki udostępniania danych muszą zostać określone w umowie między posiadaczem danych a odbiorcą danych. Co więcej, w przypadku gdy użytkownik jest podmiotem innym niż osoba, której dane dotyczą, w rozumieniu wniosku osoba ta nie jest stroną umowy. Może to poważnie zagrażać skuteczności praw do ochrony danych. Dalsze zagrożenia w tym kontekście mogą wynikać z usług pośrednictwa oraz usług pośrednictwa w zakresie danych, które mogą łączyć dane pierwotnie uznane za nieosobowe z konkretnymi osobami, których dane dotyczą[42].

59. W każdym razie EROD i EIOD podkreślają, że prawo do ochrony danych osobowych zapisane w art. 16 ust. 1 TFUE i w art. 8 Karty jako prawo odnoszące się do każdej osoby fizycznej jest niezbywalne i nie można się go zrzec jakąkolwiek umową między posiadaczem danych a odbiorcą danych[43].

60. Zgodnie z art. 8 ust. 3 wniosku posiadacz danych nie może wprowadzać rozróżnienia między „porównywalnymi kategoriami odbiorców danych", a zgodnie z art. 8 ust. 4 wniosku posiadacz danych nie może udostępniać danych odbiorcy danych na zasadzie wyłączności. Obowiązki te nie powinny jednak naruszać prawa osób, których dane dotyczą, do samostanowienia informacyjnego, z którego to prawa wynika, że osoby te są uprawnione do rozróżniania odbiorców ich danych osobowych (w szczególności gdy osoby te wyrażają zgodę na przetwarzanie, na przykład w przypadku gdy zastosowanie mają warunki określone w art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej lub przetwarzanie opiera się na zgodzie na podstawie art. 6 RODO). W związku z tym EROD i EIOD apelują o zamieszczenie we wniosku sformułowania, które skutecznie przyczyni się do przestrzegania RODO przez posiadaczy danych i odbiorców danych. W szczególności EROD i EIOD zalecają, aby zawarte w motywie 41 wyjaśnienie, że obowiązki te nie naruszają przepisów RODO, ująć w samym tekście art. 8.

61. Zgodnie z art. 9 wniosku wszelkie wynagrodzenie żądane przez posiadacza danych od osób trzecich musi być rozsądne, a w przypadku MŚP nie może przekraczać kosztów bezpośrednio związanych z udostępnieniem danych, chyba że przepisy sektorowe stanowią inaczej.

62. W odniesieniu do art. 9 wniosku dotyczącego wynagrodzenia za udostępnianie danych EROD i EIOD zdecydowanie zalecają wyeliminowanie wszelkich niejasności dotyczących transakcji pieniężnych towarzyszących udostępnianiu danych osobowych. Zgodnie z motywem 42 wniosku przepisów dotyczących prawa do żądania wynagrodzenia za udostępnianie danych osobom trzecim „nie należy

[42] Im więcej danych nieosobowych jest łączonych z innymi dostępnymi informacjami, tym większe jest ryzyko ponownej identyfikacji osób, których dane dotyczą. Zob. wspólną opinię EROD i EIOD 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi), s. 16.

[43] Zob. oświadczenie EROD w sprawie pakietu usług cyfrowych i strategii w zakresie danych, przyjęte 18 listopada 2021 r., s. 6.

rozumieć jako przepisów określających zapłatę za same dane, ale raczej – w przypadku mikroprzedsiębiorstw, małych lub średnich przedsiębiorstw – zapłatę za poniesione koszty i wymagane inwestycje związane z udostępnieniem danych". Stwierdzenie to odczytywane w związku z motywem 46 wydaje się jednak sugerować, że wręcz przeciwnie, w przypadku udostępniania danych między dużymi przedsiębiorstwami lub gdy posiadaczem danych jest małe lub średnie przedsiębiorstwo, a odbiorcą danych jest duże przedsiębiorstwo, prawo posiadacza danych do ustalenia „rozsądnego wynagrodzenia", które mają uiścić osoby trzecie, można uznać za zachętę do monetyzacji danych osobowych.

63. W tym względzie EROD i EIOD powtarzają, że ochrona danych jest prawem podstawowym zagwarantowanym w art. 8 Karty, a danych osobowych nie można uznać za towar handlowy.

64. W przypadku gdy strony nie zgadzają się co do warunków udostępniania danych, we wniosku przewidziano alternatywne metody rozstrzygania sporów, które mogą powstać między posiadaczami danych a odbiorcami danych. Zgodnie z art. 10 wniosku strony te mogą zwrócić się o pomoc do organów rozstrzygania sporów certyfikowanych przez państwa członkowskie. W przypadku gdy dane osobowe są udostępniane osobom trzecim na żądanie użytkowników **niebędących osobami, których dane dotyczą**, osoby te byłyby jednak całkowicie wykluczone z udziału w postępowaniu w sprawie rozstrzygnięcia sporu dotyczącego udostępniania ich danych osobowych między posiadaczem danych a odbiorcą danych. Ponadto biorąc pod uwagę złożone interakcje między prawami przysługującymi osobie, której dane dotyczą, na podstawie RODO oraz prawami i obowiązkami ustanowionymi we wniosku, jak również nakładanie się tych praw i obowiązków, należy wziąć pod uwagę, że decyzja stron o przekazaniu sporu do rozpatrzenia przez organ rozstrzygania sporów może kolidować z prawem osoby, której dane dotyczą, do wniesienia skargi do organu nadzorczego.

65. Ujmując rzecz bardziej ogólnie, EROD i EIOD zdecydowanie zalecają wyraźne stwierdzenie, że rozstrzyganie sporów na podstawie art. 10 nie może naruszać praw osób, których dane dotyczą, ani obowiązków administratora danych wynikających z RODO. Ponadto art. 10 ust. 5 i 9 należy zmienić w taki sposób, aby uwzględnić fakt, że osób, których dane dotyczą, nie pozbawia się możliwości korzystania z prawa do dochodzenia roszczeń przed organem nadzorczym.

66. We wniosku zachęca się również posiadacza danych do stosowania odpowiednich technicznych środków ochrony, w tym inteligentnych umów, aby zapobiec nieuprawnionemu dostępowi do danych oraz zapewnić zgodność z prawami i obowiązkami wynikającymi z wniosku, a także z uzgodnionymi postanowieniami umownymi dotyczącymi udostępniania danych (art. 11). W związku z tym należy doprecyzować, w jaki sposób inteligentne umowy mogą stanowić sposób zapewnienia posiadaczom danych i odbiorcom danych odpowiednich gwarancji, że przekazane dane są chronione przed nieuprawnionym ujawnieniem lub dostępem oraz że spełnione są uzgodnione warunki udostępniania tych danych. Aby zapewnić spójność z art. 32 RODO, EIOD i EROD podkreślają, że w zakresie, w jakim dotyczy to danych osobowych, art. 11 ust. 1 musi zawierać odniesienie do obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia poziomu bezpieczeństwa odpowiedniego do ryzyka związanego z przetwarzaniem danych osobowych.

67. W odniesieniu do art. 11 ust. 2 EROD i EIOD zalecają wyraźne doprecyzowanie, że w związku z danymi osobowymi zgoda posiadacza danych na udostępnienie danych nie może zastępować wymogu istnienia odpowiedniej podstawy prawnej zgodnie z RODO, lub ewentualnie wskazanie, że zgoda ta ma zastosowanie w przypadku przetwarzania danych nieosobowych. Ponadto należy zmienić ten ustęp tak, by stanowił on, że wszelkie polecenia posiadacza danych lub użytkownika (który

niekoniecznie jest osobą, której dane dotyczą) odnoszące się do zniszczenia danych udostępnionych odbiorcom danych i zniszczenia kopii tych danych nie mogą naruszać prawa osoby, której dane dotyczą, do ograniczenia przetwarzania, które to prawo wynika z art. 18 RODO.

68. W odniesieniu do wyjątków przewidzianych w art. 11 ust. 3 należy wyjaśnić we wniosku, kto może uznać, że sytuacje opisane w lit. a) i b) mają zastosowanie, i w jaki sposób. Ponadto w wyjątkach tych należy uwzględnić nie tylko szkodę dla posiadacza danych i jego interesy, lecz także – i przede wszystkim – szkodę dla osób, których dane dotyczą, jak również ich prawa i interesy w odniesieniu do ich prawa do prywatności i ochrony danych. W związku z tym EROD i EIOD zalecają dodanie w art. 11 nowego ustępu wyraźnie stanowiącego, że ust. 2 lit. b) ma zastosowanie w przypadku ewentualnej szkody dla osób, których dane dotyczą, lub naruszenia ich praw i interesów.

69. Ponadto zawarte w art. 12 ust. 1 odniesienie do spoczywającego na posiadaczu danych na mocy art. 5 wniosku obowiązku udostępniania danych na wniosek użytkownika sugeruje, że w odniesieniu do danych osobowych i pomimo tego, co stwierdzono w motywie 24, w przypadku gdy użytkownik jest podmiotem innym niż osoba, której dane dotyczą[44], wniosek można interpretować jako tworzący podstawę prawną udostępniania danych osobowych na mocy art. 6 ust. 1 lit. c) RODO. W związku z tym należy dodać odpowiednie, konkretne i skuteczne zabezpieczenia ochrony praw i interesów osób, których dane dotyczą, w odniesieniu do danych osobowych, zwłaszcza gdy użytkownik nie jest osobą, której dane dotyczą. W związku z tym, biorąc pod uwagę złożone interakcje między prawami przysługującymi osobie, której dane dotyczą, na podstawie RODO oraz prawami i obowiązkami ustanowionymi we wniosku, jak również nakładanie się tych praw i obowiązków, należy zmienić art. 12 ust. 2 wniosku w celu doprecyzowania, że jakiekolwiek postanowienie umowne określone w umowie o udostępnianiu danych zawartej między posiadaczami danych a odbiorcami danych, które ze szkodą dla osób, których dane dotyczą, podważa stosowanie ich praw do prywatności i ochrony danych, stanowi odstępstwo od tego prawa lub zmienia jego skutki, nie jest wiążące dla tej strony.

70. EROD i EIOD podkreślają, że rozdział IV art. 13 wniosku stanowi, iż „[p]ostanowienie umowne jest nieuczciwe, jeżeli cechuje się tym, że jego stosowanie rażąco odbiega od dobrej praktyki handlowej w zakresie dostępu do danych i korzystania z nich, co jest sprzeczne z zasadą dobrej wiary i uczciwego obrotu". Podobnie jak wspomniano powyżej w odniesieniu do spójności definicji z RODO, przepis ten nie jest wystarczająco jasny, ze względu na fakt, że pojęcie danych osobowych lub danych nieosobowych lub mieszanych zbiorów danych nie jest jasne w całym tekście.

71. Dostęp do danych i ich wykorzystywanie stanowią przetwarzanie danych osobowych w rozumieniu art. 4 pkt 2 RODO. W związku z tym w przypadku gdy dane osobowe są wykorzystywane w przetwarzaniu, zastosowanie mają określone w RODO obowiązki administratorów i podmiotów przetwarzających. To samo dotyczy przypadków, w których chodzi o mieszane zbiory danych (tj. zawierające zarówno dane osobowe, jak i nieosobowe).

---

[44] Motyw 5 wniosku, w którym stwierdza się, że przepisów wniosku „nie należy interpretować jako uznających ani tworzących **jakąkolwiek podstawę prawną upoważniającą posiadacza danych** do przechowywania **danych [osobowych]**, uzyskiwania do nich dostępu lub ich **przetwarzania**", wydaje się sprzeczny z art. 5 wniosku ustanawiającym obowiązek udostępniania danych przez posiadacza danych na wniosek użytkownika, ponieważ zgodnie z definicją zawartą w art. 4 pkt 2 RODO „przetwarzanie" danych osobowych obejmuje wszelkie operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych, w tym „ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie". Jeżeli jednak motyw 5 dotyczy przetwarzania danych przez posiadacza danych do jego własnych celów, należy to doprecyzować.

72. W tym celu EROD i EIOD wzywają współprawodawców do sprecyzowania we wniosku odpowiednich wymogów i obowiązków administratorów i podmiotów przetwarzających w przypadku przetwarzania danych osobowych, przy czym współprawodawcy powinni to uczynić w sposób określony w niniejszej opinii[45].

3.7 Dostęp do danych i ich wykorzystywanie przez organy sektora publicznego oraz instytucje, agencje lub organy Unii (rozdział V)

73. Jeżeli chodzi o „udostępnianie danych" organom sektora publicznego oraz instytucjom, agencjom lub organom Unii („organy sektora publicznego") w przypadku „wyjątkowej potrzeby" (rozdział V wniosku), EROD i EIOD mają poważne obawy co do **zgodności z prawem, konieczności i proporcjonalności** obowiązku udostępniania danych organom sektora publicznego oraz instytucjom, agencjom lub organom Unii.

74. Artykuł 14 wniosku stanowi, że posiadacz danych (z wyjątkiem MŚP) na wniosek udostępnia dane organowi sektora publicznego lub instytucji, agencji lub organowi Unii **wykazującym wyjątkową potrzebę skorzystania z żądanych danych**. Wniosek nie zawiera odniesienia do środków ustawodawczych, które należy przyjąć w celu zapewnienia podstawy prawnej tego obowiązku. EROD i EIOD zauważają, że w art. 1 ust. 2 lit. d) wniosku mowa jest o zadaniu realizowanym w interesie publicznym[46]. W tym samym duchu w art. 15 lit. c) wniosku mowa jest o realizacji zadania leżącego w interesie publicznym i „wyraźnie wskazanego w prawie". Sugeruje to, że we wniosku przewidziano art. 6 ust. 1 lit. c) RODO jako podstawę prawną przetwarzania prowadzonego przez odpowiedni organ sektora publicznego lub instytucję, agencję lub organ Unii. EROD i EIOD zauważają jednak, że ani odpowiednie zadania leżące w interesie publicznym, ani organy sektora publicznego lub instytucje, agencje lub organy Unii, którym powierzono te zadania, nie zostały wyraźnie określone we wniosku. Zamiast tego we wniosku określono szereg warunków, które skutkowałyby nałożeniem na posiadacza danych prawnego obowiązku dostarczenia danych osobowych.

75. Artykuł 17 ust. 1 lit. d) wniosku stanowi, że występując z wnioskiem o udostępnienie danych na podstawie art. 14 ust. 1, organ sektora publicznego lub instytucja, agencja lub organ Unii musi podać **podstawę prawną występowania z wnioskiem o udostępnienie danych**. EROD i EIOD uważają, że ze względu na pewność prawa art. 17 ust. 1 lit. d) powinien stanowić, iż we wniosku należy precyzyjnie wskazać przepis prawny, zgodnie z którym zadanie leżące w interesie publicznym wyraźnie powierza się organowi sektora publicznego, instytucji, agencji lub organowi Unii występującym z wnioskiem.

76. W art. 15 wniosku określono trzy możliwe scenariusze alternatywne, w których uznaje się, że istnieje wyjątkowa potrzeba skorzystania z danych. Jeżeli chodzi o przypadki określone w art. 15 lit. a) i b) wniosku, EROD i EIOD uważają, że należy do tych przepisów wyraźnie wprowadzić wymóg „wyraźnego przewidzenia prawem", ponieważ wszelkie ograniczenia prawa do danych osobowych muszą być „przewidziane ustawą" (art. 52 ust. 1 Karty, który to wymóg potwierdzono w skonsolidowanym orzecznictwie TSUE).

77. Ograniczenia muszą opierać się na podstawie prawnej, która jest odpowiednio **dostępna, przewidywalna** i sformułowana **wystarczająco precyzyjnie, aby umożliwić osobom fizycznym zrozumienie jej zakresu**. Zgodnie z zasadami konieczności i proporcjonalności podstawa prawna musi

[45] Zob. w szczególności pkt 39–39 i 67 niniejszej opinii. Zob. również pkt 43, 45, 46 i 51 niniejszej opinii.
[46] Zob. również motyw 5 wniosku.

również określać **zakres i sposób** korzystania z uprawnień przez właściwe organy oraz muszą jej towarzyszyć **wystarczające zabezpieczenia** chroniące osoby fizyczne przed arbitralną ingerencją[47].

78. W tym kontekście EROD i EIOD zauważają przede wszystkim, że **okoliczności** uzasadniające dostęp nie są określone w sposób zawężający. We wniosku mowa jest o „**wyjątkowej potrzebie**", która uzasadniałaby wniosek o udostępnienie danych, dotyczącej „**niebezpieczeństwa publicznego**" (które jest zdefiniowane szeroko[48]). EROD i EIOD zauważają, że w motywie 57 określono, że występowanie niebezpieczeństwa publicznego ustala się na podstawie odpowiednich procedur stosowanych w państwach członkowskich lub przez odpowiednie organizacje międzynarodowe. EROD i EIOD zalecają włączenie tego ważnego doprecyzowania do części normatywnej wniosku. Ponadto EIOD i EROD uważają, że **konieczne jest, aby prawodawca o wiele bardziej rygorystycznie określił hipotezy niebezpieczeństwa lub wyjątkowej potrzeby**. Należy zatem zmienić definicję „niebezpieczeństwa publicznego" zawartą w art. 2 pkt 10 wniosku, aby wyraźniej określić rodzaje sytuacji, które stanowiłyby takie niebezpieczeństwo.

79. Scenariusz, o którym mowa w art. 15 lit. c) wniosku, w rzeczywistości przedstawia dwa bardzo różne przypadki skorzystania z danych: w pierwszym dostęp do danych byłby udzielany na potrzeby realizacji zadania leżącego w interesie publicznym, zaś w drugim dostęp do danych byłby udzielany w celu zmniejszenia obciążenia administracyjnego. W odniesieniu do pierwszego przypadku skorzystania z danych sformułowanie, że brak dostępnych danych uniemożliwia organowi sektora publicznego realizację konkretnego zadania leżącego w interesie publicznym, jest **szczególnie problematyczne** ze względu na wymóg „jakości prawa" (w tym przewidywalności) przewidującego ingerencję w prawa podstawowe. Jeśli chodzi o drugi przypadek skorzystania z danych, **samo zmniejszenie obciążenia administracyjnego z trudem może przeważyć nad wpływem na podstawowe prawa i wolności zainteresowanych osób**. Jednocześnie nie spełniałoby wymogu konieczności ingerencji w podstawowe prawa i wolności. W tym względzie EROD i EIOD opowiadają się w szczególności za wyraźniejszym określeniem okoliczności, w których można wystąpić z wnioskiem.

80. EROD i EIOD zauważają, że **kategorie danych osobowych**, do których mają dostęp organy sektora publicznego, nie są wystarczająco sprecyzowane[49]. Obowiązek dostarczania danych mógłby jednak obejmować dane osobowe pochodzące z urządzeń tworzących internet rzeczy[50] i internet ciał. Takie informacje mogą dotyczyć szczególnych kategorii danych osobowych i innych danych szczególnie chronionych, takich jak lokalizacja, które umożliwiłyby wyciągnięcie wniosków na temat życia intymnego osoby, której dane dotyczą.

81. EROD i EIOD zauważają również, że we wniosku nie określono w wystarczający sposób **zabezpieczeń chroniących osoby, których dane dotyczą**. W szczególności w art. 17 ust. 2 lit. c) wniosku (który dotyczy **treści wniosków** o udostępnienie danych składanych przez organ sektora publicznego) mowa jest o respektowaniu prawnie uzasadnionych celów posiadacza danych, ale nie wspomniano ryzyka dla praw i wolności *osoby, której dane dotyczą*. Zgodnie z art. 19 ust. 1 lit. b) wniosku organ sektora

[47] Zob. m.in. TSUE, C-175/20, „SS" SIA/Valsts ieņēmumu dienests, ECLI:EU:C:2022:124, pkt 83.
[48] W art. 2 pkt 10 wniosku zdefiniowano „niebezpieczeństwo publiczne" jako „wyjątkową sytuację negatywnie wpływającą na ludność Unii, państwa członkowskiego lub jego części, która to sytuacja wiąże się z ryzykiem wystąpienia poważnych i trwałych następstw dla warunków życia lub stabilności gospodarczej, lub znacznego obniżenia wartości aktywów gospodarczych w Unii lub w odpowiednim państwie członkowskim".
[49] W motywie 56 mowa jest o „danych posiadanych przez przedsiębiorstwo".
[50] Motyw 14.

publicznego, *który otrzymał dane*, musi wdrożyć środki techniczne i organizacyjne chroniące prawa i wolności osób, których dane dotyczą. W tym względzie EROD i EIOD podkreślają, że wyżej wspomniane środki należy przedsięwziąć przede wszystkim *w chwili zbierania* danych, a nie po ich przekazaniu.

82. Artykuł 17 ust. 2 lit. d) wniosku stanowi, że wniosek musi dotyczyć, w miarę możliwości, danych *nieosobowych*. Temu zabezpieczeniu towarzyszy przepis art. 18 ust. 5, zgodnie z którym w przypadku gdy zastosowanie się do wniosku o udostępnienie danych wymaga ujawnienia danych osobowych, posiadacz danych czyni racjonalne kroki w celu pseudonimizacji danych, o ile wniosek można zrealizować za pomocą danych pseudonimicznych. EROD i EIOD uważają, że należy zmienić art. 18 ust. 5, tak aby posiadacz danych był zobowiązany do pseudonimizacji danych, a nie tylko do tego, by czynić „racjonalne kroki". W związku z tym EROD i EIOD wzywają współprawodawców do usunięcia sformułowania „czyni racjonalne kroki", ponieważ wydaje się ono ograniczać obowiązek posiadacza danych, i przypominają, że pseudonimizacja zmniejsza ryzyko dla osób, których dane dotyczą, ograniczając ilość przetwarzanych danych osobowych oraz skutki ewentualnego naruszenia ochrony danych. Ponadto EROD i EIOD zalecają współprawodawcy, aby uwzględnił fakt, że może zaistnieć potrzeba wdrożenia przez posiadacza danych innych odpowiednich zabezpieczeń zgodnie z RODO, w szczególności odpowiednich środków technicznych i organizacyjnych zapewniających minimalizację, integralność i poufność danych osobowych.

83. EROD i EIOD zauważają, ogólnie rzecz ujmując, że organowi sektora publicznego przysługuje **szeroki zakres uznania** przy występowaniu o dane zgodnie z omawianymi przepisami, ponieważ to jego wniosek (a nie same przepisy) określa między innymi: o udostępnienie jakich danych się wnioskuje (art. 17 ust. 1 lit. a)); „wyjątkową potrzebę" (lit. b)), którą jedynie w przypadku niebezpieczeństwa publicznego ustala się zgodnie z ustalonymi procedurami; cel wniosku, jak również planowane „wykorzystanie" oraz czas trwania tego wykorzystywania (lit. c)).

84. EROD i EIOD uważają, że we wniosku należy **jaśniej określić zakres i sposób korzystania z uprawnień przez organ sektora publicznego**, aby chronić osoby fizyczne przed arbitralną ingerencją[51]. EROD i EIOD w szczególności przypominają, że zgodnie z orzecznictwem TSUE[52] uregulowanie stanowiące podstawę prawną przedmiotowych środków musi zawierać jasne i precyzyjne przepisy regulujące **zakres i sposób stosowania** rozpatrywanego środka oraz ustanawiające **minimalne wymogi** służące temu, aby osoby, o których dane osobowe chodzi, miały **wystarczające gwarancje** pozwalające na skuteczną ochronę tych danych przed ryzykiem nadużyć. Uregulowanie to musi wskazywać, w jakich okolicznościach i pod jakimi warunkami można przyjąć środek przewidujący przetwarzanie takich danych, gwarantując w ten sposób, że ingerencja zostanie ograniczona do tego, co ściśle niezbędne. Potrzeba takich zabezpieczeń jest jeszcze większa, gdy w grę wchodzi ochrona szczególnych kategorii danych osobowych.

[51] Zob. w tym względzie wytyczne EIOD w sprawie oceny proporcjonalności środków ograniczających prawa podstawowe do prywatności i ochrony danych osobowych, 19 grudnia 2019 r., w których wspomniano m.in. następujące zabezpieczenia: powiadomienie osoby, na którą dane działanie będzie miało wpływ; zastrzeżenie, że dane muszą zostać zatrzymane w Unii Europejskiej; zastrzeżenie, że po upływie okresu zatrzymywania dane muszą zostać nieodwracalnie zniszczone. Zob. również TSUE, C-175/20, „SS" SIA/Valsts ieņēmumu dienests, ECLI:EU:C:2022:124, pkt 64, ale także pkt 83 i 84.

[52] Zob. TSUE, C-623/17, Privacy International/Secretary of State for Foreign and Commonwealth Affairs, ECLI:EU:C:2020:790, pkt 68.

85. Ponadto EROD i EIOD zauważają, że zgodnie z art. 17 ust. 3 wniosku organy sektora publicznego **nie mogą udostępniać danych do ponownego wykorzystania w rozumieniu dyrektywy (UE) 2019/1024**. Na podstawie art. 17 ust. 4 umożliwia się jednak wymianę danych między organami sektora publicznego w ramach wykonywania zadań, o których mowa w art. 15, lub udostępnianie danych osobie trzeciej, w przypadku gdy organy sektora publicznego zleciły tej osobie „kontrole techniczne lub inne funkcje". Biorąc pod uwagę szeroki zakres art. 15, ograniczenie ponownego wykorzystywania danych, w tym danych osobowych, nie jest zdefiniowane w wystarczająco wąski sposób. Ponadto motyw 65 wniosku stanowi, że „[d]ane udostępniane organom sektora publicznego i instytucjom, agencjom i organom Unii na podstawie występowania wyjątkowej potrzeby należy wykorzystywać wyłącznie w celu wskazanym we wniosku o ich udostępnienie, chyba że posiadacz danych, który udostępnił dane, wyraził wyraźną zgodę na wykorzystanie tych danych do innych celów". EROD i EIOD przypominają, że w przypadku gdy wniosek o udostępnienie danych dotyczy danych osobowych, wszelkie przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, byłoby regulowane przepisami art. 6 ust. 4 RODO lub art. 6 rozporządzenia (UE) 2018/1725 niezależnie od wyrażenia zgody przez posiadacza danych. W związku z tym EROD i EIOD zalecają odpowiednią zmianę wspomnianych przepisów wniosku.

86. Na podstawie **art. 21** wniosku umożliwia się dalsze przekazywanie danych przez organy sektora publicznego **osobom fizycznym lub prawnym na potrzeby prowadzenia badań naukowych lub analiz zgodnych z celem, w którym wystąpiono o dane**. EROD i EIOD przypominają o potrzebie wprowadzenia **odpowiednich zabezpieczeń**, z uwzględnieniem ewentualnego szczególnie chronionego charakteru przedmiotowych danych, zgodnie z art. 89 RODO i art. 13 rozporządzenia (UE) 2018/1725.

87. EROD i EIOD przypominają również, jak wskazano w oświadczeniu EROD w sprawie pakietu usług cyfrowych i strategii w zakresie danych, że „[s]zczególną uwagę należy zwrócić na zabezpieczenia dotyczące przetwarzania do celów badań naukowych, takie jak **wymóg weryfikacji** naukowców, którzy będą mieli dostęp do dużej ilości potencjalnie wrażliwych danych osobowych"[53]. EROD i EIOD zalecają włączenie tych wymogów do wniosku.

88. Jeżeli chodzi o art. 18 wniosku, EROD i EIOD uważają, że należy doprecyzować odniesienie do „przepisów sektorowych" (w których zgodnie z art. 18 ust. 2 określone są szczególne potrzeby w zakresie dostępności danych). Szczególna uwaga EROD i EIOD dotyczy art. 18 ust. 6 ustanawiającego kompetencje organu, o którym mowa w art. 31, między innymi w przypadku zakwestionowania wniosku o udostępnienie danych. Zważywszy że organem występującym z wnioskiem o udostępnienie danych może być instytucja, agencja lub organ UE, w art. 31 powinien znaleźć się EIOD oraz odniesienie do rozporządzenia (UE) 2018/1725. W przepisie tym należy również zawrzeć odniesienie do powiadomienia osoby, której dane dotyczą, o wniosku o udostępnienie danych oraz do możliwości zakwestionowania takiego wniosku przez osobę, której dane dotyczą (dostępnej nie tylko posiadaczowi danych), a także do prawa do skutecznego środka ochrony prawnej przed sądem przeciwko takiemu wnioskowi.

89. W odniesieniu do art. 19 wniosku EROD i EIOD zauważają, że określenie celów w sposób szeroki również osłabia zabezpieczenie wynikające z art. 19 ust. 1 lit. a). Ponadto okres zatrzymywania danych

[53] Oświadczenie EROD w sprawie pakietu usług cyfrowych i strategii w zakresie danych, przyjęte 18 listopada 2021 r., s. 7.

mający zastosowanie w zależności od celu przetwarzania danych powinien być jasno określony od samego początku.

90. Artykuł 16 ust. 2 wniosku stanowi, że „[p]rawa wynikające z niniejszego rozdziału *nie mogą być wykonywane* przez organy sektora publicznego [...] *w celu prowadzenia* działań w zakresie zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub przestępstw administracyjnych lub wykonywania kar ani działań na potrzeby administracji celnej lub podatkowej. Niniejszy rozdział *nie ma wpływu* na mające zastosowanie prawo unijne i krajowe dotyczące zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub przestępstw administracyjnych lub wykonywania sankcji karnych lub kar administracyjnych ani administracji celnej lub podatkowej."

91. Na wstępie EROD i EIOD zauważają, że art. 16 ust. 2 nie jest dostosowany do art. 1 ust. 4, który stanowi, że wniosek w całości nie ma wpływu na szereg czynności przetwarzania danych i kompetencji, które częściowo różnią się od tych określonych w art. 16 ust. 2. Ponadto EROD i EIOD zauważają, że w motywie 60 wniosku potwierdzono już, że organy sektora publicznego oraz instytucje, agencje i organy Unii powinny *korzystać z uprawnień nadanych im w przepisach sektorowych* do celów realizacji zadań w obszarze zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub przestępstw administracyjnych, wykonywania sankcji karnych i administracyjnych, a także gromadzenia danych do celów celnych bądź podatkowych.

92. Biorąc pod uwagę szczególny charakter i misję organów sektora publicznego oraz instytucji, agencji i organów Unii, które wykonują wspomniane zadania leżące w interesie publicznym, EROD i EIOD uważają jednak, że takie podmioty należy wyłączyć z zakresu stosowania rozdziału V. Co więcej, EROD i EIOD uważają, że takie podmioty powinny mieć *tylko* możliwość zobowiązania posiadaczy danych do udostępniania danych zgodnie z uprawnieniami przewidzianymi wyłącznie w przepisach sektorowych. Ponadto, w szczególności jeżeli chodzi o instytucje, agencje i organy Unii, EROD i EIOD zalecają wyraźne wskazanie w części normatywnej wniosku tych podmiotów, które będą mogły występować z wnioskiem o udostępnienie danych zgodnie z rozdziałem V, z należytym uwzględnieniem ich kompetencji określonych w aktach założycielskich.

93. Zalecenia te pozostają bez uszczerbku dla potrzeby wystarczającego sprecyzowania zbyt szerokiej definicji „niebezpieczeństwa publicznego" w art. 2 pkt 10, które uzasadniałoby skorzystanie z uprawnienia do dostępu do danych.

3.8 Zabezpieczenia danych nieosobowych w kontekście międzynarodowym (rozdział VII wniosku)

94. EROD i EIOD z zadowoleniem przyjmują przepisy wniosku dotyczące dostępu do danych, które to przepisy są ograniczone wyłącznie do danych nieosobowych i wydają się odzwierciedlać przepisy art. 48 RODO. EROD i EIOD zauważają, że zasadniczo art. 27 dotyczy przede wszystkim wniosków o uzyskanie dostępu, a nie przekazywania. Pojęcie „przekazywania" ma szczególne znaczenie w RODO, które pociąga za sobą obowiązki wymagające ujęcia go w ramy. Aby uniknąć niejasności w odniesieniu do danych nieosobowych, EROD i EIOD proponują, by w artykule tym mowa była jedynie o dostępie oraz by usunąć z tego artykułu odniesienia do przekazywania danych.

95. Ponadto przydatne byłoby wyjaśnienie wzajemnych zależności między art. 27 ust. 1 a art. 27 ust. 2 i 3 wniosku. EROD i EIOD z zadowoleniem przyjmują zawarte w art. 27 ust. 1 stwierdzenie, które obejmuje wszelkie ryzyko dostępu władz do danych nieosobowych sprzecznego z prawem Unii lub prawem odpowiedniego państwa członkowskiego. Należy jednak zmienić końcową część tego przepisu, brzmiącą „nie naruszając przepisów ust. 2 ani 3", aby doprecyzować, że nawet w przypadku braku wniosku należy w każdym przypadku wprowadzić środki przewidziane w ust. 1, tj. niezależnie od jakiegokolwiek wniosku o dostęp do danych złożonego przez państwo trzecie. Biorąc pod uwagę, że informacje dotyczące wniosku nie zawsze są dostępne, ważne jest wprowadzenie środka pozwalającego uniknąć takiej możliwości dostępu. EROD i EIOD zastanawiają się również, czy słowo „uzasadnione" w ust. 1 nie zmniejsza wpływu środków. EROD i EIOD proponują usunięcie słowa „uzasadnione" w celu zapewnienia skuteczności takich środków lub zastąpienie go bardziej zdecydowanym terminem takim jak „konieczne".

96. Ponadto EROD i EIOD zauważają, że zgodnie z art. 27 ust. 3 wniosku dostawcy usług przetwarzania danych, którzy otrzymują orzeczenie sądu lub decyzję organu administracyjnego państwa trzeciego wymagające przekazania przechowywanych w Unii danych nieosobowych lub udzielenia dostępu do tych danych, mogą zwrócić się o opinię do odpowiednich właściwych podmiotów lub organów, zgodnie z wnioskiem, w celu ustalenia, czy stosowne warunki dostępu zostały spełnione. EROD i EIOD z zadowoleniem przyjmują ten przepis nakładający wymóg zwrócenia się do właściwego organu o opinię w konkretnych przypadkach. W przepisie tym nie określono jednak konsekwencji opinii właściwego organu. EROD i EIOD proponują zatem dodać, że „jeżeli w opinii właściwych organów stwierdzono, że warunki te nie są spełnione, w szczególności ze względu na fakt, że decyzja dotyczy szczególnie chronionych danych handlowych lub ma wpływ na interesy bezpieczeństwa narodowego lub obrony Unii lub jej państw członkowskich, odbiorca nie udziela dostępu do danych".

3.9 Wdrożenie i egzekwowanie (rozdział IX wniosku)

97. Tytułem uwagi o charakterze ogólnym na temat przepisów omawianego rozporządzenia dotyczących zarządzania EROD i EIOD pragną podkreślić ryzyko stwarzane przez wniosek, które wynika z tego, że nie harmonizuje on nadzoru nad stosowaniem tego rozporządzenia przez państwa członkowskie, nie przewiduje europejskiego mechanizmu spójności, który mógłby zapewnić spójne stosowanie tego rozporządzenia na rynku wewnętrznym, ani nie przewiduje zharmonizowanych kar, co stwarza ryzyko „turystyki sądowej".

98. Artykuł 31 wniosku stanowi, że każde państwo członkowskie wyznacza właściwy organ lub właściwe organy odpowiedzialne za stosowanie i wdrażanie aktu w sprawie danych oraz że państwa członkowskie mogą ustanowić co najmniej jeden nowy organ lub oprzeć się na organach już istniejących. EROD i EIOD zwracają uwagę na ryzyko trudności operacyjnych, które mogą wynikać z wyznaczenia więcej niż jednego właściwego organu odpowiedzialnego za stosowanie i egzekwowanie omawianego rozporządzenia. EROD i EIOD mają poważne obawy, że ten projekt struktury zarządzania doprowadzi do złożoności i nieporozumień zarówno dla organizacji, jak i osób, których dane dotyczą, oraz do rozbieżności w podejściu regulacyjnym w całej Unii, a tym samym wpłynie na spójność monitorowania i egzekwowania.

99. Jeżeli chodzi o organy sektorowe, przepis art. 31 ust. 2 lit. b) jest dość niejasny i nie daje wystarczających wskazówek co do podziału obowiązków między właściwymi organami, organami ochrony danych i organami sektorowymi w odniesieniu do wdrożenia wniosku, co stwarza ryzyko

nakładania się obowiązków i konfliktu pod względem ich podziału. Na przykład w rozdziale IX wniosku nie określono dokładnej roli organów krajowych odpowiedzialnych za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (o których to organach mowa w motywie 82 oraz w art. 36 i 37 wniosku). Należy jasno określić uprawnienia i zadania poszczególnych właściwych organów, zwłaszcza w odniesieniu do egzekwowania konkretnych przepisów wniosku. EROD i EIOD zalecają na przykład, aby współprawodawcy określili, który organ jest odpowiedzialny za stosowanie i egzekwowanie przepisów rozdziału IV wniosku dotyczących nieuczciwych postanowień w umowach między przedsiębiorstwami dotyczących dostępu do danych i korzystania z nich. Ponadto wzajemna zależność między modelem zarządzania określonym we wniosku a modelami zarządzania przewidzianymi w przepisach sektorowych (np. z udziałem właściwych organów ustanowionych rozporządzeniem w sprawie przestrzeni danych dotyczących zdrowia) powinna być jaśniejsza i określona bardziej szczegółowo, aby zapewnić pewność prawa i uniknąć nieporozumień.

100. EROD i EIOD z zadowoleniem przyjmują wyznaczenie organów nadzorczych odpowiedzialnych za ochronę danych jako właściwych organów zajmujących się monitorowaniem stosowania wniosku w zakresie ochrony danych osobowych (art. 31 ust. 2 lit. a)). Wyznaczenie to jest ważne, aby uniknąć niespójności i ewentualnego konfliktu między przepisami tego rozporządzenia a RODO oraz zachować podstawowe prawo do ochrony danych osobowych określone w art. 16 TFUE i art. 8 Karty. W odniesieniu do kompetencji organów nadzorczych wniosek stanowi jednak „[n]ie naruszając ust. 1". Nie jest jasne, w jaki sposób taki przepis mógłby wpłynąć na kompetencje organów nadzorczych odpowiedzialnych za ochronę danych i organów sektorowych. W związku z tym EROD i EIOD wzywają współprawodawców do zmiany tego przepisu w celu wyeliminowania wszelkich niejasności.

101. Ponadto nie jest jasne, w jaki sposób art. 31 ust. 1 współdziała z art. 31 ust. 4 wniosku. We wniosku przedstawiono wiele scenariuszy, którym brakuje jasności. EROD i EIOD uważają, że wniosek w obecnym brzmieniu może prowadzić do konfliktów pod względem podziału obowiązków, złożoności dla organizacji i osób, których dane dotyczą, a także rozdrobnionego nadzoru w państwach członkowskich. Dlatego z uwagi na jasność EROD i EIOD zalecają skreślenie sformułowania „[n]ie naruszając ust. 1 niniejszego artykułu" (art. 31 ust. 2). EROD i EIOD zdecydowanie zalecają również współprawodawcom, by doprecyzowali art. 31 ust. 1 i 4 oraz ustanowili jasne przepisy dotyczące wyznaczania właściwych organów, organów ochrony danych, organów sektorowych i organów koordynujących, podziału obowiązków między tymi organami i mechanizmu współpracy. EROD i EIOD w szczególności podkreślają, że we wniosku nie określono uprawnień i zadań właściwego organu koordynującego, i zalecają, aby współprawodawca to skorygował.

102. W art. 31 ust. 3 wniosku nałożono na państwa członkowskie obowiązek zapewnienia, aby odpowiednie zadania i uprawnienia właściwych organów wyznaczonych na podstawie ust. 1 tego artykułu były jasno określone. EROD i EIOD zwracają uwagę, że wiele z tych uprawnień i zadań jest podobnych do tych przypisanych organom nadzorczym odpowiedzialnym za ochronę danych zgodnie z art. 58 RODO. EROD i EIOD uważają jednak, że w art. 31 ust. 3 wniosku nie zharmonizowano zadań i uprawnień właściwych organów w państwach członkowskich, a wzajemna zależność między tym przepisem a RODO nie jest jasna. Ponadto niejasne jest, w jaki sposób te zadania i uprawnienia wymienione w art. 31 ust. 3 wniosku wpłyną na zadania i uprawnienia realizowane przez organy nadzorcze odpowiedzialne za ochronę danych w toku monitorowania stosowania tego rozporządzenia w zakresie ochrony danych osobowych. Z art. 31 ust. 2 lit. a) można by wywnioskować, że zadaniami i uprawnieniami organów nadzorczych odpowiedzialnych za ochronę danych są zadania i uprawnienia ustanowione w rozdziałach VI i VII RODO. Nie jest jednak jasne, czy we wniosku powierza się tym

organom nowe zadania i uprawnienia, a jeśli tak, to w jaki sposób będą one współgrać z zadaniami i uprawnieniami przyznanymi organom nadzorczym odpowiedzialnym za ochronę danych na mocy RODO. EROD i EIOD zalecają jasne określenie przewidywanej roli organów nadzorczych odpowiedzialnych za ochronę danych w kontekście wniosku, aby zapewnić jasność i spójność monitorowania.

103. EROD i EIOD z zadowoleniem przyjmują art. 31 ust. 6 wniosku, który stanowi, że właściwe organy muszą pozostawać wolne od jakichkolwiek wpływów zewnętrznych i nie mogą zwracać się do żadnego innego podmiotu o instrukcje ani nie mogą przyjmować takich instrukcji. Aby doprecyzować ten przepis i nadać mu większe znaczenie, EROD i EIOD zalecają wyraźne wspomnienie we wniosku o niezależnym charakterze właściwych organów.

104. Zgodnie z art. 32 ust. 1 wniosku bez uszczerbku dla innych administracyjnych lub sądowych środków ochrony prawnej osoby fizyczne i prawne mają prawo wnieść skargę, indywidualnie lub, w stosownych przypadkach, zbiorowo, do odpowiedniego właściwego organu w państwie członkowskim, w którym mają miejsce zwykłego pobytu, miejsce pracy lub siedzibę, jeżeli sądzą, że ich prawa wynikające z tego rozporządzenia zostały naruszone.

105. Prawo do wniesienia skargi na podstawie art. 32 może powodować trudności operacyjne, ponieważ nie jest jasne, w jaki sposób osoby fizyczne lub prawne określą, czy chodzi o dane osobowe, i który organ jest właściwy do rozpatrzenia skargi. EROD i EIOD zdecydowanie zalecają, aby prawodawca przewidział jasny i precyzyjny mechanizm współpracy w zakresie rozpatrywania skarg między właściwymi organami (tj. organami nadzorczymi odpowiedzialnymi za ochronę danych, organami sektorowymi i organami koordynującymi) oraz wyraźnie wskazał, do którego organu można wnosić skargi. EROD i EIOD uważają, że przepisy art. 32 ust. 2 i 3 są niewystarczające i nie dostarczają wystarczających informacji ani skarżącym, ani organom nadzorczym. EROD i EIOD zalecają wyznaczenie organów koordynujących jako punktów przyjmowania wszystkich skarg związanych z omawianym rozporządzeniem i mających za zadanie przekazać te skargi odpowiednim innym organom. EROD i EIOD w szczególności zalecają wyraźne zaznaczenie, że artykuł ten nie ma wpływu na rozdział VIII RODO.

106. Nie jest również jasne, w jaki sposób przepis ten będzie współdziałał z mechanizmem kompleksowej współpracy przewidzianym w art. 56 RODO w odniesieniu do transgranicznego przetwarzania danych osobowych.

107. Ponadto EROD i EIOD zwracają uwagę na brak szczegółowych przepisów dotyczących prawa każdej pokrzywdzonej osoby fizycznej lub prawnej do skutecznego środka ochrony prawnej przed sądem w odniesieniu do niepodjęcia działań w sprawie skargi złożonej do właściwych organów, a także w odniesieniu do decyzji właściwych organów na podstawie omawianego wniosku. Może to prowadzić do powstania równoległych i niespójnych systemów egzekwowania przepisów RODO (w którym to rozporządzeniu przewidziano prawo do skutecznego środka ochrony prawnej przed sądem) i wniosku.

108. EROD i EIOD zauważają, że w motywie 82 oraz w art. 36 i 37 wniosku przewidziano możliwość wykorzystania unijnego mechanizmu sieci współpracy w zakresie ochrony konsumentów oraz umożliwiono występowanie z powództwem przedstawicielskim poprzez zmianę załączników do rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828. Nie jest jasne, w jaki sposób i w jakim stopniu mechanizm sieci współpracy w zakresie ochrony konsumentów będzie współdziałał z prawem do wniesienia skargi przewidzianym w tym artykule.

109. W odniesieniu do art. 33 EROD i EIOD zauważają, że we wniosku nie zharmonizowano kar za naruszenia przepisów wniosku (ani nie określono naruszeń, które podlegają karom, grzywien za naruszenia przepisów wniosku, ani organów właściwych do nakładania takich kar). Na przykład nie jest jasne, w jaki sposób i który organ będzie odpowiedzialny za egzekwowanie przepisów art. 5 ust. 2 zakazującego strażnikom dostępu działania w charakterze osoby trzeciej, której użytkownik może udostępniać swoje dane, ani jakie kary będą miały zastosowanie. EROD i EIOD zalecają, aby współprawodawca doprecyzował wzajemną zależność między wnioskiem a aktem o rynkach cyfrowych w odniesieniu do egzekwowania tego przepisu i obowiązujących kar.

110. EROD i EIOD zauważają, że ponieważ przepis ten ogranicza możliwość egzekwowania wniosku (zdolność do nakładania zharmonizowanych kar) i może również prowadzić do „turystyki sądowej" polegającej na wyborze państwa członkowskiego, w którym obowiązują najłagodniejsze przepisy, szkodzi deklarowanemu celowi wniosku, jakim jest zapewnienie sprawiedliwego podziału wartości danych między podmiotami gospodarki opartej o dane.

111. W odniesieniu do art. 34 EROD i EIOD zalecają, aby Komisja konsultowała się z Europejską Radą Ochrony Danych przy opracowywaniu i zaleceniu niewiążących modelowych postanowień umownych dotyczących dostępu do danych osobowych i korzystania z nich.

112. Ponadto EROD i EIOD zauważają, że we wniosku nie przewidziano europejskich ram współpracy. Ze względu na skutki wniosku we wszystkich państwach członkowskich oraz dużą liczbę transgranicznych operacji przetwarzania, które mogą wchodzić w zakres stosowania omawianego rozporządzenia, dość zaskakujące jest to, że we wniosku nie przewidziano jasnego europejskiego mechanizmu współpracy na rzecz zapewnienia jego spójnego stosowania przez państwa członkowskie (zwłaszcza w odniesieniu do rozpatrywania skarg i z uwagi na ewentualne zaangażowanie różnych właściwych organów sektorowych). EROD i EIOD zauważają, że art. 31 ust. 3 lit. f) wniosku jest niewystarczający pod tym względem, i zalecają współprawodawcy ustanowienie jasnych przepisów w celu ułatwienia współpracy między poszczególnymi zaangażowanymi organami.

113. EROD i EIOD z zadowoleniem przyjmują wyznaczenie krajowych organów ochrony danych jako właściwych organów odpowiedzialnych za monitorowanie stosowania wniosku w zakresie ochrony danych osobowych i zwracają się do współprawodawców o wyznaczenie krajowych organów ochrony danych również jako właściwych organów koordynujących przewidzianych we wniosku.

114. Organy ochrony danych dysponują wyjątkową wiedzą fachową, zarówno prawną, jak i techniczną, w zakresie monitorowania zgodności przetwarzania danych z przepisami, udzielania wskazówek podmiotom cyfrowym i osobom, których dane dotyczą, oraz stosowania mechanizmu międzyregulacyjnego, dzięki czemu znajdują się w centrum środowiska regulacji cyfrowych.

115. Ponadto EROD i EIOD są zdania, że ze względu na to, iż RODO ma zastosowanie, gdy w zbiorze danych dane osobowe i nieosobowe są nierozerwalnie związane, rola organów ochrony danych powinna przeważać w strukturze zarządzania określonej we wniosku. Współprawodawcy powinni dopilnować, aby zarządzanie to odzwierciedlało dominujący charakter podstawowego prawa do ochrony danych osobowych ustanowionego w art. 16 TFUE i art. 8 Karty oraz aby zachowało niezależność organów ochrony danych.

116. Wyznaczenie właściwych organów koordynujących innych niż organy ochrony danych mogłoby wpłynąć na spójność pod względem monitorowania stosowania przepisów RODO i prowadzić do prawdziwej złożoności dla podmiotów cyfrowych i osób, których dane dotyczą.

117. EROD i EIOD zauważają, że EIOD jest wspomniany jedynie w art. 33 ust. 4 wniosku, który to przepis odnosi się do kar (za naruszenie przepisów dotyczących udzielania organom publicznym dostępu do danych, rozdział V), i nie jest wymieniony jako „właściwy organ" w art. 31 wniosku. Biorąc pod uwagę **nadzorczą rolę** EIOD jako organu ochrony danych w instytucjach, organach i agencjach Unii Europejskiej oraz fakt, że niektóre unijne instytucje, organy i agencje mogą również działać jako użytkownik lub posiadacz danych w rozumieniu omawianego wniosku, EROD i EIOD zalecają dodanie **w art. 31 ust. 2 lit. a) odniesienia do EIOD jako organu właściwego do nadzorowania całego wniosku w zakresie, w jakim dotyczy to instytucji, organów, urzędów i agencji Unii**. Ponadto należy doprecyzować, że w stosownych przypadkach stosuje się odpowiednio art. 62 rozporządzenia (UE) 2018/1725.

Bruksela, 4 maja 2022 r.

W imieniu Europejskiej Rady Ochrony Danych	W imieniu Europejskiego Inspektora Ochrony Danych
Przewodnicząca	Europejski Inspektor Ochrony Danych
(Andrea Jelinek)	(Wojciech Wiewiorowski)