Wspólna opinia EROD i EIOD 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi)

Wersja 1.1

Historia wersji

Wersja 1.1	9 czerwca 2021 r.	Drobne zmiany redakcyjne
Wersja 1.0	10 marca 2021 r.	Przyjęcie wspólnej opinii

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 („rozporządzenie (UE) 2018/1725”),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.,

PRZYJMUJĄ NINIEJSZĄ WSPÓLNĄ OPINIĘ

1 KONTEKST

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

2. Europejska Rada Ochrony Danych (EROD) oraz Europejski Inspektor Ochrony Danych (EIOD) zwracają uwagę, że według Komisji w myśl strategii w zakresie danych „[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. Zgodnie z uzasadnieniem wniosek ten „ma na celu zwiększenie dostępności danych na potrzeby ich wykorzystywania poprzez zwiększenie zaufania do pośredników w zakresie danych oraz wzmocnienie mechanizmów udostępniania danych w całej UE. Instrument ten będzie odnosić się do następujących sytuacji:

   – udostępnianie danych sektora publicznego do ponownego wykorzystywania w sytuacjach, w których dane te są objęte prawami innych osób;

   – udostępnianie danych między przedsiębiorstwami w zamian za wynagrodzenie w dowolnej postaci;

   – umożliwianie wykorzystywania danych osobowych z pomocą »pośrednika w udostępnianiu danych osobowych«, który ma pomagać osobom fizycznym w wykonywaniu ich praw wynikających z ogólnego rozporządzenia o ochronie danych (RODO);

   – umożliwianie wykorzystywania danych z pobudek altruistycznych”[3].

4. Przedstawiając wniosek, Komisja wzięła pod uwagę w szczególności, że „[n]owe rozporządzenie zapewni ramy dobrego zarządzania wspólną europejską przestrzenią danych oraz możliwość dobrowolnego udostępniania danych przez ich posiadaczy. Będzie on stanowił uzupełnienie przyszłych

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

przepisów dotyczących zbiorów danych o wysokiej wartości w ramach dyrektywy w sprawie otwartych danych, która zapewni dostęp do niektórych zbiorów danych w całej UE za darmo, w formacie nadającym się do odczytu maszynowego i za pośrednictwem standardowych interfejsów programowania aplikacji (API)”[4].

5. W strategii w zakresie danych podkreślono również, że „[d]ostępność danych jest niezbędna do szkolenia sztucznej inteligencji (AI), dzięki czemu produkty i usługi mogą przejść szybką transformację: od rozpoznawania wzorców i dostarczania informacji do bardziej zaawansowanych technik prognozowania, sprzyjając tym samym podejmowaniu lepszych decyzji”[5].

6. Zgodnie z uzasadnieniem wniosku „[s]zczególnie ważne jest zatem zachowanie wzajemnej zależności z przepisami dotyczącymi danych osobowych. Dzięki ogólnemu rozporządzeniu o ochronie danych (RODO) i dyrektywie o prywatności i łączności elektronicznej UE ustanowiła solidne i godne zaufania ramy prawne w zakresie ochrony danych osobowych, będące standardem dla całego świata”[6].

7. EROD i EIOD zwracają również uwagę, że zgodnie z uzasadnieniem wniosek ma „na celu ułatwienie udostępniania danych, w tym poprzez zwiększenie zaufania do pośredników w udostępnianiu danych, którzy mają świadczyć usługi w poszczególnych przestrzeniach danych. Jego celem nie jest przyznanie, zmiana ani usunięcie istotnych praw w zakresie dostępu do danych i ich wykorzystywania. Przewiduje się, że tego rodzaju środki znajdą się w ewentualnym akcie o danych (2021 r.)”[7]. W czasie sporządzania niniejszej Wspólnej Opinii cel ani treść takiego aktu o danych nie są jeszcze dostępne.

2 ZAKRES WSPÓLNEJ OPINII

8. 25 listopada 2020 r. Komisja opublikowała wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi („akt w sprawie zarządzania danymi”) („wniosek”).

9. 25 listopada 2020 r. Komisja zwróciła się do EROD i EIOD o wydanie wspólnej opinii na temat wniosku na podstawie art. 42 ust. 2 rozporządzenia (UE) 2018/1725.

10. **Wniosek ten ma szczególne znaczenie w kontekście ochrony praw i wolności osób w związku z przetwarzaniem danych osobowych. Zakres niniejszej opinii ogranicza się do tych aspektów wniosku, które dotyczą ochrony danych osobowych, która – jak zauważono – stanowi znaczący, a może nawet najważniejszy, aspekt wniosku.**

11. W tym względzie EROD i EIOD zauważają, że zgodnie z motywem 3 „rozporządzenie nie narusza zatem przepisów rozporządzenia [...] (UE) 2016/679”.

12. EROD i EIOD uważają, że podstawowy cel, jakim jest zwiększenie zaufania pod kątem ułatwienia dostępu do danych oraz przyniesienia korzyści gospodarce cyfrowej w UE, znajduje swoją podstawę

[4] https://ec.europa.eu/commission/presscorner/detail/pl/qanda_20_2103#European%20Data%20Spaces
[5] Strategia w zakresie danych, s. 2–3.
[6] Uzasadnienie, s. 1.
[7] Uzasadnienie, s. 1.

w **potrzebie zapewnienia i utrzymania poszanowania i stosowania dorobku prawnego UE w dziedzinie ochrony danych osobowych**. Prawo Unii, które ma zastosowanie w tym obszarze, a w szczególności rozporządzenie UE 2016/679 (ogólne rozporządzenie o ochronie danych, RODO), należy uznawać za niezbędną podstawę opracowywania ewentualnych dalszych wniosków ustawodawczych, bez wpływania na odpowiednie dotychczasowe przepisy ani ingerowania w ich treść, także w zakresie kompetencji organów nadzorczych i innych aspektów zarządzania[8].

13. W opinii EROD i EIOD ważne jest zatem, aby **w tekście prawnym wniosku wyraźnie unikać wszelkich niespójności i możliwych sprzeczności z RODO**. Nie chodzi tylko o pewność prawa, ale również o uniknięcie sytuacji, w której wniosek bezpośrednio lub pośrednio zagrażałby podstawowemu prawu do ochrony danych osobowych ustanowionemu w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) oraz art. 8 Karty praw podstawowych Unii Europejskiej

14. W szczególności w niniejszej Wspólnej Opinii EROD i EIOD wskazują na niespójności z przepisami UE dotyczącymi ochrony danych (a także innymi przepisami UE, takimi jak dyrektywa w sprawie otwartych danych) oraz problemy dotyczące na przykład pewności prawa, które mogłyby się pojawić wskutek wejścia w życie obecnej wersji wniosku.

15. W związku z tym, że wniosek budzi szereg poważnych zastrzeżeń – wyszczególnionych w niniejszej Wspólnej Opinii – które często są wzajemnie powiązane i dotyczą ochrony podstawowego prawa do ochrony danych osobowych, **celem niniejszej Wspólnej Opinii nie jest sporządzenie wyczerpującego wykazu kwestii, którymi powinni zająć się prawodawcy, ani alternatywnych wniosków czy propozycji sformułowań**. **Służy ona natomiast poruszeniu głównych kwestii o krytycznym znaczeniu zawartych we wniosku**. Jednocześnie EROD i EIOD służą dalszymi wyjaśnieniami i chętnie wymienią więcej informacji z Komisją.

16. EROD i EIOD są także świadomi, że proces legislacyjny dotyczący wniosku trwa, i podkreślają swoją **gotowość dalszego doradzania współprawodawcom i formułowania zaleceń w toku tego procesu**, aby zapewnić w szczególności: pewność prawa z punktu widzenia osób fizycznych, podmiotów gospodarczych i organów publicznych; należytą ochronę danych osobowych osób, których dane dotyczą, zgodnie z TFUE, Kartą praw podstawowych UE i dorobkiem prawnym UE w dziedzinie ochrony danych; zrównoważone środowisko cyfrowe, w tym konieczne „mechanizmy kontroli i równowagi".

17. Ze względu na możliwe ważne powiązania z wnioskiem[9] takie wezwanie do zaangażowania organów ochrony danych dotyczy także każdego przyszłego wniosku w sprawie europejskiego aktu o danych.

---

[8] Zob. opinia EIOD 3/2020 dotycząca europejskiej strategii w zakresie danych, pkt 64: „Ponadto EIOD podkreśla, że w kontekście przyszłych mechanizmów zarządzania należy odpowiednio respektować kompetencje **niezależnych organów nadzorczych ds. ochrony danych**. Co więcej, wdrożenie strategii prowadzącej do korzystania z danych na większą skalę będzie wymagało **istotnego zwiększenia zasobów organów ochrony danych** oraz innych publicznych organów nadzoru, szczególnie pod względem **fachowej wiedzy technicznej i zdolności technicznych**. Należy zachęcać do prowadzenia wspólnych postępowań i współpracy pomiędzy wszystkimi właściwymi, publicznymi organami nadzoru, w tym organami nadzorczymi ds. ochrony danych,".

[9] Na stronie 6 oceny skutków towarzyszącej wnioskowi, SWD(2020) 295 final, stwierdzono, że (pogrubienie dodano): „inicjatywa stanowi **pierwszy krok w dwuetapowym podejściu** zapowiedzianym w europejskiej strategii w zakresie danych. **Inicjatywa** będzie dotyczyła pilnej potrzeby ułatwienia udostępniania danych za pośrednictwem wspomagających **ram zarządzania**. **Na drugim etapie** Komisja zajmie się tym, **kto jest**

3 OCENA

3.1 Uwagi ogólne

18. EROD i EIOD uznają uzasadniony cel polegający na zwiększeniu dostępności danych na potrzeby ich wykorzystywania poprzez zwiększenie zaufania do pośredników w zakresie danych oraz wzmocnienie mechanizmów udostępniania danych w całej UE, jednocześnie podkreślając, że ochrona danych osobowych stanowi niezbędny i integralny element zaufania, jakie osoby fizyczne i organizacje powinny pokładać w rozwoju gospodarki cyfrowej. Wniosek dotyczący rozporządzenia w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi) należy rozpatrywać również w świetle faktu, że gospodarka cyfrowa w coraz większym stopniu jest uzależniona od przetwarzania danych osobowych oraz rozwoju nowych technologii, takich jak analityka dużych zbiorów danych i sztuczna inteligencja.

19. EROD i EIOD podkreślają, że chociaż RODO przygotowano w związku z potrzebą wzmocnienia podstawowego prawa do ochrony danych, we wniosku wyraźnie skupiono się na uwolnieniu gospodarczego potencjału ponownego wykorzystywania i udostępniania danych. Wniosek służy zatem „poprawie warunków udostępniania danych na rynku wewnętrznym", zgodnie z motywem 3. **EROD i EIOD zwracają jednak uwagę, że we wniosku – a także towarzyszącej mu ocenie skutków – nie uwzględniono należycie potrzeby zapewnienia stopnia ochrony danych osobowych wymaganego na podstawie prawa Unii. EROD i EIOD uważają, że z punktu widzenia praw podstawowych ta tendencja w polityce prowadząca w kierunku ram gospodarki opartej na danych i nieuwzględniająca w wystarczającym stopniu aspektów ochrony danych osobowych wzbudza poważne zastrzeżenia.** W tym względzie EROD i EIOD podkreślają, że we wszystkich wnioskach, w tym przygotowywanych inicjatywach dotyczących danych, takich jak europejski akt o danych, które mogą mieć wpływ na przetwarzanie danych osobowych, należy zapewnić i wspierać poszanowanie i stosowanie dorobku prawnego UE w dziedzinie ochrony danych osobowych.

20. **EROD i EIOD podkreślają ponadto, że model Unii Europejskiej opiera się na uwzględnianiu jej wartości i praw podstawowych w rozwoju polityki, a RODO należy uważać za fundament europejskiego modelu zarządzania danymi. Jak już stwierdzono w różnych kontekstach politycznych, takich jak zwalczanie pandemii COVID-19, ramy prawne UE w dziedzinie ochrony danych osobowych należy uważać za element umożliwiający – a nie hamujący – rozwój gospodarki opartej na danych odpowiadającej wartościom i zasadom Unii.**

21. EROD i EIOD wierzą, że niniejsza Wspólna Opinia posłuży współprawodawcom jako źródło informacji, zapewniając przyjęcie instrumentu legislacyjnego, który będzie w pełni zgodny z dorobkiem prawnym UE w dziedzinie ochrony danych osobowych, a zatem zwiększy zaufanie poprzez utrzymanie stopnia ochrony zapewnianego w prawie Unii pod nadzorem niezależnych organów ochrony danych ustanowionych na podstawie art. 16 ust. 2 TFUE.

---

administratorem lub »właścicielem« danych, tj. kto posiada prawa materialne i do jakich danych może uzyskać dostęp i z nich korzystać oraz w jakich okolicznościach. **Wprowadzenie takich praw** zostanie zbadane w kontekście **aktu o danych (2021 r.)**. Rozbieżne interesy zainteresowanych stron oraz różne opinie na temat tego, co jest w tym kontekście sprawiedliwe, sprawiają, że kwestie te stają się przedmiotem gorącej dyskusji, dlatego nie należy się spieszyć".

3.2 Ogólne kwestie dotyczące powiązania wniosku z prawem Unii w dziedzinie ochrony danych osobowych

22. Wniosek obejmuje szereg odniesień do przestrzegania przepisów RODO, w którym ustanowiono przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych (zob. m.in. motyw 3, motyw 28 wniosku: „[w] przypadku gdy dostawcami usług udostępniania danych są administratorzy danych lub podmioty przetwarzające dane w rozumieniu rozporządzenia (UE) 2016/679, obowiązują ich przepisy tego rozporządzenia").

23. Zdaniem EROD i EIOD w świetle zakresu przetwarzania danych osobowych, do którego odniesiono się we wniosku, motyw 3 powinien obejmować również odniesienie do dyrektywy (WE) 2002/58 („dyrektywy o prywatności i łączności elektronicznej"), ponieważ ona także należy do dorobku prawnego UE w obszarze ochrony danych osobowych, z którym wniosek powinien być zgodny i spójny.

24. W ujęciu bardziej ogólnym EROD i EIOD uważają, że **ani duch, ani litera wniosku nie mogą obniżać stopnia ochrony i muszą zapewniać pełną zgodność ze wszystkimi zasadami i przepisami** określonymi w RODO, aby skutecznie gwarantować podstawowe prawa do ochrony danych osobowych przewidziane w art. 8 Karty praw podstawowych UE i art. 16 TFUE.

25. Biorąc pod uwagę powyższe oraz zgodnie z poniższymi akapitami Wspólnej Opinii, EROD i EIOD są zdania, że **wniosek zawiera poważne niespójności z RODO**, a także innymi przepisami prawa Unii[10], szczególnie w zakresie następujących pięciu aspektów:

a) przedmiotu i zakresu wniosku;

[10] Chociaż uwaga ta nie dotyczy ściśle przetwarzania danych osobowych, EROD i EIOD zauważają także możliwą niejasność i ewentualne niejednoznaczności dotyczące sposobu, w jaki wniosek będzie miał zastosowanie wraz z **rozporządzeniem (UE) 2018/1807 w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej**. W tym względzie należy zwrócić uwagę, że definicje „przetwarzania", „użytkownika", „użytkownika profesjonalnego" i „wymogu dotyczącego lokalizacji danych", a także inne przepisy rozporządzenia w sprawie danych nieosobowych (zob. np. art. 6 „Przenoszenie danych") mogą nie być **spójne** z definicjami i pozostałymi przepisami uwzględnionymi we wniosku ani nie pokrywać się z nimi w żaden sposób. Ponadto, jeżeli chodzi o ponowne wykorzystywanie danych będących w posiadaniu organów sektora publicznego, które to dane są chronione ze względu na poufność informacji statystycznych, należy zwrócić uwagę, że pomimo zasady określonej w art. 3 ust. 3 wniosku, warunki ponownego wykorzystania sformułowane w art. 5 ust. 3–4 nie są zgodne z ustalonymi na szczeblu UE zasadami sektorowymi dotyczącymi ochrony danych poufnych wykorzystywanych do celów statystycznych (zob. rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009 z dnia 11 marca 2009 r. w sprawie statystyki europejskiej oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE, Euratom) nr 1101/2008 w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych statystycznych objętych zasadą poufności, rozporządzenie Rady (WE) nr 322/97 w sprawie statystyk Wspólnoty oraz decyzję Rady 89/382/EWG, Euratom w sprawie ustanowienia Komitetu ds. Programów Statystycznych Wspólnot Europejskich oraz rozporządzenie Komisji (UE) nr 557/2013 z dnia 17 czerwca 2013 r. w sprawie wykonania rozporządzenia (WE) nr 223/2009 Parlamentu Europejskiego i Rady w sprawie europejskiej statystyki w zakresie dostępu do poufnych danych do celów naukowych i uchylające rozporządzenie Komisji (WE) nr 831/2002).

b) definicji lub terminologii zastosowanych we wniosku;

c) podstawy prawnej przetwarzania danych osobowych;

d) zacierania różnicy między przetwarzaniem danych osobowych a nieosobowych (niejasna relacja między wnioskiem i rozporządzeniem w sprawie swobodnego przepływu danych nieosobowych);

e) zarządzania/zadań oraz uprawnień właściwych podmiotów, które mają zostać wyznaczone zgodnie z wnioskiem, przy uwzględnieniu zadań i uprawnień organów ochrony danych odpowiedzialnych za ochronę podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych, a także za ułatwianie swobodnego przepływu danych osobowych w Unii.

A. Przedmiot i zakres

26. Zgodnie z art. 1 ust. 2 wniosku: „Niniejsze rozporządzenie nie narusza przepisów szczegółowych zawartych w innych aktach prawnych Unii dotyczących dostępu do niektórych kategorii danych lub ich ponownego wykorzystywania ani wymogów związanych z przetwarzaniem danych osobowych i nieosobowych.

Jeżeli sektorowy akt prawny Unii wymaga od organów sektora publicznego, dostawców usług udostępniania danych lub zarejestrowanych podmiotów świadczących usługi z zachowaniem altruistycznego podejścia do danych, spełnienia szczególnych dodatkowych wymogów technicznych, administracyjnych lub organizacyjnych, w tym poprzez system zezwoleń lub certyfikacji, stosuje się również te przepisy danego sektorowego aktu prawnego Unii".

27. **EROD i EIOD zalecają, aby dla zachowania przejrzystości w art. 1 wniosku wprowadzić zapis wyraźnie i jednoznacznie stwierdzający, że wniosek pozostawia nienaruszony i w żaden sposób nie wpływa na stopień ochrony osób fizycznych w związku z przetwarzaniem danych osobowych na mocy przepisów prawa unijnego i krajowego, ani też nie wiąże się ze zmianą jakichkolwiek obowiązków i praw określonych w przepisach dotyczących ochrony danych. Takie uzupełnienie zapewniłoby większą pewność prawa i zagwarantowałoby poszanowanie podstawowego prawa do ochrony danych osobowych.**

28. W tym względzie nie jest jasne dlaczego podobne doprecyzowanie zawarto w art. 9 ust. 2 wniosku w odniesieniu do dostawców usług udostępniania danych[11], a nie (*mutatis mutandis*, tj. w odniesieniu również do organów sektora publicznego, podmiotów ponownie wykorzystujących dane, organizacji o altruistycznym podejściu do danych) jako przepis horyzontalny w ramach art. 1 wniosku.

B. <u>Definicje</u> zawarte we wniosku nie są spójne z definicjami i najważniejszymi pojęciami RODO, dlatego należy je zmienić lub doprecyzować

[11] Art. 9 ust. 2 stanowi: „Niniejszy rozdział pozostaje bez uszczerbku dla stosowania innych przepisów prawa unijnego i krajowego wobec dostawców usług udostępniania danych, w tym uprawnień organów nadzorczych do zapewnienia zgodności z przepisami mającymi zastosowanie, w szczególności w odniesieniu do ochrony danych osobowych i prawa konkurencji".

29. Definicja „posiadacza danych" sformułowana w art. 2 pkt 5 wniosku: „osob[a] prawn[a] lub osob[a], której dane dotyczą, która zgodnie z mającym zastosowanie prawem unijnym lub krajowym ma prawo do udzielania dostępu do niektórych danych osobowych lub nieosobowych będących pod jej kontrolą lub do udostępnienia tych danych" nie jest zgodna z nadrzędnymi zasadami RODO ani z literą RODO.

30. W tym względzie EROD i EIOD zwracają uwagę na możliwą niepewność prawną, która może wynikać z faktu, że w RODO nie wspomniano o prawie osoby, której dane dotyczą, do udzielenia dostępu lub udostępniania własnych danych osobowych osobom trzecim, a tym bardziej o równoważnym prawie osoby prawnej, co wydaje się być wyprowadzone z definicji „posiadacza danych". Przepisy RODO gwarantują natomiast każdej osobie prawo do ochrony danych osobowych, które jej dotyczą, dzięki kompleksowemu zbiorowi zasad dotyczących przetwarzania danych osobowych. Zasady te są wiążące dla każdego podmiotu, który przetwarza dane (administratora/współadministratora danych) lub który przetwarza dane w imieniu administratora danych (podmiotu przetwarzającego)[12].

31. **W tym względzie EIOD i EROD uważają, że zamiast stwierdzenia, że osoba prawna ma prawo do udzielenia dostępu do danych osobowych lub udostępnienia ich, bardziej właściwe byłoby odniesienie się do tego, czy możliwe są pewne operacje przetwarzania danych osobowych i na jakich warunkach.**

32. Doprecyzowanie oczekiwane przez EROD i EIOD polega na wskazaniu, że w rozumieniu art. 4 pkt 2 RODO zarówno udzielenie dostępu, jak i udostępnienie danych osobowych stanowią przetwarzanie danych osobowych.

33. Zgodnie z przepisami dotyczącymi ochrony danych przetwarzanie danych osobowych jest zgodne z prawem, jeżeli osoba, której dane dotyczą (zidentyfikowana lub możliwa do zidentyfikowania osoba fizyczna, której dane osobowe dotyczą) wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów lub jeżeli można w uzasadniony sposób zastosować inną właściwą podstawę prawną zgodnie z art. 6 RODO.

34. Wspomniane względy mają zastosowanie szczególnie w świetle art. 8 Karty praw podstawowych UE: „1.Każdy ma prawo do ochrony danych osobowych, które go dotyczą. 2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą".

---

[12] Zob. również motyw 6 i 7 RODO (pogrubienie dodano):
„(6) Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać **wysoki stopień ochrony danych osobowych**.
(7) Przemiany te wymagają **stabilnych, spójniejszych ram ochrony danych** w Unii oraz **zdecydowanego ich egzekwowania**, gdyż ważna jest budowa **zaufania**, które pozwoli na rozwój gospodarki cyfrowej na rynku wewnętrznym. **Osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi**. Osoby fizyczne, podmioty gospodarcze i organy publiczne powinny zyskać większe poczucie **pewności prawa i jego stosowania w praktyce**".

35. EROD i EIOD wyrażają również zastrzeżenia w odniesieniu do brzmienia motywu 14 wniosku, w którym stwierdzono, że „[p]rzedsiębiorstwa i osoby, których dane dotyczą, powinny móc zaufać, że ponowne wykorzystywanie niektórych kategorii chronionych danych będących w posiadaniu sektora publicznego będzie odbywało się w sposób respektujący ich prawa i interesy"; art. 11 ust. 6, w którym mowa o „gwarancj[ach] umożliwiając[ych] posiadaczom danych i użytkownikom danych uzyskanie dostępu do ich danych w przypadku niewypłacalności dostawcy"; a także art. 19: „Szczególne wymogi dotyczące ochrony praw i interesów osób, których dane dotyczą, oraz podmiotów prawnych w odniesieniu do ich danych", który zgodnie z art. 19 ust. 1 lit. a) dotyczy: „cel[ów] interesu ogólnego, do których [podmiot wpisany do rejestru uznanych organizacji o altruistycznym podejściu do danych] zezwala na przetwarzanie ich danych [posiadaczy danych] przez użytkowników danych" (podkreślenie dodano).

36. W tym względzie EROD i EIOD zauważają, że interesy osób prawnych w odniesieniu do dotyczących ich informacji nie należą do tej samej kategorii co prawa i interesy osoby, której dane dotyczą, w odniesieniu do jej danych osobowych. Te pierwsze bowiem nie dotyczą godności człowieka ani prawa do prywatności czy ochrony danych, ale raczej praw własności przemysłowej, takich jak tajemnice handlowe, patenty i znaki towarowe. W związku z tym, biorąc pod uwagę wspomnianą heterogeniczność, powyższe przepisy nie tylko nie byłyby „solidne" pod względem koncepcyjnym, ale również byłyby trudne do wdrożenia i prowadziłyby do braku pewności prawa. Na przykład w przypadku niewypłacalności (o której mowa w art. 11 ust. 6) istniejące gwarancje umożliwiające posiadaczom danych uzyskanie dostępu do danych nieosobowych różniłyby się w praktyce znacząco od warunków i ograniczeń kontynuacji przetwarzania danych osobowych. Są to w rzeczywistości różne problemy, które wymagają zastosowania różnych rozwiązań[13], a odniesienie się do obu w kontekście ciążącego na dostawcy usług udostępniania danych obowiązku zapewniania ciągłości świadczenia usług (w tym udostępniania danych osobowych) jest co najmniej mylące lub nawet wprost niespójne z RODO.

37. Definicja „użytkownika danych" [14] sformułowana w art. 2 pkt 6 również jest nową definicją wprowadzoną we wniosku, a jej powiązanie – w przypadku danych osobowych – z definicją odbiorcy[15] zawartą w art. 4 pkt 9 RODO nie jest jasna. W tym względzie należy zauważyć, że art. 11 ust. 1 wniosku stanowi, co następuje: „Dostawca usług nie może wykorzystywać danych, w odniesieniu do których świadczy usługi, do celów innych niż oddanie ich do dyspozycji użytkownikom danych [...]". Ten przepis odczytywany w związku z definicją „użytkownika danych" prowadzi do braku pewności prawa, ponieważ pojęcia „odbiorcy" zdefiniowanego w RODO i „użytkownika danych" zdefiniowanego we

[13] Na przykład w przypadku niewypłacalności należy skupić się na tym, że w jej następstwie ma miejsce zmiana podmiotu administrującego przetwarzaniem danych. Nowy administrator powinien ustalić w szczególności, jakie dane można przetwarzać; określić cele, w jakich pierwotnie pozyskano dane; ustalić podstawę prawną udostępniania danych; zapewnić przestrzeganie zasad ochrony danych, w szczególności zgodności z prawem, rzetelności i przejrzystości; poinformować osoby, których dane dotyczą, o zmianach dotyczących przetwarzania ich danych i uwzględnić prawo sprzeciwu, z którego mogą zechcieć skorzystać osoby, których dane dotyczą.

[14] Art. 2 pkt 6 wniosku: „»**użytkownik danych**« oznacza **osobę fizyczną lub prawną**, która ma zgodny z prawem dostęp do **niektórych** danych i jest **upoważniona do wykorzystywania tych danych** w celach komercyjnych lub niekomercyjnych".

[15] Zgodnie z definicją określoną w art. 4 pkt 9 RODO „»odbiorca« oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią [...]".

wniosku różnią się, co może prowadzić do trudności w ich praktycznym stosowaniu. Ponadto definicja określona w art. 2 pkt 6 może być myląca, jeżeli odczytuje się ją jako odnoszącą się do osoby fizycznej lub prawnej upoważnionej (mającej prawo?) do wykorzystywania danych osobowych w celach komercyjnych i niekomercyjnych. Niejasne jest także odniesienie do takiego „upoważnienia" oraz jego znaczenie (jego źródło prawne i skutki).

38. Ponadto niejasne jest również powiązanie między pojęciem użytkownika danych jako „osoby fizycznej lub prawnej [upoważnionej do wykorzystywania tych danych w celach komercyjnych lub niekomercyjnych]" a pojęciami administratora, współadministratora oraz podmiotu przetwarzającego zdefiniowanymi w RODO. Co więcej, we wniosku odniesiono się do ewentualnej kwalifikacji jako administratora lub podmiotu przetwarzającego oraz ich obowiązków w świetle RODO wobec dostawców usług udostępniania danych [16], ale nie wobec użytkownika danych ani organizacji o altruistycznym podejściu do danych (mimo że zgodnie z RODO te ostatnie również mogą pełnić rolę administratora, współadministratora lub podmiotu przetwarzającego).

39. **W ujęciu bardziej ogólnym EROD i EIOD podkreślają, że we wniosku należy w odniesieniu do przepisów dotyczących ochrony danych osobowych zdefiniować role (administrator danych, podmiot przetwarzający dane lub współadministrator danych) każdego rodzaju „podmiotu" (dostawca usług udostępniania danych, organizacja o altruistycznym podejściu do danych, użytkownik danych), aby nie tylko uniknąć niejasności związanych z obowiązkami wynikającymi z RODO, ale również poprawić czytelność tekstu prawnego.**

40. Podobne problemy, tj. **niejasne powiązanie z definicjami i zasadami określonymi w RODO**, dotyczą definicji „udostępniania danych" sformułowanej w art. 2 pkt 7 wniosku (w której odniesiono się m.in. do „wspólnego lub indywidualnego wykorzystania udostępnianych danych"). W zakresie, w jakim dotyczy to danych osobowych, wspólne korzystanie z danych osobowych (zarówno przez posiadacza danych, osobę prawną, jak i użytkownika danych), bezpośrednio lub przez pośrednika, jest również co najmniej niejasne.

41. Podobne wątpliwości – opisane szczegółowo poniżej – dotyczą pojęcia „zezwolenia [osób prawnych na ponowne wykorzystywanie danych]", które nie zostało jednak zdefiniowane we wniosku.

42. Definicja „metadanych" zawarta w art. 2 pkt 4 jest również problematyczna z punktu widzenia ochrony danych osobowych, ponieważ są to „dane gromadzone na temat wszelkiej działalności osoby fizycznej lub prawnej w celu świadczenia usługi udostępniania danych, w tym dane dotyczące daty, godziny i geolokalizacji, czasu trwania działalności, połączeń z innymi osobami prawnymi lub fizycznymi ustanowionymi przez osobę korzystającą z usługi". Takie dane mogą obejmować dane osobowe.

43. Jak opisano bardziej szczegółowo w niniejszej Wspólnej Opinii, mając na względzie art. 11 ust. 2, wniosek można interpretować jako tworzący podstawę prawną dla przetwarzania metadanych. Art. 11 wniosku wydaje się stanowić, że warunkiem świadczenia usług udostępniania danych jest zdolność dostawcy usług do rzeczywistego wykorzystywania wspomnianych metadanych „do celów rozwoju tej usługi [udostępniania danych]". W tekście prawnym nie ma żadnych odniesień między innymi do tego,

[16] Zob. motyw 28: „W przypadku gdy dostawcami usług udostępniania danych są administratorzy danych lub podmioty przetwarzające dane w rozumieniu rozporządzenia (UE) 2016/679, obowiązują ich przepisy tego rozporządzenia".

aby dostawca usług udostępniania danych musiał przy przetwarzaniu danych osobowych opierać się na odpowiedniej podstawie prawnej zgodnie z art. 6 ust. 1 RODO.

44. **W ujęciu bardziej ogólnym EROD i EIOD uważają, że ponieważ wniosek nie narusza przepisów RODO – jak wyraźnie stwierdzono w samym wniosku – to definicje przewidziane w RODO powinny mieć do niego zastosowanie i nie powinny podlegać domniemanym zmianom ani usunięciu wskutek stosowania wniosku, natomiast nowe definicje, w stopniu, w jakim dotyczą przetwarzania danych osobowych, nie powinny w praktyce zawierać „przepisów", które nie są zgodne z duchem i literą RODO.**

45. Doprecyzowanie to ma szczególne znaczenie ze względu na łączny skutek w postaci braku jasności i braku pewności prawa wynikających z wniosku, w którym w pojedynczym przepisie zawarto więcej niż jedną niejasną definicję (zob. np. art. 7 ust. 2 lit. c) wniosku, w którym pojawia się odniesienie do uzyskania „zgody *lub* zezwolenia od podmiotów ponownie wykorzystujących dane na ponowne wykorzystywanie do celów związanych z altruistycznym podejściem do danych i innych, zgodnie z określonymi decyzjami posiadaczy danych").

46. **W związku z tym EROD i EIOD zalecają doprecyzowanie i zmianę wniosku w celu zapewnienia, aby – w stopniu, w jakim dotyczy on danych osobowych – nie było w nim żadnych niespójności z definicjami i pojęciami określonymi w RODO.**

C. Aby uniknąć braku pewności prawa, we wniosku należy lepiej wskazać <u>mającą zastosowanie podstawę prawną</u> przetwarzania danych osobowych <u>przewidzianą w RODO</u>.

47. EROD i EIOD zauważają, że w kilku przepisach wniosku odniesiono się do „zezwolenia posiadaczy danych" na wykorzystanie danych:

– art. 5 ust. 6: „organ sektora publicznego wspiera podmioty ponownie wykorzystujące dane w dążeniu do uzyskania zgody osób, których dane dotyczą, lub zgody podmiotów prawnych, których prawa i interesy mogą zostać naruszone w wyniku takiego ponownego wykorzystywania", co doprecyzowano w motywie 11: „Organy sektora publicznego powinny w stosownych przypadkach ułatwiać – za pomocą odpowiednich środków technicznych – ponowne wykorzystywanie danych na podstawie zgody osób, których dane dotyczą, lub zezwoleń osób prawnych na ponowne wykorzystywanie dotyczących ich danych";

– art. 7 ust. 2 lit. c): „pomoc organom sektora publicznego, w razie potrzeby, w uzyskaniu zgody lub zezwolenia od podmiotów ponownie wykorzystujących dane na ponowne wykorzystywanie do celów związanych z altruistycznym podejściem do danych i innych, zgodnie z określonymi decyzjami posiadaczy danych [...]";

– art. 11 ust. 11: „W przypadku gdy dostawca danych zapewnia narzędzia umożliwiające uzyskanie zgody od osób, których dane dotyczą, lub zezwoleń na przetwarzanie danych udostępnionych przez osoby prawne";

– art. 19 ust. 3: „W przypadku gdy podmiot wpisany do rejestru uznanych organizacji o altruistycznym podejściu do danych zapewnia narzędzia umożliwiające uzyskanie zgody od osób, których dane dotyczą, lub zezwoleń na przetwarzanie danych udostępnionych przez osoby prawne", co

doprecyzowano w motywie 36: „Osoby prawne mogłyby wyrażać zgodę na przetwarzanie ich danych nieosobowych do wielu różnych celów, których nie określono w momencie udzielania zgody".

48. W tym względzie EROD i EIOD zauważają, że w większości przypadków nie jest jasne, czy przedmiotem zezwolenia jest ponowne wykorzystywanie danych osobowych lub nieosobowych, czy obu rodzajów danych.

49. EROD i EIOD zauważają również, że w przypadku przetwarzania danych osobowych **„zezwolenie", o którym mowa we wniosku, nie może zastąpić konieczności spełnienia warunku jednej odpowiedniej podstawy prawnej zgodnie z art. 6 ust. 1 RODO, aby przetwarzanie danych osobowych było zgodne z prawem**. Innymi słowy, zgodnie z RODO przetwarzanie danych osobowych jest zgodne z prawem wyłącznie wówczas, gdy – i w zakresie, w jakim – ma zastosowanie co najmniej jedna podstawa prawna określona w art. 6 ust. 1 RODO. We wniosku należy jasno ująć ten aspekt, aby uniknąć wszelkich niejednoznaczności.

50. W istocie nawet gdyby zinterpretować pojęcie „zezwolenia" (które należy jednak zdefiniować w tekście prawnym wniosku) jako „decyzji (wyboru biznesowego) osoby prawnej, aby zezwolić na przetwarzanie danych osobowych, jeżeli zgodnie z art. 6 ust. 1 RODO taka osoba prawna ma podstawę prawną, aby zezwolić na takie przetwarzanie", należy zwrócić uwagę, że dosłowne odczytywanie niektórych przepisów wniosku nie wydaje się sprzyjać interpretacji zgodnej z RODO, ponieważ we wniosku określono na przykład, że „[w] przypadku gdy ponowne wykorzystywanie danych nie może być przyznane zgodnie z obowiązkami określonymi w ust. 3–5 i nie ma innej podstawy prawnej do przesłania danych na mocy rozporządzenia (UE) 2016/679, organ sektora publicznego wspiera podmioty ponownie wykorzystujące dane w dążeniu do uzyskania zgody osób, których dane dotyczą, lub zgody podmiotów prawnych" (art. 5 ust. 6 wniosku)[17]. W takich sytuacjach „zezwolenie" wydaje się alternatywą dla co najmniej jednej podstawy prawnej przewidzianej w art. 6 RODO (zgoda osoby, której dane dotyczą).

51. Motyw 6 wniosku również nie jest jasny, jeżeli chodzi o właściwą podstawę prawną przetwarzania danych osobowych, ponieważ dotyczy obowiązku polegającego na tym, aby „ogólnie rzecz biorąc" przetwarzanie danych osobowych opierało się na podstawie prawnej określonej w art. 6 RODO[18].

52. Z innego punktu widzenia, jak dalej przedstawiono szczegółowo w niniejszej opinii, EROD i EIOD zwracają uwagę na potrzebę **doprecyzowania związku między poszczególnymi scenariuszami przewidzianymi we wniosku i w art. 6 ust. 4 RODO**, dotyczącymi uregulowania sytuacji, w której przetwarzanie danych osobowych w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą.

53. **W związku z tym w świetle celu i treści wniosku EROD i EIOD uważają, że na wniosek nie można się powoływać jako na prawo Unii stanowiące w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1 RODO, aby uzasadnić przetwarzanie w celu innym niż cel, w którym dane osobowe zostały pierwotnie**

[17] Zob. także art. 7 ust. 2 lit. c); art. 11 ust. 11; art. 19 ust. 3 wniosku, wspomniane powyżej.
[18] W szczególności, motyw 6 wniosku stanowi (pogrubienie dodano): „**Ogólnie rzecz biorąc**, jeśli chodzi o dane osobowe, przetwarzanie tych danych powinno opierać się na co najmniej jednej podstawie przetwarzania określonej w art. 6 rozporządzenia (UE) 2016/679".

zebrane, jeżeli takie przetwarzanie nie odbywa się na podstawie zgody, o której mowa w art. 6 ust. 4 RODO.

54. **W świetle powyższego EROD i EIOD zalecają również określenie w tekście prawnym wniosku, że w stopniu, w jakim dotyczy on danych osobowych, ich przetwarzanie musi zawsze odbywać się w oparciu o odpowiednią podstawę prawną określoną w art. 6 RODO.**

55. Jako przykład możliwej niespójności w zakresie podstawy prawnej przetwarzania danych osobowych można wskazać przepis art. 11 ust. 2 wniosku, zgodnie z którym „[m]etadane zebrane w ramach świadczenia usługi udostępniania danych mogą być wykorzystane wyłącznie do celów rozwoju tej usługi". W tym względzie należy przypomnieć, że metadane, o których mowa we wniosku[19], mogą stanowić informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, a w takim przypadku należy je przetwarzać zgodnie z przepisami o ochronie danych, w szczególności z przepisami dotyczącymi podstawy prawnej przetwarzania. Jak wspomniano w pkt 51 niniejszej opinii, we wniosku nie odniesiono się jednak do tego kluczowego aspektu.

56. **W tej kwestii – w szerszym kontekście – EROD i EIOD uważają, że ani wspomniany przepis, ani żaden inny przepis wniosku, nie stanowią autonomicznej podstawy prawnej do ponownego wykorzystywania danych osobowych przez użytkowników danych ani do czynności przetwarzania dokonywanych przez dostawców usług udostępniania danych lub organizacje o altruistycznym podejściu do danych, ponieważ nie spełniają kryteriów wymienionych w art. 6 ust. 3 dotyczących przetwarzania, o którym mowa w art. 6 ust. 1 lit. c) i e) RODO[20].**

D. Zacieranie się granic między przetwarzaniem danych osobowych a nieosobowych oraz niejasne powiązanie wniosku z rozporządzeniem w sprawie swobodnego przepływu danych nieosobowych

57. Tytułem uwagi ogólnej EROD i EIOD uważają, że jedną z głównych kwestii o krytycznym znaczeniu, w odniesieniu do ochrony danych osobowych, która prawdopodobnie leży u źródła wspomnianych niespójności lub co najmniej niejasności tekstu prawnego, jest zacieranie się granic między

[19] Zgodnie z art. 2 pkt 4 wniosku „»metadane« oznaczają dane gromadzone na temat wszelkiej działalności osoby fizycznej lub prawnej w celu świadczenia usługi udostępniania danych, w tym dane dotyczące daty, godziny i geolokalizacji, czasu trwania działalności, połączeń z innymi osobami prawnymi lub fizycznymi ustanowionymi przez osobę korzystającą z usługi".

[20] „3. Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona:
a) w prawie Unii lub b) w prawie państwa członkowskiego, któremu podlega administrator.
Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu".

przetwarzaniem danych nieosobowych, które są regulowane w pewnym zakresie rozporządzeniem (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej („rozporządzenie w sprawie ram swobodnego przepływu danych nieosobowych")[21], a przetwarzaniem danych osobowych, przy czym to ostatnie podlega ochronie danych zagwarantowanej w dorobku prawnym UE i opiera się na innych zasadach.

58. W tym względzie EROD i EIOD podkreślają, że w praktyce trudno jest zastosować rozróżnienie między kategoriami danych osobowych a nieosobowych. W praktyce z połączenia danych nieosobowych można wywnioskować lub wygenerować dane osobowe, tj. dane dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby[22], szczególnie wtedy, gdy dane nieosobowe uzyskano w wyniku anonimizacji danych osobowych, a zatem informacji, które pierwotnie dotyczyły osób fizycznych. Ponadto w przewidzianych we wniosku scenariuszach zwiększonej dostępności, ponownego wykorzystywania i udostępniania informacji, aby „umożliwić rozpoznawanie wzorców z użyciem dużych zbiorów danych lub uczenie się maszyn"[23], im częściej dane nieosobowe łączy się z innymi dostępnymi informacjami, tym trudniej będzie zapewnić anonimizację, ze względu na podwyższone ryzyko deanonimizacji osób, których dane dotyczą. W związku z tym, biorąc pod uwagę ten scenariusz, należy zapewnić podstawowe prawa osób, których dane dotyczą, do prywatności i ochrony danych w każdym przypadku w różnych kontekstach przewidzianych we wniosku.

59. Jednocześnie mogą się pojawić sytuacje, gdy dane nieosobowe, do których RODO nie ma zastosowania, z uwagi na ich pochodzenie nie dotyczą osób fizycznych. Jest tak na przykład w przypadku danych nieosobowych pochodzących z czujników drgań montowanych w maszynach przemysłowych, które to dane łączy się z innymi danymi nieosobowymi, np. dotyczącymi geolokalizacji maszyn. Takie dane nieosobowe nie wymagają takiego samego poziomu zabezpieczeń, jak dane nieosobowe uzyskane w wyniku anonimizacji danych osobowych, ponieważ tylko te ostatnie (oraz dane spseudonimizowane) są narażone na ryzyko deanonimizacji.

60. **Aby uniknąć pomyłki co do sposobu stosowania wniosku „wraz z RODO", EROD i EIOD zalecają ponowne opracowanie wniosku, tym razem z lepszym uwzględnieniem rozróżnienia między danymi osobowymi a nieosobowymi, jak również między poszczególnymi rodzajami danych nieosobowych.**

61. Niezależnie od wątpliwości, które EIOD już wyraził w odniesieniu do pojęcia mieszanego zbioru danych oraz „nierozerwalnie związanych" danych osobowych i nieosobowych[24], EROD i EIOD przypominają zatem, że zgodnie z art. 2 ust. 2 rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych „[w] przypadku zbiorów danych obejmujących zarówno dane osobowe, jak i nieosobowe [to] rozporządzenie ma zastosowanie do części zbioru złożonej z danych nieosobowych. W przypadku gdy w zbiorze danych dane osobowe i nieosobowe są nierozerwalnie związane, [to] rozporządzenie pozostaje bez uszczerbku dla stosowania rozporządzenia (UE) 2016/679". W efekcie

[21] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (tekst mający znaczenie dla EOG), Dz.U. L 303 z 28.11.2018, s. 59.
[22] Zob. opinia EIOD 3/2020 dotycząca europejskiej strategii w zakresie danych, pkt 30.
[23] Uzasadnienie, s. 3.
[24] Zob. uwagi EIOD do wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej wydane w dniu 8 czerwca 2018 r., dostępne pod adresem: https://edps.europa.eu/sites/edp/files/publication/18-06-08-edps_formal_comments_freeflow_non_personal_data_en.pdf

mieszany zbiór danych będzie z zasady podlegał obowiązkom administratorów danych i podmiotów przetwarzających dane, a także prawom osób, których dane dotyczą, określonym w RODO. Takie uwarunkowania mają szczególne znaczenie w kontekście wniosku, ponieważ możliwe jest, że w większości przypadków zbiory danych udostępniane przez dostawcę usług udostępniania danych lub organizację o altruistycznym podejściu do danych obejmowałyby także dane osobowe. Ponieważ nie istnieje „trzecia kategoria" pomiędzy danymi osobowymi i nieosobowymi, nie zmieniłoby to charakteru ani „systemu prawnego" zbioru danych, który nadal byłby zbiorem danych osobowych[25].

62. **W świetle powyższego, EROD i EIOD zwracają uwagę na ryzyko, że wniosek tworzy równoległy zbiór przepisów, które nie są spójne z RODO ani z rozporządzeniem w sprawie ram swobodnego przepływu danych nieosobowych, co podważa jego wiarygodność i powoduje trudności w jego praktycznym zastosowaniu.**

E. Zarządzanie/zadania oraz uprawnienia właściwych podmiotów i organów, które mają zostać wyznaczone zgodnie z wnioskiem, oraz zadania i uprawnienia organów ochrony danych

63. We wniosku przewidziano wyznaczenie przez państwa członkowskie właściwych podmiotów do celów wspierania organów sektora publicznego udzielających dostępu do celów ponownego wykorzystywania danych (rozdział II wniosku) oraz wyznaczenie właściwych organów na potrzeby monitorowania przestrzegania przepisów dotyczących usług udostępniania danych i altruistycznego podejścia do danych (rozdział III i IV wniosku).

64. **W szerszym kontekście EROD i EIOD są zdania, że istnieje ryzyko ingerowania przez właściwe podmioty i organy wyznaczone na podstawie wniosku w kompetencje i zadania niezależnych organów ochrony danych, ponieważ we wniosku wiele zadań właściwych podmiotów i organów wiąże się z przetwarzaniem danych osobowych. Wyznaczenie właściwych organów/podmiotów innych niż organy ochrony danych mogłoby doprowadzić do faktycznej złożoności w przypadku podmiotów cyfrowych i osób, których dane dotyczą, a także wpłynąć na spójność w kontekście monitorowania stosowania przepisów RODO. Pozostawienie wyznaczenia właściwych podmiotów i organów w gestii państw członkowskich może się także wiązać z ryzykiem pod względem niespójności i rozbieżności podejść regulacyjnych w całej Unii.**

[25]Zob. również komunikat Komisji do Parlamentu Europejskiego i Rady, „Wytyczne dotyczące rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej", dostępny pod adresem: https://ec.europa.eu/digital-single-market/en/news/guidance-regulation-framework-free-flow-non-personal-data-european-union

3.3 Ponowne wykorzystywanie niektórych kategorii chronionych danych będących w posiadaniu organów sektora publicznego

3.3.1 Powiązanie wniosku z dyrektywą w sprawie otwartych danych i RODO

65. Chociaż w uzasadnieniu stwierdzono, że wniosek „uzupełnia dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (dyrektywa w sprawie otwartych danych)” [26], w motywie 5 doprecyzowano, że „[d]yrektywa (UE) 2019/1024 oraz przepisy sektorowe zapewniają, aby sektor publiczny umożliwiał łatwy dostęp do większej ilości produkowanych przez siebie danych na potrzeby ich wykorzystywania oraz ponownego wykorzystywania. Niektóre kategorie danych (dane objęte tajemnicą handlową, dane objęte poufnością informacji statystycznych, dane chronione prawami własności intelektualnej osób trzecich, w tym tajemnice przedsiębiorstwa i dane osobowe niedostępne na podstawie szczególnych przepisów krajowych lub unijnych, takich jak rozporządzenie (UE) 2016/679 i dyrektywa (UE) 2016/680) znajdujących się w publicznych bazach danych często jednak nie są udostępniane, nawet na potrzeby działalności badawczej lub innowacyjnej. Ze względu na szczególny charakter tych danych konieczne jest spełnienie przed ich udostępnieniem pewnych wymogów technicznych i prawnych wymogów proceduralnych, aby zapewnić poszanowanie praw innych osób w odniesieniu do takich danych. Spełnienie takich wymogów jest zazwyczaj czasochłonne i wymaga specjalistycznej wiedzy. Okoliczności te spowodowały, że dane takie są wykorzystywane w zbyt małym stopniu. Niektóre państwa członkowskie tworzą wprawdzie struktury, procesy i czasami stanowią prawo ułatwiające tego rodzaju ponowne wykorzystywanie danych, jednak działania te nie są podejmowane w całej Unii”.

66. EROD i EIOD zauważają, że pomimo wspomnianych doprecyzowań wspólna płaszczyzna wniosku i „dyrektywy w sprawie otwartych danych” nie jest jasna. W szczególności może się pojawić brak pewności prawa w przypadku przedłużającego się ponownego wykorzystywania informacji sektora publicznego, które zgodnie z art. 3 („Kategorie danych”) wniosku miałoby zastosowanie do:

„[...] danych będących w posiadaniu organów sektora publicznego, które są chronione ze względu na:

a) tajemnicę handlową;

b) poufność informacji statystycznych;

c) ochronę praw własności intelektualnej osób trzecich;

d) ochronę danych osobowych”.

67. W uzasadnieniu wniosku[27] nie doprecyzowano w wystarczającym stopniu zakresu takiego wydłużenia ponownego wykorzystywania ani zależności między wnioskiem a dyrektywą w sprawie otwartych

[26] Dz.U. L 172 z 26.6.2019, s. 56.

[27] Zob. s. 7: „W rozdziale II utworzono mechanizm **ponownego wykorzystywania niektórych kategorii chronionych danych sektora publicznego, które zależy od poszanowania praw innych osób** (szczególnie ze względu na ochronę danych osobowych, lecz także ochronę praw własności intelektualnej i tajemnicy handlowej). Mechanizm ten nie narusza sektorowych przepisów Unii dotyczących dostępu do tych danych i ich ponownego wykorzystywania. **Ponowne wykorzystywanie takich danych wykracza poza zakres stosowania**

danych. Co więcej, do tej samej kategorii (co „poszanowani[e] praw innych osób", co jest niewłaściwe, biorąc pod uwagę ochronę danych osobowych) zaliczono „ochronę danych osobowych, lecz także ochronę praw własności intelektualnej i tajemnicy handlowej".

68. Sformułowanie „dane będące w posiadaniu organów sektora publicznego, które są chronione ze względu na" m.in. „ochronę danych osobowych" (art. 3 lit. d)) wydaje się jednocześnie:

– niefortunne, ponieważ sugeruje, że regulacja ochrony danych *utrudnia* swobodny przepływ danych osobowych, a nie służy określeniu zasad swobodnego przepływu danych osobowych przy jednoczesnej ochronie praw i interesów zainteresowanych osób; *oraz*

– częściowo nieprecyzyjne, ponieważ z zakresu dyrektywy w sprawie otwartych danych nie wykluczono danych osobowych[28], ale w art. 1 ust. 2 lit. h) stwierdzono, że dyrektywa w sprawie otwartych danych nie ma zastosowania do „dokumentów wyłączonych z dostępu lub do których dostęp jest ograniczony na podstawie systemów dostępu ze względu na ochronę danych osobowych, a także części dokumentów dostępnych na podstawie tych systemów, które to części zawierają dane osobowe, których ponowne wykorzystywanie zostało określone w przepisach jako niezgodne z przepisami dotyczącymi ochrony osób fizycznych w zakresie przetwarzania danych osobowych lub jako naruszające ochronę prywatności i integralności osoby fizycznej, w szczególności zgodnie z unijnymi lub krajowymi przepisami dotyczącymi ochrony danych osobowych"[29].

69. Ten ostatni aspekt sprecyzowano jednak w motywie 7 wniosku[30]. W tym względzie EROD i EIOD zastanawiają się, dlaczego tak ważną kwestię (jak również wiele innych dotyczących ochrony danych osobowych) uwzględniono w motywie, ale nie w merytorycznej części wniosku.

70. Ponadto, zgodnie z art. 3 ust. 1 dyrektywy w sprawie otwartych danych dane osobowe, które nie są objęte tym wyjątkiem i są ogólnodostępne zgodnie z unijnymi i krajowymi systemami dostępu oraz mogą w sposób zgodny zostać ponownie wykorzystane bez osłabiania ochrony prywatności i integralności osoby fizycznej, wchodzą w zakres dyrektywy i można je udostępniać do ponownego wykorzystywania zgodnie z warunkami określonymi w tej samej dyrektywie oraz wymogami wynikającymi z przepisów dotyczących ochrony danych. W istocie zgodnie z motywem 154 RODO przepisy UE dotyczące ponownego wykorzystywania informacji sektora publicznego „nie narusza[ją] ani w żaden sposób nie wpływa[ją] na stopień ochrony osób fizycznych w związku z przetwarzaniem danych osobowych wynikający z przepisów prawa Unii i prawa państwa członkowskiego, a w szczególności nie zmienia[ją] obowiązków i praw przewidzianych w rozporządzeniu [RODO]".

---

dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych). Przepisy zawarte w tym rozdziale nie tworzą prawa do ponownego wykorzystywania takich danych, ale przewidziano w nich zestaw zharmonizowanych podstawowych warunków, na jakich ponowne wykorzystywanie takich danych może być dozwolone (np. wymóg braku wyłączności)".

[28] Zob. art. 1 dyrektywy w sprawie otwartych danych.

[29] W tym względzie zob. również motyw 52 i 53 oraz art. 1 ust. 4 i art. 10 dyrektywy w sprawie otwartych danych, przy czym ten ostatni obejmuje odniesienie wprost do danych badawczych.

[30] Dane objęte tym rozporządzeniem „**wykraczają poza zakres stosowania dyrektywy (UE) 2019/1024**, z którego wykluczone są dane niedostępne ze względu na tajemnicę handlową i poufność informacji statystycznych oraz dane, do których prawa własności intelektualnej posiadają osoby trzecie. **Dane osobowe wykraczają poza zakres dyrektywy (UE) 2019/1024, o ile system dostępu** wyklucza lub ogranicza dostęp do takich danych ze względu na ochronę danych, prywatność i integralność osoby fizycznej, w szczególności zgodnie z przepisami o ochronie danych" (pogrubienie dodano).

W tym celu, ustalając nowe zasady i przepisy dotyczące ponownego wykorzystywania informacji sektora publicznego, prawodawca unijny powinien przewidzieć niezbędne uwzględnienie takiego ponownego wykorzystywania w prawie do ochrony danych osobowych, zgodnie z RODO[31].

71. **W związku z powyższym EROD i EIOD podkreślają, że w przepisach dyrektywy w sprawie otwartych danych oraz RODO już przewidziano mechanizmy umożliwiające udostępnianie danych osobowych będących w posiadaniu organów sektora publicznego w sposób spójny z wymaganiami w zakresie ochrony podstawowych praw osób fizycznych. EROD i EIOD zalecają zatem dostosowanie rozdziału II wniosku do istniejących przepisów dotyczących ochrony danych osobowych określonych w RODO i dyrektywie w sprawie otwartych danych w celu zapewnienia, aby nie nastąpiło pogorszenie stopnia ochrony danych osobowych w UE, i jednocześnie w celu uniknięcia braku pewności prawa z perspektywy osób fizycznych, organów sektora publicznego i podmiotów ponownie wykorzystujących dane wynikającego ze wspomnianych rozbieżności. Alternatywnie, bez uszczerbku dla dalszych wskazówek przedstawionych w niniejszej Wspólnej Opinii dotyczących wpływu na prawa osób do prywatności i ochrony danych wynikające z przepisów przedmiotowego wniosku regulujących ponowne wykorzystywanie niektórych kategorii chronionych danych będących w posiadaniu organów sektora publicznego, dane osobowe można by wykluczyć z zakresu wniosku.**

3.3.2 Art. 5: warunki ponownego wykorzystywania danych przez organy sektora publicznego

72. Warunki ponownego wykorzystywania danych będących w posiadaniu organów sektora publicznego przedstawiono w art. 5 wniosku, zgodnie z motywem 11. W tym względzie EROD i EIOD uważają, że ten aspekt wniosku budzi pewne wątpliwości.

73. **EROD i EIOD ponownie podkreślają, że każde przetwarzanie danych osobowych, o którym mowa we wniosku, powinno odbywać się w pełnej zgodności z RODO, a zatem przy zastosowaniu odpowiednich zabezpieczeń danych. Oznacza to, że ponowne wykorzystywanie danych osobowych powinno się zawsze odbywać z poszanowaniem zasad zgodności z prawem, rzetelności i przejrzystości, a także ograniczenia celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania, integralności i poufności, zgodnie z art. 5 RODO.**

74. W takim scenariuszu rzetelność, przejrzystość i ograniczenie celu stanowią kluczowe zabezpieczenia umożliwiające budowanie zaufania wśród osób, których dane osobowe są w posiadaniu sektora publicznego, i utwierdzają te osoby w przekonaniu, że ponowne wykorzystywanie przekazanych przez nie informacji będzie się odbywało z poszanowaniem ich praw i interesów (zob. motyw 14 wniosku), tj. ich dane osobowe nie zostaną nieoczekiwanie wykorzystane przeciwko nim. Znaczenie zasady ograniczenia celu jest jasne w kontekście środków branych pod uwagę w celu zwalczenia pandemii COVID-19, np. dane dotyczące zdrowia, które będą przetwarzane pod nadzorem organów opieki zdrowotnej w roli administratorów danych, ale nie będą wykorzystywane w celach komercyjnych lub innych niezgodnych celach[32]. W efekcie organy sektora publicznego, które zgodnie z prawem krajowym lub prawem Unii odpowiadają za udzielanie lub odmowę dostępu na potrzeby ponownego wykorzystywania, muszą brać pod uwagę, że ponowne wykorzystywanie danych osobowych jest

[31] Zob. motyw 154, jak również art. 86 RODO, w których odniesiono się konkretnie do prawa Unii i państwa członkowskiego dotyczącego publicznego dostępu do dokumentów urzędowych.
[32] Zob. opinia EIOD w sprawie europejskiej strategii w zakresie danych, pkt 10.

dopuszczalne jedynie, gdy jest ono zgodne z zasadą ograniczenia celu, jak określono w art. 5 ust. 1 lit. b) i art. 6 RODO[33]. Należy unikać wszelkiego późniejszego wykorzystywania danych zebranych lub udostępnionych w ramach wykonywania zadania publicznego (np. w celu poprawy transportu/mobilności lub oddalenia poważnych transgranicznych zagrożeń zdrowia), w celach uzyskania zysku komercyjnego (np. ubezpieczenie, marketing itp.). Taka „zmiana celu" może stanowić nie tylko naruszenie zasad ochrony danych określonych w art. 5 RODO, ale także podważyć zaufanie osób do mechanizmu ponownego wykorzystywania, które to zaufanie jest podstawowym celem wniosku (zob. motywy 14 i 19)[34].

75. W tym względzie EROD i EIOD przypominają, że w art. 6 ust. 4 RODO wyjaśniono pojęcie „zgodnego dalszego przetwarzania" (danych osobowych). Zgodnie z definicją „ponownego wykorzystywania" określoną w art. 2 pkt 2 wniosku, gdy dotyczy ono danych osobowych, ponowne wykorzystywanie należy z punktu widzenia ochrony danych traktować jako dalsze przetwarzanie danych osobowych będących w posiadaniu organów sektora publicznego w kolejnych celach (komercyjnych lub niekomercyjnych), które nie zostały właściwie określone. W art. 5 wniosku dotyczącym warunków ponownego wykorzystywania nie wskazano jednak celów, w przypadku których ponowne wykorzystywanie mogłoby być zgodne z prawem, ani nie sprecyzowano, że cele ewentualnego późniejszego ponownego wykorzystywania należy dokładnie określić i jasno zdefiniować w prawie Unii lub państwa członkowskiego, zgodnie z art. 6 ust. 1 lit. c) lub e) i art. 6 ust. 3 RODO[35], docelowo spełniając wymagania art. 23 ust. 1 RODO, zgodnie z art. 6 ust. 4 RODO[36].

76. Ogólnie rzecz biorąc, wydaje się, że we wniosku nie określono żadnego zobowiązania prawnego organów sektora publicznego do udostępniania posiadanych danych na potrzeby ponownego wykorzystywania, a celem samego wniosku nie jest zabezpieczenie celów wymienionych w art. 23 RODO.

77. **EROD i EIOD zdecydowanie zalecają zatem zmianę wniosku w celu doprecyzowania, że ponowne wykorzystywanie danych osobowych będących w posiadaniu organów sektora publicznego dopuszcza się wyłącznie wtedy, gdy ma ono podstawę w prawie Unii lub państwa członkowskiego, w których określono wykaz jasnych i zgodnych celów, w przypadku których dalsze przetwarzanie może być zgodne z prawem lub stanowić w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 RODO**.

---

[33] W tym względzie zob. motyw 52 dyrektywy w sprawie otwartych danych.
[34] Zob. opinia EIOD w sprawie europejskiej strategii w zakresie danych, pkt 25.
[35] Art. 6 ust. 3 RODO stanowi, że w prawie Unii lub państwa członkowskiego należy, zgodnie z art. 6 ust. 1 lit. c) lub e) RODO, określić m.in. „ograniczenie celu" przetwarzania danych osobowych oraz „cel, w jakim można ujawnić dane".
[36] Z drugiej strony włączenie danych będących w posiadaniu organów sektora publicznego i chronionych na podstawie poufności informacji statystycznych wchodzącej w zakres rozdziału II wniosku, zgodnie z jego art. 3 ust. 1 lit. b) i wbrew zasadzie określonej w art. 3 ust. 3, wiąże się z ryzykiem podważenia podstawowych zasad ochrony danych w sektorze statystycznym, a w szczególności zasady ograniczenia celu, zgodnie z którą stanowczo zakazuje się wykorzystywania danych poufnych do celów niewyłącznie statystycznych, co osłabiałoby zaufanie osób fizycznych, które przekazują swoje dane osobowe do celów statystycznych (zob. motyw 27 wspomnianego rozporządzenia (WE) nr 223/2009 w sprawie statystyki europejskiej oraz art. 4 ust. 1 i 2 zalecenia Rady Europy nr R (97)18 dotyczącego ochrony danych osobowych zgromadzonych i przetwarzanych dla celów statystycznych).

78. **Ponadto zgodnie z powyższym zaleceniem, aby umożliwić „użytkownikom danych" (w rozumieniu definicji „użytkowników danych" określonej w art. 2 pkt 6 wniosku) zgodny z prawem dostęp do danych osobowych, organy sektora publicznego, które zgodnie z prawem krajowym lub prawem Unii są uprawnione do udzielania lub odmawiania dostępu na potrzeby ponownego wykorzystywania, zgodnie z art. 6 RODO muszą się opierać na odpowiedniej podstawie prawnej mającej zastosowanie do wspomnianego ujawnienia. Kwestię tę pominięto jednak w art. 5 wniosku, w którym określono warunki ponownego wykorzystywania danych będących w posiadaniu organów sektora publicznego.**

79. Ani w motywie 11 wniosku, ani w odpowiadającym mu art. 5 ust. 3–6 nie odniesiono się do prawa Unii ani państwa członkowskiego, które to prawo zapewniłoby podstawę prawną, zgodnie z art. 6 ust. 1 lit. c) lub e) RODO, ale stwierdzono, że „[w] szczególności dane osobowe powinny być przesyłane do ponownego wykorzystywania osobie trzeciej tylko w przypadku, gdy podstawa prawna zezwala na takie przesyłanie". Pod tym względem należy zauważyć, że należy się odnieść do podstawy prawnej „zgodnej z RODO". Co więcej, wspomniany motyw ogranicza się do stwierdzenia, że „[o]rgany sektora publicznego powinny w stosownych przypadkach ułatwiać – za pomocą odpowiednich środków technicznych – ponowne wykorzystywanie danych na podstawie zgody osób, których dane dotyczą, lub zezwoleń osób prawnych na ponowne wykorzystywanie dotyczących ich danych. W tym względzie organ sektora publicznego powinien wspierać potencjalne podmioty ponownie wykorzystujące dane w ubieganiu się o taką zgodę, ustanawiając – jeżeli jest to praktycznie wykonalne – mechanizmy techniczne, które umożliwiają przekazywanie zapytań o zgodę wysłanych przez podmioty ponownie wykorzystujące dane. Nie należy podawać żadnych informacji kontaktowych umożliwiających podmiotom ponownie wykorzystującym dane bezpośredni kontakt z osobami, których dane dotyczą, lub z przedsiębiorstwami".

80. Niejasne jest również brzmienie motywu 14 wniosku, jeżeli chodzi o określenie zależności między tym rozdziałem wniosku a RODO: „[...]Należy zatem wprowadzić dodatkowe zabezpieczenia na wypadek sytuacji, w których ponowne wykorzystywanie takich danych sektora publicznego odbywa się na podstawie przetwarzania danych poza sektorem publicznym. Takie dodatkowe zabezpieczenia można znaleźć w wymogu, aby organy sektora publicznego w pełni uwzględniały prawa i interesy osób fizycznych i prawnych (w szczególności ochronę danych osobowych i szczególnie chronionych danych handlowych oraz ochronę praw własności intelektualnej) w przypadku przekazywania takich danych do państw trzecich"[37].

81. **Co więcej, EROD i EIOD zwracają uwagę, że art. 5 ust. 6 wniosku stanowi, iż „[w] przypadku gdy ponowne wykorzystywanie danych nie może być przyznane zgodnie z obowiązkami określonymi w ust. 3–5 i nie ma innej podstawy prawnej do przesłania danych na mocy rozporządzenia (UE) 2016/679 [...]". W tym względzie EROD i EIOD uważają, że warunków określonych w ust. 3–5 (m.in. dotyczących dostępu do danych i ich ponowne wykorzystywanie w środowisku bezpiecznego przetwarzania) nie można uznać za zamiennik podstawy prawnej wyczerpująco opisanej w art. 6**

[37]Ponadto EROD i EIOD zauważają, że organy sektora publicznego powinny nie tylko uwzględniać ramy prawne dotyczące ochrony praw i interesów osób, których dane dotyczą, ale także ich **przestrzegać**.

RODO, o ile we wspomnianych ustępach nie znajdzie się odniesienie do prawa (Unii lub) państwa członkowskiego[38].

82. Co więcej, niejasna jest rola organu sektora publicznego we wspieraniu podmiotów ponownie wykorzystujących dane w uzyskiwaniu zgody osoby, której dane dotyczą, na ponowne ich wykorzystanie. W ramach kolejnej uwagi dotyczącej art. 5 ust. 6 wniosku EROD i EIOD zwracają uwagę, że przepisem tym nałożono na organy sektora publicznego obowiązek („wspierają"), którego charakter nie został należycie zdefiniowany. W szczególności należy wskazać zgodną z RODO podstawę prawną kontaktowania się z osobami, których dane dotyczą, w celu uzyskania ich zgody na ponowne wykorzystywanie, jak również odpowiedni obowiązek dotyczący uzyskania ważnej zgody, zgodnie z art. 7 RODO[39]. W tym względzie należy także wziąć pod uwagę wyraźny brak równowagi uprawnień, który często ujawnia się w przypadku relacji między osobą, której dane dotyczą, a organami publicznymi[40]. W tym kontekście, zgodnie z zasadą rozliczalności określoną w RODO, EROD i EIOD przypominają, że wybór właściwej podstawy prawnej przetwarzania danych osobowych, jak również wykazanie, że wybraną podstawę prawną (w tym przypadku zgodę) można stosować w sposób ważny, spoczywa na administratorze danych.

83. **Zgodnie z ustanowioną w RODO zasadą zgodności z prawem EROD i EIOD zdecydowanie zalecają zatem doprecyzowanie w warunkach ponownego wykorzystywania określonych w art. 5 wniosku, że zgodnie z RODO właściwa podstawa prawna musi wynikać z prawa Unii lub państwa członkowskiego, a organy sektora publicznego muszą ją dokładnie zidentyfikować w kontekście ewentualnego późniejszego ponownego wykorzystywania danych osobowych.**

84. Innymi kluczowymi elementami służącymi budowaniu zaufania na poziomie stanowiącym cel wniosku są zasady rzetelności i przejrzystości. Zgodnie z tymi zasadami osoby muszą być w pełni świadome, czy dane osobowe, które przekazują organom sektora publicznego lub które są dalej przetwarzane przez te same organy na potrzeby wykonywanych przez nie zadań publicznych, będą ponownie wykorzystywane i w jakich celach, a także muszą wiedzieć, jakim odbiorcom lub kategoriom odbiorców dane zostaną ujawnione, z uwzględnieniem faktu, że w większości przypadków osoby, których dane dotyczą, są na podstawie prawa krajowego zmuszane do przekazania swoich danych osobowych podmiotom publicznym ze względu na zobowiązania prawne lub ponieważ składają wniosek o publiczne działanie lub publiczną usługę[41].

85. W warunkach ponownego wykorzystywania określonych w art. 5 wniosku nie odniesiono się jednak do wynikających z RODO obowiązków organów sektora publicznego w zakresie informowania osób, których dane dotyczą, o ponownym wykorzystywaniu ich danych osobowych ani do potrzeby angażowania ich w proces umożliwiania ponownego wykorzystywania danych osobowych. Fakt ten

---

[38] Dla zachowania jasności przydatne może również być doprecyzowanie, że prawa własności intelektualnej, o których mowa w art. 5 ust. 7, nie dopuszczają (nie stanowią podstawy prawnej do) przetwarzania danych osobowych.

[39] Czy byłby to obowiązek organu sektora publicznego, czy podmiotu ponownie wykorzystującego dane?

[40] Z drugiej strony należy przypomnieć, że zgoda najczęściej nie stanowi właściwej podstawy prawnej czynności przetwarzania dokonywanych przez organy publiczne. Zob. EROD, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/579 dostępne pod adresem https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl

[41] Zob. wyrok Trybunału Sprawiedliwości Unii Europejskiej, C-201/14, Smaranda Bara i in., 1 października 2015 r., ECLI:EU:C:2015:638.

nie tylko podważa zasady rzetelności i przejrzystości określone w RODO w celu zapewnienia, aby osoby miały jasny przegląd możliwego wykorzystywania ich własnych danych osobowych i kontrolę nad takim wykorzystywaniem, ale również zaprzecza samym celom wniosku, tj. dążeniu do zwiększenia zaufania osób, których dane dotyczą, co do tego, że ponowne wykorzystywanie „będzie odbywało się w sposób respektujący ich prawa i interesy” [42]. **EROD i EIOD zalecają zatem uwzględnienie we wniosku wyraźnego odniesienia do obowiązków organów sektora publicznego w zakresie informowania osób, których dane dotyczą, wynikających z RODO, aby wesprzeć wykonywanie praw przyznanych im na podstawie prawodawstwa dotyczącego ochrony danych, szczególnie prawa do sprzeciwu, zgodnie z art. 21 RODO. W tym względzie EROD i EIOD zalecają również zdefiniowanie we wniosku odpowiednich środków, przy pomocy których osoby mogłyby w otwarty sposób i na zasadzie współpracy uczestniczyć w procesie dopuszczania ponownego wykorzystywania ich danych osobowych.**

86. Ponadto, aby osiągnąć rozsądny poziom zaufania do mechanizmu ponownego wykorzystywania, organy sektora publicznego, które zgodnie z prawem krajowym lub unijnym są odpowiedzialne za udzielanie dostępu na potrzeby ponownego wykorzystywania, przy ustalaniu zakresu i warunków udzielania dostępu na potrzeby ponownego wykorzystywania muszą przestrzegać zasad minimalizacji danych i uwzględniać specjalną ochronę wymaganą w przypadku niektórych sektorów rutynowo zajmujących się szczególnymi kategoriami danych osobowych, takich jak sektor zdrowia. Przy podejmowaniu tych decyzji należy także dokładnie rozważyć prawidłowość, ograniczenie przechowywania, integralność i poufność danych osobowych, a także możliwy wpływ na zainteresowane osoby, których dane dotyczą.

87. **W tym względzie EROD i EIOD zwracają uwagę prawodawcy, aby przy ustalaniu zasad regulujących ponowne wykorzystywanie danych osobowych oraz powiązanych warunków i konkretnych zabezpieczeń danych dostrzegł potrzebę odniesienia się do niezbędnych wymagań w zakresie ochrony danych osobowych, szczególnie w „sektorach wrażliwych”, takich jak sektor opieki zdrowotnej.**

88. W szczególności, zgodnie z RODO ocena skutków dla ochrony danych stanowi kluczowe narzędzie zapewniające właściwe uwzględnienie wymogów w zakresie ochrony danych oraz odpowiednią ochronę praw i interesów osób fizycznych, tak aby zwiększyć ich zaufanie do mechanizmu ponownego wykorzystywania. W związku z tym EROD i EIOD zalecają włączenie do tekstu wniosku zapisu mówiącego, że organy sektora publicznego muszą przeprowadzić ocenę skutków dla ochrony danych w przypadku przetwarzania danych objętego zakresem art. 35 RODO[43]. Ocena skutków dla ochrony danych pomoże określić zagrożenia i odpowiednie zabezpieczenia w zakresie ochrony danych w odniesieniu do ponownego wykorzystywania z uwzględnieniem tych zagrożeń, w szczególności w przypadku konkretnych sektorów zajmujących się rutynowo szczególnymi kategoriami danych osobowych. Decyzja o ponownym wykorzystaniu – oprócz tego, że jej podstawę stanowi prawo Unii lub prawo państw członkowskich, w szczególności w przypadku niektórych „sektorów wrażliwych” (sektor zdrowia, ale również transport lub sieci energetyczne) – powinna opierać się na tej ocenie, a także uwzględniać szczególne warunki dla podmiotów ponownie wykorzystujących dane oraz konkretne zabezpieczenia dla osób, których dane dotyczą (na przykład doprecyzowanie ryzyka

[42] Zob. motyw 14 wniosku.
[43] W tym względzie zob. motyw 53 dyrektywy w sprawie otwartych danych.

deanonimizacji danych zanonimizowanych oraz zabezpieczeń przed tym ryzykiem). Ponadto wyniki takiej oceny powinny być w miarę możliwości podawane do wiadomości publicznej jako kolejny środek podnoszący poziom zaufania i przejrzystości[44].

89. Jeżeli chodzi o warunki ponownego wykorzystywania, art. 5 ust. 3 wniosku stanowi, że organy sektora publicznego „mogą" nałożyć obowiązek ponownego wykorzystywania wyłącznie danych osobowych, które zostały uprzednio poddane anonimizacji lub pseudonimizacji. Oznacza to, że organy sektora publicznego nie mają obowiązku przetwarzania wstępnego danych osobowych, aby udostępnić podmiotom ponownie wykorzystującym dane wyłącznie dane osobowe, które zostały uprzednio poddane anonimizacji lub pseudonimizacji. Z związku z tym w przypadku gdy dostarczenie danych zanonimizowanych „nie odpowiadałoby potrzebom podmiotu ponownie wykorzystującego dane"[45] organy sektora publicznego mogą ujawniać podmiotom ponownie wykorzystującym dane nawet dane umożliwiające bezpośrednią identyfikację osób fizycznych, których te dane dotyczą. W takim przypadku organy sektora publicznego nadal mogą zezwolić na ponowne wykorzystywanie danych osobowych na miejscu lub zdalnie w bezpiecznym środowisku przetwarzania na podstawie art. 5 ust. 4 wniosku. Ze względu jednak na szybki rozwój technik deanonimizacji oraz dostępność zaawansowanych zasobów obliczeniowych, prawodawca powinien wziąć pod uwagę, że nie można uznać we wszystkich przypadkach, że anonimizacja, pseudonimizacja, a nawet wykorzystanie bezpiecznych środowisk są wolne od zagrożeń, w szczególności w perspektywie długoterminowej.

90. W tym kontekście EROD i EIOD z zadowoleniem przyjmują fakt, że w motywie 11 wniosku przewidziano, że „organ sektora publicznego może uzależnić korzystanie z takiego bezpiecznego środowiska przetwarzania od podpisania przez podmiot ponownie wykorzystujący dane umowy o poufności, zawierającej zakaz ujawniania wszelkich informacji zagrażających prawom i interesom osób trzecich, które podmiot ponownie wykorzystujący dane mógł uzyskać pomimo wprowadzonych zabezpieczeń". **EROD i EIOD zalecają jednak również umieszczenie odniesienia do takiej umowy o poufności w tekście prawnym wniosku wśród warunków ponownego wykorzystywania określonych w art. 5. Umowa ta powinna również zakazywać podmiotom ponownie wykorzystującym dane deanonimizacji osoby fizycznej, której dane dotyczą, i powinna zawierać zobowiązanie podmiotów ponownie wykorzystujących dane do prowadzenia bieżącej oceny ryzyka deanonimizacji oraz do zgłaszania wszelkich naruszeń ochrony danych skutkujących deanonimizacją zainteresowanych osób fizycznych nie tylko organowi ochrony danych i osobom, których dane dotyczą, zgodnie z art. 33 i 34 RODO, ale również zainteresowanemu organowi sektora publicznego.**

91. **W każdym przypadku EROD i EIOD podkreślają, że anonimizacji i pseudonimizacji nie należy traktować w sposób równorzędny i organy sektora publicznego powinny przypisywać im różną wagę w ocenie ponownego wykorzystywania z perspektywy ochrony danych. W rzeczywistości anonimizacja stanowi środek wspierający ponowne wykorzystywanie informacji sektora publicznego w perspektywie sprzyjającej konkurencji, przy jednoczesnym spełnieniu różnych wymogów wynikających z prawodawstwa w zakresie ochrony danych, zważywszy, że „anonimowe informacje", zgodnie z definicją w motywie 26 RODO, nie wchodzą w zakres wspomnianego**

[44] Zob. Opinia EIOD na temat wniosku dotyczącego wersji przekształconej dyrektywy w sprawie ponownego wykorzystywania informacji sektora publicznego (ISP), dostępna pod adresem: https://edps.europa.eu/sites/edp/files/publication/18-07-11_psi_directive_opinion_en.pdf

[45] Zob. motyw 11 wniosku.

prawodawstwa. Natomiast informacje, które poddano pseudonimizacji (co może prowadzić do deanonimizacji przez osobę fizyczną poprzez wykorzystanie dodatkowych informacji), powinny być nadal uznawane za „dane osobowe", co pociąga za sobą zastosowanie innych środków wymaganych na podstawie przepisów o ochronie danych, jednocześnie ograniczając ryzyko dla osób, których dane dotyczą, oraz pomagając organom sektora publicznego i podmiotom ponownie wykorzystującym dane w wypełnianiu obowiązków w zakresie ochrony danych (w szczególności zasad uwzględnienia ochrony danych w fazie projektowania i domyślnej ochrony danych oraz minimalizacji danych). To ostatnie dotyczy również środków przewidzianych w art. 5 ust. 4 wniosku, które organy sektora publicznego mogą nakładać jako warunki ponownego wykorzystywania.

3.3.3 Art. 5 ust. 11: ponowne wykorzystywanie „szczególnie chronionych" danych nieosobowych

92. W art. 5 ust. 11 wprowadzono koncepcję danych nieosobowych, które w prawie Unii uznano za szczególnie chronione w odniesieniu do przekazywania ich do państw trzecich. Motyw 19 wniosku zawiera kilka przykładów: „w obszarze zdrowia niektóre zbiory danych będące w posiadaniu podmiotów publicznego systemu opieki zdrowotnej takich jak szpitale publiczne", „które uznano za szczególnie chronione", „na przykład w kontekście europejskiej przestrzeni danych dotyczących zdrowia lub w innych przepisach sektorowych". W odniesieniu do takich danych nieosobowych Komisja powinna przyjąć akty delegowane ustanawiające warunki szczegółowe mające zastosowanie do przekazywania takich danych do państw trzecich.

93. W tym względzie EROD i EIOD zauważają, że nawet jeśli informacje zawarte w zbiorze danych zanonimizowanych nie stwarzają ryzyka bezpośredniej identyfikacji lub wyodrębnienia osoby fizycznej, to w połączeniu z innymi dostępnymi informacjami mogą one pociągać za sobą ryzyko pośredniej identyfikacji, a zatem prawdopodobnie będą objęte zakresem definicji danych osobowych. W istocie im więcej informacji będzie dostępnych i im częściej dane będą ponownie wykorzystywane i wzajemnie udostępniane, tym trudniej będzie zapewnić anonimizację na przestrzeni czasu [46]. W związku z powyższym EIOD i EROD pragną zwrócić uwagę na fakt, że już obecnie – i w coraz większym stopniu w przyszłości – często znaczna część danych generowanych i przetwarzanych przy pomocy technik sztucznej inteligencji, uczenia się maszyn, internetu rzeczy, przetwarzania w chmurze i analizy dużych zbiorów danych może być objęta zakresem definicji danych osobowych. W ramach tego scenariusza **EROD i EIOD wzywają prawodawcę, aby wziął pod uwagę fakt, że nawet przewidziane we wniosku ponowne wykorzystywanie szczególnie chronionych danych nieosobowych może mieć wpływ na ochronę danych osobowych, w szczególności w przypadku, gdy takie dane nieosobowe są wynikiem anonimizacji danych osobowych, a zatem informacji pierwotnie dotyczących osób fizycznych.** Również w tych przypadkach należy w pełni zapewnić przestrzeganie praw podstawowych osób, których dane dotyczą, do prywatności i ochrony danych.

[46] W tym względzie zob. opinia Grupy Roboczej Art. 29 05/2014 w sprawie technik anonimizacji (WP 216) oraz wyrok Trybunału Sprawiedliwości z dnia 19 października 2016 r. w sprawie C-582/14, Patrick Breyer przeciwko Bundesrepublik Deutschland, w której odniesiono się do motywu 26 dyrektywy 95/46/WE, a także zbadano prawne i praktyczne środki, za pomocą których można dokonać deanonimizacji dzięki wykorzystaniu dodatkowych danych będących w posiadaniu osób trzecich. Kwestia ta zostanie doprecyzowana w planowanych wytycznych EROD dotyczących anonimizacji/pseudonimizacji.

Ponadto EROD i EIOD zdecydowanie zalecają doprecyzowanie koncepcji „szczególnie chronionych danych nieosobowych", co najmniej poprzez podanie konkretnych przykładów.

3.3.4 Art. 6: opłaty za ponowne wykorzystywanie danych

94. Jeżeli chodzi o opłaty przewidziane w art. 6 wniosku, EROD i EIOD zauważają, że dyrektywa w sprawie otwartych danych zawiera wyraźne odniesienie do „kosztów anonimizacji" w motywach 36 i 38 oraz w art. 6 ust. 1, 4 i 5. W dyrektywie w sprawie otwartych danych przewidziano w szczególności wyjątek od bezpłatnego ponownego wykorzystywania dokumentów, aby umożliwić organom sektora publicznego obciążanie podmiotów ponownie wykorzystujących dane uzasadnionymi wydatkami, które organy te ponoszą z tytułu przetwarzania wstępnego, agregowania lub anonimizacji danych osobowych oferowanych do ponownego wykorzystywania, w sytuacjach, w których zastosowanie takich technik byłoby uzasadnione w świetle zwiększonego ryzyka wynikającego z oferowania takich danych do ponownego wykorzystywania.

95. Biorąc pod uwagę, że w niektórych przypadkach pseudonimizacja lub anonimizacja informacji będących w posiadaniu organów sektora publicznego może być złożonym, czasochłonnym i kosztownym zadaniem wymagającym wiedzy fachowej, która nie zawsze może być dostępna, EROD i EIOD zalecają włączenie do art. 6 ust. 5 wniosku zapisu, że **opłaty pobierane przez organy sektora publicznego za zezwolenie na ponowne wykorzystywanie danych mogą należycie uwzględniać koszty poniesione przez organy sektora publicznego w związku z pseudonimizacją lub anonimizacją** danych osobowych udostępnionych do ponownego wykorzystywania.

96. Należy również zauważyć, że **we wniosku dokonano odwrócenia ustanowionej w dyrektywie w sprawie otwartych danych zasady „bezpłatnego" ponownego wykorzystywania.** Art. 6 ust. 1 wniosku stanowi w istocie, że „[o]rgany sektora publicznego, które zezwalają na ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1, mogą pobierać opłaty za zezwolenie na ponowne wykorzystywanie takich danych". W tym względzie wzajemna zależność z dyrektywą w sprawie otwartych danych jest zatem niejasna.

97. Ponadto można zauważyć, że chociaż art. 6 ust. 5 wniosku stanowi, że „[o]płaty wynikają z kosztów związanych z przetwarzaniem wniosków o ponowne wykorzystywanie [...]", wydaje się, że wniosek wprowadza zachęty finansowe dla organów sektora publicznego, aby te zezwalały na ponowne wykorzystywanie danych osobowych.

98. Należy zauważyć, że w art. 6 ust. 4 wprowadzono obowiązek, zgodnie z którym organy sektora publicznego powinny „wprowadza[ć] środki zachęcające do ponownego wykorzystywania kategorii danych, o których mowa w art. 3 ust. 1, [które obejmują dane osobowe] do celów niekomercyjnych oraz przez małe i średnie przedsiębiorstwa, zgodnie z zasadami pomocy państwa".

99. Aspekt ten, również w świetle kwestii o krytycznym znaczeniu zawartych we wniosku i opisanych w ogólnych uwagach do niniejszej Wspólnej Opinii, jest problematyczny z punktu widzenia ochrony danych zarówno z perspektywy prawnej, jak i praktycznego wdrażania. W szczególności brak jasności co do rodzaju zachęt i ich adresatów może rodzić dodatkowe pytania o to, czy zgoda, jako jedna z podstaw prawnych, na którą powołano się w art. 5 ust. 6 wniosku w odniesieniu do ponownego wykorzystywania danych osobowych, będzie właściwą podstawą prawną, zwłaszcza w odniesieniu do

swobody wyboru osób fizycznych w kwestii odmowy udzielenia zgody na ponowne wykorzystywanie ich danych osobowych lub jej wycofania[47].

3.3.5 Aspekty zarządzania i aspekty instytucjonalne: art. 7 (właściwe podmioty) art. 8 (pojedynczy punkt informacyjny)

100. We wniosku przewiduje się, że państwa członkowskie będą musiały ustanowić pojedynczy punkt kontaktowy do celów ponownego wykorzystywania danych sektora publicznego (art. 8), a także utworzyć organy odpowiedzialne za wspieranie – za pomocą środków technicznych i pomocy prawnej – organów sektora publicznego w zakresie ponownego wykorzystywania danych sektora publicznego (art. 7). Zgodnie z art. 7 ust. 3 takim „właściwym podmiotom" można powierzyć zadanie udzielania dostępu do ponownego wykorzystywania danych, w tym danych osobowych.

101. W związku z tym, jeśli chodzi o właściwe podmioty, będą one między innymi pomagać organom sektora publicznego w uzyskaniu zgody lub zezwolenia na ponowne wykorzystywanie i można im również powierzyć zadanie udzielanie dostępu do danych będących w posiadaniu określonego organu sektora publicznego, w tym danych osobowych, w celu ich ponownego wykorzystywania.

102. Po pierwsze, należy doprecyzować przepis art. 7 ust. 2 lit. c), w szczególności ze względu na niejasność użytej terminologii („zezwolenie od podmiotów ponownie wykorzystujących dane na ponowne wykorzystywanie"; „cele związane z altruistycznym podejściem do danych i inne"; „zgodnie z określonymi decyzjami posiadaczy danych"). Ogólny sens tego przepisu (właściwe podmioty zapewniają „pomoc organom sektora publicznego, w razie potrzeby, w uzyskaniu zgody lub zezwolenia *od podmiotów ponownie wykorzystujących dane na ponowne wykorzystywanie* do celów związanych z altruistycznym podejściem do danych i innych, zgodnie z określonymi decyzjami posiadaczy danych [...]") jest zatem również niejasny.

103. Po drugie, mimo że podmioty te pełnią zasadniczo funkcje wspierające i doradcze na rzecz organów sektora publicznego w zakresie ponownego wykorzystywania danych, niektóre z ich zadań dotyczą wdrażania zabezpieczeń określonych w przepisach o ochronie danych oraz wspierania ochrony praw i interesów osób fizycznych w odniesieniu do ich danych osobowych. W rozdziale II wniosku nie sprecyzowano jednak, czy organy nadzorcze odpowiedzialne za ochronę danych – którym na podstawie RODO również przyznaje się m.in. uprawnienia doradcze – mogą zostać wyznaczone jako właściwy podmiot na podstawie art. 7 wniosku[48].

---

[47] Jak stwierdzono w wytycznych EROD 05/2020 dotyczących zgody na podstawie RODO, co do zasady wszelki element niewłaściwej presji lub niewłaściwego wpływu na osobę, której dane dotyczą (mogący się przejawiać na wiele różnych sposobów), uniemożliwiający osobie, której dane dotyczą, swobodne okazanie woli, spowoduje nieważność zgody.

[48] Tak jak ma to miejsce na przykład w kontekście istniejących przestrzeni danych, takich jak francuskie centrum danych dotyczących zdrowia, w przypadku którego francuski organ ochrony danych jest podmiotem właściwym do wydawania zezwoleń na dostęp do konkretnych danych osobowych. W tym względzie należy również zwrócić uwagę na uprawnienia doradcze przyznane organom ochrony danych w kontekście oceny skutków dla ochrony danych, aby zapewnić ich zgodność z przepisami dotyczącymi ochrony danych osobowych zgodnie z art. 57 ust. 1 lit. l) i art. 58 ust. 3 lit. a) RODO.

104. W tym względzie EIOD i EROD po pierwsze podkreślają, że wyznaczenie i mnożenie właściwych podmiotów, które mogą zajmować się, do pewnego stopnia, przetwarzaniem danych osobowych na podstawie rozdziału II wniosku, mogłoby doprowadzić do rzeczywistej złożoności w odniesieniu do organów sektora publicznego, podmiotów ponownie wykorzystujących dane i osób, których dane dotyczą, a także wpłynąć na spójność w kontekście monitorowania stosowania przepisów RODO. **W związku z tym w zakresie, w jakim dane osobowe są objęte ponownym wykorzystywaniem na podstawie wniosku, EROD i EIOD uważają, że organy nadzorcze odpowiedzialne za ochronę danych powinny być jedynymi podmiotami właściwymi do sprawowania nadzoru nad takim przetwarzaniem danych osobowych. Organom tym należy zapewnić odpowiednie zasoby, aby umożliwić im skuteczne i efektywne wykonywanie tego zadania.**

105. **Ponadto w przypadku wyznaczenia konkretnych podmiotów do pomocy organom sektora publicznego i podmiotom ponownie wykorzystującym dane oraz powierzenia im zadania udzielania dostępu do ponownego wykorzystywania danych, w tym danych osobowych, takie podmioty nie mogą być określane mianem „właściwych", ponieważ nie działałyby jako organ nadzorczy posiadający zdolność do monitorowania i egzekwowania przepisów dotyczących przetwarzania danych osobowych. W celu zapewnienia pewności prawa i spójności stosowania dorobku prawnego UE w dziedzinie ochrony danych osobowych działania i obowiązki takich wyznaczonych podmiotów podlegają również bezpośredniej kompetencji i bezpośredniemu nadzorowi organów ochrony danych, w przypadkach dotyczących danych osobowych.**

106. **Jeśli chodzi o ich kompetencje i zadania wynikające z przepisów RODO, organy ochrony danych posiadają już konkretną wiedzę specjalistyczną w zakresie monitorowania zgodności przetwarzania danych, a także zwiększania świadomości administratora i podmiotu przetwarzającego dane w kwestii ich obowiązku związanego z przetwarzaniem danych osobowych. W związku z tym w celu zapewnienia spójności między ramami instytucjonalnymi przewidzianymi w rozdziale II wniosku a przepisami RODO EROD i EIOD zalecają doprecyzowanie, że głównymi organami właściwymi do sprawowania nadzoru i egzekwowania przepisów rozdziału II dotyczących przetwarzania danych osobowych są organy nadzorcze odpowiedzialne za ochronę danych. Te ostatnie powinny ściśle współpracować z konkretnymi podmiotami wyznaczonymi na podstawie wniosku do pomocy organom sektora publicznego i podmiotom ponownie wykorzystującym dane, którym powierzono zadanie udzielania dostępu do danych w celu ich ponownego wykorzystywania, w razie potrzeby w porozumieniu z innymi odpowiednimi organami sektorowymi, tak aby zapewnić spójne stosowanie tych przepisów.**

107. EROD i EIOD zauważają również, że w art. 8 ust. 4 wniosku przewidziano mechanizm odwoławczy dla podmiotów ponownie wykorzystujących dane, które chcą zaskarżyć decyzję o odmowie dostępu do danych do celów ponownego wykorzystywania, który to mechanizm różni się od tego ustanowionego na podstawie dyrektywy w sprawie otwartych danych. W szczególności zgodnie z dyrektywą w sprawie otwartych danych (zob. art. 4 ust. 4) środki odwoławcze obejmują możliwość kontroli przez bezstronny organ odwoławczy posiadający odpowiednią wiedzę specjalistyczną taki jak, między innymi, „organ nadzorczy ustanowiony zgodnie z rozporządzeniem (UE) 2016/679 lub krajowy organ sądowy – którego decyzje są wiążące dla danego organu sektora publicznego". W tym względzie, bez uszczerbku dla uwag poczynionych już w niniejszej Wspólnej Opinii na temat potrzeby doprecyzowania wzajemnej zależności między wnioskiem a dyrektywą w sprawie otwartych danych, EROD i EIOD zwracają uwagę prawodawcy na niespójności istniejące między tymi dwoma zestawami przepisów.

3.4 Wymogi mające zastosowanie do dostawców usług udostępniania danych

W uzasadnieniu stwierdzono, że „[r]ozdział III ma na celu zwiększenie zaufania w zakresie udostępniania danych osobowych i nieosobowych oraz obniżenie kosztów transakcji związanych z udostępnianiem danych między przedsiębiorstwami i między konsumentami a przedsiębiorstwami poprzez utworzenie systemu zgłaszania dostawców usług udostępniania danych. Dostawcy ci będą musieli spełnić szereg wymogów, w szczególności wymóg zachowania neutralności w odniesieniu do udostępnianych danych. Nie mogą oni wykorzystywać takich danych do innych celów. W przypadku dostawców usług udostępniania danych oferujących usługi osobom fizycznym konieczne będzie również spełnienie dodatkowego kryterium polegającego na przyjęciu na siebie obowiązków powierniczych wobec osób fizycznych, które korzystają z tych danych. Podejście to ma na celu zapewnienie, aby usługi udostępniania danych funkcjonowały w sposób otwarty i oparty na współpracy, przy jednoczesnym wzmocnieniu pozycji osób fizycznych i prawnych poprzez umożliwienie im lepszego rozeznania w ich danych i większej kontroli nad nimi. Za monitorowanie zgodności z wymogami związanymi ze świadczeniem takich usług odpowiedzialny będzie właściwy organ wyznaczony przez państwa członkowskie”[49].

108. W art. 9 ust. 1 wniosku, jak wskazano w motywie 22, określono trzy różne rodzaje usług udostępniania danych. Są to:

- w lit. a) – usługi pośrednictwa między posiadaczami danych będącymi osobami prawnymi a potencjalnymi użytkownikami danych;

- w lit. b) – usługi pośrednictwa między osobami, których dane dotyczą, a potencjalnymi użytkownikami danych;

- w lit. c) – usługi świadczone przez „spółdzielnie danych”.

109. Pierwszy rodzaj usługi udostępniania danych, o którym mowa w art. 9 ust. 1 lit. a), obejmuje „usługi pośrednictwa między posiadaczami danych będącymi osobami prawnymi a potencjalnymi użytkownikami danych, w tym udostępnianie środków technicznych lub innych środków umożliwiających świadczenie takich usług; usługi te mogą obejmować dwustronną lub wielostronną wymianę danych lub tworzenie platform lub baz danych umożliwiających wymianę lub wspólne wykorzystywanie danych, jak również tworzenie specjalnej infrastruktury do wzajemnych połączeń między posiadaczami danych i użytkownikami danych”.

110. Motyw 22 stanowi: „Oczekuje się, że dostawcy usług udostępniania danych (pośrednicy w zakresie danych) będą odgrywali kluczową rolę w gospodarce opartej na danych jako narzędzie ułatwiające agregowanie i wymianę znacznych ilości istotnych danych. Pośrednicy w zakresie danych oferujący usługi, które łączą poszczególne podmioty, mogą przyczynić się do skutecznego łączenia danych, jak również do ułatwienia dwustronnego udostępniania danych. Wyspecjalizowani pośrednicy w zakresie danych, którzy są niezależni zarówno od posiadaczy danych, jak i użytkowników danych, mogą odgrywać rolę polegającą na ułatwianiu powstawania nowych ekosystemów opartych na danych, niezależnych od jakiegokolwiek podmiotu o znaczącej pozycji rynkowej. Niniejsze rozporządzenie

[49] Uzasadnienie, s. 8.

powinno obejmować wyłącznie dostawców usług udostępniania danych, których głównym celem jest nawiązanie relacji biznesowych, prawnych i potencjalnie również technicznych między posiadaczami danych, w tym osobami, których dane dotyczą, z jednej strony a potencjalnymi użytkownikami z drugiej strony oraz pomoc obu stronom w przeprowadzaniu transakcji dotyczących zasobów danych. Powinno ono obejmować tylko usługi mające na celu pośredniczenie między nieokreśloną liczbą posiadaczy i użytkowników danych, z wyłączeniem usług udostępniania danych, które mają być wykorzystywane przez zamkniętą grupę posiadaczy i użytkowników danych".

111. **W świetle powyższego EROD i EIOD uważają, że kwestia, która została przedstawiona w uwagach ogólnych niniejszej Wspólnej Opinii jako nadrzędny problem, a mianowicie ryzyko, że wniosek tworzy równoległy zbiór przepisów, które nie są spójne z RODO, jest szczególnie widoczna w odniesieniu do rozdziału III wniosku. W istocie niejasna jest wzajemna zależność między przepisami art. 9 wniosku, odnoszącymi się do „posiadaczy danych", „potencjalnych użytkowników danych", „wymiany lub wspólnego wykorzystywania danych", „wzajemnych połączeń między posiadaczami danych i użytkownikami danych", a przepisami i zasadami ustanowionymi w RODO.**

112. Przypominamy, że usługa udostępniania danych jako platforma mająca na celu „pośredniczenie między nieokreśloną liczbą posiadaczy i użytkowników danych", z wyłączeniem wykorzystywania przez zamkniętą grupę użytkowników danych, w zakresie, w jakim to pośredniczenie dotyczy danych osobowych, musi być zgodna w szczególności z zasadą ochrony danych w fazie projektowania oraz domyślnej ochrony danych przewidzianej w art. 25 RODO[50].

[50] Zob. art. 25 ust. 2: „Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe **nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych**".
Zob. również EROD, Wytyczne 4/2019 dotyczące artykułu 25 Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych, s. 20:
„Kluczowe elementy ograniczenia celu w kontekście uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochrony danych mogą obejmować:
– ustalenie z góry – prawnie uzasadnione cele należy określić przed przystąpieniem do fazy projektowania przetwarzania;
– specyfikę – należy podać konkretne i wyraźne cele, w których przetwarzane są dane osobowe;
– ukierunkowanie na cel – cel przetwarzania powinien być decydujący przy projektowaniu przetwarzania i stanowić podstawę granic przetwarzania;
– niezbędność – na podstawie celu określa się, jakie dane osobowe są niezbędne do przetwarzania;
– zgodność – każdy nowy cel musi być zgodny z celem pierwotnym, dla którego zebrano dane, i musi prowadzić do istotnych zmian w projekcie;
– ograniczenie dalszego przetwarzania – administrator nie powinien łączyć zbiorów danych ani prowadzić dalszego przetwarzania do nowych, niezgodnych celów;
– ograniczenie ponownego wykorzystania – administrator powinien stosować środki techniczne, w tym haszowanie i szyfrowanie, aby ograniczyć możliwość ponownego wykorzystania danych osobowych. Administrator powinien również dysponować środkami organizacyjnymi, takimi jak polityka i zobowiązania umowne, które ograniczają możliwość ponownego, nieuprawnionego wykorzystywania danych osobowych;
– przegląd – administrator ma obowiązek regularnie sprawdzać, czy przetwarzanie jest niezbędne do celów, dla których zebrano dane, a także testować projekt pod względem ograniczenia celu".

113. EROD i EIOD wskazują również na zasady ochrony danych dotyczące przejrzystości (i ograniczenia celu) przetwarzania danych osobowych. Jak stwierdzono w wytycznych Grupy Roboczej Art. 29 w sprawie przejrzystości, „osoba, której dane dotyczą, powinna [...] być w stanie z wyprzedzeniem określić zakres i skutki przetwarzania [...]", „innymi słowy, jaki rzeczywisty wpływ na osobę, której dane dotyczą, będzie miało konkretne przetwarzanie opisane w oświadczeniu o ochronie prywatności/informacji o polityce prywatności"[51].

114. **Koncepcja usługi udostępniania danych jako platformy „pośredniczącej między nieokreśloną liczbą posiadaczy i użytkowników danych", będącej swego rodzaju rynkiem otwartych danych, byłaby sprzeczna z wyżej wymienionymi zasadami ochrony danych: uwzględnienie ochrony prywatności już w fazie projektowania i domyślna ochrona prywatności, przejrzystość i ograniczenie celu, jeżeli platforma nie pozwala na dokonanie przez osobę, której dane dotyczą, wstępnego wyboru celów i użytkowników jej danych osobowych oraz na uprzednie poinformowanie jej o tych celach i użytkownikach. W celu zapewnienia jasności we wniosku należy sprecyzować ten aspekt, co najmniej w motywie.**

115. **Zakres pojęcia pośrednika w zakresie danych między posiadaczami danych a osobami prawnymi jest również niejasny i dlatego powinien zostać lepiej określony**[52].

116. Ogólnie rzecz biorąc, można również zauważyć, że we wniosku nie określono, **w jaki sposób (zgodnie z jaką podstawą prawną RODO) dostawcy usług udostępniania danych będą gromadzić dane osobowe do celów udostępniania**.

---

[51] Grupa Robocza Art. 29, Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, WP 260 rev. 01, s. 7.

[52] Motyw 22 stanowi: „[...] Należy wykluczyć dostawców **usług w chmurze**, jak również **dostawców usług, którzy uzyskują dane od posiadaczy danych, agregują, wzbogacają lub przekształcają dane i udzielają licencji na wykorzystywanie** powstałych danych użytkownikom danych bez ustanawiania bezpośredniej relacji między posiadaczami danych a użytkownikami danych, na przykład **brokerów reklam lub danych, przedsiębiorstwa doradcze w zakresie danych, dostawców produktów uzyskanych z danych, powstałych w wyniku wniesienia wartości dodanej** w dane przez dostawcę usług. Jednocześnie należy umożliwić dostawcom usług udostępniania danych **dostosowywanie udostępnianych danych – takie jak konwertowanie ich na konkretne formaty – w zakresie, w jakim poprawia to użyteczność** danych dla użytkownika danych, w przypadku gdy użytkownik danych sobie tego życzy. Ponadto niniejsze rozporządzenie **nie powinno obejmować usług, które koncentrują się na pośrednictwie w udostępnianiu treści, w szczególności treści chronionych prawem autorskim**.
Niniejsze rozporządzenie nie powinno obejmować **platform wymiany danych, które to platformy są użytkowane wyłącznie przez jednego posiadacza danych** w celu umożliwienia wykorzystywania posiadanych danych, ani platform opracowanych w kontekście przedmiotów i urządzeń podłączonych do internetu rzeczy, których głównym celem jest zapewnienie funkcji podłączonego przedmiotu lub urządzenia i umożliwienie świadczenia usług o wartości dodanej. Do celów niniejszego rozporządzenia „dostawców informacji skonsolidowanych" w rozumieniu art. 4 ust. 1 pkt 53 dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE, jak również „dostawców świadczących usługę dostępu do informacji o rachunku" w rozumieniu art. 4 pkt 19 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 nie należy uznawać za dostawców usług udostępniania danych. Podmioty, które ograniczają swoją działalność do ułatwiania wykorzystywania danych udostępnianych na podstawie altruistycznego podejścia do danych i które prowadzą działalność o charakterze niekomercyjnym, nie powinny być objęte przepisami rozdziału III niniejszego rozporządzenia, ponieważ działalność ta służy celom leżącym w interesie ogólnym dzięki zwiększaniu ilości danych dostępnych do takich celów".

117. Nie jest również jasne, **czy dostawcy usług udostępniania danych mogą pośredniczyć w przekazywaniu danych dozwolonych do ponownego wykorzystania przez organy sektora publicznego** na podstawie rozdziału II wniosku.

118. Ze względu na przejrzystość oraz w celu zwiększenia (a nie zmniejszenia) poziomu zaufania obywateli kluczowe jest również wyraźne zaznaczenie we wniosku, że usługa udostępniania danych będzie świadczona po opłaceniu „kosztu" przez posiadaczy i użytkowników danych. Aspekt ten można wywnioskować ze sformułowania art. 11 ust. 3 wniosku[53], ale jest on niejasny i niekompletny (nie daje jasnego obrazu transakcji pieniężnych towarzyszących przetwarzaniu danych osobowych). Wyraźna zachęta do „monetyzacji" danych osobowych zwiększa również znaczenie kontroli zgodności z zasadami ochrony danych[54]. Niestety, w tym względzie, jak również w odniesieniu do pozostałych rozdziałów wniosku, ocena skutków[55] nie uwzględnia ryzyka związanego z ochroną danych.

119. Ponadto EROD i EIOD zauważają, że wniosek nie daje jasnego obrazu, np. za pośrednictwem zawartych w motywach przykładów „przypadków użycia" usług udostępniania danych (których „aspekt transakcji pieniężnej" – jak podkreślono – powinien być wyjaśniony opinii publicznej i zainteresowanym osobom, gdy ma to miejsce). Np. w motywie 22 wyjaśniono, co nie jest platformą wymiany danych, którą można uznać za „pośrednika w zakresie danych": „Niniejsze rozporządzenie nie powinno obejmować platform wymiany danych, które to platformy są użytkowane wyłącznie przez jednego posiadacza danych w celu umożliwienia wykorzystywania posiadanych danych, ani platform opracowanych w kontekście przedmiotów i urządzeń podłączonych do internetu rzeczy, których głównym celem jest zapewnienie funkcji podłączonego przedmiotu lub urządzenia i umożliwienie świadczenia usług o wartości dodanej". Nie przedstawiono w nim jednak w tym względzie przewidywanego przypadku użycia.

3.4.1 Pośrednicy w zakresie danych na podstawie art. 9 ust. 1 lit. b): usługi pośrednictwa między osobami, których dane dotyczą, a potencjalnymi użytkownikami danych[56].

120. EROD i EIOD zauważają, że przepisy związane z usługami pośrednictwa między osobami, których dane dotyczą, zamierzającymi udostępnić swoje dane osobowe a potencjalnymi użytkownikami danych, w ramach wykonywania praw przewidzianych w rozporządzeniu (UE) 2016/679 zgodnie z art. 9 ust. 1

[53] Art. 11 ust. 3 wniosku stanowi, że: „dostawca usług zapewnia, aby procedura dostępu do usługi była sprawiedliwa, przejrzysta i niedyskryminująca zarówno dla posiadaczy danych, jak i użytkowników danych, w tym w odniesieniu do **cen**".

[54] W tym względzie EROD opracowuje wytyczne w sprawie gromadzenia i wykorzystywania danych osobowych za wynagrodzeniem finansowym.

[55] Ocena skutków towarzysząca aktowi w sprawie zarządzania danymi, SWD(2020) 295 final, dostępna pod adresem: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2020:0295:FIN:EN:PDF

[56] Art. 9 ust. 1 lit. b) wniosku odnosi się do: „usług pośrednictwa między osobami, których dane dotyczą, zamierzającymi udostępnić swoje dane osobowe a potencjalnymi użytkownikami danych, w tym udostępniania technicznych lub innych środków umożliwiających świadczenie takich usług, w ramach wykonywania praw przewidzianych w rozporządzeniu (UE) 2016/679".

lit. b), należy stosować bez uszczerbku dla skutecznego stosowania praw osób, których dane dotyczą, i obowiązków administratora zgodnie z RODO.

121. We wniosku nie określono jednak warunków, na jakich tacy dostawcy usług mieliby skutecznie pomagać osobom fizycznym w wykonywaniu ich praw na podstawie RODO, ani nie wskazano, do jakiego przetwarzania danych osobowych taka pomoc miałaby się odnosić i wobec jakich dokładnie użytkowników danych[57].

122. Przede wszystkim EROD i EIOD uważają, że skuteczne wykonywanie praw osób, których dane dotyczą, oraz możliwe tryby takiego wykonywania są przewidziane w RODO, pod nadzorem krajowych organów nadzorczych zgodnie z art. 51 tego rozporządzenia. Brak jasności co do dokładnego trybu udzielania pomocy w wykonywaniu praw osób, których dane dotyczą, a także co do odbiorców takiego procesu i ich obowiązków wobec osób, których dane dotyczą, może prowadzić do dalszego braku pewności prawa w zakresie skutecznego wykonywania praw osób, których dane dotyczą, zgodnie z RODO.

123. **EROD i EIOD zalecają zatem, aby wniosek odzwierciedlał ramy prawne UE (RODO), zgodnie z którymi takie tryby, jak również związane z nimi obowiązki mające zastosowanie do dostawców i odbiorców usług udostępniania danych, mogą zostać doprecyzowane przez Europejską Radę Ochrony Danych, zgodnie z art. 70 RODO[58].**

124. Nie jest również jasne, czy usługi pośrednictwa, o których mowa w art. 9 ust. 1 lit. b) wniosku i których definicji nie podano w art. 2, odnoszą się wyłącznie do (i w jakim zakresie) systemów zarządzania danymi osobowymi (PIMS). EROD i EIOD zwracają uwagę na różnicę między systemami zarządzania danymi osobowymi, umożliwiającymi zarządzanie danymi osobowymi i ułatwiającymi wykonywanie praw osób, których dane dotyczą („interakcja z osobą, której dane dotyczą”)[59], z jednej strony, a dostawcami usług udostępniania danych między przedsiębiorstwami (których korelacja z „brokerami danych” jest niejasna), z drugiej strony. To właśnie w odniesieniu do tych ostatnich, gdy osoba, której dane dotyczą, jest bardziej oddalona i istnieje ryzyko, że nie będzie miała jasnego oglądu sytuacji i kontroli nad udostępnianiem jej danych osobowych, krytyczne aspekty z punktu widzenia ochrony danych mogą być poważniejsze[60].

---

[57] Art. 11 ust. 10 wniosku jest nadal dość niejasny w swoim sformułowaniu: „dostawca usług oferujący usługi osobom, których dane dotyczą, **działa w najlepszym interesie osób, których dane dotyczą, ułatwiając im wykonywanie ich praw**, w szczególności doradzając im w zakresie potencjalnego wykorzystania danych i standardowych warunków związanych z takim wykorzystaniem”.

[58] W tym względzie EROD pracuje obecnie nad wytycznymi dotyczącymi praw osób, których dane dotyczą.

[59] Zob. opinia EIOD w sprawie systemów zarządzania danymi osobowymi, 20 października 2016 r., dostępna pod adresem: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf

[60] Zob. opinia EIOD w sprawie europejskiej strategii w zakresie danych, pkt 20: „Jednocześnie EIOD podkreśla potrzebę zachowania ostrożności w odniesieniu do roli brokerów danych, którzy są aktywnie zaangażowani w gromadzenie ogromnych zbiorów danych, w tym danych osobowych z różnych źródeł. Dysponują oni różnymi źródłami danych wykorzystywanych do usług związanych z danymi, takich jak dane, które są ujawniane do innych niepowiązanych celów; dane z rejestrów publicznych (otwarte dane), a także dane »wyłowione« z internetu i mediów społecznościowych, często z naruszeniem przepisów o ochronie danych. W tym kontekście Europejski Inspektor Ochrony Danych zauważa, że działalność »brokerów dużych zbiorów danych« podlega wzmożonej kontroli i jest badana przez wiele krajowych organów ochrony danych”.

125. We wszystkich przypadkach zastosowanie mają jednak zasady przejrzystości, rzetelności i ograniczenia celu.

126. W swojej opinii na temat systemów zarządzania danymi osobowymi EIOD wskazał, że „w każdym przypadku kluczowe znaczenie ma zapewnienie przejrzystości modelu biznesowego w stosunku do osób fizycznych, których dane są przetwarzane, tak aby osoby te były świadome wchodzących w grę interesów (dostawcy systemów zarządzania danymi osobowymi i inni usługodawcy) i mogły korzystać z systemów zarządzania danymi osobowymi z pełną świadomością”[61].

127. Wniosek zawiera pewne wyjaśnienia dotyczące dostawców usług udostępniania danych, którzy nie mają siedziby w Unii, w celu stwierdzenia, czy taki dostawca oferuje usługi w Unii. To doprecyzowanie w motywie 27 wniosku wydaje się zgodne z motywem 23 RODO. Ze względu na pewność prawa przydatne mogłoby być doprecyzowanie, że w przypadku przetwarzania danych osobowych wspomniani wyżej dostawcy usług udostępniania danych niemający siedziby w Unii podlegają przepisom i zasadom RODO.

3.4.2 Pośrednicy w zakresie danych na podstawie art. 9 ust. 1 lit. c): „spółdzielnie danych”

128. EROD i EIOD podkreślają, że pojęcie „usług świadczonych przez spółdzielnie danych”, wprowadzone w art. 9 ust. 1 lit. c) wniosku [62], pozostaje niejasne zarówno pod względem charakteru, jak i obowiązków. W tym względzie należy wprowadzić jasną definicję takich dostawców usług udostępniania danych, jak również dotyczących ich obowiązków, aby uniknąć wszelkiego braku pewności prawa w zakresie świadczenia takich usług.

129. Chociaż we wniosku określono, że spółdzielnie danych „dążą do wzmocnienia pozycji osób fizycznych przy dokonywaniu świadomych wyborów przed wyrażeniem zgody na wykorzystywanie danych, wywierając wpływ na zasady i warunki organizacji użytkowników danych związane

[61] Zob. opinia EIOD w sprawie systemów zarządzania danymi osobowymi, 20 października 2016 r., pkt 52, s. 13, dostępna pod adresem: https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf
Zob. także pkt 53, s. 13: „Model systemu zarządzania danymi osobowymi wydaje się zachęcać do debaty na temat tego, kto jest »właścicielem« naszych danych osobowych. Osoby fizyczne w UE mają podstawowe prawo do ochrony swoich danych osobowych oparte na art. 8 Karty praw podstawowych UE. Szczegółowe prawa i obowiązki związane z korzystaniem z tego prawa są uregulowane bardziej szczegółowo w niedawno przyjętym RODO. Kwestie te nie są specyficzne dla systemów zarządzania danymi osobowymi: dane osobowe są często postrzegane jako »waluta«, którą płaci się za tzw. »darmowe« usługi w internecie. Tendencja ta nie oznacza jednak, że dane osobowe osób fizycznych można zgodnie z prawem uznać za własność, którą można swobodnie handlować jak każdą inną własnością na rynku. Wręcz przeciwnie, z zasady systemy zarządzania danymi osobowymi nie będą mogły »sprzedawać« danych osobowych, a ich rola będzie polegała raczej na umożliwieniu osobom trzecim korzystania z danych osobowych **do określonych celów** i **w określonych okresach**, z zastrzeżeniem **warunków określonych przez same osoby fizyczne** oraz **wszelkich innych zabezpieczeń przewidzianych w obowiązującym prawie ochrony danych**”.

[62] Art. 9 ust. 1 lit. c) wniosku odnosi się do „usług świadczonych przez spółdzielnie danych, tj. usług wspierających osoby, których dane dotyczą, lub jednoosobowe firmy, lub mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa, które są członkami spółdzielni lub **które przyznają spółdzielni uprawnienia do negocjowania warunków przetwarzania danych przed wyrażeniem przez nie zgody**, w **dokonywaniu świadomych wyborów przed wyrażeniem zgody na przetwarzanie danych** oraz **umożliwiających ustanowienie mechanizmów wymiany poglądów na temat celów i warunków przetwarzania danych, które najlepiej będą odzwierciedlały interesy osób, których dane dotyczą, lub osób prawnych**”.

z wykorzystywaniem danych lub potencjalnie rozwiązując spory między członkami grupy dotyczące sposobu wykorzystywania danych, w przypadku gdy dane takie odnoszą się do kilku osób w obrębie grupy, których dane dotyczą”[63], należy przypomnieć, że obowiązki w zakresie przejrzystości, jak również warunki ważnej zgody osoby, której dane dotyczą, zgodnie z art. 6 ust. 1 lit. a) rozporządzenia (UE) 2016/679 oraz warunek przetwarzania danych osobowych w ramach tej podstawy prawnej, są określone i przewidziane w tym samym rozporządzeniu.

130. **EROD i EIOD uważają zatem, że pozycji osób fizycznych w dokonywaniu świadomego wyboru lub rozwiązywania potencjalnych sporów dotyczących sposobu wykorzystania danych nie należy traktować jako warunków podlegających negocjacjom, lecz raczej jako obowiązki administratorów zgodnie z rozporządzeniem (UE) 2016/679. W tym względzie należy również wskazać, że odniesienie w motywie 24 wniosku do danych, które „odnosiłyby się” do kilku osób, których dane dotyczą, w zakresie, w jakim dotyczy to danych osobowych, może nie być spójne z definicją danych osobowych zawartą w rozporządzeniu (UE) 2016/679[64], która odnosi się do „informacji o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”.**

131. Ponadto, jak przypomniano w motywie 24 wniosku, „prawa wynikające z rozporządzenia (UE) 2016/679 mogą być wykonywane tylko przez każdą osobę fizyczną i nie mogą być powierzone ani przekazane spółdzielni danych”. EROD i EIOD uważają, że artykulacja takich zasad z możliwością przyznania spółdzielniom danych uprawnień do „negocjowania warunków przetwarzania danych przed wyrażeniem przez nie zgody” jest co najmniej niejasna, jeśli nie wprost sprzeczna. „Warunki” przetwarzania danych osobowych są w istocie warunkami zapisanymi w RODO, a zatem nie można ich zmienić ani zastąpić umową lub innego rodzaju ustaleniami prywatnymi.

3.4.3 Art. 10: system zgłaszania – ogólne wymogi kwalifikujące do rejestracji – treść zgłoszenia; wynik (i termin) zgłoszenia. Art. 11: warunki świadczenia usług udostępniania danych

132. W rozdziale III wniosku, w art. 9 ust. 1, ustanowiono dla dostawców usług udostępniania danych obowiązek dokonania zgłoszenia do właściwego organu (zgłoszenie obowiązkowe). Art. 10 ust. 1 i 2 zawiera przepisy dotyczące określania jurysdykcji państwa członkowskiego do celów wniosku. Jest to jurysdykcja państwa członkowskiego głównej jednostki organizacyjnej dostawcy usług udostępniania danych lub państwa członkowskiego siedziby przedstawiciela prawnego dostawcy usług udostępniania danych niemającego siedziby w Unii.

133. Informacje, które należy zawrzeć w zgłoszeniu określono w art. 10 ust. 6 lit. a)–h) wniosku[65]. Ponadto art. 10 ust. 7 stanowi, że „[n]a wniosek dostawcy usług właściwy organ wydaje w terminie jednego

[63] Motyw 24 wniosku.
[64] Definicja na podstawie art. 4 pkt 1 RODO.
[65] „Zgłoszenie zawiera następujące informacje:
a) nazwę dostawcy usług udostępniania danych;
b) status prawny, formę prawną i numer rejestracyjny dostawcy, jeżeli dany dostawca jest zarejestrowany w rejestrze handlowym lub innym podobnym rejestrze publicznym;
c) adres głównej jednostki organizacyjnej dostawcy w Unii, jeżeli ma to zastosowanie, oraz drugorzędnego oddziału w innym państwie członkowskim, o ile takowy istnieje, lub adres przedstawiciela prawnego wyznaczonego zgodnie z ust. 3;
d) stronę internetową, na której można znaleźć informacje o dostawcy usług i jego działalności, jeśli taka istnieje;

tygodnia standardowe oświadczenie, potwierdzające, że dostawca usług przedłożył zgłoszenie, o którym mowa w ust. 4".

134. System zgłaszania, jak podkreślono w uzasadnieniu, „obejmuje obowiązek zgłaszania wraz z monitorowaniem *ex post* przez właściwe organy państw członkowskich zgodności z wymogami dotyczącymi prowadzenia działalności"[66]. Aspekt ten omówiono bardziej szczegółowo w motywach 30 i 31 wniosku[67].

135. W związku z tym „weryfikacja" dostawcy usług udostępniania danych ogranicza się do sprawdzenia przez właściwy organ wymogów (głównie formalnych) określonych w art. 10 i odbywa się w bardzo krótkim terminie (jeden tydzień od daty zgłoszenia).

136. **W tym względzie EROD i EIOD zauważają, że system „weryfikacji" jest niemal „deklaratywny" i że Komisja wybrała najbardziej „luźny" system (w przeciwieństwie na przykład do systemu zezwoleń). EROD i EIOD zauważają, że co najmniej w odniesieniu do przetwarzania danych osobowych system powinien spełniać bardziej ochronną funkcję (tj. zapewniać więcej kontroli i zabezpieczeń dla osób, których dane dotyczą, w tym w odniesieniu do kluczowych aspektów ochrony danych). Pozwoliłoby to również na zapewnienie wyższego poziomu zaufania, do którego dąży Komisja.**

137. **W celu rozwiązania tego problemu należy w szczególności zmienić motyw 31 wniosku.**

138. Zgodnie z zasadą rozliczalności w zakresie ochrony danych dostawcy usług udostępniania danych powinni być w stanie m.in. wykazać, że wprowadzili strategie i procedury umożliwiające osobom, których dane dotyczą, łatwe korzystanie z przysługujących im indywidualnych praw ochrony danych (procedury zapewniające przestrzeganie praw osób, których dane dotyczą), a także powinni dokumentować decyzje dotyczące udostępniania danych (w tym w szczególności cele, w których dane osobowe będą udostępniane, oraz odbiorców lub kategorie odbiorców, którym będą one ujawniane), wykazując zgodność z przepisami dotyczącymi ochrony danych[68]. Aspekty te (które powinny stanowić

---

e) wskazanie osoby wyznaczonej do kontaktów przez dostawcę usług i dane kontaktowe;
f) opis usługi, którą dostawca usług zamierza świadczyć;
g) planowaną datę rozpoczęcia działalności;
h) państwa członkowskie, w których dostawca usług zamierza świadczyć usługi".

[66] Uzasadnienie, s. 5.

[67] „(30) Należy ustanowić procedurę zgłaszania usług udostępniania danych, aby zapewnić zarządzanie danymi na terenie Unii oparte na godnej zaufania wymianie danych. Korzyści płynące z godnego zaufania otoczenia najlepiej osiągnąć poprzez nałożenie szeregu wymogów dotyczących świadczenia usług udostępniania danych, ale **bez konieczności wydawania przez właściwy organ jakiejkolwiek jednoznacznej decyzji lub aktu administracyjnego na potrzeby świadczenia takich usług**.
(31) Aby wesprzeć skuteczne transgraniczne świadczenie usług, należy wymagać od dostawcy usług udostępniania danych **przesłania zgłoszenia wyłącznie do wyznaczonego właściwego organu państwa członkowskiego, w którym znajduje się jego główna jednostka organizacyjna lub w którym znajduje się jego przedstawiciel prawny**. Takie **zgłoszenie nie powinno mieć szerszego zakresu niż zwykłe oświadczenie o zamiarze świadczenia takich usług i powinno zawierać wyłącznie informacje określone w niniejszym rozporządzeniu**" (pogrubienie dodano).

[68] Zgodnie z art. 30 RODO: „Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje: a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela

główny element systemu przyznawania znaku jakości przewidzianego we wniosku [69]) w efekcie przyczynią się do wzbudzenia większego zaufania społeczeństwa do dostawców usług udostępniania danych.

139. EROD i EIOD zauważają również, że świadczenie usług udostępniania danych, zgodnie z art. 11, podlega warunkom określonym w ust. 1–11. W tym względzie EROD i EIOD zauważają, że chociaż wśród warunków znajduje się odniesienie do zgodności z przepisami dotyczącymi konkurencji (w ust. 9), te (wyczerpująco wymienione) warunki nie obejmują zgodności z przepisami o ochronie danych.

140. **W świetle powyższego oraz biorąc pod uwagę potencjalne ryzyko dla osób, których dane dotyczą, związane z przetwarzaniem danych osobowych, które może być podjęte przez dostawców usług udostępniania danych, EROD i EIOD uważają, że deklaratywny system zgłaszania dostawców określony we wniosku nie przewiduje wystarczająco rygorystycznej procedury weryfikacji mającej zastosowanie do takich usług. EROD i EIOD zalecają zbadanie alternatywnych procedur, które powinny w szczególności uwzględniać bardziej systematyczne włączanie narzędzi rozliczalności i zgodności w odniesieniu do przetwarzania danych osobowych zgodnie z RODO, w szczególności przestrzegania kodeksu postępowania lub mechanizmu certyfikacji.**

141. Można również zauważyć, że zabezpieczenia przewidziane w rozdziale IV wniosku w odniesieniu do organizacji o altruistycznym podejściu do danych (art. 18 – „Wymagania dotyczące przejrzystości"; art. 19 – „Szczególne wymogi") nie są przewidziane we wniosku w odniesieniu do dostawców usług udostępniania danych, pomimo możliwego wpływu tych usług udostępniania danych na prawa i wolności zainteresowanych osób.

142. Ta różnica między dwoma systemami zgłaszania może prowadzić do interpretacji *a contrario*, zgodnie z którą wymogi ustanowione dla organizacji o altruistycznym podejściu do danych i odnoszące się do ochrony danych osobowych w zakresie, w jakim dane osobowe są przetwarzane (np. informowanie posiadaczy danych o każdym przetwarzaniu poza Unią[70]), nie mają zastosowania do dostawców usług udostępniania danych.

143. **W tym względzie EROD i EIOD zauważają w szczególności, że organizacje zaangażowane w rozwiązania dotyczące „łączenia danych" lub udostępniania danych powinny przestrzegać**

---

administratora oraz inspektora ochrony danych; b) cele przetwarzania; c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych; d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych; e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń; f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych; g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1. [...]".

[69] Ocena skutków towarzysząca wnioskowi odnosi się do przyznawania znaku jakości lub certyfikacji, m.in. na stronie 19: „Wzajemne uznawanie mechanizmów certyfikacji/przyznawania znaku jakości oraz systemu zaufania dla altruistycznego podejścia do danych umożliwi gromadzenie i wykorzystywanie danych na niezbędną skalę"; na stronie 25: „ramy certyfikacji/przyznawania znaku jakości pośrednikom w zakresie danych"; na stronie 26: „ramy certyfikacji lub przyznawania znaku jakości pozwoliłyby nowym pośrednikom w zakresie danych zwiększyć swoją widoczność jako godnych zaufania organizatorów/instruktorów udostępniania lub łączenia danych".

[70] Art. 19 ust. 1 lit. b) wniosku.

pewnych wspólnych norm, w odniesieniu do których nadzór przez niezależne organy ochrony danych jest wyraźnie przywoływany we wniosku, związanych nie tylko z warunkami interoperacyjności, ale również z warunkami zapewnienia zgodności z prawem przetwarzania danych osobowych i ułatwienia wykonywania praw osób, których dane dotyczą (np. poprzez rozwiązania dotyczące współadministratorów na podstawie art. 26 RODO).

144. Ponadto EROD i EIOD zauważają, że wniosek odnosi się do scenariuszy (wykorzystanie metadanych do rozwoju usługi udostępniania danych na podstawie art. 11 ust. 2; ciągły dostęp posiadaczy i użytkowników danych do danych przechowywanych przez dostawcę usług udostępniania danych po ogłoszeniu przez niego niewypłacalności na podstawie art. 11 ust. 6), które wymagają doprecyzowania w celu dostosowania ich do przepisów i zasad dotyczących ochrony danych osobowych.

145. EROD i EIOD zauważają również, że uwagi poczynione w ramach uwag ogólnych zawartych w niniejszej opinii dotyczące definicji stosowanych we wniosku oraz kwestii podstawy prawnej przetwarzania danych osobowych na podstawie RODO są również istotne w odniesieniu do przepisów rozdziału III wniosku.

146. Ponadto, w szczególności w odniesieniu do celu, jakim jest zapewnienie lepszej kontroli nad dostępem i wykorzystaniem danych osobowych przez osobę, której dane dotyczą, należy przypomnieć, że zasada ograniczenia celu ma szczególne znaczenie w odniesieniu do pośredników w zakresie danych między przedsiębiorstwami. Motyw 26 wniosku[71], który wydaje się utożsamiać cel przetwarzania danych osobowych z pośrednictwem w udostępnianiu danych, bez dalszego doprecyzowania może budzić obawy z punktu widzenia ochrony danych[72].

147. EROD i EIOD są zdania, że uwagi poczynione w sekcji 3.3 niniejszej Wspólnej Opinii dotyczące ponownego wykorzystywania danych osobowych będących w posiadaniu organów sektora publicznego są również istotne w odniesieniu do usług udostępniania danych:

– wszelkie udostępnianie danych osobowych lub dostęp do nich musi mieć ściśle określony zakres i cel oraz musi odbywać się w pełnej zgodności z RODO, z uwzględnieniem wymogów zgodności z prawem, ograniczenia celu i uzasadnionych oczekiwań osób, których dane dotyczą;

– powinno być jasne, że każdy „podmiot" łańcucha przetwarzania danych, w tym dostawca usług udostępniania danych i użytkownik (użytkownicy), przekazuje osobom, których dane dotyczą, informacje na podstawie art. 13 i 14 RODO (często odpowiednim przepisem RODO w tym kontekście będzie art. 14, mający zastosowanie w przypadku, gdy osoba, której dane dotyczą, nie uzyskała danych osobowych). Zaleca się dodanie w tym względzie, że dostawca usług udostępniania danych zapewnia

[71] Motyw 26 wniosku: „Kluczowym elementem zapewniającym zaufanie i lepszą kontrolę posiadaczom danych i użytkownikom danych w odniesieniu do usług udostępniania danych jest neutralność dostawców takich usług względem danych udostępnianych między posiadaczami danych a użytkownikami danych. Dlatego koniecznie jest, aby dostawcy usług udostępniania danych **działali jedynie jako pośrednicy** w transakcjach i nie wykorzystywali udostępnianych danych do **żadnych innych celów** [...]".

[72] Zob. także art. 2 pkt 4 wniosku: „»metadane« oznaczają dane gromadzone na temat wszelkiej działalności osoby fizycznej lub prawnej **w celu świadczenia usługi udostępniania danych"**; art. 2 pkt 7: „»udostępnianie danych« oznacza udostępnianie danych przez posiadacza danych podmiotowi wykorzystującemu dane, **w celu wspólnego lub indywidualnego wykorzystania udostępnianych danych**"; art. 11 ust. 1: „Dostawca usług nie może wykorzystywać danych, w odniesieniu do których świadczy usługi, **do celów innych niż oddanie ich do dyspozycji użytkownikom danych**".

osobie, której dane dotyczą, łatwe w obsłudze narzędzia dające jej pełny obraz tego, w jaki sposób jej dane osobowe są udostępniane, jak również łatwe w obsłudze narzędzie do wycofania zgody w przypadku, gdy świadczona usługa obejmuje narzędzie do uzyskiwania zgody od osób, których dane dotyczą, w odniesieniu do przetwarzania ich danych osobowych na podstawie art. 11 ust. 11 wniosku;

– ocena skutków dla ochrony danych stanowi kluczowe narzędzie zapewniające właściwe uwzględnienie wymogów w zakresie ochrony danych oraz odpowiednią ochronę praw i interesów osób fizycznych, tak aby zwiększyć ich zaufanie do mechanizmu ponownego wykorzystywania. W związku z tym EROD i EIOD zalecają włączenie do tekstu wniosku zapisu mówiącego, że **dostawcy usług udostępniania danych (i użytkownik danych) muszą przeprowadzić ocenę skutków dla ochrony danych w przypadku przetwarzania danych objętego zakresem art. 35 RODO**. Udostępnianie danych przewidziane we wniosku może wiązać się z przetwarzaniem na dużą skalę, w ramach którego łączone są dane z różnych źródeł, potencjalnie obejmując szczególne kategorie danych lub dane osobowe wymagających szczególnej opieki grup osób, których dane dotyczą. W takim przypadku administratorzy mają obowiązek przeprowadzenia oceny skutków dla ochrony danych zgodnie z art. 35 RODO. Ponadto, gdy tylko jest to możliwe, dostawca usług udostępniania danych oraz użytkownik (użytkownicy) podają do wiadomości publicznej wyniki takich ocen jako środek zwiększający zaufanie i przejrzystość.

3.4.4 Art. 12 i 13: właściwe organy i monitorowanie przestrzegania przepisów (określonych w art. 10 i 11)

148. Art. 12 ust. 3 wniosku stanowi, że „[w]yznaczone właściwe organy, organy ochrony danych, krajowe organy ochrony konkurencji, organy odpowiedzialne za cyberbezpieczeństwo oraz inne odpowiednie organy sektorowe wymieniają się informacjami, które są niezbędne do wykonywania ich zadań w odniesieniu do dostawców usług udostępniania danych”.

149. Sformułowanie to przewiduje jeszcze mniejszą rolę organów ochrony danych niż sformułowanie użyte we wniosku w odniesieniu do organizacji o altruistycznym podejściu do danych[73], które odnosi się do „współpracy z organami ochrony danych”.

[73] Art. 20 ust. 3: „Właściwy organ wykonuje swoje zadania [organu odpowiedzialnego za rejestr uznanych **organizacji o altruistycznym podejściu do danych** oraz za monitorowanie zgodności z wymogami określonymi w rozdziale IV wniosku] **we współpracy z organem ochrony danych**, jeżeli zadania te związane są z przetwarzaniem danych osobowych, oraz z odpowiednimi organami sektorowymi tego samego państwa członkowskiego. W przypadku wszelkich **kwestii wymagających oceny zgodności z rozporządzeniem (UE) 2016/679** właściwy organ w pierwszej kolejności zwraca się o opinię lub decyzję do właściwego organu nadzoru ustanowionego na mocy tego rozporządzenia i stosuje się do tej opinii lub decyzji”.
Należy również zauważyć, że w motywie 28 – w odniesieniu do **dostawców usług udostępniania danych** – określono, że przedmiotowe „rozporządzenie powinno **pozostawać bez uszczerbku dla** obowiązku przestrzegania przez dostawców usług udostępniania danych rozporządzenia (UE) 2016/679 oraz **odpowiedzialności organów nadzorczych za zapewnienie zgodności z tym rozporządzeniem**”. Takiego samego doprecyzowania **nie** wprowadzono w odniesieniu do organizacji o altruistycznym podejściu do danych.

150. W tym względzie, jak podkreślono w sekcji 3.7 niniejszej Wspólnej Opinii, EROD i EIOD przypominają, że wiele przepisów tego rozdziału, jak również pozostałych rozdziałów wniosku, odnosi się do przetwarzania danych osobowych oraz że organy ochrony danych są organami „konstytucyjnie" właściwymi do sprawowania nadzoru związanego z ochroną danych osobowych zgodnie z art. 8 Karty Praw Podstawowych UE i art. 16 TFUE.

151. Uwzględniając art. 13 wniosku – „Monitorowanie przestrzegania przepisów" – niezależnie od motywu 28, który stanowi, że „wniosek powinien pozostawać bez uszczerbku dla odpowiedzialności organów nadzorczych za zapewnienie zgodności z RODO", EROD i EIOD uważają, że zarządzanie zgodnością i jej monitorowanie powinny być lepiej zdefiniowane, aby zapewnić bardziej odpowiednią weryfikację dostawców usług udostępniania danych (i organizacji o altruistycznym podejściu do danych), w tym pod kątem zgodności z RODO; oraz aby uniknąć jednocześnie nakładania się lub konfliktu kompetencji między organami ustanowionymi na podstawie wniosku (które, zgodnie z brzmieniem art. 12 ust. 3 i art. 20 ust. 3, nie są organami ochrony danych) a organami ochrony danych.

152. **EROD i EIOD uważają zatem, że taką lepszą definicję zarządzania zapewniłoby wyznaczenie organów ochrony danych jako głównych właściwych organów do monitorowania i nadzorowania zgodności z przepisami rozdziału III wniosku.**

153. Wyznaczenie organów ochrony danych jako głównych organów właściwych do nadzoru i egzekwowania przepisów na podstawie rozdziału III wniosku zapewniłoby również bardziej spójne podejście regulacyjne w państwach członkowskich, a tym samym przyczyniłoby się do spójnego stosowania wniosku. Jeśli chodzi o ich kompetencje i zadania wynikające z przepisów RODO, organy ochrony danych posiadają już konkretną wiedzę specjalistyczną w zakresie monitorowania zgodności przetwarzania danych, audytu konkretnych czynności przetwarzania danych i udostępniania danych, oceny odpowiednich środków zapewniających wysoki poziom bezpieczeństwa przechowywania i przekazywania danych osobowych, a także zwiększania świadomości administratorów i podmiotów przetwarzających w kwestii ich obowiązków związanych z przetwarzaniem danych osobowych.

154. Wyznaczenie organów ochrony danych jako głównego organu właściwego do nadzoru i egzekwowania przepisów na podstawie rozdziału III jest poparte przewidzianym w art. 12 ust. 3 przepisem umożliwiającym wymianę informacji między organami ochrony danych, krajowymi organami ochrony konkurencji, organami odpowiedzialnymi za cyberbezpieczeństwo i innymi odpowiednimi organami sektorowymi w celu zapewnienia spójnego stosowania tych przepisów.

155. Ponadto EROD i EIOD uważają, że podczas monitorowania zgodności uprawnienie właściwych organów nie może ograniczać się do „uprawnienia do żądania informacji", jak wynika z art. 13 ust. 2 wniosku. Ograniczenie to zdecydowanie wynika z deklaratywnego charakteru „systemu przyznawania znaku jakości" przewidzianego we wniosku, aczkolwiek nie jest ono adekwatne do poziomu weryfikacji, jaki jest wymagany w przypadku przyznawania znaku jakości, ze względu na wysokie oczekiwania co do zgodności z ochroną danych wynikające z takiego przyznawania znaku jakości, zwłaszcza w stosunku do osób, których dane dotyczą.

156. Ponadto EROD i EIOD podkreślają, że należy zapewnić organom ochrony danych odpowiednie zasoby, aby umożliwić im skuteczne i efektywne sprawowanie niezbędnego nadzoru.

3.5 Altruistyczne podejście do danych

3.5.1 Wzajemna zależność między altruistycznym podejściem do danych a zgodą w rozumieniu RODO

157. Pojęcie „altruistyczne podejście do danych", o którym mowa we wniosku, obejmuje sytuacje, w których osoby fizyczne lub prawne dobrowolnie udostępniają dane do ponownego wykorzystania, bez żądania wynagrodzenia, do „celów realizowanych w interesie ogólnym, takich jak cele badań naukowych lub poprawa jakości usług publicznych"[74].

158. Można argumentować, że wniosek nie „tworzy", lecz „formalizuje/kodyfikuje" możliwość dobrowolnego udostępniania danych przez posiadaczy danych (zdefiniowanych we wniosku jako m.in. osoby, których dane dotyczą), przewidzianą już w RODO. Osoba, której dane dotyczą, może już bowiem wyrazić zgodę na przetwarzanie dotyczących jej danych osobowych m.in. do celów badań naukowych.

159. Pomimo definicji zawartej w art. 2 pkt 10 wniosku („»altruistyczne podejście do danych« oznacza zgodę udzielaną przez osoby, których dane dotyczą, na przetwarzanie dotyczących ich danych osobowych lub zezwolenia innych posiadaczy danych na wykorzystywanie ich danych nieosobowych bez żądania wynagrodzenia, do celów realizowanych w interesie ogólnym, takich jak cele badań naukowych lub poprawa jakości usług publicznych") pojęcie „altruistyczne podejście do danych" nadal nie jest jasno i wystarczająco zdefiniowane. W szczególności nie jest jasne, czy zgoda przewidziana we wniosku odpowiada pojęciu „zgody" w rozumieniu RODO, w tym warunkom zgodności z prawem takiej zgody. Co więcej, nie jest jasne, jaka jest wartość dodana „altruistycznego podejścia do danych", biorąc pod uwagę już istniejące ramy prawne w zakresie zgody w rozumieniu RODO, które przewidują szczegółowe warunki ważności zgody.

160. RODO i wniosek są równolegle stosowane w przypadku przetwarzania danych osobowych przez organizacje o altruistycznym podejściu do danych. EROD i EIOD popierają cel polegający na ułatwieniu przetwarzania danych osobowych w dobrze zdefiniowanych celach realizowanych w interesie ogólnym, przy czym cel ten należy nadal realizować w pełnej zgodności z mającymi zastosowanie przepisami i zasadami dotyczącymi ochrony danych. W szczególności EROD i EIOD podkreślają, że jednym z głównych celów RODO jest zapewnienie, aby osoba, której dane dotyczą, zachowała kontrolę nad swoimi danymi osobowymi. W tym kontekście EROD i EIOD podkreślają, że **należy spełnić wszystkie wymogi związane ze zgodą, określone w RODO**.

161. EROD i EIOD ponownie podkreślają, że **podstawowe prawo do ochrony danych osobowych nie może w żadnym przypadku zostać „uchylone" przez osobę, której dane dotyczą**, nawet w drodze „aktu altruizmu" związanego z danymi osobowymi. Administrator (organizacja o altruistycznym podejściu do danych) pozostaje w pełni związany przepisami i zasadami dotyczącymi ochrony danych osobowych, nawet jeżeli osoba, której dane dotyczą, udzieliła organizacji o altruistycznym podejściu do danych zgody na przetwarzanie dotyczących jej danych osobowych w jednym lub większej liczbie określonych celów.

[74] Art. 2 pkt 10 wniosku.

162. **W świetle powyższego we wniosku należy sprecyzować w części merytorycznej, że odnosi się on do zgody zdefiniowanej w art. 4 pkt 11 RODO oraz że zgodnie z art. 7 ust. 3 organizacja o altruistycznym podejściu do danych zapewnia, aby wycofanie zgody było równie łatwe jak jej wyrażenie[75].**

163. EROD i EIOD podkreślają również fakt, że dane przetwarzane przez organizacje o altruistycznym podejściu do danych mogą obejmować szczególne kategorie danych osobowych, np. dane dotyczące zdrowia.

164. Co więcej, EROD i EIOD podkreślają, że zgodnie z zasadą minimalizacji danych, jeżeli jest to możliwe i adekwatne do celu, dane powinny być przetwarzane w formie zanonimizowanej.

165. EROD i EIOD z zadowoleniem przyjmują fakt, że w art. 22 ust. 3 wniosku określono, iż w przypadku gdy dane osobowe są przekazywane organizacji o altruistycznym podejściu do danych, formularz zgody zapewnia osobom fizycznym możliwość udzielenia i wycofania zgody na konkretną operację przetwarzania danych, zgodnie z RODO.

166. W tym względzie EROD i EIOD uważają, że zasady wycofania zgody oraz związane z tym konsekwencje powinny być jasne. Należy w szczególności wyjaśnić, w jaki sposób zarówno organizacja o altruistycznym podejściu do danych, jak i użytkownicy danych stosują się do wniosków o wycofanie, w tym poprzez usunięcie danych osobowych zgodnie z art. 17 ust. 1 lit. b) RODO. EROD i EIOD przypominają, że przy podejmowaniu decyzji dotyczących „altruistycznego podejścia do danych" może zaistnieć konieczność przeprowadzenia przez organizacje o altruistycznym podejściu do danych oceny skutków dla ochrony danych zgodnie z art. 35 RODO.

167. Badania naukowe często wiążą się z przetwarzaniem i udostępnianiem szczególnych kategorii danych osobowych na dużą skalę, a zatem w niektórych przypadkach można je uznać za przetwarzanie danych wysokiego ryzyka zgodnie z RODO. Ponadto oceny skutków dla ochrony danych w tym kontekście powinny być przeprowadzane przy udziale inspektora ochrony danych i rady ds. przeglądu etycznego, a w przypadkach, w których jest to możliwe i stanowi dobrą praktykę, oceny skutków lub ich podsumowanie powinny być podawane do wiadomości publicznej.

168. Zgodnie z RODO zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, której dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego, w tym elektronicznego, lub ustnego oświadczenia.

169. W motywie 33 RODO podkreślono, że w momencie gromadzenia danych często nie da się w pełni zidentyfikować celu przetwarzania danych osobowych na potrzeby badań naukowych. W związku z tym osoby, których dane dotyczą, powinny mieć możliwość wyrażenia zgody na niektóre obszary

---

[75] Zob. EROD, Wytyczne 05/2020 dotyczące zgody, pkt 121–122:
„121. W art. 6 przewidziano warunki zgodnego z prawem przetwarzania danych osobowych i opisano sześć zgodnych z prawem podstaw, na których administrator może się opierać. Zastosowanie jednej z tych sześciu podstaw musi zostać ustalone przed przetwarzaniem i w odniesieniu do określonego celu.
122. W tym miejscu należy wspomnieć, że **jeżeli administrator postanowi opierać się na zgodzie w odniesieniu do dowolnej części przetwarzania, musi być gotowy przestrzegać tego wyboru i zaprzestać danej części przetwarzania, jeżeli dana osoba wycofa zgodę.** Poinformowanie, że dane będą przetwarzane na podstawie zgody, podczas gdy administrator w praktyce opiera się na innej zgodnej z prawem podstawie, byłoby zdecydowanie nieuczciwe względem zainteresowanych osób".

badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych[76]. Znajduje to również odzwierciedlenie w motywie 38 wniosku.

170. EROD i EIOD podkreślają jednak, że udzielanie tego rodzaju zgody do celów interesu ogólnego[77] jako takiego (nieokreślonego ściśle i odnoszącego się do potencjalnie innego i znacznie szerszego zakresu niż badania naukowe) nie jest dozwolone na podstawie RODO.

171. W istocie motyw 35 wniosku odnosi się do „celów interesu ogólnego" i zawiera (nie definicję, ale) niewyczerpujący wykaz przykładów, który obejmuje stosowane i finansowane ze środków prywatnych badania i rozwój technologiczny oraz analizę danych[78].

172. **W świetle powyższego EROD i EIOD uważają, że Komisja powinna lepiej zdefiniować cele leżące w interesie ogólnym takiego „altruistycznego podejścia do danych". EROD i EIOD uważają, że ten brak definicji może prowadzić do braku pewności prawa, a także do obniżenia stopnia ochrony danych osobowych w UE. Na przykład wymóg, aby organizacja o altruistycznym podejściu do danych informowała posiadacza danych (w tym osobę, której dane dotyczą) „o celach interesu ogólnego, do których zezwala na przetwarzanie ich danych przez użytkowników danych", jest zgodny z zasadą, zgodnie z którą dane gromadzi się do określonych, wyraźnych i prawnie uzasadnionych celów i nie powinny być one dalej przetwarzane w sposób niezgodny z tymi celami (zasada ograniczenia celu,**

---

[76] Zob. niedawno przyjęte wytyczne EROD 05/2020 dotyczące zgody, w szczególności w odniesieniu do zgody na badania naukowe, s. 30–32.

[77] Zob. EROD, Wytyczne 03/2020 w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych w kontekście pandemii COVID-19, pkt 42–45:
„42. Na mocy art. 5 ust. 1 lit. b) RODO dane powinny być co do zasady »zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami«.
43. W ramach »domniemania zgodności« art. 5 ust. 1 lit. b) RODO stanowi jednak, że »dalsze przetwarzanie [...] **do celów badań naukowych** [...] nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami«. Ze względu na jego horyzontalny i złożony charakter temat ten zostanie bardziej szczegółowo omówiony w planowanych **wytycznych EROD w sprawie przetwarzania danych dotyczących zdrowia do celów badań naukowych**.
44. Art. 89 ust. 1) RODO stanowi, że przetwarzanie danych do celów naukowych »podlega **odpowiednim zabezpieczeniom**« i że »zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych. Środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele«.
45. Wymogi określone w art. 89 ust. 1 RODO podkreślają znaczenie zasady minimalizacji danych oraz zasady integralności i poufności, jak również zasady uwzględniania ochrony danych w fazie projektowania i zasady domyślnej ochrony danych (zob. poniżej). W związku z tym, biorąc pod uwagę wrażliwy charakter danych dotyczących zdrowia oraz ryzyko związane z ponownym wykorzystywaniem danych dotyczących zdrowia do celów badań naukowych, należy podjąć zdecydowane środki w celu zapewnienia odpowiedniego stopnia bezpieczeństwa zgodnie z wymogami art. 32 ust. 1 RODO".
Zob. także dokument EROD w odpowiedzi na wniosek Komisji Europejskiej o przedstawienie wyjaśnień dotyczących spójnego stosowania RODO, ze szczególnym uwzględnieniem badań w dziedzinie zdrowia, przyjęty w dniu 2 lutego 2021 r.

[78] Motyw 35: „Cele takie obejmują opiekę zdrowotną, przeciwdziałanie zmianie klimatu, poprawę mobilności, ułatwianie tworzenia statystyk publicznych lub poprawę świadczenia usług publicznych. Za cele interesu ogólnego należy również uznać wsparcie badań naukowych, obejmujące na przykład rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych. Niniejsze rozporządzenie ma na celu przyczynienie się do powstania pul danych udostępnianych na podstawie altruistycznego podejścia do danych, mających wielkość wystarczającą do umożliwienia analizy danych i uczenia się maszyn, w tym również w kontekście transgranicznym w Unii".

na podstawie art. 5 lit. b) RODO). W związku z tym we wniosku należy przedstawić wyczerpujący wykaz jasno określonych celów. Jednocześnie EROD i EIOD odnotowują doprecyzowanie zawarte w motywie 38 wniosku[79]. Doprecyzowanie to należy zawrzeć w części merytorycznej wniosku, a nie tylko w motywie, i powinno mu towarzyszyć wyraźne rozróżnienie we wniosku pomiędzy:

– zgodą na niektóre obszary badań naukowych;

– dalszym przetwarzaniem do celów badań naukowych lub historycznych lub do celów statystycznych;

– oraz przetwarzaniem do celów interesu ogólnego (które zostaną określone we wniosku).

173. Ponadto EROD i EIOD zauważają, że występujący w motywie 36 termin „repozytoria danych”[80], o którym mowa tylko w tym motywie, a nie w merytorycznej części wniosku, i który odnosi się do przetwarzania zarówno danych osobowych, jak i nieosobowych, wymaga wyjaśnienia.

3.5.2 Art. 16–17: system rejestracji – ogólne wymogi kwalifikujące do rejestracji – treść rejestracji; wynik (i termin) rejestracji

174. W rozdziale IV wniosku przewidziano możliwość rejestrowania się organizacji o „altruistycznym podejściu do danych” jako „uznana w Unii organizacja o altruistycznym podejściu do danych”[81], ze zdeklarowanym celem zwiększenia zaufania obywateli do ich działalności. W tym względzie EROD i EIOD podkreślają, że we wniosku nie sprecyzowano, czy rejestracja jest obowiązkowa czy nie, ani czy przepisy rozdziału IV mają zastosowanie również w przypadku, gdy organizacje o altruistycznym podejściu do danych nie są zarejestrowane.

175. Wymogi ogólne dotyczące rejestracji wymieniono w art. 16; wymogi dotyczące rejestracji określono w art. 17, a w szczególności w art. 17 ust. 4 lit. a)–i). „Weryfikacja” organizacji o altruistycznym podejściu do danych ogranicza się wyłącznie do sprawdzenia przez właściwy organ wymogów określonych w art. 16 i art. 17 ust. 4 i następuje w ciągu dwunastu tygodni od daty złożenia wniosku. We wniosku nie określono jednak, jakiego rodzaju weryfikację powierzono właściwemu organowi.

---

[79] Motyw 38: „Uznane w Unii organizacje o altruistycznym podejściu do danych **powinny mieć możliwość gromadzenia odpowiednich danych bezpośrednio od osób fizycznych i prawnych lub przetwarzania danych zgromadzonych przez inne osoby**.
Zazwyczaj altruistyczne podejście do danych opiera się na zgodzie osób, których dane dotyczą, w rozumieniu art. 6 ust. 1 lit. a) i art. 9 ust. 2 lit. a), wyrażonej zgodnie z wymogami dotyczącymi zgody zgodnej z prawem, określonymi w art. 7 rozporządzenia (UE) 2016/679.
Zgodnie z rozporządzeniem (UE) 2016/679 **cele badań naukowych** można uzasadnić zgodą na **niektóre obszary badań naukowych**, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych, lub tylko na niektóre obszary badań lub elementy projektów badawczych.
Art. 5 ust. 1 lit. b) rozporządzenia (UE) 2016/679 stanowi, że **dalsze przetwarzanie do celów badań naukowych lub historycznych lub do celów statystycznych** nie powinno być uznawane w myśl art. 89 ust. 1 rozporządzenia (UE) 2016/679 za niezgodne z pierwotnymi celami”.

[80] Motyw 36: „Podmioty prawne, które starają się wspierać realizację **celów interesu ogólnego** poprzez udostępnianie na dużą skalę odpowiednich danych w oparciu o altruistyczne podejście do danych i które spełniają określone wymogi, powinny mieć możliwość zarejestrowania się jako »uznana w Unii organizacja o altruistycznym podejściu do danych«. Może to doprowadzić do powstania **repozytoriów danych** [...]”.

[81] Motyw 36 wniosku.

176. W tym względzie EROD i EIOD zauważają, że system przewidujący solidniejsze gwarancje w przypadku przetwarzania danych osobowych byłby bardziej odpowiedni do zapewnienia odpowiednich kontroli i ostatecznie zwiększenia zaufania niż „lżejszy" system rejestracji (system niemal zwyczajnie „deklaratywny") określony we wniosku i podobny do systemu przewidzianego dla dostawców usług udostępniania danych.

177. EROD i EIOD podkreślają, że fakt, iż z prawnego, technicznego i organizacyjnego punktu widzenia nie ma prawie żadnych wymogów, które należy spełnić, aby stać się „uznaną w Unii organizacją o altruistycznym podejściu do danych" (lub „dostawcą usługi udostępniania danych") jest problematyczny. Na przykład organizacja uprawniona na podstawie art. 15 ust. 3 wniosku do tego, aby „w swoich pisemnych i ustnych komunikatach określać się mianem »uznanej w Unii organizacji o altruistycznym podejściu do danych«" („efekt przyznawania znaku jakości"), będzie najprawdopodobniej gromadzić dane osobowe, wykorzystując oczekiwania obywateli, w szczególności co do pełnej zgodności z zasadami ochrony danych przez tę samą organizację.

178. EROD i EIOD podkreślają, że organizacje o altruistycznym podejściu do danych muszą być podmiotami godnymi zaufania. Jeżeli chodzi o wymogi ogólne dotyczące rejestracji (przewidziane w art. 16 wniosku), EROD i EIOD uważają również, że należy wyjaśnić niezależność organizacji o altruistycznym podejściu do danych od podmiotów nastawionych na zysk (np. prawną, organizacyjną, ekonomiczną) przewidzianą w art. 16 lit. b) wniosku[82].

179. **W szczególności EROD i EIOD zalecają wprowadzenie bezpośredniego odniesienia do wymogów dotyczących ochrony danych w art. 16, zwłaszcza do wymogów technicznych i organizacyjnych umożliwiających stosowanie standardów ochrony danych i wykonywanie praw osób, których dane dotyczą.**

180. **W świetle powyższych elementów oraz biorąc pod uwagę potencjalne skutki dla osób, których dane dotyczą, związane z przetwarzaniem danych osobowych, które może podjąć organizacja o altruistycznym podejściu do danych, EROD i EIOD uważają, że w systemie rejestracji ustanowionym we wniosku nie przewidziano wystarczająco rygorystycznej procedury weryfikacji mającej zastosowanie do takiej organizacji. EROD i EIOD zalecają zbadanie alternatywnych procedur, które powinny w szczególności uwzględniać bardziej systematyczne włączanie narzędzi rozliczalności i zgodności w odniesieniu do przetwarzania danych osobowych zgodnie z RODO, w szczególności przestrzegania kodeksu postępowania lub mechanizmu certyfikacji.**

[82] „Aby kwalifikować się do rejestracji, organizacja o altruistycznym podejściu do danych musi: [...] b) prowadzić działalność o charakterze niekomercyjnym i **być niezależna od jakiegokolwiek podmiotu nastawionego na zysk**" (pogrubienie dodano).

3.5.3 Art. 18–19: wymogi dotyczące przejrzystości oraz „szczególne wymogi dotyczące ochrony praw i interesów osób, których dane dotyczą, oraz podmiotów prawnych w odniesieniu do ich danych”

181. EROD i EIOD zauważają, że wymogi towarzyszące systemowi rejestracji powinny służyć wzmocnieniu, a **nie zastępować obowiązki organizacji o altruistycznym podejściu do danych jako administratorów lub podmiotów przetwarzających na podstawie RODO**.

182. EROD i EIOD zauważają, że motyw 36 wniosku jest niejasny w tym względzie, ponieważ wydaje się sugerować, że środki do celów wycofania zgody powinna zapewnić organizacja o altruistycznym podejściu do danych działająca jako podmiot przetwarzający [83]. Kwalifikacja organizacji o altruistycznym podejściu do danych jako podmiotu przetwarzającego, a nie administratora, wymaga jednak dalszej oceny, ponieważ nie wydaje się, aby był to jedyny możliwy scenariusz w kontekście wniosku.

183. Należy również jasno określić zezwalający skutek rejestracji (jako organizacji o altruistycznym podejściu do danych), w szczególności w odniesieniu do aspektu podstawy prawnej przetwarzania danych osobowych zgodnie z RODO[84]. W tym względzie EROD i EIOD podkreślają, że **system rejestracji nie może zastąpić konieczności posiadania odpowiedniej podstawy prawnej w odniesieniu do przetwarzania danych osobowych na podstawie art. 6 ust. 1 RODO,** aby przetwarzanie danych było zgodne z prawem. Innymi słowy, zgodnie z RODO przetwarzanie danych osobowych jest zgodne z prawem wyłącznie wówczas, gdy – i w zakresie, w jakim – ma zastosowanie co najmniej jedna podstawa prawna na podstawie art. 6 ust. 1 RODO.

184. Uwzględniając art. 18 wniosku, EROD i EIOD mają wątpliwości co do zachowania niezależności przez organizację o altruistycznym podejściu do danych w przypadkach, w których jej finansowanie opiera się na „opłatach wniesionych przez osoby fizyczne lub prawne przetwarzające dane” [85] (tj. dane przekazane tym osobom fizycznym lub prawnym przez organizację o altruistycznym podejściu do danych). Ponadto EROD i EIOD uważają, że we wniosku należałoby lepiej wyjaśnić, w jakich sytuacjach

---

[83] Motyw 36 stanowi: „**Dalsze zabezpieczenia** powinny obejmować umożliwienie **przetwarzania odpowiednich danych w bezpiecznym środowisku przetwarzania** prowadzonym przez zarejestrowany podmiot, **mechanizmy nadzoru**, takie jak rady lub zarządy ds. etyki, mające zapewnić utrzymywanie przez administratora danych wysokich standardów etyki naukowej, **skuteczne środki techniczne umożliwiające wycofanie lub zmianę zgody** w dowolnym momencie, **w oparciu o obowiązki informacyjne podmiotów przetwarzających dane na podstawie rozporządzenia (UE) 2016/679**, a także **środki służące stałemu informowaniu osób**, których dane dotyczą, o wykorzystywaniu udostępnionych przez nie danych” (pogrubienie dodano).

[84] W tym względzie motyw 38 wniosku stanowi, co następuje (pogrubienie dodano): „Uznane w Unii organizacje o altruistycznym podejściu do danych **powinny mieć możliwość gromadzenia odpowiednich danych bezpośrednio od osób fizycznych i prawnych** lub przetwarzania danych zgromadzonych przez inne osoby. **Zazwyczaj** altruistyczne podejście do danych opiera się na zgodzie osób, których dane dotyczą, w rozumieniu art. 6 ust. 1 lit. a) i art. 9 ust. 2 lit. a), wyrażonej zgodnie z wymogami dotyczącymi zgody zgodnej z prawem, określonymi w art. 7 rozporządzenia (UE) 2016/679. Zgodnie z rozporządzeniem (UE) 2016/679 cele badań naukowych można uzasadnić zgodą na niektóre obszary badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych, lub tylko na niektóre obszary badań lub elementy projektów badawczych. Art. 5 ust. 1 lit. b) rozporządzenia (UE) 2016/679 stanowi, że dalsze przetwarzanie do celów badań naukowych lub historycznych lub do celów statystycznych nie powinno być uznawane w myśl art. 89 ust. 1 rozporządzenia (UE) 2016/679 za niezgodne z pierwotnymi celami”.

[85] Zob. art. 18 ust. 1 lit. d) wniosku.

organizacja o altruistycznym podejściu do danych może pobierać opłaty od osób fizycznych lub prawnych za przetwarzanie danych „powierzonych" przez osoby, których dane dotyczą, w ramach „altruistycznego podejścia do danych".

185. Również w tym przypadku, jak zauważono w odniesieniu do ponownego wykorzystywania danych będących w posiadaniu organów sektora publicznego, istnieje problem związany z zachętami dla administratora do przetwarzania danych osobowych w większej ilości, w tym przypadku do intensywniejszego stosowania „altruistycznego podejścia do danych". Zakwalifikowanie organizacji o altruistycznym podejściu do danych jako zarejestrowanych podmiotów prowadzących działalność o charakterze niekomercyjnym (motyw 36) – co EROD i EIOD przyjmują z zadowoleniem – tylko częściowo rozwiązuje wyżej wspomniany problem.

186. Ponadto sformułowanie w motywie 36 w odniesieniu do wymogów dotyczących organizacji o altruistycznym podejściu do danych budzi zastrzeżenia, ponieważ odnosi się do „dobrowolnego spełniania wymogów" również względem kwestii związanych z (obowiązkowym) przestrzeganiem RODO[86].

187. Motyw ten jest również niespójny (chyba że podkreśli się fakultatywny charakter wymogów określonych w motywie 36) z częścią merytoryczną wniosku, mianowicie z art. 17 ust. 3, w którym odniesiono się do organizacji o altruistycznym podejściu do danych, które nie mają jednostki organizacyjnej w Unii.

188. **Jeżeli chodzi o art. 19 wniosku, EROD i EIOD są zdania, że należy dodać wyraźne odniesienie do art. 13 i 14 RODO, aby zapewnić spójność między tym artykułem wniosku a obowiązkami dotyczącymi zasady przejrzystości określonymi w RODO, oraz aby organizacja o altruistycznym podejściu do danych i użytkownicy danych dostarczali osobie, której dane dotyczą, niezbędnych informacji na temat przetwarzania dotyczących jej danych osobowych**.

189. Ponadto EROD i EIOD uważają, że obecne brzmienie art. 19 ust. 1 lit. a)[87] wydaje się niejasne i trudne do pogodzenia z przepisami RODO.

190. **Jeżeli chodzi o ten rozdział wniosku, wyraźny nacisk na dostarczanie danych zanonimizowanych, gdy jest to możliwe i właściwe do celu przetwarzania danych, zgodnie z zasadą minimalizacji danych,**

---

[86] Motyw 36 stanowi (pogrubienie dodano): „[...] **Dobrowolne spełnianie** przez takie zarejestrowane podmioty **szeregu wymogów** powinno budzić zaufanie, że dane udostępniane w celach altruistycznych służą celom interesu ogólnego. **Zaufanie** takie powinno wynikać w szczególności z **miejsca prowadzenia działalności w Unii**, a także z wymogu, aby zarejestrowane podmioty **prowadziły działalność o charakterze niekomercyjnym**, z wymogów dotyczących **przejrzystości** oraz z istnienia określonych **zabezpieczeń** służących ochronie praw i interesów **osób, których dane dotyczą, oraz przedsiębiorstw**. **Dalsze zabezpieczenia** powinny obejmować umożliwienie przetwarzania odpowiednich danych w **bezpiecznym środowisku przetwarzania** prowadzonym przez zarejestrowany podmiot, **mechanizmy nadzoru**, takie jak rady lub zarządy ds. etyki, mające zapewnić utrzymywanie przez administratora danych wysokich standardów etyki naukowej, skuteczne **środki techniczne umożliwiające wycofanie lub zmianę zgody** w dowolnym momencie, w oparciu o obowiązki informacyjne podmiotów przetwarzających dane na podstawie rozporządzenia (UE) 2016/679, a także środki służące **stałemu informowaniu** osób, których dane dotyczą, o wykorzystywaniu udostępnionych przez nie danych".

[87] Art. 19 ust. 1 lit. a) stanowi (pogrubienie dodano): „Każdy podmiot wpisany do rejestru uznanych organizacji o altruistycznym podejściu do danych informuje posiadaczy danych: a) **o celach interesu ogólnego, do których zezwala na przetwarzanie ich danych przez użytkowników danych**, w sposób łatwy do zrozumienia".

miałby również szczególne znaczenie dla ochrony zainteresowanych osób przed nadmiernym ryzykiem dla ich podstawowych praw i wolności, zwłaszcza w przypadku przetwarzania szczególnych kategorii danych.

3.5.4 Art. 20 i 21: właściwe organy odpowiedzialne za rejestrację oraz monitorowanie przestrzegania przepisów

191. **Jeżeli chodzi o art. 20 ust. 3 wniosku, EROD i EIOD uważają, że należy usprawnić zarządzanie zgodnością i jej monitorowanie w celu zapewnienia lepszej weryfikacji organizacji o altruistycznym podejściu do danych, w tym przestrzegania RODO, oraz zapewnienia, aby nadzór dotyczący przepisów wniosku był jasno określony w sposób, który gwarantuje, że w przypadku danych osobowych wymogi w zakresie ochrony danych będą w pełni przestrzegane i pozostaną w kompetencji organów ochrony danych ustanowionych na mocy RODO.**

192. **Wyznaczenie organów ochrony danych jako głównych organów właściwych do nadzoru i egzekwowania przepisów na podstawie rozdziału IV wniosku zapewniłoby również bardziej spójne podejście regulacyjne w państwach członkowskich, a tym samym przyczyniłoby się do spójnego stosowania wniosku. Jeśli chodzi o ich kompetencje i zadania wynikające z przepisów RODO, organy ochrony danych posiadają już konkretną wiedzę specjalistyczną w zakresie monitorowania zgodności przetwarzania danych, audytu konkretnych czynności przetwarzania danych i udostępniania danych, oceny odpowiednich środków zapewniających wysoki poziom bezpieczeństwa przechowywania i przekazywania danych osobowych, a także zwiększania świadomości administratorów i podmiotów przetwarzających w kwestii ich obowiązków związanych z przetwarzaniem danych osobowych.**

193. Ponadto EROD i EIOD uważają, że podczas monitorowania zgodności uprawnienie właściwych organów nie może ograniczać się do „uprawnienia do żądania informacji", jak wynika z art. 21 ust. 2 wniosku. Ograniczenie to zdecydowanie wynika z deklaratywnego charakteru „systemu przyznawania znaku jakości" przewidzianego we wniosku, aczkolwiek nie jest ono adekwatne do poziomu weryfikacji, jaki jest wymagany w przypadku przyznawania znaku jakości, ze względu na wysokie oczekiwania co do zgodności z ochroną danych wynikające z takiego przyznawania znaku jakości, zwłaszcza w stosunku do osób, których dane dotyczą.

194. EROD i EIOD podkreślają, że należy zapewnić organom ochrony danych odpowiednie zasoby, aby umożliwić im skuteczne i efektywne sprawowanie niezbędnego nadzoru. Ponadto EROD i EIOD zauważają w tym względzie, że w motywie 28, który odnosi się do dostawców usług udostępniania danych, określono, że przedmiotowe „rozporządzenie powinno pozostawać bez uszczerbku dla obowiązku przestrzegania przez dostawców usług udostępniania danych rozporządzenia (UE) 2016/679 oraz odpowiedzialności organów nadzorczych za zapewnienie zgodności z tym rozporządzeniem". Takie samo doprecyzowanie należy wprowadzić w odniesieniu do organizacji o altruistycznym podejściu do danych.

3.5.5 Art. 22: europejski formularz zgody na potrzeby altruistycznego podejścia do danych

195. W art. 22 wniosku upoważniono Komisję do przyjęcia w drodze aktów wykonawczych „europejskiego formularza zgody na potrzeby altruistycznego podejścia do danych” [88]. W tym względzie, jak określono w motywie 41, art. 22 stanowi, że formularz zgody jest ustanawiany w drodze aktu wykonawczego przez Komisję, wspieraną przez Europejską Radę ds. Innowacji w zakresie Danych, w porozumieniu z EROD.

196. **W tym względzie EROD i EIOD uważają, że za pomocą wniosku należy ustanowić bardziej wiążący, lepiej ustrukturyzowany i zinstytucjonalizowany mechanizm niż zwykłe konsultacje z EROD.**

3.6 Międzynarodowe przekazywanie danych: art. 5 ust. 9–13; motywy 17 i 19; art. 30

197. Nawet jeżeli przepisy przewidziane we wniosku dotyczące przekazywania danych do państw trzecich wydają się *a priori* ograniczone wyłącznie do danych nieosobowych, podczas ich stosowania prawdopodobnie pojawią się kwestie spójności prawnej i politycznej z unijnymi ramami prawnymi ochrony danych, w szczególności w przypadku gdy dane osobowe i dane nieosobowe ze zbioru danych są nierozerwalnie powiązane.

198. Chociaż wyłączenie danych osobowych wydaje się intencją Komisji, ograniczenie zakresu przepisów dotyczących przekazywania danych do danych nieosobowych nie zawsze jednak znajduje we wniosku wyraźne odzwierciedlenie. W szczególności art. 5 ust. 9 i art. 5 ust. 10 odnoszące się do przekazywania danych będących w posiadaniu organów sektora publicznego mogą mieć zastosowanie do danych osobowych, jeżeli te dane osobowe są jednocześnie danymi poufnymi lub danymi chronionymi prawami własności intelektualnej[89].

199. **Jednocześnie we wniosku przewidziano przepis (art. 5 ust. 11), który można uznać za bardziej „chroniący” dane nieosobowe niż dane osobowe, ponieważ zgodnie z wnioskiem Komisja mogłaby ostatecznie przyjąć w drodze aktu delegowanego[90] szczegółowe warunki przekazywania danych nieosobowych do niektórych państw trzecich, nawet włącznie z zakazem przekazywania[91].**

200. **Możliwość przyjęcia przez Komisję w drodze aktu wykonawczego [92] „decyzji stwierdzających odpowiedni stopień ochrony”, dotyczących przekazywania danych nieosobowych do danego państwa trzeciego, może również prowadzić do powstania pytań o wzajemne oddziaływanie**

---

[88] Art. 22 ust. 1: „Aby ułatwić gromadzenie danych w oparciu o altruistyczne podejście do danych, Komisja może przyjąć akty wykonawcze w celu opracowania europejskiego formularza zgody na potrzeby altruistycznego podejścia do danych. Formularz umożliwia uzyskiwanie zgody we wszystkich państwach członkowskich w jednolitym formacie. Te akty wykonawcze przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 29 ust. 2”.

[89] Zob. art. 5 ust. 10 wniosku: „Organy sektora publicznego przekazują dane poufne lub dane chronione prawami własności intelektualnej do podmiotu ponownie wykorzystującego dane, który zamierza przekazać te dane do państwa trzeciego innego niż państwo wyznaczone zgodnie z ust. 9, jeżeli podmiot ponownie wykorzystujący dane zobowiązuje się do: a) wypełniania obowiązków nałożonych zgodnie z ust. 7–8 nawet po przekazaniu danych do państwa trzeciego; oraz b) uznania jurysdykcji sądów państwa członkowskiego organu sektora publicznego w odniesieniu do wszelkich sporów związanych z wypełnieniem obowiązku określonego w lit. a)”.

[90] Zob. motyw 19 wniosku.

[91] Zob. motyw 19 wniosku.

[92] Zob. art. 5 ust. 9–11 wniosku.

i spójność z narzędziami przekazywania danych przewidzianymi w RODO w odniesieniu do przekazywania danych osobowych do tego samego państwa trzeciego.

201. **W każdym razie, aby zapewnić spójność z ramami prawnymi ochrony danych, należy przypomnieć w tym względzie, że w przypadku „mieszanych zbiorów danych" zastosowanie ma RODO, a w szczególności jego rozdział V.**

202. EROD i EIOD zwracają uwagę, że art. 30 wniosku[93] odnosi się wyłącznie do danych nieosobowych, a ust. 2 tego artykułu wydaje się odzwierciedlać przepisy art. 48 RODO (z tą różnicą, że w art. 30 ust. 2 wprowadzono ograniczenie czasowe w odniesieniu do przedmiotowych umów międzynarodowych).

203. Zgodnie z art. 30 ust. 3 wniosku podmioty (organ sektora publicznego, podmiot, któremu przyznano prawo do ponownego wykorzystywania danych, dostawca usług udostępniania danych, organizacja o altruistycznym podejściu do danych), które otrzymują decyzję wymagającą przekazania danych nieosobowych przechowywanych w Unii lub udzielenia dostępu do takich danych wydaną przez sąd lub organ administracyjny państwa trzeciego, zwracają się o opinię do właściwych organów lub podmiotów zgodnie z wnioskiem w celu ustalenia, czy mające zastosowanie warunki przekazania zostały spełnione (art. 30 ust. 3 ostatnie zdanie).

204. Konsultacja z właściwym organem jest niezbędna, jeżeli zastosowanie się do decyzji sądu lub organu administracyjnego państwa trzeciego „wiązałoby się z ryzykiem narażenia adresata na konflikt z prawem Unii lub z prawem danego państwa członkowskiego" (art. 30 ust. 3)[94].

205. W porównaniu z art. 48 RODO przepis ten wydaje się iść o krok dalej, ponieważ w szczególnych przypadkach wymaga konsultacji z właściwym organem. W tym względzie można zatem zasadniczo uznać, że przepis bardziej „chroni" dane nieosobowe niż dane osobowe, ponieważ w RODO nie przewidziano takiego powiadomienia.

---

[93] Art. 30, „Dostęp międzynarodowy", zamieszczony w rozdziale VIII, „Postanowienia końcowe".

[94] Wspomniane powyżej warunki zawarte w art. 30 ust. 3 wydają się wystarczające, aby **zastąpić warunki określone w ust. 2, a tym samym zastąpić przepisy międzynarodowe, o których mowa w tym ustępie**. Art. 30 ust. 4 stanowi: „Jeżeli spełnione są warunki określone w ust. 2 **lub 3**, **organ sektora publicznego, osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału 2, dostawca usług udostępniania danych lub podmiot wpisany do rejestru uznanych organizacji o altruistycznym podejściu do danych, w zależności od przypadku, dostarcza minimalną ilość danych dozwoloną w odpowiedzi na wniosek**, w oparciu o właściwą interpretację wniosku" (pogrubienie dodano).
Te przepisy wniosku mogą być **niespójne z innymi przepisami prawa Unii lub państw członkowskich, w szczególności dotyczącymi współpracy sądowej w sprawach karnych lub cywilnych**. Znaczenie tego spostrzeżenia dla przepisów dotyczących ochrony danych wynika z faktu, że **w przypadku błędnej interpretacji pojęcia danych nieosobowych istnieje duże ryzyko, że organy sektora publicznego, dostawcy usług udostępniania danych, organizacje o altruistycznym podejściu do danych, podmioty ponownie wykorzystujące dane i użytkownicy danych będą przekazywać dane osobowe do państwa trzeciego zapewniającego tym osobom (znacznie) niższy standard ochrony**.

3.7 Przepisy horyzontalne dotyczące uwarunkowań instytucjonalnych; skargi; grupa ekspertów Europejskiej Rady ds. Innowacji w zakresie Danych; akty delegowane; kary, ocena i przegląd, zmiany w rozporządzeniu w sprawie utworzenia jednolitego portalu cyfrowego, środki przejściowe i wejście w życie

3.7.1 Art. 23: wymogi odnoszące się do właściwych organów

206. W rozdziale V wniosku określono wymogi dotyczące funkcjonowania właściwych organów wyznaczonych do monitorowania i wdrażania ram zgłaszania dostawców usług udostępniania danych oraz podmiotów o altruistycznym podejściu do danych. Z rozdziałów III i IV wniosku wynika, że takie właściwe organy różnią się od organów ochrony danych. W istocie wymogi określone w art. 23 wniosku wskazują na „techniczny" charakter tych organów, które są „prawnie odrębne i funkcjonalnie niezależne od jakiegokolwiek dostawcy usług udostępniania danych lub podmiotu wpisanego do rejestru uznanych organizacji o altruistycznym podejściu do danych".

207. W tym względzie na podstawie rozdziału III rola organów nadzorczych odpowiedzialnych za ochronę danych wydaje się ograniczona do zwykłej wymiany informacji z właściwym organem, a na podstawie rozdziału IV do współpracy z tym organem i wydawania na wniosek właściwego organu opinii lub decyzji w kwestiach wymagających oceny zgodności z RODO. Ponadto we wniosku nie określono, w jaki sposób i w jakim zakresie organy ochrony danych będą współdziałać z takimi właściwymi organami, ani też jakie przewidziano zasoby finansowe i kadrowe, aby umożliwić organom ochrony danych wykonywanie zadań wymaganych w ramach takiego współdziałania.

208. EROD i EIOD zauważają, że wiele przepisów wniosku, nad którymi nadzór powierzono właściwym organom wyznaczonym zgodnie z art. 12 i 20, dotyczy ochrony danych osobowych. Mając to na uwadze, **EROD i EIOD podkreślają, że należy w pełni respektować kompetencje i uprawnienia niezależnych organów nadzorczych, ponieważ powierzono im odpowiedzialność za ochronę podstawowych praw i wolności osób fizycznych w odniesieniu do przetwarzania danych oraz ułatwianie swobodnego przepływu danych osobowych, jak określono w RODO i rozporządzeniu (UE) 2018/1725, zgodnie z art. 16 TFUE i art. 8 Karty Praw Podstawowych UE oraz zgodnie z odpowiednim orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej [95] . W związku z powyższym EROD i EIOD zalecają, aby we wniosku wyraźnie uznano, że w sprawach obejmujących dane osobowe głównymi właściwymi organami odpowiedzialnymi za monitorowanie zgodności z przepisami zawartymi w rozdziałach III i IV wniosku są organy ochrony danych, w razie potrzeby w porozumieniu z innymi odpowiednimi organami sektorowymi. Jak wskazano powyżej, organom**

[95] Zob. m.in. wyrok TSUE z dnia 9 marca 2010 r., Komisja Europejska/Republika Federalna Niemiec, sprawa C-518/07 dostępna pod adresem: https://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=en&jge=&td=%3BALL&jur=C%2CT%2CF&num=C-518%252F07&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pl&avg=&cid=2455752
W wyroku z dnia 9 marca 2010 r. Trybunał uznał, że organy ochrony danych powinny pozostawać poza jakimkolwiek wpływem z zewnątrz, czy to bezpośrednim czy pośrednim. Już samo ryzyko wpływu z zewnątrz wystarczy, aby dojść do wniosku, że organ ochrony danych nie może działać w sposób całkowicie niezależny.

tym należy zapewnić odpowiednie zasoby, aby umożliwić im skuteczne i efektywne sprawowanie niezbędnego nadzoru.

3.7.2 Art. 24: skargi; art. 25: prawo do skutecznego środka zaskarżenia

209. EROD i EIOD zwracają uwagę, że art. 24 stanowi, iż „[o]soby fizyczne i prawne mają prawo do wniesienia skargi do odpowiedniego właściwego organu krajowego przeciwko dostawcy usług udostępniania danych lub podmiotowi wpisanemu do rejestru uznanych organizacji o altruistycznym podejściu do danych", jednak nie określono w nim możliwej treści takiej skargi (tj. jakiego rodzaju naruszenia wniosku może ona dotyczyć). Wydaje się również, że złożenie skargi przeciwko organom sektora publicznego lub podmiotom ponownie wykorzystującym dane, o czym mowa w rozdziale II wniosku, nie jest możliwe zgodnie z art. 24 wniosku i nie przewidziano tego w tym artykule.

210. Ponadto w art. 25 określono prawo każdej pokrzywdzonej osoby fizycznej lub prawnej do skutecznego środka zaskarżenia w odniesieniu do niepodjęcia działań w sprawie skargi złożonej do właściwego organu, a także decyzji właściwych organów, o których mowa w art. 13, 17 i 21 (decyzji dotyczących odpowiednio nadzoru nad usługami udostępniania danych; rejestracji organizacji o altruistycznym podejściu do danych; monitorowania przestrzegania przepisów przez zarejestrowane organizacje o altruistycznym podejściu do danych).

211. EROD i EIOD zauważają, że wspomniane przepisy wniosku dotyczące prawa do wniesienia skargi do odpowiedniego właściwego organu krajowego (art. 24) oraz prawa do skutecznego środka zaskarżenia w odniesieniu do niepodjęcia działań lub decyzji wspomnianego właściwego organu (art. 25) mogą zwiększyć ryzyko powstania niespójnych systemów opartych na RODO i systemów opartych na wniosku, na które to ryzyko zwrócono uwagę w niniejszej opinii. Na przykład skargi związane z usługami pośrednictwa dającymi osobom, których dane dotyczą, możliwość skorzystania z praw przewidzianych w RODO (zob. art. 9 ust. 1 lit. b)) na podstawie wniosku wchodziłyby w zakres kompetencji właściwych organów. Innymi słowy, niespójności oraz nakładanie się „prawa materialnego" nasilałyby się i przekładały na pokrywanie się kompetencji w postępowaniach administracyjnych i sądowych.

212. Z tego powodu **EROD i EIOD wzywają do sformułowania we wniosku jasnej, jednoznacznej i dokładnej definicji zasad materialnych, nadzór nad którymi należy powierzyć właściwym organom**, **oraz definicji mechanizmu monitorowania zapewniającego pełną spójność z RODO**.

3.7.3 Art. 26 i 27: skład i zadania grupy ekspertów Europejskiej Rady ds. Innowacji w zakresie Danych

213. W rozdziale VI wniosku „powołano formalną grupę ekspertów (»Europejska Rada ds. Innowacji w zakresie Danych«), która będzie ułatwiała opracowywanie najlepszych praktyk przez organy państw członkowskich, w szczególności w zakresie przetwarzania wniosków o ponowne wykorzystywanie danych, które są objęte prawami innych osób (na podstawie rozdziału II), zapewnienia spójnej praktyki odnośnie do ram zgłaszania dostawców usług udostępniania danych (na podstawie rozdziału III) oraz altruistycznego podejścia do danych (rozdział IV). Ponadto formalna grupa ekspertów będzie

wspierała Komisję i doradzała jej w zakresie zarządzania normalizacją międzysektorową oraz przygotowywania strategicznych wniosków dotyczących tej normalizacji”[96].

214. EROD i EIOD zauważają, że nowo ustanowionej Europejskiej Radzie ds. Innowacji w zakresie Danych, „w skład której wchodzą przedstawiciele właściwych organów wszystkich państw członkowskich, Europejskiej Rady Ochrony Danych, Komisji, odpowiednich przestrzeni danych oraz inni przedstawiciele właściwych organów w poszczególnych sektorach” (art. 26 ust. 1), powierzone zostaną zadania wymienione w art. 27 lit. a)–e)[97], które również mają znaczenie w odniesieniu do przetwarzania danych osobowych.

215. **EROD i EIOD z zadowoleniem przyjmują włączenie EROD, jako członka Europejskiej Rady ds. Innowacji w zakresie Danych. EROD i EIOD są jednak zdania, że w stopniu, w jakim przepisy odnoszące się do Europejskiej Rady ds. Innowacji w zakresie Danych dotyczą przetwarzania danych osobowych, mogą one rzutować na zadania oraz kompetencje krajowych organów ochrony danych i EROD w zakresie ochrony podstawowych praw i wolności osób fizycznych oraz ułatwiania swobodnego przepływu danych osobowych w Unii [98] (w szczególności przy uwzględnieniu szerokiego zakresu zadań powierzonych EROD na podstawie art. 70 RODO, które polegają na doradzaniu Komisji i wydawaniu wytycznych, zaleceń oraz najlepszych praktyk, a także zadań powierzonych EROD na podstawie art. 57 rozporządzenia (UE) 2018/1725).**

216. **W związku z tym EROD i EIOD zalecają doprecyzowanie w tekście prawnym, że w zakresie przetwarzania danych osobowych „właściwym organem” są organy nadzorcze odpowiedzialne za ochronę danych ustanowione na mocy prawa krajowego i Unii. Co więcej, jasne powinno być, że doradzanie Komisji Europejskiej w kwestiach ochrony danych oraz opracowanie spójnych praktyk dotyczących przetwarzania danych osobowych nie wchodzi w zakres kompetencji Europejskiej Rady ds. Innowacji w zakresie Danych, ponieważ w art. 70 RODO zadania te wprost przypisano EROD.**

---

[96] Uzasadnienie, s. 8.

[97] „Rada ma następujące zadania:
a) doradzanie i wspieranie Komisji w rozwijaniu spójnej praktyki organów sektora publicznego i właściwych podmiotów, o których mowa w art. 7 ust. 1, **rozpatrujących wnioski o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1**;
b) doradzanie i wspieranie Komisji w rozwijaniu spójnej praktyki właściwych organów w zakresie stosowania **wymogów mających zastosowanie do dostawców usług udostępniania danych**;
c) doradzanie Komisji w zakresie **ustalania priorytetów dotyczących norm międzysektorowych, które mają być stosowane i opracowywane do celów wykorzystywania danych i międzysektorowego udostępniania danych**, międzysektorowego porównywania i wymiany najlepszych praktyk w odniesieniu do wymogów sektorowych w zakresie bezpieczeństwa i procedur dostępu, przy jednoczesnym uwzględnieniu specyficznych dla danego sektora działań normalizacyjnych;
d) wspieranie Komisji w **zwiększaniu interoperacyjności danych, jak również usług udostępniania danych** między różnymi sektorami i w różnych dziedzinach, w oparciu o istniejące normy europejskie, międzynarodowe lub krajowe;
e) ułatwianie współpracy między właściwymi organami krajowymi na podstawie niniejszego rozporządzenia poprzez budowanie zdolności i wymianę informacji, w szczególności poprzez ustanowienie metod skutecznej wymiany informacji dotyczących procedury zgłaszania dostawców usług udostępniania danych oraz rejestracji i monitorowania uznanych organizacji o altruistycznym podejściu do danych”.

[98] Zob. np. art. 27 lit. a), zgodnie z którym do zadań Rady należy „doradzanie i wspieranie Komisji w rozwijaniu spójnej praktyki organów sektora publicznego i właściwych podmiotów, o których mowa w art. 7 ust. 1, rozpatrujących wnioski o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1”.

217. **EROD i EIOD zalecają także, aby w celu zapewnienia dokładności i jasności prawa, a także uniknięcia możliwego nieporozumienia zmienić nazwę Europejskiej Rady ds. Innowacji w zakresie Danych na „Grupę Ekspertów Komisji ds. Zarządzania Danymi" lub podobną, tak aby lepiej odzwierciedlała ona *status prawny* oraz *charakter* organu ustanowionego na mocy art. 26 wniosku.**

3.7.4 Art. 31: kary, jakie mają być nakładane za naruszenia przepisów wniosku

218. **We wniosku nie ujednolicono kar za naruszenia przepisów wniosku** (**ani nie sprecyzowano naruszeń, które będą karane, grzywien za naruszenia przepisów, ani organów odpowiedzialnych za nakładanie takich kar**), biorąc pod uwagę, że „[p]aństwa członkowskie przyjmują przepisy dotyczące kar mających zastosowanie w przypadku naruszeń [przedmiotowego] rozporządzenia i podejmują wszelkie działania niezbędne do zapewnienia ich wdrożenia. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach do dnia [data rozpoczęcia stosowania rozporządzenia] oraz niezwłocznie informują Komisję o wszelkich późniejszych zmianach ich dotyczących".

219. EROD i EIOD zwracają uwagę, że ten przepis, który ogranicza możliwość egzekwowania przepisów wniosku (zdolność do nakładania ujednoliconych sankcji), a w przypadku najbardziej pobłażliwego państwa członkowskiego potencjalnie prowadzi także do wyboru sądu ze względu na możliwość korzystniejszego rozstrzygnięcia sprawy (ang. *forum-shopping*), szkodzi określonemu celowi wniosku polegającemu na zwiększeniu zaufania do ponownego wykorzystywania, usług udostępniania danych oraz altruistycznego podejścia do danych.

3.7.5 Art. 33: zmiana rozporządzenia (UE) 2018/1724

220. Ten artykuł wniosku zmienia rozporządzenie w sprawie utworzenia jednolitego portalu cyfrowego (rozporządzenie (UE) 2018/1724)[99], wprowadzając następujące procedury administracyjne: zgłoszenie jako dostawca usług udostępniania danych; rejestracja jako europejska organizacja o altruistycznym podejściu do danych. W rezultacie oczekuje się odpowiednio: potwierdzenia przyjęcia zgłoszenia, potwierdzenia rejestracji.

221. **W tym względzie EROD i EIOD zauważają, że system zawiadamiania i rejestracji przeanalizowany już w niniejszej Opinii nie może zastąpić konieczności posiadania odpowiedniej podstawy prawnej dotyczącej przetwarzania danych osobowych zgodnie z art. 6 ust. 1 RODO, aby przetwarzanie danych było zgodne z prawem. Innymi słowy, zgodnie z RODO przetwarzanie danych osobowych jest zgodne z prawem wyłącznie wówczas, gdy – i w zakresie, w jakim – ma zastosowanie odpowiednia podstawa prawna określona w art. 6 ust. 1 RODO. We wniosku należy jasno doprecyzować ten aspekt, aby uniknąć wszelkich niejednoznaczności.**

Bruksela, 10 marca 2021 r.

[99] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1724 z dnia 2 października 2018 r. w sprawie utworzenia jednolitego portalu cyfrowego w celu zapewnienia dostępu do informacji, procedur oraz usług wsparcia i rozwiązywania problemów, a także zmieniające rozporządzenie (UE) nr 1024/2012 (tekst mający znaczenie dla EOG), Dz.U. L 295 z 21.11.2018, s. 1-38.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

W imieniu Europejskiego Inspektora Ochrony Danych

Europejski Inspektor Ochrony Danych

(Wojciech Wiewiórowski)

Przyjęto