



**Wspólna opinia EROD i EIOD
03/2022 w sprawie wniosku
dotyczącego rozporządzenia
w sprawie europejskiej przestrzeni
danych dotyczących zdrowia**

przyjęta 12 lipca 2022 r.

SPIS TREŚCI

1	Kontekst	5
2	Zakres opinii	6
3	Ocena.....	6
3.1	Uwagi ogólne	7
3.2	Powiązania między wnioskiem a unijnymi przepisami o ochronie danych	8
3.3	Powiązania między wnioskiem a aktem w sprawie zarządzania danymi, aktem w sprawie danych i aktem w sprawie sztucznej inteligencji.....	10
4	Przepisy ogólne (rozdział I)	11
4.1	Artykuł 1: Przedmiot i zakres stosowania wniosku.....	11
4.2	Artykuł 2: Definicje	13
5	Pierwotne wykorzystywanie elektronicznych danych dotyczących zdrowia (rozdział II).....	15
6	Systemy elektronicznej dokumentacji medycznej i aplikacje wspierające dobrostan (rozdział III) 20	
7	Wtórne wykorzystywanie elektronicznych danych dotyczących zdrowia (rozdział IV).....	24
8	Działania dodatkowe (rozdział V).....	27
8.1	Przechowywanie elektronicznych danych osobowych dotyczących zdrowia w UE oraz zgodność międzynarodowego przekazywania danych z rozdziałem V RODO.....	28
8.2	Zamówienia publiczne i finansowanie unijne.....	31
8.3	Krajowe punkty kontaktowe państwa trzeciego lub systemy ustanowione na szczeblu międzynarodowym.....	31
9	Zarządzanie i koordynacja na szczeblu europejskim (rozdział VI).....	32
10	Przekazanie uprawnień i Komitet (rozdział VII).....	33
11	Różne (rozdział VIII).....	34

Streszczenie

Niniejsza wspólna opinia EROD i EIOD ma na celu zwrócenie uwagi na szereg nadrzędnych kwestii dotyczących wniosku w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz wezwanie współprawodawców do podjęcia zdecydowanych działań.

EROD i EIOD zauważają, że wniosek ma na celu wspieranie osób fizycznych w przejmowaniu kontroli nad ich danymi dotyczącymi zdrowia, wspieranie wykorzystywania danych dotyczących zdrowia do poprawy jakości opieki zdrowotnej, badań naukowych, innowacji i kształtowania polityki oraz umożliwienie UE pełnego wykorzystania potencjału, jaki tkwi w bezpiecznym i zabezpieczonym udostępnianiu, wykorzystywaniu i ponownym wykorzystywaniu danych dotyczących zdrowia. „Ułatwianie wykorzystania elektronicznych danych dotyczących zdrowia”, zarówno w odniesieniu do pierwotnego, jak i wtórnego wykorzystywania takich danych, mogłoby bowiem istotnie przyczynić się do realizacji zarówno interesu publicznego, jak i interesów poszczególnych osób, których dane dotyczą/pacjentów.

Chociaż z zadowoleniem przyjmuje się starania na rzecz wzmocnienia kontroli i praw osób, których dane dotyczą, w odniesieniu do ich danych osobowych dotyczących zdrowia, należy podkreślić, że we wniosku tym przewidziano głównie pewne dodatki do niektórych przewidzianych już w RODO praw osób, których dane dotyczą. W rzeczywistości wniosek może nawet osłabić ochronę prawa do prywatności i ochrony danych, w szczególności biorąc pod uwagę kategorie danych osobowych i cele związane z wtórnym wykorzystywaniem danych.

EROD i EIOD zauważają, że przepisami zawartymi w omawianym wniosku dodaje się kolejny poziom do już złożonego (wielopoziomowego) zestawu przepisów (zawartych zarówno w prawie UE, jak i w prawie państw członkowskich) dotyczących przetwarzania danych dotyczących zdrowia (w sektorze opieki zdrowotnej). Powiązania między tymi różnymi przepisami muszą być (całkowicie) jasne.

EROD i EIOD uważają w szczególności, że ważne jest doprecyzowanie związku między przepisami omawianego wniosku a przepisami RODO oraz przepisami państw członkowskich. EROD i EIOD odnotowują zamiar i starania znajdujące odzwierciedlenie w omawianym wniosku dotyczącym europejskiej przestrzeni danych dotyczących zdrowia, aby pozostać w granicach RODO. Można to zauważyć na przykład w tym, że ustanawiane w nim na mocy prawa Unii podstawy prawne lub wyjątki odnoszące się do przetwarzania danych dotyczących zdrowia są zgodne ze strukturą RODO przewidzianą w jego art. 6 i 9. Jeżeli chodzi o pożądany poziom jasności tych przepisów, wymagane są jednak znaczące dalsze działania (poprawa przepisów i ich dalsze doprecyzowanie), w szczególności w odniesieniu do wzajemnych powiązań między tymi przepisami a ustawodawstwem państw członkowskich przyjętym na podstawie art. 9 ust. 4 RODO. Kwestie te znalazły odzwierciedlenie w uwagach do rozdziału II i IV wniosku.

Jeżeli chodzi o zakres wniosku, EROD i EIOD zalecają wyłączenie z art. 33 ust. 1 lit. f) wniosku odpowiednio aplikacji wspierających dobrostan i innych aplikacji z zakresu e-zdrowia, a także danych dotyczących dobrostanu i zachowania mających znaczenie dla zdrowia. Jeżeli dane te zostaną utrzymane, przetwarzanie do celów wtórnego wykorzystywania danych osobowych pochodzących z aplikacji wspierających dobrostan i innych aplikacji cyfrowych powinno podlegać uprzedniej zgodzie w rozumieniu RODO. Ponadto EROD i EIOD przypominają, że takie przetwarzanie może wchodzić w zakres dyrektywy 2002/58/WE („dyrektywa o prywatności i łączności elektronicznej”).

EROD i EIOD zdecydowanie zalecają również, aby nie rozszerzać na ten wniosek zakresu przewidzianych w RODO wyjątków dotyczących praw osoby, której dane dotyczą, w szczególności w art. 38 ust. 2 wniosku. Takie odstępstwo ogranicza możliwość sprawowania przez osoby, których dane dotyczą, skutecznej kontroli

nad swoimi danymi osobowymi zamiast ją wzmocnić, a zatem wydaje się sprzeczne z celem określonym w art. 1 ust. 2 lit. a) wniosku.

EROD i EIOD z zadowoleniem przyjmują fakt, że we wniosku odniesiono się do praw wynikających z RODO (np. prawa do bezpłatnego dostępu oraz prawa do otrzymania kopii danych). EROD i EIOD zauważają jednak, że przedstawiony we wniosku opis praw nie jest spójny z RODO. Jak wspomniano powyżej, taka sytuacja może prowadzić do niepewności prawa dla osób, których dane dotyczą, gdyż te mogą nie być w stanie rozróżnić tych dwóch rodzajów praw. W tym celu oraz aby uniknąć złożoności w praktycznym wdrożeniu, EROD i EIOD wzywają współprawodawców do zapewnienia jasności prawa w odniesieniu do wzajemnych powiązań między prawami osób, których dane dotyczą, wprowadzonymi we wniosku, a zawartymi w RODO ogólnymi przepisami odnoszącymi się do praw osób, których dane dotyczą.

EROD i EIOD odnotowują przepisy zawarte w rozdziale III, które mają na celu poprawę interoperacyjności elektronicznych dokumentacji medycznych i ułatwienie połączenia aplikacji wspierających dobrostan z takimi dokumentacjami. EROD i EIOD są jednak zdania, że tych ostatnich nie należy włączać do wtórnego wykorzystywania danych dotyczących zdrowia na podstawie rozdziału IV wniosku. Po pierwsze dlatego, że wobec danych dotyczących zdrowia generowanych przez aplikacje wspierające dobrostan i inne aplikacje z zakresu e-zdrowia nie obowiązują takie same wymogi w zakresie jakości i charakteru co wobec danych generowanych przez wyroby medyczne. Ponadto aplikacje te generują ogromne ilości danych i mogą być wysoce inwazyjne, ponieważ odnoszą się do każdego kroku, jaki ludzie podejmują w życiu codziennym. Nawet jeśli dane dotyczące zdrowia można by rzeczywiście oddzielić od innych rodzajów danych, można by łatwo wyciągnąć wnioski, na przykład dotyczące zwyczajów żywieniowych i inne nawyki, ujawniających informacje szczególnie wrażliwe, takie jak przekonania religijne.

Jeżeli chodzi o cele wtórnego wykorzystywania danych dotyczących zdrowia wymienione w art. 34 ust. 1 wniosku, EROD i EIOD rozumieją, że art. 34 ust. 1 lit. f) i g) wniosku może obejmować wszelkie formy „działa[ń] w zakresie rozwoju i innowacji w odniesieniu do produktów i usług przyczyniających się do ochrony zdrowia publicznego lub zabezpieczenia społecznego” lub „działa[ń] w zakresie trenowania, testowania i oceny algorytmów, w tym w wyrobach medycznych, systemach sztucznej inteligencji i aplikacjach z zakresu e-zdrowia, przyczyniających się do ochrony zdrowia publicznego lub zabezpieczenia społecznego”. EROD i EIOD są zdania, że we wniosku należy dokładniej określić te cele i wskazać, kiedy występuje wystarczający związek z ochroną zdrowia publicznego lub zabezpieczeniem społecznym. Będzie to miało zasadnicze znaczenie dla zapewnienia równowagi z odpowiednim uwzględnieniem celów wniosku oraz ochrony danych osobowych osób, których dane dotyczą, których dotyczy przetwarzanie.

Ponadto art. 34 ust. 1 wniosku zawiera kilka rodzajów wtórnego wykorzystywania, które wchodziłyby w zakres poszczególnych kategorii podstaw wyjątku przewidzianych w art. 9 ust. 2 RODO. EROD i EIOD uważają jednak, że nie znajduje to odzwierciedlenia w kryteriach, zgodnie z którymi organy ds. dostępu do danych dotyczących zdrowia powinny oceniać zastosowania danych i podejmować decyzje w ich sprawie (art. 45 wniosku) w celu wydania zezwolenia na dostęp do danych (art. 46 wniosku). EROD i EIOD podkreślają w tym względzie, że odnośne kryteria przewidziane w art. 46 wniosku ograniczają się do przepisów i zasad w nim przewidzianych i nie zapewniają jasności co do tego, w jaki sposób przepisy te odnoszą się do zasad i przepisów przewidzianych w RODO, w szczególności do art. 9 ust. 2 RODO.

W odniesieniu do rozdziału V EROD i EIOD uznają, że infrastruktura wymiany elektronicznych danych dotyczących zdrowia przewidziana w omawianym wniosku dotyczącym europejskiej przestrzeni danych dotyczących zdrowia w żaden sposób nie ma na celu (ani nie może doprowadzić do) utworzenia centralnej bazy danych UE zawierającej dane dotyczące zdrowia i co najwyżej ułatwi wymianę takich danych dotyczących zdrowia ze zdecentralizowanych baz danych. Ze względu na dużą ilość przetwarzanych danych,

ich wysoce wrażliwy charakter, ryzyko niezgodnego z prawem dostępu oraz konieczność pełnego zapewnienia skutecznego nadzoru nad nimi, EROD i EIOD wzywają jednak do dodania do omawianego wniosku przepisu, który wymagałby przechowywania elektronicznych danych osobowych dotyczących zdrowia w UE/EOG, bez uszczerbku dla dalszego przekazywania danych zgodnie z rozdziałem V RODO.

Ponadto w odniesieniu do modelu zarządzania ustanowionego we wniosku należy starannie dostosować zadania i kompetencje nowych organów publicznych, w szczególności z uwzględnieniem zadań i kompetencji krajowych organów nadzoru, EROD i EIOD w dziedzinie przetwarzania danych osobowych (dotyczących zdrowia). Należy unikać powielania kompetencji oraz określić dziedziny i wymogi dotyczące współpracy.

Europejska Rada Ochrony Danych i Europejski Inspektor Ochrony Danych

uwzględniając art. 42 ust. 2 rozporządzenia 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE,

uwzględniając Porozumienie EOG, 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 rozporządzenia Parlamentu Europejskiego i Rady w sprawie aktu prawnego o europejskiej przestrzeni danych dotyczących zdrowia („wniosek”) przyczyni się do realizacji określonej przez Komisję wizji przeprowadzenia transformacji cyfrowej w UE do 2030 r.¹
2. Europejska Rada Ochrony Danych (EROD) i Europejski Inspektor Ochrony Danych (EIOD) zauważają, że zdaniem Komisji wniosek ma na celu wspieranie osób fizycznych w przejmowaniu kontroli nad ich danymi dotyczącymi zdrowia, wspieranie wykorzystywania danych dotyczących zdrowia do poprawy jakości opieki zdrowotnej, badań naukowych, innowacji i kształtowania polityki oraz umożliwienie UE pełnego wykorzystania potencjału, jaki tkwi w bezpiecznym i zabezpieczonym udostępnianiu, wykorzystywaniu i ponownym wykorzystywaniu danych dotyczących zdrowia².
3. Jak wyjaśniono w uzasadnieniu, wniosek jest zgodny z nadrzędnymi celami UE. Cele te obejmują utworzenie silniejszej Europejskiej Unii Zdrowotnej, wdrażanie Europejskiego filaru praw socjalnych, poprawę funkcjonowania rynku wewnętrznego, propagowanie synergii z unijną agendą na rzecz cyfrowego rynku wewnętrznego oraz realizację ambitnego programu badań naukowych i innowacji. Ponadto wniosek zapewni istotny zestaw elementów wspierających tworzenie Europejskiej Unii Zdrowotnej przez zachęcanie do innowacji i prowadzenia badań oraz lepsze radzenie sobie z przyszłymi kryzysami zdrowotnymi.

¹ Uzasadnienie, s. 2.

² https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_pl

2 ZAKRES OPINII

4. 3 maja 2022 r. Komisja opublikowała wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie aktu prawnego o europejskiej przestrzeni danych dotyczących zdrowia („wniosek”).
5. 4 maja 2022 r. Komisja zwróciła się do EROD i EIOD o wydanie wspólnej opinii w sprawie wniosku („opinia”) na podstawie art. 42 ust. 2 rozporządzenia (UE) 2018/1725³.
6. Wniosek ten ma szczególne znaczenie w kontekście ochrony podstawowych praw i wolności osób w związku z przetwarzaniem ich danych osobowych. Zakres opinii ogranicza się do aspektów wniosku dotyczących danych osobowych i związanych z nimi, które stanowią jeden z głównych filarów wniosku.
7. EROD i EIOD z zadowoleniem przyjmują uzasadnienie wniosku, w którym stwierdza się, że „[b]iorąc pod uwagę, że znaczna ilość danych elektronicznych, które mają być dostępne w europejskiej przestrzeni danych dotyczących zdrowia, to dane osobowe dotyczące zdrowia osób fizycznych w UE, niniejszy wniosek został opracowany w pełnej zgodności nie tylko z RODO, ale także z rozporządzeniem (UE) 2018/1725 (unijne rozporządzenie o ochronie danych)”.
8. W tym samym duchu EROD i EIOD podkreślają, że konieczne jest zapewnienie i utrzymanie zasad poszanowania i stosowania dorobku prawnego UE w dziedzinie ochrony danych. W przypadku gdy kontekst wniosku obejmuje dane osobowe bardzo ważne jest zatem, aby w tekście prawnym wniosku wyraźnie unikać wszelkich niespójności i możliwych sprzeczności z ogólnym rozporządzeniem o ochronie danych⁴ („RODO”), dyrektywą o prywatności i łączności elektronicznej⁵ oraz rozporządzeniem 2018/1725. Nie chodzi tylko o pewność prawa, ale również o uniknięcie sytuacji, w której wniosek bezpośrednio lub pośrednio zagrażałby podstawowym prawom do prywatności i ochrony danych osobowych ustanowionym w art. 7 i 8 Karty praw podstawowych Unii Europejskiej („Karta”) oraz art. 16 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”).
9. Ponieważ wniosek, jak wyjaśniono bardziej szczegółowo w opinii, budzi szereg obaw dotyczących ochrony praw podstawowych do prywatności i ochrony danych osobowych, celem niniejszej opinii nie jest przedstawienie wyczerpującego wykazu wszystkich kwestii ani przedstawienie alternatywnych propozycji brzmienia w każdym możliwym przypadku. Opinia służy natomiast poruszeniu głównych zawartych we wniosku kwestii o krytycznym znaczeniu dla prywatności i danych osobowych.

3 OCENA

³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE, Dz.U. L 295 z 21.11.2018, s. 39.

⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Dz.U. L 119 z 4.5.2016, s. 1.

⁵ Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, Dz.U. L 201 z 31.7.2002, s. 37.

3.1 Uwagi ogólne

10. EROD i EIOD uznają cel wniosku, jakim jest rozszerzenie wykorzystania elektronicznych danych dotyczących zdrowia do celów świadczenia opieki zdrowotnej na rzecz osoby, od której dane te zostały zebrane („pierwotne wykorzystywanie”) oraz poprawa jakości badań naukowych, innowacji, kształtowania polityki, bezpieczeństwa pacjentów, medycyny personalizowanej, statystyk publicznych lub działań regulacyjnych („wtórne wykorzystywanie”). EROD i EIOD uznają również cel wniosku, jakim jest poprawa funkcjonowania rynku wewnętrznego w drodze ustanowienie jednolitych ram prawnych w zakresie rozwoju, wprowadzania do obrotu i wykorzystywania systemów elektronicznej dokumentacji medycznej („systemy elektronicznej dokumentacji medycznej”).
11. EROD i EIOD podkreślają jednak, że ochrona danych osobowych stanowi integralny element zaufania, jakie osoby fizyczne i organizacje powinny pokładać w rozwoju gospodarki cyfrowej⁶ i sprawiedliwym dostępie do opieki zdrowotnej, w szczególności w kontekście przetwarzania danych dotyczących zdrowia w ramach europejskiej przestrzeni danych dotyczących zdrowia.
12. EROD i EIOD podkreślają w tym względzie, że sukces europejskiej przestrzeni danych dotyczących zdrowia będzie zależał od solidnej podstawy prawnej przetwarzania zgodnie z unijnymi przepisami o ochronie danych, ustanowienia silnego mechanizmu zarządzania danymi oraz skutecznych i w pełni zgodnych z RODO zabezpieczeń praw i interesów osób fizycznych. Należy zapewnić wystarczające gwarancje dotyczące zgodnego z prawem, odpowiedzialnego i etycznego zarządzania opartego na wartościach UE, w tym poszanowania praw podstawowych. W tym zakresie EROD i EIOD są zdania, że europejska przestrzeń danych dotyczących zdrowia powinna służyć jako przykład przejrzystości, skutecznej rozliczalności i właściwej równowagi między interesami poszczególnych osób, których dane dotyczą, a wspólnym interesem społeczeństwa jako całości.
13. W kolejnych rozdziałach opinii EROD i EIOD przedstawiają zalecenia dotyczące sposobu zapewnienia zgodności odpowiednich przepisów wniosku nie tylko z unijnymi ramami prawnymi w zakresie ochrony danych, ale również z obecną interpretacją mającego zastosowanie orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej („TSUE”). Ze względu na szeroki zakres praw i obowiązków określonych we wniosku w odniesieniu do dostępu do szczególnych kategorii danych osobowych, ich wykorzystywania i udostępniania, jak w przypadku danych dotyczących zdrowia, ogólne odniesienia do RODO i rozporządzenia 2018/1725 mogą okazać się niewystarczające. W tym względzie EROD i EIOD uważają, że może istnieć ryzyko błędnej interpretacji kluczowych przepisów dotyczących ochrony danych, co z kolei może prowadzić do obniżenia stopnia ochrony przyznawanej obecnie osobom, których dane dotyczą, na mocy obowiązujących unijnych ram prawnych w zakresie ochrony danych (RODO, rozporządzenie 2018/1725 i dyrektywa o prywatności i łączności elektronicznej). W związku z powyższym EROD i EIOD uważają, że konieczne są dalsze specyfikacje, które zostaną szczegółowo opisane w pozostałej części niniejszej opinii.
14. EROD i EIOD z zadowoleniem odnotowują, że wniosek ma również na celu przyczynienie się do ograniczenia obecnego rozdrobnienia przepisów mających zastosowanie do przetwarzania danych dotyczących zdrowia i do badań naukowych. Jednocześnie EROD i EIOD wyrażają wątpliwość co do pełnej zgodności niektórych przepisów zawartych w rozdziałach II i IV wniosku (dotyczących w szczególności dostępu pracowników służby zdrowia do objętych ograniczeniem elektronicznych danych osobowych dotyczących zdrowia, systematycznej rejestracji odpowiednich danych

⁶ Wspólna opinia dotycząca aktu w sprawie zarządzania danymi.

dotyczących zdrowia przez pracowników służby zdrowia lub postępowania z nieoczekiwanymi ustaleniami organów ds. dostępu do danych dotyczących zdrowia w odniesieniu do osób fizycznych) z prawem państwa członkowskiego w sektorze e-zdrowia, wobec braku ogólnych uprawnień ustawodawczych UE w zakresie harmonizacji w tej dziedzinie. W tym względzie należy przypomnieć, że zgodnie z art. 168 TFUE Unia zachęca do współpracy między państwami członkowskimi w dziedzinie zdrowia publicznego oraz, jeśli to konieczne, wspiera ich działania w drodze uzupełnienia polityki krajowej, przy jednoczesnym poszanowaniu obowiązków państw członkowskich w zakresie określania ich polityki dotyczącej zdrowia, jak również organizacji i świadczenia usług zdrowotnych i opieki medycznej.

3.2 Powiązania między wnioskiem a unijnymi przepisami o ochronie danych

15. EROD i EIOD z zadowoleniem przyjmują motyw 4 wniosku, zgodnie z którym „[p]rzetwarzanie elektronicznych danych osobowych dotyczących zdrowia podlega przepisom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, a w przypadku instytucji i organów Unii – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725. W stosownych przypadkach odniesienia do przepisów rozporządzenia (UE) 2016/679 należy rozumieć również jako odniesienia do odpowiednich przepisów rozporządzenia (UE) 2018/1725 w przypadku instytucji i organów Unii”.
16. Ponadto zgodnie z uzasadnieniem wniosek opiera się na art. 114 i 16 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”). W świetle wniosku, chociaż art. 114 TFUE ma na celu poprawę funkcjonowania rynku wewnętrznego za pomocą środków służących zbliżeniu przepisów krajowych, wniosek służy zwiększeniu wykorzystania elektronicznych danych dotyczących zdrowia przy jednoczesnym wzmocnieniu praw wynikających z art. 16 TFUE.
17. EROD i EIOD podkreślają w tym względzie, że zgodnie z orzecznictwem TSUE art. 16 TFUE stanowi właściwą podstawę prawną, gdy jednym z celów lub elementów składowych norm przyjmowanych przez prawodawcę Unii jest ochrona danych osobowych⁷. Ponadto EROD i EIOD przypominają, że stosowanie art. 16 TFUE wiąże się również z koniecznością zapewnienia niezależnego nadzoru nad przestrzeganiem wymogów dotyczących przetwarzania danych osobowych, co jest również wymagane na mocy art. 8 Karty⁸.
18. W odniesieniu do argumentu dotyczącego niezależnego nadzoru EROD i EIOD podkreślają, że zgodnie z motywem 43 wniosku organom nadzorczym należy powierzyć zadanie egzekwowania odpowiednich przepisów RODO i rozporządzenia 2018/1725, zwłaszcza w odniesieniu do przetwarzania danych osobowych do celów wtórnego wykorzystywania w kontekście rozdziału IV wniosku. W związku z tym EROD i EIOD zalecają włączenie odpowiedniego przepisu do części normatywnej tekstu.
19. Jeżeli chodzi o odwołanie się do art. 16 TFUE jako (jednej z dwóch⁹) podstawy prawnej wniosku, EROD i EIOD uznają, że **celem** wniosku jest określenie „dodatkowych prawnie wiążących przepisów i zabezpieczeń”¹⁰ w odniesieniu do ochrony danych dotyczących zdrowia. Takie przepisy mają charakter „dodatkowy” w stosunku do przepisów RODO. We wniosku przewidziano „szczegółowe

⁷ Opinia z dnia 26 lipca 2017 r., PNR Canada, opinia 1/15, ECLI:EU:C:2017:592, pkt 96.

⁸ Akt w sprawie sztucznej inteligencji, Dz.U.

⁹ EIOD i EROD, zgodnie ze swoimi uprawnieniami, nie zajmą się w niniejszej opinii kwestią uzasadnienia odwołania się do podwójnej podstawy prawnej i ograniczą się do rozważań związanych z odwołaniem się do art. 16 TFUE.

¹⁰ Uzasadnienie wniosku, s. 6.

wymogi i normy”¹¹, które są dostosowane do przetwarzania elektronicznych danych dotyczących zdrowia i mają na celu „urzeczywistnieni[e] możliwości, jakie daje RODO w zakresie prawa Unii w odniesieniu do kilku celów”¹².

20. Jeżeli chodzi o **treść** wniosku, EROD i EIOD pragną przedstawić dwie uwagi ogólne.
21. Po pierwsze, wniosek zawiera głównie przepisy dotyczące przetwarzania danych osobowych (dotyczących zdrowia), zarówno do wykorzystywania pierwotnego, jak i wtórnego. Biorąc pod uwagę wpływ tych przepisów na ogólny punkt ciężkości wniosku, EROD i EIOD zgadzają się, że w treści wniosku uczyniono art. 16 TFUE niezbędną podstawą prawną. Pozostaje to bez uszczerbku dla zawartych w niniejszej opinii uwag dotyczących wzajemnego oddziaływania szeregu przepisów przewidzianych we wniosku z przepisami RODO, które to oddziaływanie zdecydowanie wymaga dalszych wyjaśnień, a niekiedy dalszej analizy i zmian, jak omówiono w dalszej części niniejszej opinii.
22. EROD i EIOD zauważają również, że zgodnie z motywem 37 omawiany wniosek ma na celu skorzystanie w prawie Unii z wyjątków określonych w art. 9 ust. 2 lit. g), i) oraz j) RODO. EROD i EIOD zauważają również, że w odniesieniu do wtórnego wykorzystywania danych dotyczących zdrowia we wniosku nałożono na posiadaczy danych w rozumieniu art. 6 ust. 1 lit. c) RODO obowiązek ujawniania danych osobowych organom ds. dostępu do danych dotyczących zdrowia. Jednocześnie EROD i EIOD rozumieją, że celem wniosku nie jest stworzenie podstawy prawnej dla osób składających wnioski o udostępnienie danych w związku z art. 6 RODO, ani zmiana wymogów informacyjnych wynikających z RODO lub dyrektywy o prywatności i łączności elektronicznej, ani też zmiana jakichkolwiek praw w nich określonych.
23. Po drugie, EROD i EIOD odnotowują, że wniosek zawiera co najmniej jedno wyraźne odstępstwo od przepisu RODO: W art. 38 ust. 2 wniosku zwalnia się bowiem niektóre podmioty (organy ds. dostępu do danych dotyczących zdrowia) ze stosowania przepisów art. 14 RODO dotyczących informacji, które mają być podawane osobom, których dane dotyczą. EROD i EIOD są zdania, że takie odstępstwo ogranicza możliwość sprawowania przez osoby, których dane dotyczą, skutecznej kontroli nad swoimi danymi osobowymi zamiast ją wzmocnić, a zatem wydaje się sprzeczne z celem określonym w art. 1 ust. 2 lit. a) wniosku. Ponadto EROD i EIOD powątpiewają, czy konieczne i uzasadnione jest wprowadzenie ograniczenia prawa do informacji, jak wyjaśniono bardziej szczegółowo w pkt 26, 34, 96 i 97 niniejszej opinii, również w świetle art. 23 RODO.
24. Ogólnie rzecz biorąc, EROD i EIOD przestrzegają przed prawodawstwem ustanawiającym odstępstwa od zadań i uprawnień organów nadzorczych ds. ochrony danych oraz ogólnie obowiązujących przepisów RODO zgodnie z art. 8 Karty. Takie przepisy nieuchronnie wpływają na centralne znaczenie przepisów horyzontalnych przyjętych na podstawie art. 16 TFUE i mogą z czasem je podważać. W zakresie, w jakim wniosek dotyczy przetwarzania danych osobowych, nadzór nad nim należy powierzyć niezależnym organom nadzorczym.
25. W każdym razie EROD i EIOD powątpiewają, czy ograniczenie prawa do informacji jest w tym kontekście konieczne i uzasadnione. Zarówno art. 14 ust. 5 lit. b), jak i art. 14 ust. 5 lit. c) RODO zwalniają bowiem administratorów z obowiązku przestrzegania art. 14 RODO w niektórych przypadkach, a mianowicie gdy 1) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby

¹¹ Tamże.

¹² Tamże.

niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art.89 ust.1, lub o ile obowiązek, o którym mowa w ust.1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania¹³; oraz gdy 2) pozyskiwanie lub ujawnianie danych osobowych jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą. W zakresie, w jakim wniosek w sprawie europejskiej przestrzeni danych dotyczących zdrowia wyraźnie przewiduje pozyskiwanie lub ujawnianie danych osobowych, należy raczej ocenić, czy omawiany wniosek zawiera odpowiednie zabezpieczenia chroniące prawnie uzasadnione interesy osób, których dane dotyczą.

26. Ponadto EROD i EIOD zauważają, że chociaż wniosek obejmuje również aplikacje wspierające dobrostan i inne aplikacje z zakresu e-zdrowia, w art. 1 ust. 4 wniosku nie uwzględniono dyrektywy o prywatności i łączności elektronicznej. Chociaż EROD i EIOD podają w wątpliwość włączenie takich aplikacji do zakresu rozdziału IV wniosku, jak zostanie to wyjaśnione w następnym rozdziale, EROD i EIOD zalecają uwzględnienie odniesienia do dyrektywy o prywatności i łączności elektronicznej, gdyby postanowienia dotyczące tych aplikacji miały pozostać we wniosku.
27. Ponadto art. 1 ust. 4 wniosku powinien również zawierać odniesienie do rozporządzenia 2018/1725, a ponadto odpowiednie przepisy rozporządzenia 2018/1725 powinny być wyraźnie wskazane w całym wniosku¹⁴. Wyraźne odniesienia do odpowiednich artykułów rozporządzenia 2018/1725 w części normatywnej wniosku wydają się bardziej niż uzasadnione, po pierwsze dlatego, że Komisja będzie działać jako podmiot przetwarzający elektroniczne dane dotyczące zdrowia przekazywane za pośrednictwem infrastruktury MojeZdrowie@UE (MyHealth@EU) art. 12 ust. 7 wniosku), po drugie – ponieważ instytucje, organy, urzędy i agencje Unii mogą uzyskać regularny dostęp do elektronicznych danych dotyczących zdrowia (motyw 41 wniosku), a po trzecie – ponieważ dane będące w posiadaniu instytucji UE można również udostępniać na potrzeby wtórnego wykorzystywania (motyw 46 wniosku).

3.3 Powiązania między wnioskiem a aktem w sprawie zarządzania danymi, aktem w sprawie danych i aktem w sprawie sztucznej inteligencji

28. EROD i EIOD zauważają, że zgodnie z art. 1 ust. 4 wniosku „rozporządzenie nie narusza przepisów innych aktów prawnych Unii dotyczących dostępu do elektronicznych danych dotyczących zdrowia, ich udostępniania lub wtórnego wykorzystywania ani wymogów związanych z przetwarzaniem danych w odniesieniu do elektronicznych danych dotyczących zdrowia, w szczególności rozporządzeń (UE) 2016/679, (UE) 2018/1725, [...] [akt w sprawie zarządzania danymi, COM(2020) 767 final] i [...] [akt w sprawie danych, COM(2022) 68 final]”. Ponadto zgodnie z art. 1 ust. 5 wniosku „(...) rozporządzenie nie narusza przepisów rozporządzenia (UE) 2017/745 i rozporządzenia [...] [akt w sprawie sztucznej inteligencji, COM(2021) 206 final] w odniesieniu do bezpieczeństwa wyrobów medycznych i systemów

¹³ W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia i informację publicznie.

¹⁴ Zgodnie z motywem 4 wniosku odniesienia do przepisów RODO należy rozumieć również jako odniesienia do odpowiadających im przepisów rozporządzenia 2018/1725. Chociaż cel motywu 4 jest jasny, EROD i EIOD zdecydowanie zalecają, aby odpowiednie przepisy rozporządzenia 2018/1725 zostały wyraźnie wskazane w części normatywnej wniosku jako takie.

sztucznej inteligencji, które wchodzi w interakcję z systemami elektronicznej dokumentacji medycznej”.

29. Choć EROD i EIOD z zadowoleniem przyjmują wyraźne odniesienie do tego, że wniosek nie narusza przepisów aktu w sprawie zarządzania danymi, aktu w sprawie danych, ani aktu w sprawie sztucznej inteligencji („AI”), EROD i EIOD są zdania, że należy lepiej uwzględnić konkretne powiązania pomiędzy wnioskiem a wyżej wymienionymi inicjatywami stanowiącymi część pakietu cyfrowego, a także z rozporządzeniem w sprawie wyrobów medycznych¹⁵. Aby zilustrować tę kwestię i tylko w charakterze przykładu, we wniosku wprowadzono definicję „posiadacza danych” w art. 2 ust. 2 lit. y), która może nie być spójna z definicją posiadacza danych zawartą w akcie w sprawie zarządzania danymi i akcie w sprawie danych. Taka niespójność mogłaby prowadzić do braku pewności prawa co do tego, jakie podmioty byłyby objęte taką definicją, mimo że stanowiłoby to centralny aspekt wniosku, ponieważ zasadniczo określałoby, jakie podmioty będą podlegały obowiązkowi udostępniania elektronicznych danych dotyczących zdrowia do celów wtórnego wykorzystywania.
30. EROD i EIOD zauważają ponadto, że ogólnym celem wniosku jest zapewnienie, by osoby fizyczne w UE miały większą kontrolę nad swoimi elektronicznymi danymi dotyczącymi zdrowia, co nie może zostać osiągnięte, jeżeli wzajemne powiązanie między odpowiednimi rozporządzeniami nie zostanie jasno określone. Pewność prawa ma zasadnicze znaczenie nie tylko z punktu widzenia zagwarantowania, by poszczególne zainteresowane strony czuły się bezpieczne przy podejmowaniu działań w nowych ramach, ale również z punktu widzenia zagwarantowania praw osób fizycznych. W związku z powyższym EROD i EIOD zalecają dalsze wyjaśnienie powiązania wniosku z wyżej wymienionymi inicjatywami i instrumentami prawnymi.

4 PRZEPISY OGÓLNE (ROZDZIAŁ I)

4.1 Artykuł 1: Przedmiot i zakres stosowania wniosku

31. EROD i EIOD z zadowoleniem przyjmują fakt, że wniosek ma na celu między innymi wzmocnienie praw osób fizycznych związanych z dostępnością i kontrolą ich elektronicznych danych dotyczących zdrowia.
32. EROD i EIOD zdają sobie sprawę, że pandemia COVID-19 znacznie przyspieszyła stosowanie wyrobów medycznych, aplikacji wspierających dobrostan lub urządzeń nasobnych wśród ogółu społeczeństwa. Tego rodzaju technologia generuje jednak ogromne ilości danych, w tym często szczególnych kategorii danych osobowych, i może być wysoce inwazyjna. Oprócz śledzenia ludzkich działań i decyzji możliwe jest teraz śledzenie ludzkich ciał, umysłów i emocji na poziomie, którego nawet sami ludzie nie są w stanie osiągnąć. Dane te można wykorzystać do przewidywania działań ludzi i manipulowania ich zachowaniem, nawet na poziomie grupy.
33. EROD i EIOD zauważają, że zgodnie z art. 1 ust. 2 lit. a) wniosku pierwszym celem wniosku jest wzmocnienie praw osób fizycznych związanych z dostępnością i kontrolą ich elektronicznych danych dotyczących zdrowia. Jednocześnie EROD i EIOD zauważają również, że w przeciwieństwie do pierwotnego wykorzystywania, w przypadku którego wniosek umożliwia osobom fizycznym

¹⁵ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylecia dyrektyw Rady 90/385/EWG i 93/42/EWG, Dz.U. L 117/1 z 5.5.2017.

ograniczenie dostępu do ich danych osobowych, taka możliwość nie jest dostępna w odniesieniu do wtórnego wykorzystywania danych. Ponadto zgodnie z art. 38 ust. 2 wniosku „organy ds. dostępu do danych dotyczących zdrowia nie mają obowiązku przekazywania szczegółowych informacji, o których mowa w art. 14 rozporządzenia (UE) 2016/679, każdej osobie fizycznej w odniesieniu do wykorzystania jej danych na potrzeby projektów objętych obowiązkiem posiadania zezwolenia na dostęp do danych (...)”. EROD i EIOD podkreślają, że prawo do informacji i prawo sprzeciwu są ze sobą nierozzerwalnie związane. EROD i EIOD są zdania, że ze względu na ograniczenie prawa do informacji przewidzianego w RODO wniosek może nie doprowadzić do osiągnięcia celów określonych w jego art. 1 ust. 2 lit. a). W rzeczywistości przewidywane podejście wydaje się podważać prawa osób fizycznych do prywatności i do ochrony danych osobowych, w szczególności biorąc pod uwagę bardzo szeroką definicję wtórnego wykorzystywania i minimalne kategorie danych elektronicznych do wtórnego wykorzystywania wprowadzone we wniosku, które nie ograniczają się wyłącznie do badań naukowych, ale obejmują również inne cele, takie jak innowacje.

34. Ponadto EROD i EIOD zauważają, że art. 1 ust. 3 lit. a) wniosku stanowi, że wniosek ma zastosowanie do „(...) producentów i dostawców **systemów elektronicznej dokumentacji medycznej i aplikacji wspierających dobrostan** wprowadzanych do obrotu i do używania w Unii oraz użytkowników takich produktów”, podczas gdy w art. 33 ust. 1 lit. f) i n) wniosku wymienia się wśród minimalnych kategorii danych elektronicznych do wtórnego wykorzystywania elektroniczne dane dotyczące zdrowia wygenerowane przez daną osobę, w tym dane dotyczące **wyrobów medycznych, aplikacji wspierających dobrostan lub innych aplikacji z zakresu e-zdrowia** (podkreślenie dodane). Po pierwsze, istnieje niespójność między zakresem wniosku a kategoriami danych wymienionymi w art. 33 ust. 1 lit. f) wniosku: w tym pierwszym zawarto odniesienie wyłącznie do producentów i dostawców systemów elektronicznej dokumentacji medycznej i aplikacji wspierających dobrostan, natomiast te ostatnie obejmują również wyroby medyczne dodatkowo do aplikacji wspierających dobrostan lub innych aplikacji z zakresu e-zdrowia. EROD i EIOD zakładają więc, że wyroby medyczne również wchodzi w zakres wniosku. W związku z tym, ze względu na jasność prawa, EROD i EIOD zalecają dodanie producentów i dostawców wyrobów medycznych do art. 1 ust. 3 lit. a) wniosku.
35. Ponadto EROD i EIOD podkreślają, że wymogi dotyczące jakości i cech charakterystycznych danych odnoszące się do danych dotyczących zdrowia generowanych przez aplikacje wspierające dobrostan i inne aplikacje z zakresu e-zdrowia różnią się od wymogów obowiązujących w odniesieniu do danych generowanych przez wyroby medyczne (te ostatnie podlegają obowiązującym normom i przepisom). Prócz tego należy zauważyć, że aplikacje z zakresu e-zdrowia mogą potencjalnie gromadzić dane osobowe wykraczające poza dane dotyczące zdrowia: na przykład gromadzenie danych osobowych dotyczących zwyczajów żywieniowych i innych nawyków może pośrednio umożliwiać ujawnienie informacji szczególnie chronionych, takich jak przekonania religijne.
36. W związku z powyższym, chociaż EIOD i EIOD rozumieją ewentualną potrzebę uwzględnienia wyrobów medycznych w zakresie stosowania wniosku, **EROD i EIOD zalecają wyłączenie z art. 33 ust. 1 lit. f) i n) wniosku odpowiednio aplikacji wspierających dobrostan i innych aplikacji z zakresu e-zdrowia, a także danych dotyczących dobrostanu i zachowania mających znaczenie dla zdrowia**. Jeżeli dane te zostaną utrzymane, przetwarzanie do celów wtórnego wykorzystywania danych osobowych pochodzących z aplikacji wspierających dobrostan i innych aplikacji cyfrowych powinno podlegać uprzedniej zgodzie w rozumieniu RODO. Ponadto EROD i EIOD przypominają, że takie przetwarzanie może wchodzić w zakres dyrektywy 2002/58/WE („dyrektywa o prywatności i łączności elektronicznej”).

37. EROD i EIOD odnotowują, że zgodnie z art. 2 ust. 2 wniosku definicja posiadacza danych wyraźnie obejmuje instytucje Unii Europejskiej. **Instytucje Unii Europejskiej mogą być jednak zarówno administratorem danych osobowych i danych dotyczących zdrowia (a tym samym posiadaczem danych), jak i użytkownikiem danych osobowych i danych dotyczących zdrowia**¹⁶. Wyjaśniono to w motywie 41 oraz art. 34, 45 i 48 wniosku. W związku z tym oraz ze względu na pewność prawa, EROD i EIOD **zalecają wyjaśnienie, czy instytucje Unii Europejskiej są objęte również definicją użytkownika danych**. Co więcej, EROD i EIOD przypominają, że ponieważ instytucje, organy, urzędy i agencje Unii nie podlegają jurysdykcjom krajowym, należy doprecyzować kary, które mogą być nakładane przez organy ds. dostępu do danych dotyczących zdrowia, jak przewidziano w art. 43 wniosku.

4.2 [Artykuł 2: Definicje](#)

38. EROD i EIOD zauważają, że art. 2 wniosku zawiera odpowiednie definicje pozwalające zrozumieć rozporządzenie jako całość. EROD i EIOD są jednak zdania, że zakres kilku z nich jest bardzo szeroki i otwarty na interpretację, co z kolei może prowadzić do niepewności prawa.
39. Po pierwsze, w art. 2 ust. 1 lit. a) wniosku stwierdza się, że zastosowanie mają **definicje zawarte w rozporządzeniu (UE) 2016/679**. Jednocześnie we wniosku wprowadza się nowe definicje i zawiera on odniesienia do konkretnych pojęć przewidzianych w innych rozporządzeniach, takich jak akt w sprawie danych. We wniosku wprowadzono na przykład definicję „odbiorcy danych”, chociaż taka definicja została już określona w art. 4 ust. 9 RODO. Ponieważ wniosek ma na celu uzupełnienie niektórych przepisów RODO, EROD i EIOD zalecają wyjaśnienie, ze względu na pewność prawa, dlaczego konieczne są dodatkowe definicje lub, w najbardziej skrajnych przypadkach, w drodze wyjątku, wskazanie definicji RODO, które nie mają zastosowania.
40. W art. 2 ust. 2 lit. a) wniosku zdefiniowano „**elektroniczne dane osobowe dotyczące zdrowia**” jako dane dotyczące zdrowia i dane genetyczne w rozumieniu RODO, a także dane odnoszące się do czynników warunkujących zdrowie lub dane przetwarzane w związku z udzielaniem świadczeń zdrowotnych, przetwarzane w formie elektronicznej; W tym względzie warto podkreślić, że w motywie 35 RODO jest już mowa o „informacjach zbieranych podczas świadczenia usług opieki zdrowotnej”. Ponadto w motywie 54 wniosku odniesiono się również do „czynników warunkujących zdrowie”, w szczególności w kontekście przetwarzania takich danych dotyczących zdrowia ze względu na interes publiczny. Aby zapewnić jak największą zgodność z RODO, EROD i EIOD zalecają zmianę

¹⁶ Instytucje, organy i jednostki organizacyjne Unii przetwarzają dane dotyczące zdrowia głównie w poniższych kontekstach:

1. rekrutacja (badanie lekarskie poprzedzające rekrutację),
2. ochrona zdrowia w miejscu pracy (coroczne badanie lekarskie) / bezpieczeństwo i higiena pracy
3. zwrot kosztów leczenia (wspólny system ubezpieczenia chorobowego),
4. zwolnienia chorobowe (orzeczenia lekarskie) i procedury stwierdzania inwalidztwa, oraz
5. wykonanie zadania przewidzianego w misji i instytucji Unii Europejskiej (np. Europejskiego Centrum ds. Zapobiegania i Kontroli Choroby Europejskiej Agencji Leków).

Operacje przetwarzania danych dotyczących zdrowia mogą stwarzać szczególne i wyższe ryzyko dla praw i wolności osób, których dane dotyczą, będących pracownikami, pracownikami zatrudnionymi na czas określony, pracownikami kontraktowymi, ekspertami krajowymi, stażystami w tych organach, kandydatami na wyższe wymienione stanowiska i osobami odwiedzającymi instytucje Unii Europejskiej. Zagrożenia te są podobne do tych, na jakie narażone są osoby, których dane dotyczą, gdy ich dane dotyczące zdrowia są przetwarzane przez administratorów niebędących instytucjami UE.

definicji zawartej w art. 2 ust. 2 lit. a) wniosku w taki sposób, aby odnosiła się ona jedynie do „danych dotyczących zdrowia i danych genetycznych zdefiniowanych w rozporządzeniu (UE) 2016/679, które są przetwarzane w formie elektronicznej”.

41. Z drugiej strony w art. 2 ust. 2 lit. b) wniosku zdefiniowano „**elektroniczne dane nieosobowe dotyczące zdrowia**” jako dane dotyczące zdrowia i dane genetyczne w formacie elektronicznym, które nie wchodzi w zakres definicji danych osobowych zawartej w art. 4 ust. 1 RODO. W tym względzie EROD i EIOD podkreślają ponownie¹⁷, że w praktyce trudno jest zastosować rozróżnienie między kategoriami danych osobowych a nieosobowych. Z połączenia danych nieosobowych można bowiem wywnioskować lub wygenerować dane osobowe, tj. dane dotyczące określonej lub możliwej do określenia osoby, szczególnie wtedy, gdy dane nieosobowe uzyskano w wyniku anonimizacji danych osobowych, a w jeszcze większym stopniu w kontekście przetwarzania danych dotyczących zdrowia. W związku z powyższym EROD i EIOD przyjmują do wiadomości ryzyko deanonimizacji przewidziane w motywie 64 wniosku i zalecają doprecyzowanie, że w przypadku mieszanych zbiorów danych (w których dane osobowe i nieosobowe są „nierozzerwalnie powiązane”) zastosowanie mają środki ochrony przewidziane w RODO i we wniosku dotyczącym elektronicznych danych osobowych dotyczących zdrowia.
42. W art. 2 ust. 2 lit. d) i art. 2 ust. 2 lit. e) wniosku zdefiniowano odpowiednio „**pierwotne wykorzystywanie elektronicznych danych dotyczących zdrowia**” i „**wtórne wykorzystywanie elektronicznych danych dotyczących zdrowia**”. EROD i EIOD uważają, że definicje te mogą prowadzić do niepewności prawa i niespójności z RODO, w szczególności w przypadku definicji wtórnego wykorzystywania elektronicznych danych dotyczących zdrowia. W szczególności druga część art. 2 ust. 2 lit. e) wniosku stanowi, że „[w]ykorzystane dane mogą obejmować elektroniczne dane osobowe dotyczące zdrowia zgromadzone początkowo w kontekście pierwotnego wykorzystywania, ale także elektroniczne dane dotyczące zdrowia zgromadzone do celów wtórnego wykorzystywania”. EROD i EIOD są zdania, że ponieważ pojęcie „wtórnego wykorzystywania danych osobowych” nie występuje w RODO, druga część definicji „wtórnego wykorzystywania elektronicznych danych dotyczących zdrowia” odbiega od pojęcia „dalszego przetwarzania danych osobowych” zawartego w RODO. To ostatnie pojęcie należy bowiem rozumieć w odniesieniu do celu, w którym określony administrator danych początkowo zgromadził dane, niezależnie od ich aspektów jakościowych. W związku z tym EROD i EIOD zalecają skorygowanie tych definicji w świetle RODO, a w szczególności wyjaśnienie związku między definicją wtórnego wykorzystywania elektronicznych danych dotyczących zdrowia w rozumieniu wniosku a pojęciem „dalszego wykorzystywania danych osobowych” w rozumieniu RODO, biorąc zwłaszcza pod uwagę szczególny system już przewidziany w RODO w odniesieniu do badań naukowych.
43. W art. 2 ust. 2 lit. f) wniosku zdefiniowano „**interoperacyjność**” jako „zdolność organizacji, jak również aplikacji lub wyrobów tego samego producenta lub różnych producentów do współdziałania na rzecz osiągnięcia celów korzystnych dla wszystkich stron, w tym wymiany informacji i wiedzy między tymi organizacjami, aplikacjami lub wyrobami bez zmiany treści danych, za pomocą obsługiwanych przez nie procesów”. EROD i EIOD są w tym względzie zdania, że taka definicja może wymagać dodatkowych wyjaśnień co do jej powiązania z już istniejącymi definicjami interoperacyjności zawartymi w innych aktach prawnych, takich jak akt w sprawie zarządzania danymi i rozporządzenie eIDAS.

¹⁷ Wspólna opinia EROD i EIOD dotycząca aktu w sprawie zarządzania danymi, pkt 58.

44. W art. 2 ust. 2 lit. y) wniosku zdefiniowano „**posiadacza danych**” jako „każdą osobę fizyczną lub prawną, która jest podmiotem lub organem w sektorze ochrony zdrowia lub opieki zdrowotnej lub która prowadzi badania naukowe w odniesieniu do tych sektorów, a także instytucje, organy, urzędy i agencje Unii, które mają prawo lub obowiązek – zgodnie z niniejszym rozporządzeniem, mającym zastosowanie prawem Unii lub przepisami krajowymi wdrażającymi prawo Unii – lub, w przypadku danych nieosobowych, poprzez kontrolę projektu technicznego produktu i powiązanych usług, możliwość udostępniania, w tym rejestracji, dostarczania, ograniczania dostępu lub wymiany niektórych danych”. Jak już podkreślono w pkt 29 powyżej, jest to definicja o zasadniczym znaczeniu, która jednak jest tak szeroka, że nie pozwala na jasne określenie, kto mógłby zostać zakwalifikowany jako posiadacz danych¹, oraz na zrozumienie, jakie jest jej powiązanie z definicją posiadacza danych zawartą w akcie w sprawie danych i akcie w sprawie zarządzania danymi. Jeżeli przepis ten nie określa jasno, kto jest objęty tą definicją, może prowadzić do braku pewności prawa co do tego, kto ma obowiązek udostępniania danych do celów wtórnego wykorzystywania na podstawie art. 33 ust. 1 i art. 44 wniosku, co z kolei może naruszać prawa do prywatności i ochrony danych osób, których dane dotyczą. Ponadto definicja ta jest niezgodna z art. 3 ust. 8 wniosku, w którym odniesiono się również do sektora zabezpieczenia społecznego, obecnie nieobjętego tą samą definicją zawartą w art. 2 ust. 2 lit. y) wniosku. EROD i EIOD są zatem zdania, że ze względu na pewność prawa ważne jest wyjaśnienie tego pojęcia.
45. W art. 2 ust. 2 lit. z) wniosku „**użytkownika danych**” zdefiniowano jako „osobę fizyczną lub prawną, która ma zgodny z prawem dostęp do elektronicznych danych osobowych lub nieosobowych dotyczących zdrowia do celów wtórnego wykorzystywania”. EROD i EIOD są w tym względzie zdania, że związek z definicją „odbiorcy danych” zawartą w art. 2 ust. 2 lit. k) wniosku oraz definicją „odbiorcy” zawartą w RODO jest niejasny. Wspomniany brak jasności odnosi się również do wzajemnych powiązań z pojęciem „użytkownika danych” w akcie w sprawie zarządzania danymi. Ponadto EROD i EIOD odnoszą się do zalecenia zawartego w pkt 37 niniejszej opinii w sprawie uwzględnienia instytucji Unii Europejskiej w tej definicji. Co więcej, EIOD i EROD uważają, że zamiast stwierdzenia, że osoba prawna ma zgodny z prawem dostęp do elektronicznych danych osobowych dotyczących zdrowia, bardziej właściwe byłoby odniesienie się do tego, czy i w jakich warunkach taki dostęp byłby możliwy.

5 PIERWOTNE WYKORZYSTYWANIE ELEKTRONICZNYCH DANYCH DOTYCZĄCYCH ZDROWIA (ROZDZIAŁ II)

46. EROD i EIOD zauważają, że w odniesieniu do pierwotnego wykorzystywania elektronicznych danych dotyczących zdrowia, jak przewidziano we wniosku, należy zapewnić równowagę między ułatwieniem dostępności zapisów elektronicznych, zarówno na szczeblu krajowym, unijnym, jak i międzynarodowym, a ogólnym wpływem na prawa i wolności osób fizycznych, a także na prawa określone w RODO. EROD i EIOD uważają, że aby osiągnąć ten cel, współprawodawca powinien wziąć pod uwagę następujące aspekty wniosku.
47. Przede wszystkim EROD i EIOD zauważają, że w art. 3 wniosku odniesiono się do praw osób fizycznych w związku z pierwotnym wykorzystywaniem ich elektronicznych danych osobowych dotyczących

zdrowia¹⁸. EROD i EIOD mają poważne obawy co do powiązań takich nowo wprowadzonych praw z prawami przewidzianymi w art. 15–22 RODO. EROD i EIOD są w szczególności zaniepokojeni nakładaniem się praw przewidzianych we wniosku z prawami przewidzianymi w RODO oraz ryzykiem niepewności prawa, jakie to nakładanie się może spowodować w odniesieniu do osób, których dane dotyczą. W związku z tym EROD i EIOD, ze względu na pewność prawa, wzywają współprawodawcę do wyjaśnienia związku między tymi prawami i zapewnienia, aby nie ograniczały one (bezpośrednio ani pośrednio) zakresu praw osób fizycznych przewidzianych w unijnych przepisach o ochronie danych.

48. W art. 3 wniosku wprowadza się prawo osób fizycznych do niezwłocznego dostępu oraz prawo do udzielania dostępu do danych lub zwracania się o ich przekazanie wybranym przez nich odbiorcom, a także prawo do ograniczania dostępu pracowników służby zdrowia do całości lub części elektronicznych danych dotyczących zdrowia tych osób oraz prawo do uzyskiwania informacji na temat świadczeniodawców i pracowników służby zdrowia, którzy uzyskali dostęp do ich elektronicznych danych dotyczących zdrowia w kontekście opieki zdrowotnej. Jak stwierdzono w motywie 1 wniosku, „[c]elem niniejszego rozporządzenia jest ustanowienie europejskiej przestrzeni danych dotyczących zdrowia, aby poprawić dostęp osób fizycznych do ich elektronicznych danych osobowych dotyczących zdrowia i kontrolę nad nimi w kontekście opieki zdrowotnej (pierwotne wykorzystywanie elektronicznych danych dotyczących zdrowia) [...]”. W motywie 6 wniosku wyjaśniono, że europejska przestrzeń danych dotyczących zdrowia opiera się na prawach osób, których dane dotyczą, wynikających z RODO i dalej prawa te rozwija, służąc zarazem spójnemu stosowaniu tych praw w odniesieniu do elektronicznych danych dotyczących zdrowia.
49. W tym kontekście EROD i EIOD podkreślają, że na chwilę sporządzania niniejszej opinii nie przeprowadzono jeszcze oceny skutków dla ochrony danych¹⁹ w odniesieniu do wniosku. W rezultacie nie przeprowadzono oceny, w jaki sposób przewidywane zmiany mogą wpływać na prawa i wolności osoby, której dane dotyczą, ani oceny związanego z nimi ryzyka.
50. Ponadto EROD i EIOD z zadowoleniem przyjmują fakt, że we wniosku odniesiono się do praw wynikających z RODO (np. prawa do bezpłatnego dostępu oraz prawa do otrzymania kopii danych)²⁰. EROD i EIOD zauważają jednak, że przedstawiony we wniosku opis praw nie jest spójny z RODO. Jak wspomniano powyżej, taka sytuacja może prowadzić do niepewności prawa dla osób, których dane dotyczą, gdyż te mogą nie być w stanie rozróżnić tych dwóch rodzajów praw. W tym celu oraz aby uniknąć złożoności w praktycznym wdrożeniu, EROD i EIOD wzywają współprawodawców do zapewnienia jasności prawa w odniesieniu do wzajemnych powiązań między prawami osób, których

¹⁸ Jeżeli chodzi na przykład o prawo nowej osoby, której dane dotyczą, do ograniczenia dostępu pracowników służby zdrowia do całości lub części jej elektronicznych danych dotyczących zdrowia, ustanowione w art. 3 ust. 9 wniosku, nie jest jasne, czy przepisy i określone zabezpieczenia, które mają zostać ustanowione w prawie państw członkowskich zgodnie z tymi samymi przepisami, muszą być zgodne z przepisami przewidzianymi w art. 18 ust. 2 i 3 RODO dotyczącymi prawa do ograniczenia przetwarzania danych.

¹⁹ Wnioskowi towarzyszy dokument roboczy służb Komisji – sprawozdanie z oceny skutków (dok. 8751/22 ADD 3 z 6 maja 2022 r.), który zawiera jedynie ogólny przegląd trzech wariantów strategicznych dotyczących wpływu na prawa podstawowe. Nie stanowi to oceny skutków dla ochrony danych w rozumieniu RODO ani też oceny tego, co byłoby niezbędne do przeprowadzenia dogłębnej analizy oceny ryzyka, jakie przetwarzanie szczególnych kategorii danych na bardzo dużą skalę pociągałoby za sobą, ani do zapewnienia koniecznych środków łagodzących i zabezpieczeń.

²⁰ Zob. na przykład art. 15 ust. 1 i 3 RODO w odniesieniu do istnienia prawa dostępu i prawa do uzyskania kopii danych, oraz art. 12 ust. 5 RODO, w którym przewidziano bezpłatne korzystanie z tych praw.

dane dotyczą, wprowadzonymi we wniosku, a zawartymi w RODO ogólnymi przepisami odnoszącymi się do praw osób, których dane dotyczą.

51. Ma to jeszcze większe znaczenie dla zapewnienia, aby osoby, których dane dotyczą, mające ograniczoną możliwość dostępu do usług cyfrowych i korzystania z nich, nie były zmuszone do polegania na osobach trzecich w celu korzystania z przysługujących im praw podstawowych, i w związku z tym nie były zobowiązane do ujawniania swojej prywatności i danych osobowych innym osobom fizycznym, aby móc wystąpić o dostęp do swoich danych, zgodnie z art. 3 ust. 5 lit. b) wniosku.
52. EROD i EIOD zauważają, że reprezentowanie osoby, której dane dotyczą, podczas wykonywania jej praw do ochrony danych musi spełniać pewne wymogi pewności prawa. Pojęcie upoważnienia wprowadzone w art. 3 ust. 5 wniosku, dotyczące ogólnych usług pełnomocnictwa w zakresie dostępu, może nie być wystarczające, aby zagwarantować, by osoby, których dane dotyczą, nie były w żaden sposób zmuszane do zapewnienia dostępu do swoich danych w ich imieniu innym wybranym przez siebie osobom fizycznym²¹.
53. Ponadto EROD i EIOD podkreślają, że tak szerokie pojęcie upoważnienia bez żadnych zabezpieczeń otwiera drogę do ewentualnego nadużywania prawa dostępu do elektronicznych danych dotyczących zdrowia. Wymóg, aby przedstawiciel był jedynie osobą fizyczną, nie musi bowiem konieczne uniemożliwiać przedsiębiorstwom prywatnym dostępu do danych. W związku z tym, aby zapobiec takim ewentualnym nadużyciom, EROD i EIOD zalecają ustanowienie dodatkowych zabezpieczeń towarzyszących takiemu mechanizmowi udzielania upoważnienia.
54. W odniesieniu do prawa do sprostowania danych przewidzianego w art. 3 ust. 7 wniosku EROD i EIOD odnotowują, że z wniosku nie wynika jasno, kto będzie odpowiedzialny za zapewnienie sprostowania danych. Jest to problematyczne, biorąc pod uwagę fakt, że w tym kontekście istnieje wiele źródeł i odbiorców danych osobowych na szczeblu krajowym, ale także unijnym, a nawet międzynarodowym. EPDB i EIOD podkreślają, że zgodnie z RODO taki obowiązek spoczywa na administratorze danych. Ponieważ jednak w tym kontekście istnieje kilku administratorów danych, którzy przyczyniają się do udostępnienia elektronicznych danych dotyczących zdrowia, EROD i EIOD wzywają współprawodawców do wyjaśnienia we wniosku, w jaki sposób w praktyce zapewniona zostanie zgodność z prawem do sprostowania danych.
55. EROD i EIOD zauważają, że art. 3 ust. 8 wniosku stanowi, że osoby fizyczne mają prawo udzielić posiadaczowi danych z sektora opieki zdrowotnej lub zabezpieczenia społecznego dostępu do swoich elektronicznych danych dotyczących zdrowia lub zwrócić się do niego o przekazanie ich elektronicznych danych dotyczących zdrowia wybranemu przez nie odbiorcy danych z sektora zdrowia lub zabezpieczenia społecznego niezwłocznie, nieodpłatnie i bez przeszkód ze strony posiadacza danych lub producentów systemów, z których korzysta ten posiadacz danych. EROD i EIOD podkreślają w tym względzie, że odbiorca danych musi zostać właściwie zidentyfikowany przez system, wraz z wykazaniem, że podmiot otrzymujący dane należy do sektora zdrowia lub zabezpieczenia społecznego.

²¹ Należy wziąć pod uwagę fakt, że w niektórych państwach członkowskich można to zrobić zgodnie z prawem tylko przy udziale notariusza, niezależnie od tego, czy osoba uzyskująca dostęp jest opiekunem prawnym, czy nie. Należy pamiętać, że przyczyna interwencji notariusza musi być związana z koniecznością zapewnienia swobodnego wyrażania woli przez osoby, których dane dotyczą.

56. Ponadto EROD i EIOD są zdania, że zgodnie z zasadą samostanowienia osoby, której dane dotyczą, przy podejmowaniu decyzji, któremu odbiorcy danych jej dane dotyczące zdrowia zostaną udostępnione zgodnie z art. 3 ust. 8 wniosku, ten ostatni powinien również zapewnić, aby osoba, której dane dotyczą, mogła również decydować, które dane mają być przekazane, zgodnie z tym, co przewidziano w art. 3 ust. 9 wniosku. W szczególności EROD i EIOD podkreślają, że we wniosku należy przewidzieć możliwość przekazywania wyłącznie danych niezbędnych do danego celu, co można osiągnąć za pomocą wymogu przyjęcia technicznych środków gwarantujących uwzględnienie ochrony prywatności już w fazie projektowania, aby zapewnić zgodność z zasadą minimalizacji danych.
57. Ponadto EROD i EIOD zauważają, że chociaż w art. 3 ust. 8 wniosku wprowadzono nowe prawo osoby, której dane dotyczą, do przekazania jej elektronicznych danych dotyczących zdrowia wybranemu przez nią odbiorcy danych, to nie ustanowiono odpowiadającego mu wyraźnego obowiązku posiadacza danych do dokonania takiego przekazania. Ponieważ w art. 9 ust. 1 RODO nie zezwala się zasadniczo na przetwarzanie danych osobowych dotyczących zdrowia, a także danych genetycznych, chyba że zastosowanie ma jedno z odstępstw określonych w art. 9 ust. 2 RODO, EROD i EIOD zalecają współprawodawcy dostosowanie art. 3 ust. 8 wniosku do art. 6 RODO i art. 9 ust. 2 RODO oraz wyjaśnienie powiązań tego przepisu z ewentualnymi dalszymi warunkami, w tym ograniczeniami, dotyczącymi przetwarzania danych dotyczących zdrowia lub danych genetycznych, które państwa członkowskie mogły utrzymać lub wprowadzić na podstawie art. 9 ust. 4 RODO.
58. EROD i EIOD z zadowoleniem przyjmują przepis zawarty w art. 3 ust. 10 wniosku, ponieważ gwarantuje on osobom, których dane dotyczą, skuteczną kontrolę nad ich danymi osobowymi, umożliwiając im zidentyfikowanie potencjalnego bezprawnego dostępu do ich danych dotyczących zdrowia. EROD i EIOD uważają jednak, że nie jest jasne, czy prawo do uzyskania informacji realizowane jest za pomocą automatycznej procedury powiadamiania w każdym przypadku, gdy dostęp do danych jest możliwy, czy tylko na wniosek. EROD i EIOD uważają, że pierwszy wariant jest najbardziej odpowiednim rozwiązaniem, aby wzmocnić pozycję osoby, której dane dotyczą. W związku z tym EROD i EIOD zalecają, aby kwestia ta została uwzględniona przez współprawodawców i w związku z tym odpowiednio wyjaśniona.
59. W odniesieniu do art. 4 ust. 1 wniosku EROD i EIOD zauważają, że pracownicy służby zdrowia a) mają dostęp do elektronicznych danych dotyczących zdrowia osób fizycznych, które leczą, niezależnie od państwa członkowskiego ubezpieczenia i państwa członkowskiego leczenia, oraz b) zapewniają, aby elektroniczne dane osobowe dotyczące zdrowia osób fizycznych, które leczą, były aktualizowane o informacje dotyczące udzielonych świadczeń zdrowotnych. W związku z tym, jako że – jak zauważają EROD i EIOD – kwestię dostępu do elektronicznych danych osobowych dotyczących zdrowia można już rozwiązać i uregulować na szczeblu krajowym, EROD i EIOD zalecają, aby współprawodawcy wyjaśnili związek między tym przepisem a przepisami krajowymi, które już regulują tę kwestię.
60. Po pierwsze, w odniesieniu do art. 4 ust. 1 wniosku EROD i EIOD podkreślają, że art. 9 ust. 1 RODO zasadniczo nie zezwala na przetwarzanie danych osobowych dotyczących zdrowia oraz danych genetycznych, chyba że zastosowanie ma jeden z odstępstw przewidzianych w art. 9 ust. 2 RODO. W związku z tym EROD i EIOD zalecają dostosowanie art. 4 ust. 1 wniosku do art. 9 ust. 2 lit. h) RODO.
61. Po drugie, EROD i EIOD są zdania, że przepis ten nie jest zgodny z przewidzianymi w RODO zasadami minimalizacji danych i ograniczenia celu, ponieważ dostępu udziela się nie tylko w razie konieczności i na zasadzie wiedzy koniecznej. W związku z tym, a także w celu zapewnienia odpowiednich zabezpieczeń osobom, których dane dotyczą, EROD i EIOD zalecają, aby dostęp ten odbywał się wyłącznie zgodnie z zasadą wiedzy koniecznej.

62. Po trzecie, EROD i EIOD podkreślają, że pojęcie „pracownika służby zdrowia” obejmuje bardzo zróżnicowane zawody o odrębnym charakterze i wymagające różnego rodzaju zaangażowania, podejmowania decyzji i odpowiedzialności (np. lekarze, pielęgniarki, technicy laboratoryjni i obrazowania, dietetycy, fizjoterapeuci, psychologowie, farmaceuci). W związku z tym EROD i EIOD zalecają, aby nie wszystkie dane dotyczące zdrowia były udostępniane wszystkim pracownikom służby zdrowia bez rozróżnienia, lecz jedynie te, do których dostęp uznaje się za niezbędny do wykonania określonego zadania. EROD i EIOD podkreślają w tym kontekście znaczenie zasad konieczności i proporcjonalności. EROD i EIOD zauważają, że zgodnie z art. 4 ust. 2 wniosku państwa członkowskie, zgodnie z zasadą minimalizacji danych, ustanawiają przepisy określające kategorie elektronicznych danych osobowych dotyczących zdrowia wymaganych przez różne zawody związane ze służbą zdrowia. EROD i EIOD odnotowują, że we wniosku wyraźnie nakłada się tę odpowiedzialność na państwa członkowskie, czyniąc ją obowiązkiem. EROD i EIOD zalecają z tego względu zastąpienie słowa „mogą” słowem „muszą”, aby zapewnić określenie takich przepisów przez państwa członkowskie.
63. EROD i EIOD zauważają, że art. 4 ust. 3 wniosku stanowi, pracownikom służby zdrowia zapewnia się dostęp co najmniej do priorytetowych kategorii elektronicznych danych, o których to kategoriach mowa w art. 5 wniosku, bez określania, czy wszystkie kategorie priorytetowe są dostępne dla wszystkich pracowników służby zdrowia. Jak wskazano powyżej, EROD i EIOD są zdania, że dostępu należy udzielać wyłącznie z uwzględnieniem tego, co jest konieczne do celów leczenia. EROD i EIOD uważają, że związek między art. 4 ust. 2 i art. 4 ust. 3 wniosku należy doprecyzować we wniosku.
64. W art. 4 ust. 4 wniosku przewidziano możliwość odstępstwa od ograniczeń dostępu wybranych przez osobę, której dane dotyczą, przewidzianych w art. 3 ust. 9 wniosku, w przypadku gdy dostęp jest niezbędny do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej. W związku z tym EROD i EIOD zalecają współprawodawcom sprecyzowanie, że prawo osób fizycznych do uzyskania informacji na temat dostępu pracowników służby zdrowia do ich elektronicznych danych dotyczących zdrowia, o którym mowa w art. 3 ust. 10, obejmuje dostęp do informacji objętych ograniczeniami przewidzianymi w art. 3 ust. 9 wniosku.
65. W art. 7 wniosku zobowiązuje się państwa członkowskie do zapewnienia, aby pracownicy służby zdrowia „systematycznie” rejestrowali odpowiednie dane dotyczące zdrowia dotyczące świadczeń zdrowotnych udzielanych przez nich osobom fizycznym, w formie elektronicznej w systemie elektronicznej dokumentacji medycznej. EROD i EIOD są zaniepokojeni odniesieniem do takiej systematycznej rejestracji, ponieważ wydaje się, że nie jest ona zgodna z ogólną zasadą minimalizacji danych. EROD i EIOD proponują w związku z tym zmianę tekstu wniosku w drodze skreślenia terminu „systematycznie” w celu dostosowania przepisu do zasady minimalizacji danych.
66. EROD i EIOD z zadowoleniem przyjmują przepisy dotyczące elektronicznego zarządzania identyfikacją zawarte w art. 9 wniosku, ponieważ uważają, że bezpieczna identyfikacja i uwierzytelnianie osób fizycznych i pracowników służby zdrowia korzystających z elektronicznych usług opieki zdrowotnej lub dostępu do danych osobowych dotyczących zdrowia jest jednym z podstawowych elementów ochrony praw osób, których dane dotyczą. W tym względzie EROD i EIOD podkreślają, że konieczne może być rozważenie różnych mechanizmów identyfikacji i uwierzytelniania pracowników służby zdrowia w zależności od tego, czy uzyskują oni dostęp do danych w charakterze specjalistów, czy też w charakterze prywatnym.
67. Jeżeli chodzi o ustanowienie organu ds. e-zdrowia, o którym mowa w art. 10 wniosku, EROD i EIOD są zaniepokojeni faktem, że niektóre z ich zadań mogą pokrywać się z zadaniami organów nadzorczych ds. ochrony danych zgodnie z RODO, w szczególności w odniesieniu do praw osoby, której dane

dotyczą, i bezpieczeństwa przetwarzania danych. Ze względu na pewność prawa i w celu poprawy czytelności tekstu prawnego EROD i EIOD proponują przeniesienie przepisu zawartego w art. 3 ust. 11 zdanie ostatnie wniosku do art. 10 wniosku.

68. W odniesieniu do art. 11 wniosku, w którym ustanawia prawo osób fizycznych i prawnych do wniesienia skargi do organu ds. e-zdrowia, EROD i EIOD uważają, że samo przekazanie informacji o istnieniu skargi organom ochrony danych nie jest wystarczające, aby umożliwić im zbadanie i ocenę wszelkich aspektów skargi związanych z ochroną danych. W związku z tym EROD i EIOD zalecają wyjaśnienie, że jeżeli skarga ma jakiś związek z ochroną danych, nawet jeżeli sprawa dotyczy nowych praw osób fizycznych wprowadzonych w art. 3 wniosku, organ ds. e-zdrowia przesyła kopię skargi właściwemu organowi nadzorcemu ds. ochrony danych.
69. Ogólnie rzecz biorąc, EROD i EIOD proponują wprowadzenie obowiązku konsultacji z organami ochrony danych i obowiązku współpracy z nimi w odniesieniu do oceny skarg oraz wdrażania wniosku w każdym przypadku, gdy skargi dotyczą aspektów ochrony danych. Ponadto EROD i EIOD podkreślają, że organy ochrony danych są jedynymi właściwymi organami odpowiedzialnymi za kwestie związane z ochroną danych i w związku z tym powinny pozostać jedynym punktem kontaktowym dla osoby, której dane dotyczą, w odniesieniu do tych kwestii, również w celu uniknięcia dezorientacji osób, których dane dotyczą, co do warunków, w jakich mogą one egzekwować swoje prawa do ochrony danych.
70. W art. 13 wniosku przewidziano możliwość świadczenia dodatkowych transgranicznych usług e-zdrowia za pośrednictwem infrastruktury MojeZdrowie@UE (MyHealth@EU) oraz możliwość wymiany danych z innymi infrastrukturami lub innymi usługami w dziedzinie zdrowia, opieki lub zabezpieczenia społecznego. W tym samym przepisie wymaga się od państw członkowskich i Komisji dążenia do zapewnienia interoperacyjności infrastruktury MojeZdrowie@UE (MyHealth@EU) z systemami technologicznymi ustanowionymi na szczeblu międzynarodowym na potrzeby wymiany elektronicznych danych dotyczących zdrowia.
71. EROD i EIOD zauważają, że omawiane możliwości są przedstawione w sposób ogólny i nie jest jasne, w jakich okolicznościach i na jakich warunkach elektroniczne dane dotyczące zdrowia mogą być udostępniane uczestnikom w państwach trzecich. W świetle zabezpieczeń wymaganych na mocy rozdziału V RODO w odniesieniu do międzynarodowego przekazywania danych EROD i EIOD zalecają współprawodawcom wyjaśnienie, że kontrola zgodności, którą ma przeprowadzić Komisja w odniesieniu do krajowego punktu kontaktowego państwa trzeciego lub systemu ustanowionego na szczeblu międzynarodowym, obejmuje również spełnienie wymogów rozdziału V RODO, przed stwierdzeniem w drodze aktu wykonawczego, że taki krajowy punkt kontaktowy lub system jest zgodny z wymogami infrastruktury MojeZdrowie@UE (MyHealth@EU) do celów elektronicznej wymiany danych dotyczących zdrowia.

6 SYSTEMY ELEKTRONICZNEJ DOKUMENTACJI MEDYCZNEJ I APLIKACJE WSPIERAJĄCE DOBROSTAN (ROZDZIAŁ III)

72. W rozdziale III wniosku skoncentrowano się na wdrożeniu obowiązkowego systemu certyfikacji własnej systemów elektronicznej dokumentacji medycznej, w ramach którego te ostatnie muszą spełniać zasadnicze wymogi dotyczące interoperacyjności i bezpieczeństwa określone w załączniku II do wniosku. Jak podkreślono w uzasadnieniu, „[t]akie podejście jest konieczne, aby zapewnić kompatybilność elektronicznej dokumentacji medycznej między poszczególnymi systemami

i umożliwić łatwe przekazywanie między nimi elektronicznych danych dotyczących zdrowia”. EROD i EIOD z zadowoleniem przyjmują fakt, że zgodnie z art. 15 i 17 wniosku systemy elektronicznej dokumentacji medycznej muszą podlegać uprzedniej procedurze oceny zgodności, zanim będą mogły zostać wprowadzone do obrotu lub w inny sposób oddane do użytku w UE.

73. EROD i EIOD zauważają jednak, że niektóre zasadnicze wymogi określone w załączniku II do wniosku odnoszą się do aspektów związanych z ochroną danych osobowych, takich jak te dotyczące wdrażania praw osób fizycznych określonych w rozdziale II wniosku lub bezpiecznego przetwarzania elektronicznych danych dotyczących zdrowia²². Ponadto wspólne specyfikacje, które mają zostać przyjęte przez Komisję w drodze aktów wykonawczych w odniesieniu do zasadniczych wymogów określonych w załączniku II, zgodnie z art. 23 ust. 3 wniosku, mogą obejmować elementy dotyczące ochrony danych, takie jak wymogi dotyczące jakości danych, w tym kompletności i dokładności elektronicznych danych dotyczących zdrowia, a także wymogi i zasady dotyczące bezpieczeństwa, poufności, integralności, bezpieczeństwa pacjentów i ochrony elektronicznych danych dotyczących zdrowia²³.
74. Po pierwsze, EROD i EIOD podkreślają, że zgodność systemów elektronicznej dokumentacji medycznej z zasadniczymi wymaganiami dotyczącymi interoperacyjności i bezpieczeństwa określonymi w załączniku II do wniosku niekoniecznie oznacza, że operacje przetwarzania leżące u podstaw ich funkcjonowania są same w sobie zgodne z prawem, ponieważ może zaistnieć konieczność spełnienia przez administratora dalszych wymogów wynikających z unijnych przepisów o ochronie danych. Chociaż EROD i EIOD zdają sobie sprawę, że wyżej wymienione zasadnicze wymagania i wspólne specyfikacje nie są bezpośrednio powiązane z unijnymi przepisami o ochronie danych, niektóre z nich mogą mieć jednak znaczący wpływ na istotne aspekty ochrony danych osobowych osób, których dane dotyczą. EROD i EIOD zauważają w tym względzie, że nie wydaje się, aby wyżej wskazane wymagania należycie uwzględniały zasady minimalizacji danych i ochrony danych już w fazie projektowania jako kluczowych aspektów, które należy wziąć pod uwagę przy opracowywaniu systemu elektronicznej dokumentacji medycznej w celu odpowiedniej ochrony interesów i praw osób, których dane dotyczą, w odniesieniu do ochrony danych i prywatności. Ponadto wymagania dotyczące okresów zatrzymywania danych i praw dostępu określone w pkt 3.8 załącznika II do wniosku nie uwzględniają określonego celu operacji przetwarzania danych jako kluczowego elementu, który należy rozważyć przy opracowywaniu funkcji przechowywania systemów elektronicznej dokumentacji medycznej dodatkowo do „źródła i kategorii elektronicznych danych dotyczących zdrowia”.
75. Biorąc pod uwagę ryzyko stwarzane przez przepisy dotyczące obowiązkowej dostępności, transgranicznej wymiany, dostępu i dalszego wykorzystywania elektronicznych danych dotyczących zdrowia zawartych w systemach elektronicznej dokumentacji medycznej, a także skutki dla osób, których sprawa dotyczy, EROD i EIOD są zdania, że w celu wzmocnienia ochrony osób fizycznych i ich zaufania do tych systemów najbardziej odpowiednio byłoby wprowadzenie realizowanej przez osobę trzecią procedury oceny zgodności systemów elektronicznej dokumentacji medycznej z przepisami²⁴,

²² Zob. np. pkt 1.3 i wymagania dotyczące bezpieczeństwa wymienione w pkt 3 załącznika II, takie jak te dotyczące zapobiegania nieuprawnionemu dostępowi w pkt 3.1; mechanizmów służących identyfikacji i uwierzytelnianiu w pkt 3.2; mechanizmów kontroli dostępu w pkt 3.3; mechanizmów rejestrowania dostępu do danych w pkt 3.4 oraz mechanizmów ograniczania dostępu pracowników służby zdrowia w pkt 3.5.

²³ Zob. art. 23 ust. 3 lit. c) i e) wniosku oraz art. 10 ust. 2 lit. h) wniosku.

²⁴ Zob. np. prowadzona przez stronę trzecią procedura oceny zgodności przewidziana w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych,

przy czym odbywałoby się to w drodze zaangażowania jednostek notyfikowanych w ocenę środków, w tym rozwiązań technicznych, wprowadzonych przez producenta w celu spełnienia wymagań w zakresie interoperacyjności i bezpieczeństwa określonych w załączniku II do wniosku. W tym względzie EROD i EIOD z zadowoleniem odnotowują, że kwestia ta jest objęta szczegółową oceną w kontekście oceny i przeglądu proponowanego rozporządzenia przeprowadzanych przez Komisję po pięciu latach od jego wejścia w życie.

76. Ponadto EROD i EIOD zalecają zmianę wniosku w celu uściślenia związku między obowiązkowym systemem certyfikacji własnej systemów elektronicznej dokumentacji medycznej a wymogami ochrony danych. Ponadto należy zauważyć, że w każdym przypadku, gdy wspólne specyfikacje, o których mowa w art. 23 wniosku, mają wpływ na wymogi ochrony danych odnoszące się do systemów elektronicznej dokumentacji medycznej, akty wykonawcze, które mają zostać przyjęte przez Komisję na podstawie art. 23 wniosku, powinny podlegać konsultacjom zarówno z EIOD, jak i EROD zgodnie z art. 42 ust. 2 rozporządzenia 2018/1725. Te same uwagi mają zastosowanie do dobrowolnego oznakowania aplikacji wspierającej dobrostan, które w równym stopniu opiera się na zasadniczych wymaganiach określonych w załączniku II do wniosku oraz na wspólnych specyfikacjach, o których mowa w art. 23 wniosku.
77. W odniesieniu do postępowania w przypadku ryzyka stwarzanego przez systemy elektronicznej dokumentacji medycznej oraz w przypadku poważnych incydentów, a także do wdrażania działań naprawczych, zgodnie z art. 29 wniosku, EROD i EIOD zalecają ustanowienie obowiązku informowania organów ochrony danych i współpracy z nimi, w stosownych przypadkach. Nie jest bowiem jasne, czy odniesienie do ryzyka dla „innych aspektów ochrony interesu publicznego” wśród rodzajów ryzyka, jakie może stwarzać system elektronicznej dokumentacji medycznej, pociągające za sobą interwencję organu nadzoru rynku, może obejmować ochronę danych osobowych. Ponadto nie można wykluczyć, że poważny incydent związany z systemem elektronicznej dokumentacji medycznej²⁵ może wynikać z wadliwego działania lub pogorszenia właściwości lub działania systemu elektronicznej dokumentacji medycznej, co ma również wpływ na ochronę danych osobowych.
78. EROD i EIOD przyjmują zasadniczo z zadowoleniem art. 31 wniosku dotyczący dobrowolnego oznakowania aplikacji wspierających dobrostan, ponieważ może to zapewnić użytkownikom takich aplikacji przejrzystość w odniesieniu do ich kluczowych funkcji, pomagając tym samym użytkownikom w wyborze wiarygodnych aplikacji wspierających dobrostan. Art. 31 i 32 wniosku odnoszą się jednak wyłącznie do interoperacyjności aplikacji wspierających dobrostan z systemami elektronicznej dokumentacji medycznej i ustanawia się w nich mechanizm dobrowolny ograniczony do wymagań w zakresie interoperacyjności i bezpieczeństwa określonych w załączniku II do wniosku w celu zapewnienia, aby aplikacje te mogły przekazywać elektroniczne dane dotyczące zdrowia do systemów elektronicznej dokumentacji medycznej.
79. EROD i EIOD podkreślają w tym względzie, że oznakowanie towarzyszące aplikacjom wspierającym dobrostan zgodnie z art. 31 wniosku niekoniecznie oznacza, że operacje przetwarzania leżące u podstaw funkcjonowania takiej aplikacji są same w sobie zgodne z prawem i mogą być w związku z tym realizowane przez użytkownika. Administrator będzie musiał spełnić dalsze wymogi wynikające z unijnych przepisów o ochronie danych. EROD i EIOD zalecają wyjaśnienie tej kwestii we wniosku,

zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylecia dyrektyw Rady 90/385/EWG i 93/42/EWG.

²⁵ Zob. definicja zawarta w art. 2 ust. 2 lit. q) wniosku.

przynajmniej w motywie. W motywie 35 wniosku stwierdzono, że „[j]eżeli dane generowane przez aplikacje wspierające dobrostan są przydatne w kontekście opieki zdrowotnej, użytkowników tego typu aplikacji wspierających dobrostan, w tym aplikacji mobilnych, należy informować, czy takie aplikacje można połączyć z systemami elektronicznej dokumentacji medycznej lub krajowymi elektronicznymi rozwiązaniami w zakresie zdrowia i wykorzystywać do przesyłania danych do takich systemów lub rozwiązań”. We wniosku nie określono jednak warunków, na jakich takie aplikacje wspierające dobrostan mogą być zgodnie z prawem połączone i dostarczać dane osobowe do systemów elektronicznej dokumentacji medycznej (lub do krajowych rozwiązań w zakresie e-zdrowia) na mocy przepisów o ochronie danych. Z wykazu minimalnych kategorii danych elektronicznych do wtórnego wykorzystywania, zawartego w art. 33 wniosku, wynika natomiast, że pośrednio²⁶ – po umieszczeniu w systemie elektronicznej dokumentacji medycznej – lub bezpośrednio – w zakresie, w jakim są one gromadzone lub przetwarzane przez podmioty spełniające definicję posiadacza danych zgodnie z art. 2 ust. 2 lit. y) wniosku²⁷ – dane osobowe generowane przez aplikacje wspierające dobrostan mieszczą się w tych kategoriach, a zatem podlegają obowiązkowi udostępnienia przez posiadacza danych do wtórnego wykorzystywania zgodnie z przepisami rozdziału IV wniosku.

80. Obowiązkowa dostępność elektronicznych danych dotyczących zdrowia generowanych przez wyroby medyczne, aplikacje wspierające dobrostan lub aplikacje z zakresu e-zdrowia do celów wtórnego wykorzystywania musi być oceniana w świetle szybkiego rozwoju technologicznego w zakresie technologii mobilnych i technologii nasobnych oraz rosnącej popularności aplikacji i urządzeń do obsługi skwantyfikowanego „ja”, które umożliwiają obywatelom rejestrowanie wszelkiego rodzaju aspektów dotyczących osobowości, umysłu, ciała, wzorców zachowań i miejsca pobytu. Tego rodzaju przetwarzanie danych bezwzględnie zasługuje na znaczną uwagę, ponieważ trudno uznać, że dane dotyczące zdrowia są przetwarzane przez osoby, których dane dotyczą. Jednocześnie wiąże się to jednak z rzeczywistym zagrożeniem dla prywatności, zwłaszcza w przypadku gdy takie dane są przetwarzane w dodatkowych celach lub połączone z innymi danymi, lub przekazywane osobom trzecim. Takie rodzaje przetwarzania danych mogą stwarzać szczególne ryzyko, w tym ryzyko nierównego lub nieuczciwego traktowania w oparciu o dane dotyczące zakładanego lub faktycznego stanu zdrowia danej osoby, uzyskane na przykład za sprawą profilowania, z bardzo intymnych szczegółów dotyczących życia prywatnego tej osoby, niezależnie od tego, czy wnioski dotyczące jej stanu zdrowia są prawidłowe. Ryzyko to może być również związane z wiarygodnością i prawidłowością danych generowanych przez wyroby medyczne, aplikacje wspierające dobrostan lub inne aplikacje z zakresu e-zdrowia. W tym kontekście EROD i EIOD przyznają, że w art. 33 ust. 3 podjęto próbę określenia, jakie dane generowane przez wyroby medyczne, aplikacje wspierające dobrostan lub inne aplikacje z zakresu e-zdrowia są udostępniane do wtórnego wykorzystywania. EROD i EIOD podkreślają jednak, że nadal nie jest jasne, jakiego rodzaju dane należą do tej kategorii, lub kto miałby oceniać ich ważność i jakość po wprowadzeniu ich przez osoby fizyczne do ich własnych elektronicznych dokumentacji medycznych zgodnie z art. 3 ust. 6 i art. 33 ust. 1 lit. a) wniosku lub po ich bezpośrednim udostępnieniu przez posiadaczy danych zgodnie z art. 33 ust. 1 lit. f) i n) wniosku.
81. W związku z tym EROD i EIOD zalecają wyłączenie z zakresu rozdziału IV wniosku aplikacji wspierających dobrostan i innych aplikacji z zakresu e-zdrowia. EROD i EIOD podkreślają, że jeżeli dane zostaną uwzględnione w zakresie rozdziału IV, użytkownicy muszą zachować swobodę decydowania, czy i które z ich danych osobowych wygenerowanych przez aplikację wspierającą dobrostan i inne

²⁶ Zob. art. 3 ust. 6 i 33 ust. 1 lit. a) wniosku.

²⁷ Zob. art. 33 ust. 1 lit. f) i n) wniosku.

aplikacje z zakresu e-zdrowia – niezależnie od faktu, że zostały one umieszczone w ich własnych elektronicznych dokumentacjach medycznych – będą udostępniane innym odbiorcom i dalej przetwarzane do celów wtórnego wykorzystywania. Dlatego EROD i EIOD zalecają zmianę wniosku w celu zapewnienia, aby osoby, których dane dotyczą, były odpowiednio informowane o dostępnych dla nich wyborach w odniesieniu do potencjalnego dalszego wykorzystania ich elektronicznych danych dotyczących zdrowia, w tym danych generowanych przez aplikacje wspierające dobrostan i inne aplikacje z zakresu e-zdrowia. Po drugie, szczegółowe warunki dalszego przetwarzania takich danych osobowych muszą być jasno określone zgodnie z przepisami o ochronie danych, a także należy ustanowić odpowiednie mechanizmy zapewniające poszanowanie woli osób, których dane dotyczą, w odniesieniu do dalszego przetwarzania ich danych osobowych dotyczących zdrowia generowanych przez aplikacje wspierające dobrostan i inne aplikacje z zakresu e-zdrowia.

7 WTÓRNE WYKORZYSTYWANIE ELEKTRONICZNYCH DANYCH DOTYCZĄCYCH ZDROWIA (ROZDZIAŁ IV)

82. EIOD i EIOD dostrzegają, że celem rozdziału IV wniosku jest ułatwienie wtórnego wykorzystywania elektronicznych danych dotyczących zdrowia, i z zadowoleniem przyjmują fakt, że takie wtórne wykorzystywanie elektronicznych danych dotyczących zdrowia może przynieść znaczne korzyści dla dobra publicznego. EROD i EIOD są jednak zdania, że takie dalsze czynności przetwarzania nie są pozbawione ryzyka dla praw i wolności osób, których dane dotyczą.
83. EROD i EIOD odnotowują, zgodnie z motywem 37 wniosku, że „[...] rozporządzenie stanowi podstawę prawną – zgodnie z art. 9 ust. 2 lit. g), h), i) oraz j) rozporządzenia (UE) 2016/679 – wtórnego wykorzystywania danych dotyczących zdrowia, poprzez ustanowienie zabezpieczeń dotyczących przetwarzania do celów zgodnych z prawem, godnego zaufania zarządzania w zakresie zapewniania dostępu do danych dotyczących zdrowia (za pośrednictwem organów ds. dostępu do danych dotyczących zdrowia) i przetwarzania danych w bezpiecznym środowisku, a także funkcji przetwarzania danych określonych w zezwoleniu na dostęp do danych.” W tym samym motywie stwierdza się w tym kontekście, że osoba składająca wniosek o udostępnienie danych wykazuje podstawę prawną zgodnie z art. 6 RODO, w oparciu o którą można złożyć wniosek o dostęp do danych w świetle wniosku, co niekoniecznie znajduje odzwierciedlenie w części normatywnej wniosku. Z drugiej strony EROD i EIOD zauważają, że art. 34 ust. 1 wniosku zawiera wykaz celów, w których elektroniczne dane dotyczące zdrowia mogą być przetwarzane na potrzeby wtórnego wykorzystywania, które obejmują między innymi badania naukowe dotyczące sektorów ochrony zdrowia lub opieki zdrowotnej.
84. EROD i EIOD zgłaszają w związku z tym trzy główne obawy.
85. **Po pierwsze**, EROD i EIOD zauważają brak właściwego określenia celów wymienionych w art. 34 ust. 1 wniosku, w których dane dotyczące zdrowia elektronicznego mogą być dalej przetwarzane, a w szczególności wyrażają zaniepokojenie w odniesieniu do art. 34 ust. 1 lit. f) i g) wniosku, który może obejmować wszelkie formy „działa[ń] w zakresie rozwoju i innowacji w odniesieniu do produktów i usług przyczyniających się do ochrony zdrowia publicznego lub zabezpieczenia społecznego” lub „działa[ń] w zakresie trenowania, testowania i oceny algorytmów, w tym w wyrobach medycznych, systemach sztucznej inteligencji i aplikacjach z zakresu e-zdrowia, przyczyniających się do ochrony zdrowia publicznego lub zabezpieczenia społecznego”. EROD i EIOD zdecydowanie zalecają, aby we wniosku dokładniej określić te cele i ustalić, kiedy istnieje

wystarczający związek ze zdrowiem publicznym lub zabezpieczeniem społecznym, aby zapewnić równowagę z odpowiednim uwzględnieniem celów wniosku oraz ochrony danych osobowych osób, których dane dotyczą, których dotyczy przetwarzanie.

86. **Po drugie**, w świetle powyższych uwag i pomimo sformułowań zawartych w motywie 37 wniosku EROD i EIOD uważają, że wniosek wymaga dalszych usprawnień w celu zapewnienia zgodności z art. 9 RODO.
87. Cele, w których elektroniczne dane dotyczące zdrowia mogą być przetwarzane na potrzeby wtórnego wykorzystywania na podstawie art. 34 ust. 1 wniosku obejmują bowiem kilka rodzajów wtórnego wykorzystywania, które wchodziłyby w zakres poszczególnych kategorii podstaw wyjątku przewidzianych w art. 9 ust. 2 RODO. EROD i EIOD uważają jednak, że nie znajduje to odzwierciedlenia w kryteriach, zgodnie z którymi organy ds. dostępu do danych dotyczących zdrowia powinny oceniać zastosowania danych i podejmować decyzje w ich sprawie (art. 45 wniosku) w celu wydania zezwolenia na dostęp do danych (art. 46 wniosku). EROD i EIOD podkreślają w tym względzie, że odnośne kryteria przewidziane w art. 46 wniosku ograniczają się do przepisów i zasad w nim przewidzianych i nie zapewniają jasności co do tego, w jaki sposób przepisy te odnoszą się do zasad i przepisów przewidzianych w RODO, w szczególności do art. 9 ust. 2 RODO.
88. Ponadto EROD i EIOD dążą do szczegółowego wyjaśnienia, w jaki sposób i w jakich przypadkach art. 9 ust. 2 lit. j) RODO miałyby zastosowanie w odniesieniu do przetwarzania danych dotyczących zdrowia „do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych” (na podstawie prawa Unii lub prawa państwa członkowskiego) oraz „odpowiednich zabezpieczeń” wymaganych na mocy art. 89 ust. 1 RODO.
89. **Po trzecie**, EROD i EIOD rozważają, w jaki sposób ten interpretowany na mocy prawa Unii wyjątek od art. 9 ust. 2 RODO można pogodzić z art. 9 ust. 4 RODO oraz możliwość wprowadzenia przez prawo państwa członkowskiego dalszych warunków, w tym ograniczeń w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia. EROD i EIOD są w tym względzie zdania, że we wniosku można by wyjaśnić, w jaki sposób wynikający z wniosku wyjątek od art. 9 ust. 1 RODO, który nie został jeszcze wyraźnie określony w żadnym z przepisów wniosku służy pogodzeniu ze wszystkimi poszczególnymi przepisami krajowymi państw członkowskich.
90. W związku z tym **EROD i EIOD wzywają, aby wniosek zapewniał pełną zgodność z art. 9 ust. 2 RODO, w szczególności w odniesieniu do jego stosowania do celów wymienionych w art. 34 ust. 1 lit. f) i g) wniosku**. Ponadto EROD i EIOD zalecają również odpowiednią zmianę art. 46 wniosku, aby właściwie uwzględnić i odzwierciedlić różnice w celach i wymogach w zakresie wtórnego wykorzystywania elektronicznych danych dotyczących zdrowia.
91. W odniesieniu do **minimalnych kategorii elektronicznych danych dotyczących zdrowia do celów wtórnego wykorzystywania** EROD i EIOD zauważają, że na mocy art. 33 ust. 1 wniosku ustanawia się obowiązek prawny, zgodnie z którym posiadacze danych udostępniają – na mocy prawa Unii – określone kategorie elektronicznych danych dotyczących zdrowia do wtórnego wykorzystywania. EROD i EIOD zauważają, że w art. 41 ust. 1 wniosku wskazano, że ten (nowy) obowiązek prawny uzupełnia wszelkie inne zobowiązania prawne (już) przewidziane w innych przepisach unijnych lub krajowych wdrażających prawo Unii. Jak wskazano w motywie 37 wniosku, EROD i EIOD zauważają, że art. 33 ust. 1 wniosku służyłby jako podstawa prawna zgodnie z art. 6 ust. 1 lit. c) RODO i przewidywałby również wyjątek od zawartego w art. 9 ust. 1 RODO zakazu przetwarzania (udostępniania i dostarczania) przez posiadacza danych elektronicznych danych osobowych dotyczących zdrowia. EROD i EIOD przyznają w tym względzie, że chociaż taki obowiązek prawny

spoczywający na posiadaczach danych – co do zasady – wpisuje się w system RODO, może zarazem prowadzić do braku pewności prawa.

92. W tym względzie art. 33 ust. 5 wniosku stanowi, że „[j]eżeli prawo krajowe wymaga zgody osoby fizycznej, organy ds. dostępu do danych dotyczących zdrowia opierają się na obowiązkach określonych w niniejszym rozdziale w celu zapewnienia dostępu do elektronicznych danych dotyczących zdrowia”. Przede wszystkim EROD i EIOD są zdania, że nie jest jasne, o jakiego rodzaju „wymogach dotyczących zgody” zawartych w prawie krajowym jest mowa w tym przepisie. W szczególności **EROD i EIOD zwracają uwagę na brak jasności co do tego, na jakim etapie procedury przewidzianej we wniosku w odniesieniu do wtórnego wykorzystywania elektronicznych danych dotyczących zdrowia organy ds. dostępu do danych dotyczących zdrowia mogą nie uwzględniać takich wymogów określonych w prawie krajowym**, w szczególności gdy wchodzi one w zakres art. 9 ust. 4 RODO. Ponadto EROD i EIOD zalecają dalsze wyjaśnienie i doprecyzowanie w odniesieniu do art. 46 ust. 6 lit. f) wniosku, w którym przewidziano, że organ ds. dostępu do danych dotyczących zdrowia może wprowadzić „szczegółowe warunki dotyczące udzielonego zezwolenia na dostęp do danych”.
93. W art. 36 wniosku przewidziano **ustanowienie organów ds. dostępu do danych dotyczących zdrowia**. EROD i EIOD podkreślają w tym względzie, że odpowiedzialność organu ds. dostępu do danych dotyczących zdrowia za ocenę podstawy prawnej zaproponowanej przez użytkownika danych będzie wymagać dostępności odpowiedniej fachowej wiedzy prawnej w tym organie. EROD i EIOD zauważają, że jak dotąd nie zostało to wyraźnie określone w art. 36 wniosku. EROD i EIOD podkreślają jednak, że ocena podstawy prawnej przez organ ds. dostępu do danych dotyczących zdrowia może – zawsze – zostać poddana kontroli i – w razie potrzeby – zostać unieważniona przez odpowiedni organ ochrony danych. EROD i EIOD wzywają w tym celu do doprecyzowania wzajemnych zależności między rolą organu ds. dostępu do danych dotyczących zdrowia a rolą odpowiedniego organem ochrony danych w kontekście wszelkich kwestii związanych z ochroną danych.
94. Potrzeba wyjaśnienia związku między wnioskiem a prawodawstwem państw członkowskich znajduje dalsze odzwierciedlenie w kontekście **wniosek o wydanie zezwolenia na dostęp do danych w kontekście transgranicznego dostępu do elektronicznych danych osobowych dotyczących zdrowia do celów wtórnego wykorzystywania** (sekcja 4 art. 52–54 wniosku). EROD i EIOD zauważają, że chociaż wniosek ma na celu ułatwienie transgranicznego wtórnego wykorzystywania danych za sprawą ustanowienia „krajowych punktów kontaktowych” i infrastruktury transgranicznej (Dane zdrowotne @ UE), użytkownicy danych prawdopodobnie nadal będą musieli przedkładać wnioski do odpowiednich organów ds. dostępu do danych dotyczących zdrowia w każdym państwie członkowskim. Zgodnie z wiedzą EROD i EIOD art. 45 ust. 3 wniosku przewiduje bowiem jedynie ograniczoną koordynację między zaangażowanymi organami ds. dostępu do danych dotyczących zdrowia do celów uzyskania zezwolenia na dostęp do danych. EROD i EIOD są jednak zdania, że wniosek nie zawiera odpowiednich wyjaśnień co do konkretnych przepisów krajowych, które będą miały zastosowanie w kontekście zezwoleń na transgraniczny dostęp do danych (prawa odpowiednich organów ds. dostępu do danych dotyczących zdrowia lub prawa osoby wnioskującej o udostępnienie danych), w tym podstawy prawnej, która będzie musiała zostać określona (przez osobę wnioskującą) i oceniona (przez organ ds. dostępu do danych dotyczących zdrowia). Ponadto należy również zauważyć w tym względzie, że zarówno po stronie organu ds. dostępu do danych dotyczących zdrowia, jak i po stronie użytkownika danych mogą występować (znaczące) luki w wiedzy fachowej niezbędnej do przewyciężenia problemów z identyfikacją i oceną różnic w (wymogach, które należy spełnić, przewidzianych) w przepisach państwa członkowskiego dotyczących (takiej) podstawy prawnej.

95. EROD i EIOD zauważają, że w art. 38 ust. 2 wniosku przewidziano, że organy ds. dostępu do danych dotyczących zdrowia nie mają obowiązku przekazywania szczegółowych informacji, o których mowa w art. 14 RODO, każdej osobie fizycznej w odniesieniu do wykorzystania jej danych na potrzeby projektów objętych obowiązkiem posiadania zezwolenia na dostęp do danych. EROD i EIOD są w tym względzie zdania, że wprowadzone wyłączenie może mieć niezamierzone konsekwencje dla podstawowych praw i wolności osób, których dane dotyczą, ze względu na brak wskazania konkretnych warunków, w których takie wyłączenie miałoby zastosowanie.
96. Ponadto EROD i EIOD przypominają o znaczeniu obowiązków w zakresie przejrzystości wobec osób, których dane dotyczą, i wzywają współprawodawcę do określenia konkretnych sytuacji w celu zapewnienia, aby organy ds. dostępu do danych dotyczących zdrowia nie mogły powoływać się na takie przepisy systemowo. W związku z powyższym EROD i EIOD zalecają odpowiednią zmianę tego przepisu, biorąc pod uwagę, że wymogi określone w art. 14 RODO nie mogą być systematycznie uchylane bez adekwatnej i stosownej oceny i uzasadnienia potrzeby powołania się na takie wyłączenie²⁸. Jeżeli ograniczenie prawa do informacji zostanie utrzymane, EROD i EIOD zwracają uwagę współprawodawców na potrzebę rozważenia warunków przewidzianych w art. 23 RODO.
97. W art. 40 wniosku przewidziano i określono altruistyczne podejście do danych w kontekście zdrowia. EROD i EIOD są w tym względzie zdania, że przepis ten jest niejasny, w szczególności w odniesieniu do jego związku z odpowiednim przepisem wprowadzonym w akcie w sprawie zarządzania danymi. EROD i EIOD zalecają w związku z tym odpowiednie wyjaśnienie tego przepisu.
98. EROD i EIOD z zadowoleniem przyjmują przepis zawarty w art. 44 ust. 3 wniosku, który stanowi, że w przypadku gdy organy ds. dostępu do danych dotyczących zdrowia muszą zapewnić dostęp do danych w formie spseudonimizowanym, użytkownicy danych nie mogą deanonimizować elektronicznych danych dotyczących zdrowia przekazanych im w takim formacie (informacje umożliwiające odwrócenie pseudonimizacji są dostępne wyłącznie dla organów ds. dostępu do danych dotyczących zdrowia). Ponadto EROD i EIOD z zadowoleniem przyjmują fakt, że ten sam przepis wniosku stanowi, że w przypadku nieprzestrzegania przez użytkownika danych środków zastosowanych przez organ ds. dostępu do danych dotyczących zdrowia w celu zapewnienia pseudonimizacji ten pierwszy podlega odpowiednim karom.
99. Ponadto art. 48 wniosku stanowi, na zasadzie odstępstwa od art. 46 wniosku zezwolenie na dostęp do danych nie jest wymagane do uzyskania dostępu do elektronicznych danych dotyczących zdrowia na podstawie tego samego artykułu przez organy sektora publicznego oraz instytucje, organy, urzędy i agencje Unii. EROD i EIOD uważają, że również w tym przypadku powinien istnieć wymóg uzyskania zezwolenia, co umożliwiłoby sprawdzenie, czy spełnione zostały wszystkie stosowne wymogi, w tym kryteria zgodności z prawem i konieczności. Ponadto EROD i EIOD uważają taki wymóg za istotny z punktu widzenia propagowania przejrzystości, ponieważ we wniosku przewidziano, że organy ds. dostępu do danych dotyczących zdrowia przekazują ogółowi społeczeństwa informacje na temat wszystkich zezwoleń na dostęp do danych wydanych zgodnie z art. 46.

8 DZIAŁANIA DODATKOWE (ROZDZIAŁ V)

²⁸ Zob. również pkt 25 powyżej.

8.1 Przechowywanie elektronicznych danych osobowych dotyczących zdrowia w UE oraz zgodność międzynarodowego przekazywania danych z rozdziałem V RODO

100. Rozdział V wniosku ma na celu przedstawienie innych środków promujących budowanie zdolności przez państwa członkowskie, które będą towarzyszyć rozwojowi europejskiej przestrzeni danych dotyczących zdrowia. Ponadto rozdział ten reguluje międzynarodowy dostęp i przekazywanie w przypadku elektronicznych danych *nieosobowych* (dotyczących zdrowia), a także międzynarodowy dostęp i przekazywanie w przypadku elektronicznych danych *osobowych* dotyczących zdrowia.
101. Jeżeli chodzi o międzynarodowy dostęp do elektronicznych danych *osobowych* dotyczących zdrowia i ich przekazywanie w art. 63 wniosku stwierdzono, że państwa członkowskie „mogą utrzymać lub wprowadzić dalsze warunki, w tym ograniczenia, zgodnie z art. 9 ust. 4 rozporządzenia (UE) 2016/679 i na warunkach w nim określonych”.
102. **Po pierwsze**, EROD i EIOD pragną przypomnieć, że w wyroku w sprawie Digital Rights Ireland TSUE uznał, że brak wymogu zatrzymywania danych w UE oznacza, że nie można uznać, że „[...] dyrektywa ta w pełni gwarantuje kontrolę poszanowania wymogów ochrony i bezpieczeństwa, o których mowa w dwóch poprzednich punktach, przez niezależny organ, czego wyraźnie wymaga art. 8 ust. 3 karty [...]. Tymczasem kontrola taka, dokonywana na podstawie prawa Unii, stanowi zasadniczy element poszanowania ochrony osób w odniesieniu do przetwarzania danych osobowych”²⁹. Innymi słowy, TSUE wyraźnie orzekł w przedmiotowej sprawie, że kontrola poszanowania wymogów ochrony i bezpieczeństwa przez niezależny organ nadzorczy nie może być w pełni zapewniona w przypadku braku wymogu zatrzymywania odnośnych danych w UE. Brak wymogu zatrzymywania danych w UE był jednym z powodów, które skłoniły TSUE do stwierdzenia, że prawodawca Unii przekroczył granice, które wyznacza poszanowanie zasady proporcjonalności na gruncie art. 7, 8 i art. 52 ust. 1 karty³⁰.
103. Konieczność nałożenia wymogu przechowywania danych osobowych w UE w pewnych szczególnych przypadkach została następnie potwierdzona i uzupełniona w wyroku w sprawie Tele 2, w którym TSUE uznał, że „[u]względniając ilość zatrzymywanych danych, ich newralgiczny charakter oraz prawdopodobieństwo bezprawnego uzyskania dostępu do nich, dostawcy usług łączności elektronicznej, aby zapewnić integralność i poufność tych danych, muszą zapewnić za pomocą środków technicznych i organizacyjnych szczególnie wysoki poziom ochrony i bezpieczeństwa. W szczególności uregulowanie krajowe powinno ustanawiać zarówno wymóg przechowywania danych na terytorium Unii, jak też nieodwracalnego ich niszczenia po upływie okresu ich przechowywania.” (podkreślenia dodane)³¹. Ponownie TSUE podkreślił, że aby zagwarantować

²⁹ Wyrok Trybunału (wielka izba) z dnia 8 kwietnia 2014 r., Digital Rights Ireland Ltd, sprawy połączone C-293/12 i C-594/12; pkt 68. Zob. też opinia rzecznika generalnego Cruza Villalóna przedstawiona 12 grudnia 2013 r. w tej samej sprawie w pkt 78 i 79, w której stwierdzono, że brak przepisu ustanawiającego obowiązek „przechowywania przez nich samych danych, które mają być zatrzymywane na terytorium państwa członkowskiego, podlegających jurysdykcji państwa członkowskiego”, „zwiększa ryzyko wykorzystania niezgodnie z wymogami wynikającymi z prawa do poszanowania życia prywatnego” i „znacznie zwiększa ryzyko, że dane mogą być dostępne lub ujawnione z naruszeniem tej regulacji”.

³⁰ Wyrok Trybunału (wielka izba) z dnia 8 kwietnia 2014 r., Digital Rights Ireland Ltd, sprawy połączone C-293/12 i C-594/12; pkt 69.

³¹ Wyrok Trybunału (wielka izba) z dnia 21 grudnia 2016 r., Tele2 Sverige AB/Post- och telestyrelsen i Secretary of State for the Home Department/Tom Watson i in., sprawy połączone C-203/15 i C-698/15, pkt 122. Zob. również opinia rzecznika generalnego Saugmandsgaarda Øe przedstawiona w dniu 19 lipca 2016 r., Tele2 Sverige

niezbędny poziom bezpieczeństwa i ochrony rzeczonych danych, odpowiednie przepisy **muszą** wymagać zatrzymywania danych w UE.

104. EROD i EIOD uważają, że ustalenia poczynione przez Trybunał w tych dwóch przełomowych wyrokach są również istotne w kontekście wniosku, ponieważ będą miały zastosowanie do (i) przetwarzania dużej ilości danych osobowych, (ii) o wysoce wrażliwym charakterze oraz (iii) w przypadku których nie istnieje obiektywny element pozwalający stwierdzić, że ryzyko bezprawnego dostępu jest mniejsze niż ryzyko stwierdzone w kontekście wyroków, o których mowa powyżej.³² W szczególności EROD i EIOD podkreślają, że prawdopodobieństwo, że ustalenie Trybunału będzie miało zastosowanie do rzeczonych danych, jest tym większe, jeśli wziąć pod uwagę, że dane dotyczące zdrowia prawdopodobnie zostaną uznane za jeszcze bardziej wrażliwe niż dane telekomunikacyjne (tj. dane omawiane w dwóch wyrokach, o których mowa powyżej).
105. EROD i EIOD dzielą w tym kontekście obawy Trybunału dotyczące potrzeby ograniczenia ryzyka bezprawnego dostępu i nieskutecznego nadzoru w odniesieniu do niektórych rodzajów danych i niektórych rodzajów operacji przetwarzania. EROD i EIOD zauważają w szczególności, że w przypadku gdy infrastruktura przetwarzania znajduje się w państwach członkowskich spoza UE/EOG, realizowana przez unijny organ nadzorczy ds. ochrony danych kontrola przestrzegania unijnych przepisów o ochronie danych może nie zawsze być w pełni zapewniona.
106. Ponadto EROD i EIOD zauważają, że Komisja zaproponowała niedawno wymogi dotyczące przechowywania danych w innym kontekście: W art. 17 ust. 1 lit. c) wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach Unii przewidziano, że „przechowywanie i przetwarzanie szczególnie chronionych informacji jawnych odbywa się w Unii”³³. Ogólnie rzecz biorąc, EROD i EIOD zauważają, że prawo UE zawiera już kilka przykładów istniejących aktów prawnych nakładających obowiązek przechowywania danych osobowych w UE, które to akty prawne zazwyczaj jeszcze bardziej ograniczają możliwość przekazywania danych³⁴. EROD i EIOD stwierdzają zatem, że

AB/Post- och telestyrelsen i Secretary of State for the Home Department/Tom Watson i in., sprawy połączone C-203/15 i C-698/15, pkt 239–241.

³² EROD i EIOD za uważają, że ryzyko bezprawnego dostępu jest tak duże, że skłoniło Komisję do wprowadzenia specjalnego przepisu dotyczącego danych nieosobowych (art. 62 wniosku).

³³ Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie bezpieczeństwa i informacji w instytucjach, organach, urzędach i agencjach Unii;

COM(2022) 119 final; <https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:52022PC0119>

³⁴ Zob. art. 6 ust. 8 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania: „Przechowywanie, przetwarzanie i analiza danych PNR przez JIP odbywa się wyłącznie w bezpiecznym miejscu lub bezpiecznych miejscach na terytorium państw członkowskich”; art. 3 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS); art. 41 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiającego system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określającego warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniającego konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011; art. 39 rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II).

w niektórych szczególnych sytuacjach prawo UE wymaga, aby dane były przechowywane w UE w celu ograniczenia ryzyka bezprawnego dostępu i zapewnienia skutecznego nadzoru.

107. **Po drugie**, EROD i EIOD zauważają, że w art. 62 wniosku dotyczącym dostępu międzynarodowego do elektronicznych danych nieosobowych dotyczących zdrowia i ich przekazywania odniesiono się w kilku przypadkach do elektronicznych danych nieosobowych dotyczących zdrowia „przechowywanych w UE”, co wydaje się wskazywać na ogólne założenie, że ta kategoria danych musiałaby być przechowywana w UE. EIOD i EROD uważają, że należy przyjąć takie samo podejście w odniesieniu do danych osobowych wchodzących w zakres wniosku, ponieważ trudno byłoby uzasadnić wymóg przechowywania elektronicznych danych nieosobowych dotyczących zdrowia w UE, ale brak takiego samego wymogu w odniesieniu do elektronicznych danych osobowych dotyczących zdrowia.
108. **Po trzecie**, EROD i EIOD pragną wyjaśnić w tym kontekście, że obowiązek przechowywania danych osobowych w UE nie wyklucza przekazywania elektronicznych danych osobowych dotyczących zdrowia do państw trzecich lub organizacji międzynarodowych. Możliwe jest bowiem pogodzenie ogólnego wymogu przechowywania danych osobowych w UE z zezwoleniem na konkretne przekazywanie danych zgodnie z rozdziałem V RODO (np. w kontekście badań naukowych, wydatków na opiekę, współpracy międzynarodowej). W związku z tym EROD i EIOD uważają, że obowiązek przechowywania danych w UE byłby proporcjonalny i nie wykraczałby poza to, co jest konieczne do osiągnięcia zamierzonego celu, jakim jest ustanowienie dodatkowego zabezpieczenia w celu ograniczenia ryzyka bezprawnego dostępu do odnośnych danych i nieskutecznego nadzoru nad nimi ze względu na ich wysoce wrażliwy charakter.
109. **Po czwarte**, EROD i EIOD zauważają również, że art. 63 wniosku stanowi, że państwa członkowskie mogą utrzymać lub wprowadzić dalsze warunki, w tym ograniczenia, zgodnie z art. 9 ust. 4 RODO i na warunkach w nim określonych. Takie ograniczenia nałożone na szczeblu krajowym mogą obejmować obowiązek przechowywania danych w UE. EROD i EIOD zwracają uwagę na fakt, że taki obowiązek ma już zastosowanie w kilku państwach członkowskich, i uznają za prawdopodobne, że kilka państw członkowskich nałożyłoby lub nadal nakładałoby podobne obowiązki, gdyby kwestia ta nie została zharmonizowana na szczeblu UE.
110. W związku z powyższym EROD i EIOD uważają, że zasadnicze znaczenie ma unikanie w całej UE niespójnego i rozdrobnionego podejścia, które doprowadziłoby do różnego stopnia ochrony osób, których dane dotyczą, co byłoby sprzeczne z jednym z zasadniczych celów RODO³⁵. EROD i EIOD uważają zatem, że dodatkowe obowiązki, w tym przechowywanie elektronicznych danych osobowych dotyczących zdrowia w UE, należy w jak największym stopniu uwzględnić na szczeblu UE, tj. we wniosku, w celu zapewnienia jednolitego wysokiego poziomu ochrony osób, których dane dotyczą, w całej UE, a także w celu zapewnienia właściwego funkcjonowania rynku wewnętrznego, zgodnie z art. 114 TFUE, na którym opiera się wniosek.
111. Z powyższych powodów i z należyтым uwzględnieniem wysoce wrażliwego charakteru rzeczonych danych osobowych **EROD i EIOD uważają, że w art. 63 wniosku należy nałożyć na przetwarzających**

³⁵ Zob. motyw 53 RODO odnoszący się do art. 9 ust. 4 RODO: Warunki te nie powinny jednak utrudniać swobodnego przepływu danych osobowych w Unii, jeżeli odnoszą się do transgranicznego przetwarzania takich danych.

elektroniczne dane osobowe dotyczące zdrowia administratorów i podmioty przetwarzające mające jednostkę organizacyjną w UE w zakresie przewidzianym we wniosku obowiązek przechowywania tych danych w UE. Jak wyjaśniono powyżej, taki wymóg przechowywania elektronicznych danych osobowych dotyczących zdrowia w UE powinien **pozostawać bez uszczerbku dla możliwości przekazywania elektronicznych danych osobowych dotyczących zdrowia zgodnie z rozdziałem V RODO.**³⁶ EROD i EIOD zalecają również przypomnienie w preambule, że przetwarzający elektroniczne dane osobowe dotyczące zdrowia administratorzy i podmioty przetwarzające nadal podlegają przepisom art. 48 RODO dotyczącym przekazywania lub ujawniania niedozwolonych na mocy prawa Unii i powinni przestrzegać tego przepisu w przypadku wniosku o udzielenie dostępu złożonego przez państwo trzecie³⁷.

8.2 Zamówienia publiczne i finansowanie unijne

112. EROD i EIOD odnotowują, że art. 60 wniosku odnosi się do kwestii dodatkowych wymogów dotyczących zamówień publicznych i finansowania unijnego. EROD i EIOD uważają, że powyższe zalecenia (dotyczące przechowywania danych w UE i zgodności z rozdziałem 5, a w szczególności z art. 48 RODO) zostałyby najlepiej wdrożone, gdyby przewidziano ich wbudowanie na wczesnym etapie procedury zamówienia publicznego³⁸ lub usług finansowania świadczonych przez przetwarzających dane osobowe dotyczące zdrowia administratorów i podmioty przetwarzające mających jednostkę organizacyjną w UE.
113. W związku z tym **EROD i EIOD zalecają, aby w art. 60 wniosku określić również, jako warunek zamawiania lub finansowania usług świadczonych przez przetwarzających elektroniczne dane osobowe dotyczące zdrowia administratorów i podmioty przetwarzające mające jednostkę organizacyjną w UE, że tacy administratorzy i podmioty przetwarzające (i) będą przechowywać te dane w UE oraz (ii) należyte wykazali, że nie podlegają przepisom państwa trzeciego sprzecznym z unijnymi przepisami o ochronie danych.**

8.3 Krajowe punkty kontaktowe państwa trzeciego lub systemy ustanowione na szczeblu międzynarodowym

114. EROD i EIOD zauważają, że w art. 13 ust. 3 i art. 52 ust. 5 wniosku przewidziano możliwość uznania krajowych punktów kontaktowych państwa trzeciego lub systemów utworzonych na szczeblu międzynarodowym za zgodne z wymogami odpowiednio infrastruktury `MojeZdrowie@UE` (`MyHealth@EU`) i `DaneZdrowotne@UE` (`HealthData@EU`). EROD i EIOD przypominają, że

³⁶ Oraz przy założeniu spełnienia pozostałych warunków przewidzianych w RODO, w szczególności w art. 6 RODO dotyczącym obowiązku zapewnienia zgodności przetwarzania z prawem.

³⁷ Art. 48 RODO: „Wyrok sądu lub trybunału oraz decyzja organu administracyjnego państwa trzeciego wymagające od administratora lub podmiotu przetwarzającego przekazania lub ujawnienia danych osobowych mogą zostać uznane lub być egzekwowalne wyłącznie, gdy opierają się na umowie międzynarodowej, takiej jak umowa o wzajemnej pomocy prawnej, obowiązującej między wzywającym państwem trzecim a Unią lub państwem członkowskim, bez uszczerbku dla i innych podstaw przekazania na mocy niniejszego rozdziału.”

³⁸ Motyw 78 RODO stanowi w tym względzie, że „[z]asadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych”. Ponadto w motywie 77 dyrektywy 2014/24/UE w sprawie zamówień publicznych przewidziano, że „opracowując specyfikacje techniczne, instytucje zamawiające powinny uwzględniać wymogi wynikające z unijnego prawa w dziedzinie ochrony danych, zwłaszcza w odniesieniu do projektowania procesu przetwarzania danych osobowych (uwzględnienie ochrony danych już w fazie projektowania)”.

przekazywanie wynikające z podłączenia do infrastruktury MojeZdrowie@UE i DaneZdrowotne@UE oraz korzystania z nich powinno być zgodne z rozdziałem V RODO.

115. EROD i EIOD zauważają, że w art. 13 ust. 3 i art. 52 ust. 5 wniosku przewidziano możliwość uznania krajowych punktów kontaktowych państwa trzeciego lub systemów utworzonych na szczeblu międzynarodowym za zgodne z wymogami odpowiednio infrastruktury MojeZdrowie@UE i DaneZdrowotne@UE. EROD i EIOD przypominają, że przekazywanie wynikające z podłączenia do infrastruktury MojeZdrowie@UE i DaneZdrowotne@UE oraz korzystania z nich powinno być zgodne z rozdziałem V RODO.
116. W szczególności EROD i EIOD zauważają, że zarówno w art. 13 ust. 3, jak i art. 52 ust. 5 wniosku odniesiono się do kontroli zgodności, które Komisja ma przeprowadzić przed wydaniem aktu wykonawczego stanowiącego, że krajowy punkt kontaktowy państwa trzeciego lub system ustanowiony na szczeblu międzynarodowym spełnia wymogi infrastruktury MojeZdrowie@UE lub DaneZdrowotne@UE. EROD i EIOD zauważają również, że motyw 26 wniosku dotyczący infrastruktury MojeZdrowie@UE odnosi się do konieczności zapewnienia przez te kontrole „przestrzegania przez te krajowe punkty kontaktowe specyfikacji technicznej, przepisów o ochronie danych i innych wymogów [...]”. **EROD i EIOD zalecają w tym względzie bezpośrednie wyjaśnienie zarówno w art. 13 ust. 3, jak i w art. 52 ust. 5 wniosku, że kontrole zgodności powinny zapewniać przestrzeganie przepisów rozdziału V RODO, gdy krajowy punkt kontaktowy państwa trzeciego lub system ustanowiony na szczeblu międzynarodowym zostanie podłączony do infrastruktury MojeZdrowie@UE lub DaneZdrowotne@UE.**

9 ZARZĄDZANIE I KOORDYNACJA NA SZCZEBLU EUROPEJSKIM (ROZDZIAŁ VI)

117. EROD i EIOD odnotowują, że w art. 64 wniosku ustanawia się Radę ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia, organ koordynujący, którego celem jest ułatwienie współpracy i wymiany informacji między państwami członkowskimi. EROD i EIOD zauważają, że Rada ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia będzie składać się z przedstawicieli organów ds. e-zdrowia i organów ds. dostępu do danych dotyczących zdrowia ze wszystkich państw członkowskich oraz że **Radzie ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia będzie przewodniczyć Komisja.** EROD i EIOD zauważają, że zgodnie z wnioskiem przedstawiciele EROD i EIOD mogą być zapraszani na posiedzenia, podczas których omawiane są kwestie ochrony danych. **EROD i EIOD są zdania, że ich przedstawiciele powinni być stałymi członkami Rady ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia (a zatem nie tylko być potencjalnie zapraszani) i powinni uczestniczyć we wszystkich dyskusjach na temat kwestii ochrony danych osobowych, co zapewni spójną interpretację i stosowanie przepisów wprowadzonych we wniosku w odniesieniu do przepisów RODO.**
118. Ponadto w art. 65 ust. 1 wniosku określono zadania Rady ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia w zakresie pierwotnego wykorzystywania elektronicznych danych dotyczących zdrowia. EROD i EIOD zauważają, że Komisja będzie mogła wydawać pisemne opinie i prowadzić wymianę najlepszych praktyk w sprawach związanych z wdrażaniem wniosku, w szczególności w odniesieniu do przepisów zawartych w rozdziałach II i III wniosku (art. 65 ust. 1 lit. b) pkt (i)) oraz wszelkich aspektów pierwotnego wykorzystywania elektronicznych danych dotyczących zdrowia (art. 65 ust. 1 lit. b) pkt (iii)). Ponieważ w rozdziale II wniosku przewidziano prawa do ochrony danych

podobne do RODO (zob. pkt 28), EROD i EIOD uważają, że Rada ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia nie powinna mieć możliwości wydawania pisemnych opinii dotyczących kwestii związanych z prawami do ochrony danych. **EROD i EIOD podkreślają, że w przeciwnym razie wniosek może doprowadzić do rozbieżności w interpretacji lub stosowaniu praw do ochrony danych** określonych przez EROD i EIOD. EROD i EIOD zauważają ponadto, że przepis ten spowoduje niepewność prawa, co będzie również sprzeczne z celami wniosku w zakresie poprawy funkcjonowania rynku wewnętrznego poprzez **ustanowienie jednolitych ram prawnych** (motyw 1 wniosku). Ponadto w art. 65 ust. 2 wniosku określono zadania Rady ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia związane z wtórnym wykorzystywaniem elektronicznych danych dotyczących zdrowia. EROD i EIOD ponawiają ostrzeżenie dotyczące kompetencji Rady ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia w zakresie wydawania pisemnych opinii dotyczących kwestii związanych z prawami do ochrony danych w odniesieniu do wtórnego wykorzystywania elektronicznych danych dotyczących zdrowia.

119. Ponadto zgodnie z art. 65 ust. 1 lit. d) i art. 65 ust. 2 lit. d) wniosku EROD i EIOD zauważają, że Rada ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia będzie mogła prowadzić wymianę informacji dotyczących zagrożeń i incydentów związanych z ochroną danych oraz pierwotnym i wtórnym wykorzystaniem elektronicznych danych dotyczących zdrowia, oraz informacji dotyczących postępowania z tymi zagrożeniami i incydentami. **EROD i EIOD podkreślają po raz kolejny, że wniosek może doprowadzić do rozbieżności między EROD, EIOD i Radą ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia w odniesieniu do identyfikacji naruszeń ochrony danych lub postępowania w przypadku naruszeń**, ponieważ Rada ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia będzie mogła prowadzić wymianę informacji na temat sposobów postępowania z incydentami związanymi z ochroną danych. Ponadto występuje niejasność co do odbiorców informacji, które Rada ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia będzie udostępniać. Ogólnie rzecz biorąc, EROD i EIOD zalecają współprawodawcy określenie wzajemnych zależności między EROD, EIOD i Radą ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia w kwestiach ochrony danych, które powinny pozostać wyłączną kompetencją organów ochrony danych.
120. W odniesieniu do tego samego rozdziału EROD i EIOD zauważają, że art. 66 wniosku stanowi, że Komisja powołuje dwie podgrupy zajmujące się współadministracją infrastruktur transgranicznych `MojeZdrowie@UE` i `DaneZdrowotne@UE` (art. 12 i 52 wniosku). **EROD i EIOD zauważają, że zakres zadań grup ds. współadministracji nie jest jasno określony i że zadania te mogą pokrywać się z zadaniami Rady ds. Europejskiej Przestrzeni Danych Dotyczących Zdrowia** przewidzianymi w art. 65 wniosku. Mówiąc ogólniej, EROD i EIOD zalecają jasne określenie wzajemnych zależności między poszczególnymi organami, grupami i organizacjami, o których mowa we wniosku.
121. Ponadto EROD i EIOD odnotowują pewne niespójności między zadaniami podgrup a uprawnieniami Komisji do przyjmowania aktów wykonawczych lub delegowanych dotyczących tych samych zagadnień. Na przykład zgodnie z art. 52 ust. 13 wniosku Komisja może określić wymogi, specyfikacje techniczne, architekturę informatyczną infrastruktury `Dane zdrowotne @ UE` w drodze aktów wykonawczych, natomiast jedna z dwóch podgrup będzie również podejmować decyzje dotyczące rozwoju i eksploatacji tejże infrastruktury. **EROD i EIOD zalecają zatem, by wyjaśnić wzajemne zależności między Komisją a tymi podgrupami.**

10 PRZEKAZANIE UPRAWNIENÍ I KOMITET (ROZDZIAŁ VII)

122. W rozdziale VII wniosku nadano Komisji uprawnienie do przyjmowania aktów delegowanych w odniesieniu do kilku konkretnych aspektów uregulowanych we wniosku. EROD i EIOD zauważają w tym względzie, że niezależnie od zaangażowania państw członkowskich w proces decyzyjny, uprawnienie do podejmowania decyzji o zmianie lub rozszerzeniu niektórych z zasadniczych kwestii, o których mowa we wniosku, nadal pozostawia Komisji znaczny margines swobody w zakresie zmiany lub rozszerzenia zakresu tegoż wniosku w sposób, który mógłby mieć wpływ na prawa do ochrony danych i wyłączną kompetencję państw członkowskich w zakresie określania krajowych polityk w dziedzinie zdrowia.
123. EROD i EIOD uważają w szczególności, że art. 5 ust. 2 i art. 33 ust. 7 wniosku budzą obawy, ponieważ na ich podstawie Komisja jest uprawniona do zmiany wykazu priorytetowych kategorii elektronicznych danych dotyczących zdrowia, które mają być udostępniane i wymieniane między państwami członkowskimi do celów pierwotnego wykorzystywania, a także wykazu elektronicznych danych dotyczących zdrowia, z zastrzeżeniem obowiązkowej dostępności i dostępu osób trzecich do celów wtórnego wykorzystywania. Ponieważ wszelkie zmiany takich kategorii danych osobowych, w szczególności szczególnych kategorii danych, mogą wymagać ponownej oceny zagrożeń dla praw podstawowych i interesów osób, których sprawa dotyczy, kwestie te stanowią kwestie merytoryczne, które należy uznać za istotne elementy zgodnie z art. 290 TFUE.
124. W związku z tym EROD i EIOD uważają, że takie kwestie nie powinny być wyłączone z zakresu prawodawstwa, w ramach którego wszelkie ograniczenie praw podstawowych musi być wyraźnie motywowane potrzebą osiągnięcia niezbędnej przewidywalności instrumentu prawnego, natomiast w drodze przyjmowania aktów delegowanych można by dodawać jedynie bardziej szczegółowe pola danych (podkategorie danych) należące do już określonych kategorii danych ustanowionych w art. 5 ust. 1 i art. 33 ust. 1 wniosku.
125. Ponadto EROD i EIOD zauważają, że kryteria przewidziane w art. 5 ust. 2 lit. b) wniosku, które mają pomóc Komisji w podejmowaniu decyzji o dodaniu priorytetowych kategorii elektronicznych danych dotyczących zdrowia do wykazu ustanowionego w art. 5 ust. 1 wniosku, wydają się niejasne i powinny być ściślej określone³⁹.
126. Ponadto mimo że art. 67 ust. 4 wniosku stanowi, że Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie, którzy mogą posiadać pewną wiedzę fachową w kwestiach związanych z ochroną danych, EROD i EIOD zalecają wprowadzenie jasnego odniesienia do art. 42 rozporządzenia 2018/1725, aby wyraźnie zaznaczyć, że w stosownych przypadkach zasięga się opinii EIOD i EROD, gdy proponuje się takie akty delegowane.

11 RÓŻNE (ROZDZIAŁ VIII)

127. EROD i EIOD odnotowują, że w rozdziale VIII wniosku przypisano odpowiedzialność za ustanowienie kar mających zastosowanie w przypadku naruszeń rozporządzenia w sprawie państw członkowskich UE. EROD i EIOD uważają, że mogłoby to potencjalnie prowadzić do znacznej niepewności prawa w odniesieniu do właściwego egzekwowania ustanowionych we wniosku przepisów w różnych państwach członkowskich, ze względu na różnice w określaniu wysokości kar, które mogą być znaczne w zależności od państwa członkowskiego ze względu na znaczące różnice minimalnej i maksymalnej

³⁹ Zgodnie z najnowszymi informacjami kryteria te odnoszą się do „kategorii stosowanej w znacznej liczbie systemów elektronicznej dokumentacji medycznej stosowanych w państwach członkowskich”.

kwoty egzekwowanej. EROD i EIOD zauważają w tym względzie, że należy ustanowić zharmonizowane przepisy dotyczące kar, aby zapewnić sprawiedliwe i bezpieczne egzekwowanie przepisów, zwłaszcza w kontekście spraw transgranicznych.

128. Ponadto EROD i EIOD zauważają, że zgodnie z wcześniejszymi uwagami dotyczącymi certyfikacji własnej systemów elektronicznej dokumentacji medycznej okresy oceny i przeglądu ustanowione na mocy art. 70 wniosku są zbyt długie, aby zapewnić właściwe wdrożenie na czas.

W imieniu Europejskiego Inspektora Ochrony
Danych

Europejski Inspektor Ochrony Danych

(Wojciech Wiewiórowski)

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

¹ Nie jest na przykład jasne, czy producenci mogliby być zaliczeni do tej kategorii.