Oświadczenie nr 05/2021 dotyczące aktu w sprawie zarządzania danymi w świetle zmian legislacyjnych

Przyjęte 19 maja 2021 r.

Europejska Rada Ochrony Danych przyjęła następujące oświadczenie:

W dniu 9 marca 2021 r. EIOD i EROD przyjęli wspólną opinię w sprawie wniosku dotyczącego rozporządzenia w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi) [1], którą przedstawiono również Parlamentowi Europejskiemu na posiedzeniu Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w dniu 16 marca 2021 r.[2]

Europejska Rada Ochrony Danych uważnie śledzi prace współprawodawców nad tą ważną inicjatywą ustawodawczą, która – przypominamy – zawiera przepisy dotyczące przetwarzania danych, w tym danych osobowych, w kontekście ponownego wykorzystywania danych będących w posiadaniu organów sektora publicznego, „usług udostępniania danych" (obejmujących również tzw. brokerów danych) oraz w kontekście przetwarzania danych (w tym danych dotyczących zdrowia) przez organizacje zajmujące się „altruistycznym podejściem do danych".

Akt w sprawie zarządzania danymi poważnie wpłynie na prawa i wolności osób fizycznych i społeczeństwa obywatelskiego jako ogółu w całej UE. W większości przypadków przetwarzanie danych osobowych rzeczywiście stanowiłoby podstawową działalność wspomnianych podmiotów[3], a tym samym naruszałoby podstawowe prawa do prywatności i ochrony danych osobowych, zapisane w art. 7 i 8 Karty praw podstawowych Unii Europejskiej („Karta") oraz w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE"). Prawa te są nadrzędnym wyrazem wartości Unii Europejskiej.

[1] Wspólna opinia EROD-EIOD nr 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi), dostępna pod adresem: Wspólna opinia EROD-EIOD nr 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi) | Europejski Inspektor Ochrony Danych (europa.eu)

[2] Zob. projekt porządku dziennego posiedzenia pod tym adresem.

[3] Jeżeli nie jest to działalność wyłączna, na przykład w przypadku podmiotów świadczących usługi udostępniania danych na mocy art. 9 lit. b) aktu w sprawie zarządzania danymi, wyłącznie w odniesieniu do danych osobowych.

Bez solidnych zabezpieczeń w zakresie ochrony danych istnieje ryzyko, że gospodarka cyfrowa nie będzie miała zrównoważonego charakteru (lub też zaufanie do niej). Innymi słowy, ponowne wykorzystywanie, wymiana i dostępność danych mogą generować korzyści, ale także różnego rodzaju ryzyko szkód dla osób, których sprawa dotyczy, i społeczeństwa jako całości, wpływając na osoby fizyczne pod względem gospodarczym, politycznym i społecznym[4].

Aby zaradzić tym zagrożeniom i ograniczyć je, a także aby zwiększyć zaufanie osób fizycznych, należy wdrożyć zasady i zabezpieczenia w zakresie ochrony danych już na wczesnym etapie projektowania przetwarzania danych, zwłaszcza gdy przetwarzanie to dotyczy danych osobowych, które nie zostały uzyskane bezpośrednio od danej osoby fizycznej. Ponadto akt w sprawie zarządzania danymi musi być spójny nie tylko z RODO, ale również z innymi przepisami unijnymi i krajowymi, w szczególności z dyrektywą w sprawie otwartych danych[5], a tym samym spełniać założenia nadrzędnej zasady praworządności, oraz gwarantować pewność prawa organom administracji publicznej, osobom prawnym i osobom fizycznym, których sprawa dotyczy.

W uzasadnieniu aktu w sprawie zarządzania danymi stwierdza się, że *„szczególnie ważne jest zachowanie wzajemnej zależności z przepisami dotyczącymi danych osobowych. Dzięki ogólnemu rozporządzeniu o ochronie danych (RODO) i dyrektywie o prywatności i łączności elektronicznej UE ustanowiła solidne i godne zaufania ramy prawne w zakresie ochrony danych osobowych, będące standardem dla całego świata”*.[6]

Zapewnienie spójności między aktem w sprawie zarządzania danymi a dorobkiem prawnym UE w dziedzinie ochrony danych

Jak podkreślono we wspólnej opinii, **akt w sprawie zarządzania danymi zawiera jednak kilka istotnych niespójności z RODO, niezależnie od stwierdzenia zawartego w motywie, że pozostaje on „bez uszczerbku” dla RODO**[7].

Europejska Rada Ochrony Danych zauważa, że niespójności te nie zostały dotychczas uwzględnione w projekcie sprawozdania Komisji Przemysłu, Badań Naukowych i Energii (ITRE) z dnia 26 marca 2021 r.[8] Europejska Rada Ochrony Danych z zadowoleniem przyjmuje jednak fakt, że niektóre krytyczne kwestie poruszone we wspólnej opinii zostały omówione w tekście kompromisowym prezydencji Rady z dnia 30 marca 2021 r.[9]

[4] Przykładowo, w przypadku braku odpowiednich zabezpieczeń w zakresie ochrony danych, zgromadzone dane mogłyby zostać wykorzystane do stworzenia szczegółowych profili osób fizycznych i wykorzystane w sposób naruszający ich interesy (np. dyskryminacja cenowa lub manipulacja w kontekście kampanii wyborczych). Zob. przypis 60 na s. 31 wspólnej opinii w sprawie ryzyka wykorzystania danych osobowych do celów niepowiązanych.
[5] Dyrektywa (UE) 2019/1024 Parlamentu Europejskiego i Rady z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 172 z 26.6.2019, s. 56).
[6] Uzasadnienie, s. 1.
[7] Zob. sekcja 3.2 wspólnej opinii.
[8] Dostępne pod tym adresem.
[9] Dostępne pod tym adresem.

Aby zaradzić tym niespójnościom, wzywamy współprawodawców, by starannie rozważyli, co następuje[10]:

• Po pierwsze, należy wyjaśnić **„wzajemne zależności" między aktem w sprawie zarządzania danymi a RODO** na mocy art. 1 aktu w sprawie zarządzania danymi, uznając RODO za rozporządzenie dostarczające „elementów składowych" dla wszelkich solidnych i godnych zaufania ram prawnych.

• Po drugie, **definicje/terminologia** stosowane w akcie w sprawie zarządzania danymi wymagają integracji i zmian w celu dostosowania ich do RODO.

• Po trzecie, **w akcie w sprawie zarządzania danymi należy wyjaśnić bez żadnych dwuznaczności, że przetwarzanie danych osobowych musi zawsze opierać się na odpowiedniej podstawie prawnej na mocy art. 6 RODO**, a także na szczególnym wyjątku na mocy art. 9 w przypadku przetwarzania szczególnych kategorii danych osobowych.

• Po czwarte, jako warunek wstępny dla jasnych ram prawnych, **przepisy aktu w sprawie zarządzania danymi powinny określać, czy odnoszą się do danych nieosobowych, danych osobowych czy obu tych kategorii**, a także precyzować, że w przypadku **„mieszanych zestawów danych**" zastosowanie ma RODO[11].

• Po piąte, wymóg konstytucyjny (na mocy art.16 ust. 2 TFUE), zgodnie z którym **niezależne organy nadzorcze ustanowione na mocy RODO (organy ochrony danych) są „wyznaczonymi organami" właściwymi w zakresie ochrony danych osobowych i ułatwiania swobodnego przepływu danych osobowych**, powinien znaleźć odzwierciedlenie w akcie w sprawie zarządzania danymi.

Oznacza to, że **organy ochrony danych muszą być głównymi właściwymi organami w kontekście aktu w sprawie zarządzania danymi i w zakresie, w jakim dotyczy to danych osobowych**, z uwzględnieniem organów sektora publicznego, podmiotów ponownie wykorzystujących dane, dostawców usług w zakresie udostępniania danych, użytkowników danych, organizacji o altruistycznym podejściu do danych, jak również w zakresie opracowywania wytycznych dotyczących technologii służących zwiększaniu ochrony prywatności (PET) lub systemów zarządzania ochroną danych osobowych (PIMS) w celu wspierania odpowiedzialnych innowacji w zakresie danych.

Jak przypomniano we wspólnej opinii[12], „[w] zależności od swoich kompetencji i zadań na mocy RODO organy ochrony danych dysponują już szczególną wiedzą fachową w zakresie monitorowania zgodności przetwarzania danych, kontroli konkretnych czynności przetwarzania danych i udostępniana danych, oceny odpowiednich środków służących zapewnieniu wysokiego stopnia bezpieczeństwa w odniesieniu do przechowywania i przekazywania danych osobowych, a także w zakresie propagowania wśród administratorów i podmiotów przetwarzających wiedzy na temat ich

[10] Zob. sekcja 3.2 wspólnej opinii, gdzie te krytyczne aspekty zostały przywołane na początku jako punkty rozwinięte we wspólnej opinii.

[11] W przypadku, gdy **zbiory danych łączą w sobie zarówno dane osobowe, jak i nieosobowe**, w komunikacie Komisji do Parlamentu Europejskiego i Rady, *Wytyczne dotyczące rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej*, COM/2019/250 final, podkreślono, że „jeżeli część obejmująca dane nieosobowe i część obejmująca dane osobowe są ze sobą »nierozerwalnie związane«, prawa i obowiązki dotyczące ochrony danych wynikające z ogólnego rozporządzenia o ochronie danych mają w pełni zastosowanie do całego mieszanego zbioru danych również wtedy, gdy dane osobowe stanowią jedynie niewielką część zbioru danych".

[12] Zob. pkt 153 wspólnej opinii.

obowiązków związanych z przetwarzaniem danych osobowych". Oczywiście skuteczne wykonywanie nowych zadań w ramach aktu w sprawie zarządzania danymi, które mają być przede wszystkim powierzone niezależnym organom ochrony danych oraz Europejskiej Radzie Ochrony Danych, zgodnie z art. 16 ust. 2 TFUE, wymaga zapewnienia odpowiednich zasobów ludzkich, finansowych i informatycznych.

Europejska Rada Ochrony Danych z zadowoleniem przyjmuje w tym względzie dodatkowe brzmienie art. 1 ust. 3 kompromisowego tekstu Rady oraz konkretne odniesienie do uprawnień organów nadzorczych. W celu zapewnienia jasności i z uwagi na swobodę działania współprawodawców EROD zaleca wprowadzenie do tekstu prawnego aktu w sprawie zarządzania danymi (art. 1) następującego brzmienia art. 1 ust. 3 kompromisowej propozycji Rady (słowa pogrubione zostały dodane: „**kompetencji i**"):

„Prawo Unii i prawo krajowe o ochronie danych osobowych mają zastosowanie do wszelkich danych osobowych przetwarzanych w związku z niniejszym rozporządzeniem. W szczególności niniejsze rozporządzenie pozostaje bez uszczerbku dla rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE, w tym dla ***kompetencji i*** *uprawnień organów nadzorczych. W przypadku sprzeczności między przepisami niniejszego rozporządzenia a prawem Unii w zakresie ochrony danych osobowych, pierwszeństwo mają przepisy prawa Unii. Niniejsze rozporządzenie nie tworzy podstawy prawnej do przetwarzania danych osobowych*."

Ponadto EROD wzywa współprawodawców do dopilnowania, by jej ogólne zalecenie dotyczące wyznaczonych właściwych organów i zarządzania na szczeblu Unii znalazło odzwierciedlenie w ich odpowiednich stanowiskach w sprawie wniosku Komisji, a tym samym zostało wyraźnie uwzględnione w tekście prawnym aktu w sprawie zarządzania danymi.

W szczególności uwzględniając definicje zawarte w akcie w sprawie zarządzania danymi

We wspólnej opinii wskazano, że **należy stosować definicje przewidziane w RODO i nie należy ich w sposób dorozumiany zmieniać ani usuwać w akcie w sprawie zarządzania danymi, ponieważ spowodowałoby to rozmycie definicji obu tych ram prawnych, a tym samym brak pewności prawa**[13]. Ponadto nowe definicje wprowadzone w akcie w sprawie zarządzania danymi w zakresie, w jakim odnoszą się do przetwarzania danych osobowych, nie powinny w rzeczywistości zawierać „przepisów", które są niezgodne z RODO[14]. Jest to rzeczywiście kluczowa kwestia, na którą EROD chciałaby zwrócić uwagę współprawodawców.

Z jednej strony w akcie w sprawie zarządzania danymi należy zawrzeć definicje „danych osobowych", „osoby, której dane dotyczą", „zgody" i „przetwarzania" odnoszące się do definicji zawartych w RODO[15]; z drugiej strony definicje „metadanych", „posiadacza danych", „użytkownika danych", „udostępniania danych", „altruistycznego podejścia do danych" zawarte w akcie w sprawie zarządzania danymi powinny zostać zmienione, aby uniknąć niespójności i braku pewności prawa oraz aby były zgodne z „charakterem przedmiotowych praw", a mianowicie z osobistym charakterem

[13] Zob. podsekcja 3.2.B wspólnej opinii.
[14] Zob. pkt 44 wspólnej opinii.
[15] Zob. w tym względzie kompromisowy tekst Rady z dnia 30 marca 2021 r.

prawa do ochrony danych osobowych jako prawa odnoszącego się do każdej osoby[16] oraz jako prawa niezbywalnego, którego „nie można się zrzec" ani uczynić przedmiotem praw własności[17].

W związku z tym EROD wyraża ubolewanie z powodu odniesienia do „wymiany, łączenia danych lub obrotu danymi" dodanego w kompromisowym tekście Rady w odniesieniu do definicji „dostawcy usług udostępniania danych", ponieważ w odniesieniu do danych osobowych sugeruje ono ideę legitymizacji obrotu nimi, a tym samym jest niespójne z osobistym charakterem prawa do ochrony danych osobowych. W istocie, biorąc pod uwagę, że ochrona danych jest prawem podstawowym zagwarantowanym w art. 8 Karty oraz uwzględniając, że jednym z głównych celów RODO jest zapewnienie osobom, których dane dotyczą, kontroli nad dotyczącymi ich danymi osobowymi, **EROD powtarza, że danych osobowych nie można uznać za „towary podlegające wymianie handlowej"**. **Istotną konsekwencją tego jest to, że nawet jeśli osoba, której dotyczą dane, może wyrazić zgodę na przetwarzanie jej danych osobowych, nie może ona zrzec się swoich praw podstawowych**[18]**.** W związku z tym administrator, któremu osoba, której dane dotyczą, udzieliła zgody na przetwarzanie jej danych osobowych, nie jest uprawniony do „wymiany" danych osobowych lub „obrotu" danymi osobowymi (jako tzw. „towarem") w sposób, który skutkowałby naruszeniem wszystkich mających zastosowanie zasad i przepisów dotyczących ochrony danych.

Jako przykład przepisu, który mógłby prowadzić do interpretacji niezgodnej z wyżej wspomnianym „charakterem osobistym", art. 2 ust. 5 aktu w sprawie zarządzania danymi definiuje „posiadacza danych" (w tym osoby prawne) jako posiadającego między innymi prawo do udzielenia dostępu do danych osobowych będących pod jego kontrolą lub do udostępniania tych danych[19]. W tym względzie EROD zauważa, że RODO gwarantuje każdej osobie fizycznej prawo do ochrony danych osobowych, ustanawiając mechanizmy kontroli i równowagi w celu ochrony osoby fizycznej w przypadku przetwarzania jej danych osobowych[20]. Przetwarzanie danych osobowych musi być zgodne z zasadami (w tym zasadami: zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych, prawidłowości) i przepisami, w tym dotyczącymi praw osób, których dane dotyczą (na przykład: prawo do informacji, w tym o profilowaniu, które dotyczy danej osoby; prawo dostępu; prawo do sprostowania; do usunięcia danych; do niepodlegania w pełni zautomatyzowanemu podejmowaniu decyzji, które w istotny sposób wpływają na jej sytuację), których osoba, której dane dotyczą, nie może się zrzec. W tym względzie EROD zauważa, że zamiast odnosić się do osoby prawnej, która „ma prawo do udzielenia dostępu lub do udostępniania" danych osobowych, definicja

[16] Zob. pkt 34 wspólnej opinii, odnoszący się do art. 8 Karty: *„1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą. 2. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą".*

[17] W tym względzie w pkt 118 wspólnej opinii: „wyraźna zachęta do »monetyzacji« danych osobowych zwiększa również znaczenie przestrzegania zasad ochrony danych" oraz przypis 54: „W związku z tym EROD opracowuje wytyczne dotyczące gromadzenia i wykorzystywania danych osobowych za wynagrodzeniem finansowym". Zob. również przypis 61 na s. 30 wspólnej opinii.

[18] Zob. Wytyczne 2/2019 w sprawie przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. b) rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) w kontekście świadczenia usług online na rzecz osób, których dane dotyczą, dostępne pod adresem: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_pl.pdf

[19] Zob. pkt 29–31 wspólnej opinii. Zob. również niejasne odniesienie do „**ich**" danych w art. 11 ust. 6, art. 19 i art. 19 ust. 1 lit. a), również podkreślone we wspólnej opinii.

[20] Zobacz pkt 29 i nast. wspólnej opinii.

posiadacza danych powinna – jeśli w ogóle powinna być utrzymana – odnosić się do przetwarzania danych osobowych i jego warunków zgodnie z obowiązującym prawem o ochronie danych[21].

Jak określono w proponowanym brzmieniu art. 1 aktu w sprawie zarządzania danymi, w odniesieniu do danych osobowych pierwszeństwo ma prawo ochrony danych (w stosunku do norm kolizyjnych)[22]. Niemniej jednak **istotne jest, aby uniknąć norm kolizyjnych lub sprzecznej interpretacji w całym tekście rozporządzenia, również w celu poprawy natychmiastowej czytelności tekstu prawnego.**

W tym sensie należy wprowadzić definicję terminu „zezwolenie" (przez osoby prawne na ponowne wykorzystywanie danych), aby bez żadnych niejasności wyjaśnić, do jakich (rodzajów danych) dokładnie się on odnosi. Jak stwierdzono we wspólnej opinii, uważamy, że w celu zapewnienia jasności termin ten powinien odnosić się wyłącznie do danych nieosobowych[23].

Obawy związane z rozdziałami sektorowymi aktu w sprawie zarządzania danymi

Europejska Rada Ochrony Danych ma również poważne obawy dotyczące rozdziałów „sektorowych" aktu w sprawie zarządzania danymi (II, III i IV) i pragnie przypomnieć niektóre z nich poniżej:

• W odniesieniu do rozdziału II aktu w sprawie zarządzania danymi przypominamy, że we wspólnej opinii zaleca się **włączenie do części merytorycznej aktu w sprawie zarządzania danymi specyfikacji zawartej w motywie 7**, a mianowicie, że „[...] dane osobowe wykraczają poza zakres dyrektywy (UE) 2019/1024 [nasza uwaga: i wchodzą w zakres aktu w sprawie zarządzania danymi], o ile system dostępu wyklucza lub ogranicza dostęp do takich danych ze względu na ochronę danych, prywatność i integralność osoby fizycznej, w szczególności zgodnie z przepisami o ochronie danych[24]".

Oznacza to, że akt w sprawie zarządzania danymi będzie miał zastosowanie w szczególności do zakresu wyłączonego z dyrektywy w sprawie otwartych danych zgodnie z art. 1 ust. 2 lit. h), tj. do: *„dokumentów wyłączonych z dostępu lub do których dostęp jest ograniczony na podstawie systemów dostępu ze względu na ochronę danych osobowych, a także części dokumentów dostępnych na podstawie tych systemów, które to części zawierają dane osobowe, których ponowne wykorzystywanie zostało określone w przepisach jako niezgodne z przepisami dotyczącymi ochrony osób fizycznych w zakresie przetwarzania danych osobowych lub jako naruszające ochronę prywatności i integralności osoby fizycznej, w szczególności zgodnie z unijnymi lub krajowymi przepisami dotyczącymi ochrony danych osobowych".* Biorąc pod uwagę wrażliwość przedmiotowych danych osobowych, aby zagwarantować, że stopień ochrony danych osobowych w UE nie zostanie obniżony, a także ze względu na pewność prawa, we wspólnej opinii zaleca się **dostosowanie rozdziału II wniosku do obowiązujących przepisów dotyczących ochrony danych osobowych określonych w RODO i do**

[21] Zob. pkt 31 wspólnej opinii.
[22] W tym samym znaczeniu zob. dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/770 z dnia 20 maja 2019 r. w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych i usług cyfrowych, Dz.U. L 136 z 22.5.2019, s. 1, art. 3 ust. 8: „Prawo Unii dotyczące ochrony danych osobowych ma zastosowanie do danych osobowych przetwarzanych w związku z umowami, o których mowa w ust. 1. W szczególności niniejsza dyrektywa pozostaje bez uszczerbku dla rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE. W przypadku kolizji pomiędzy przepisami niniejszej dyrektywy a prawem Unii dotyczącym ochrony danych osobowych pierwszeństwo ma prawo Unii dotyczące ochrony danych osobowych".
[23] Zob. pkt 47 i nast. wspólnej opinii.
[24] Zob. pkt 69 wspólnej opinii.

dyrektywy w sprawie otwartych danych. Alternatywnie we wspólnej opinii zachęca się współprawodawców do rozważenia **wyłączenia danych osobowych** z zakresu tego rozdziału[25].

Ponadto, z uwagi na fakt, że zgoda osoby, której dane dotyczą może nie zostać uznana za wyrażoną dobrowolnie z powodu braku równowagi sił, która często występuje w relacji między osobą, której dane dotyczą a organami publicznymi, we wspólnej opinii wyrażono obawy dotyczące art. 5 ust. 6 aktu w sprawie zarządzania danymi[26], a w szerszym ujęciu zachęca się współprawodawców **do wyraźnego określenia we wniosku odpowiednich modeli „uczestnictwa obywatelskiego", dzięki którym osoby fizyczne mogą w sposób otwarty i oparty na współpracy uczestniczyć w procesie określania scenariuszy umożliwiających ponowne wykorzystanie ich danych osobowych, zgodnie z oddolnym podejściem do projektów otwartych danych**.

We wspólnej opinii zaleca się również **zmianę aktu w sprawie zarządzania danymi, aby wyjaśnić, że ponowne wykorzystywanie danych osobowych będących w posiadaniu organów sektora publicznego może być dozwolone wyłącznie wtedy, gdy jest ono uzasadnione prawem Unii lub państwa członkowskiego**, które ustanawia wykaz wyraźnych zgodnych celów, do których dalsze przetwarzanie może być zgodnie z prawem dopuszczone, lub stanowi niezbędny i proporcjonalny środek w społeczeństwie demokratycznym służący zabezpieczeniu celów, o których mowa w art. 23 RODO[27].

Europejska Rada Ochrony Danych przypomina ponadto, że włączenie danych będących w posiadaniu organów sektora publicznego chronionych ze względu na poufność informacji statystycznych do zakresu rozdziału II aktu w sprawie zarządzania danymi, zgodnie z art. 3 ust. 1 lit. b), może być sprzeczne z zasadą, zgodnie z którą dane osobowe gromadzone do celów statystycznych mogą być wykorzystywane wyłącznie do tego celu[28]. Poszanowanie tej zasady jest kluczowe, aby nie podważać zaufania danej osoby, gdy przekazuje ona swoje dane osobowe do celów statystycznych[29].

• W odniesieniu do rozdziału III, wśród warunków świadczenia usługi (usług) udostępniania danych, **w akcie w sprawie zarządzania danymi należy określić, że dostawca musi dysponować procedurami zapewniającymi zgodność z prawem Unii i prawem krajowym w zakresie ochrony danych osobowych, w tym procedurami zapewniającymi wykonywanie praw osób, których dane dotyczą**. W szczególności dostawca udostępnia osobie, której dane dotyczą, łatwo dostępne narzędzia umożliwiające jej nie tylko udzielenie, ale również *wycofanie* zgody; oraz zapewnia narzędzia

[25] Zob. pkt 71 wspólnej opinii.

[26] Artykuł 5 ust. 6: „W przypadku gdy ponowne wykorzystywanie danych nie może być przyznane zgodnie z obowiązkami określonymi w ust. 3–5 i nie ma innej podstawy prawnej do przesłania danych na mocy rozporządzenia (UE) 2016/679, organ sektora publicznego wspiera podmioty ponownie wykorzystujące dane w dążeniu do uzyskania zgody osób, których dane dotyczą, lub zgody podmiotów prawnych, których prawa i interesy mogą zostać naruszone w wyniku takiego ponownego wykorzystywania, o ile jest to możliwe bez ponoszenia nieproporcjonalnych kosztów przez sektor publiczny. W wykonywaniu tego zadania organy sektora publicznego mogą być wspomagane przez właściwe podmioty określone w art. 7 ust. 1."

[27] Zob. pkt 77 wspólnej opinii. Zob. również pkt 75 oraz 76 wspólnej opinii.

[28] Zob. motyw 27 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 223/2009 z dnia 11 marca 2009 r. w sprawie statystyki europejskiej; jak również art. 4 ust. 1 i 2 zalecenia Rady Europy nr R (97)18 dotyczącego ochrony danych osobowych gromadzonych i przetwarzanych do celów statystycznych.

[29] Zob. przypis 36 wspólnej opinii.

pozwalające na uzyskanie pełnego obrazu tego, w jaki sposób i do jakich konkretnych celów jej dane osobowe są udostępniane[30].

Ponadto w akcie w sprawie zarządzania danymi przypomina się o **obowiązku przeprowadzenia w stosownych przypadkach oceny skutków dla ochrony danych zgodnie z art. 35 RODO** oraz, w przypadku pozostałego wysokiego ryzyka dla osób, których sprawa dotyczy, o obowiązku skonsultowania się z organem ochrony danych przed rozpoczęciem przetwarzania zgodnie z art. 36 RODO[31].

• **Te same wymagania powinny zostać określone w akcie w sprawie zarządzania danymi w odniesieniu do organizacji o altruistycznym podejściu do danych**[32]. Te gwarancje ochrony danych muszą zostać włączone do aktu w sprawie zarządzania danymi również ze względu na oznakowanie – jako dostawca usług udostępniania danych lub jako „uznana w UE organizacja o altruistycznym podejściu do danych" – które byłoby wykorzystywane przez te podmioty prawne w celu uzyskania zgody na przetwarzanie ich danych osobowych przez osobę, której dane dotyczą, która zakładałaby, że zapewniono wysoki stopień ochrony takich danych.

W świetle powyższego, jak stwierdzono we wspólnej opinii, **EROD uważa, że deklaratywny system zgłaszania/rejestracji przewidziany w akcie w sprawie zarządzania danymi odpowiednio dla dostawców usług udostępniania danych i organizacji o altruistycznym podejściu do danych nie przewiduje wystarczająco rygorystycznej procedury weryfikacyjnej**, biorąc pod uwagę ewentualny wpływ przetwarzania danych osobowych, którego takie podmioty mogą dokonywać, na osoby, których dane dotyczą. W związku z tym **EROD zaleca zbadanie alternatywnych procedur, które powinny w szczególności uwzględniać bardziej systematyczne uwzględnianie narzędzi rozliczalności i zgodności w odniesieniu do przetwarzania danych osobowych zgodnie z RODO, w szczególności przestrzeganie kodeksu postępowania lub mechanizmu certyfikacji**[33].

Europejska Rada Ochrony Danych wyraża ubolewanie, że w kompromisowym tekście Rady z dnia 30 marca 2021 r. przewidziano obecnie (wyraźnie), że rejestracja jako uznana organizacja o altruistycznym podejściu do danych nie jest warunkiem wstępnym prowadzenia działań altruistycznych, co jeszcze bardziej osłabia kontrole i zabezpieczenia dla osób, których dane dotyczą w odniesieniu do kluczowych aspektów ochrony danych. Zabezpieczenia te są szczególnie ważne również ze względu na niejasność definicji „altruistycznego podejścia do danych" w akcie w sprawie zarządzania danymi.

Ponadto **w akcie w sprawie zarządzania danymi należy przedstawić dokładną definicję „celów interesu ogólnego", które byłyby realizowane przez organizacje o altruistycznym podejściu do danych**[34]. Ponadto należy opracować europejski formularz zgody na potrzeby altruistycznego podejścia do danych przez organizacje o altruistycznym podejściu do danych w porozumieniu z EROD, a nie z (mającą powstać) Europejską Radą ds. Innowacji w zakresie Danych[35].

[30] Zob. podsekcja 3.4.1 i pkt 147 wspólnej opinii.
[31] Zob. pkt 147 wspólnej opinii.
[32] Zob. podsekcja 3.5.1 wspólnej opinii.
[33] Zob. pkt 140 i 180 wspólnej opinii.
[34] Zob. pkt 159–160 i 170–171 wspólnej opinii.
[35] Zob. podsekcja 3.5.5 wspólnej opinii.

• We wspólnej opinii odnotowano wymóg „niezależności" dostawców usług udostępniania danych, jak również „niezależności" organizacji o altruistycznym podejściu do danych w akcie w sprawie zarządzania danymi. W odniesieniu do organizacji o altruistycznym podejściu do danych we wspólnej opinii zaleca się **wyjaśnienie kwestii niezależności (np. prawnej, organizacyjnej, ekonomicznej) organizacji o altruistycznym podejściu do danych od podmiotów nastawionych na zysk**[36]. Uwzględniając dostawców usług udostępniania danych, EROD pragnie teraz zwrócić uwagę na motyw 22 aktu w sprawie zarządzania danymi: „[..] *Wyspecjalizowani pośrednicy w zakresie danych, którzy są niezależni zarówno od posiadaczy danych, jak i użytkowników danych, mogą odgrywać rolę polegającą na ułatwianiu powstawania nowych ekosystemów opartych na danych, niezależnych od jakiegokolwiek podmiotu o znaczącej pozycji rynkowej. [..]*" Europejska Rada Ochrony Danych podkreśla, że ten rodzaj niezależności dostawców usług udostępniania danych ma kluczowe znaczenie zarówno z punktu widzenia konkurencji, jak i ochrony danych[37].

Wnioski

Podsumowując, EROD wzywa współprawodawców do zajęcia się ważnymi kwestiami krytycznymi wyjaśnionymi we wspólnej opinii, unikając w ten sposób sytuacji, w której akt w sprawie zarządzania danymi tworzy równoległy zestaw przepisów, niezgodny z RODO, a także z innymi przepisami prawa Unii, co skutkowałoby niewystarczającymi zabezpieczeniami dla danych osób, których sprawa dotyczy, i trudnościami w praktycznym stosowaniu.

Niniejsze oświadczenie, przywołujące niektóre z kluczowych punktów wspólnej opinii, pozostaje bez uszczerbku dla ewentualnego przyszłego bardziej szczegółowego oświadczenia lub opinii na temat przyszłych stanowisk współprawodawców.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

[36] Zob. pkt 78 wspólnej opinii.

[37] Zob. w szczególności: Oświadczenie EROD w sprawie wpływu koncentracji gospodarczych na ochronę danych, przyjęte w dniu 27 sierpnia 2018 r., „Większa koncentracja na rynkach cyfrowych może zagrażać poziomowi ochrony danych i swobodom przysługującym konsumentom usług cyfrowych"; Oświadczenie EROD w sprawie wpływu połączeń przedsiębiorstw na prywatność, przyjęte w dniu 19 lutego 2020 r.