

Oświadczenie



Oświadczenie w sprawie pakietu usług cyfrowych i strategii w zakresie danych przyjęte 18 listopada 2021 r.

Europejska Rada Ochrony Danych (EROD) przyjęła następujące oświadczenie:

Od listopada 2020 r. Komisja Europejska przedstawiła kilka wniosków ustawodawczych w ramach strategii cyfrowej i strategii w zakresie danych, przede wszystkim akt o usługach cyfrowych (DSA), akt o rynkach cyfrowych (DMA), akt w sprawie zarządzania danymi (DGA) oraz akt w sprawie sztucznej inteligencji (AIR). W najbliższym czasie przedstawiony ma zostać piąty wniosek – „akt w sprawie danych” – jako jedna z kilku inicjatyw zapowiedzianych w europejskiej strategii w zakresie danych¹.

Celem tych wniosków jest ułatwienie dalszego wykorzystywania i wymiany danych (osobowych) przez większą liczbę podmiotów publicznych i prywatnych w ramach gospodarki opartej na danych, ułatwienie wykorzystania konkretnych technologii, takich jak duże zbiory danych (Big Data) i sztuczna inteligencja, oraz uregulowanie działalności platform internetowych i strażników dostępu. Przetwarzanie danych osobowych jest lub stanie się głównym elementem działalności różnych podmiotów, modeli biznesowych i technologii, których dotyczą te wnioski. Łączne skutki przyjęcia i wdrożenia proponowanych aktów będą zatem miały znaczny wpływ na realizację podstawowych praw do prywatności i ochrony danych osobowych przewidzianych w art. 7 i 8 Karty praw podstawowych Unii Europejskiej („Karta UE”) oraz w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”).

Europejska Rada Ochrony Danych (EROD) i Europejski Inspektor Ochrony Danych (EIOD) wydali już wspólne opinie na temat aktu w sprawie zarządzania danymi² i aktu w sprawie sztucznej inteligencji, a Europejski Inspektor Ochrony Danych wydał opinie na temat europejskiej strategii w zakresie danych, aktu o rynkach cyfrowych i aktu o usługach cyfrowych³. W opiniach tych podkreślono szereg

¹ Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Europejska strategia w zakresie danych”, COM(2020) 66 final.

² EROD wydała również oświadczenie 05/2021 dotyczące aktu w sprawie zarządzania danymi w świetle zmian legislacyjnych.

³ EIOD wydał również wstępną opinię w sprawie europejskiej przestrzeni danych dotyczących zdrowia. Przegląd wszystkich opinii i oświadczeń wydanych przez EROD i EIOD przedstawiono w załączniku.

obaw i sformułowano zalecenia, jak zbliżyć treść wniosków do obowiązującego prawodawstwa Unii w zakresie ochrony danych. Europejska Rada Ochrony Danych ubolewa nad tym, że do tej pory współprawodawcy nie zastosowali się w pełni do wielu z tych zaleceń⁴.

W poniższym oświadczeniu Europejska Rada Ochrony Danych zwraca uwagę na szereg obaw związanych ze wszystkimi tymi aktami i wzywa współprawodawców do podjęcia zdecydowanych działań. Nasze obawy można podzielić na trzy kategorie: 1) brak ochrony podstawowych praw i wolności osób fizycznych; 2) fragmentaryczny nadzór; 3) ryzyko wystąpienia niespójności.

Europejska Rada Ochrony Danych uważa, że jeśli proponowane akty nie zostaną zmienione, w negatywny sposób wpłyną na podstawowe prawa i wolności osób fizycznych i poskutkują znaczną niepewnością prawa, która podważyłaby zarówno istniejące, jak i przyszłe ramy prawne. W związku z tym omawiane wnioski mogą nie osiągnąć przewidzianego w nich celu, jakim jest stworzenie warunków dla innowacji i wzrostu gospodarczego.

1. BRAK OCHRONY PODSTAWOWYCH PRAW I WOLNOŚCI OSÓB FIZYCZNYCH

W omawianych wnioskach dokonano pewnych wyborów, które mogą mieć długotrwały wpływ na podstawowe prawa i wolności osób fizycznych i całego społeczeństwa. Wprawdzie nadrzędnym celem tych wniosków jest ograniczenie różnych rodzajów ryzyka, jednak Europejska Rada Ochrony Danych ma poważne obawy odnośnie do szeregu dokonanych wyborów i uważa, że podstawowe prawa i wolności osób fizycznych wymagają dodatkowej ochrony. Konkretnie przykłady:

- Proponowany akt w sprawie sztucznej inteligencji (AIR) pozwoliłby na stosowanie **systemów sztucznej inteligencji klasyfikujących osoby fizyczne** na podstawie danych biometrycznych (np. rozpoznawanie twarzy) według **pochodzenia etnicznego, płci, a także orientacji politycznej lub seksualnej** lub innych zakazanych przesłanek dyskryminacyjnych, a także na stosowanie systemów sztucznej inteligencji, których trafność naukowa nie została udowodniona lub które stoją w bezpośredniej sprzeczności z podstawowymi wartościami UE⁵. Europejska Rada Ochrony Danych uważa, że takie systemy powinny być zakazane w UE, i wzywa współprawodawców do uwzględnienia takiego zakazu w akcie w sprawie sztucznej inteligencji. Ponadto Europejska Rada Ochrony Danych uważa, że wykorzystywanie sztucznej inteligencji do **wykrywania emocji osoby fizycznej** jest wysoce niepożądane i powinno być zakazane, z wyjątkiem konkretnych ściśle określonych przypadków użycia, a mianowicie do celów zdrowotnych lub badawczych, z zastrzeżeniem odpowiednich zabezpieczeń, warunków i ograniczeń⁶.
- W tym samym duchu, biorąc pod uwagę znaczny negatywny wpływ na podstawowe prawa i wolności osób fizycznych, Europejska Rada Ochrony Danych przypomina, że

⁴ W poniższym oświadczeniu omawiamy zastrzeżenia dotyczące pierwotnego tekstu wniosków przedstawionych przez Komisję i nie odnosimy się do żadnego późniejszego stanowiska Parlamentu Europejskiego ani Rady Unii Europejskiej, chyba że wyraźnie wskazano inaczej.

⁵ Np. poligraf, załącznik III pkt 6 b) i 7 a) aktu w sprawie sztucznej inteligencji. Wspólna opinia EROD i EIOD dotycząca aktu w sprawie sztucznej inteligencji, pkt 32.

⁶ Wspólna opinia EROD i EIOD dotycząca aktu w sprawie sztucznej inteligencji, pkt 35.

akt w sprawie sztucznej inteligencji **powinien zawierać zakaz wszelkiego wykorzystywania sztucznej inteligencji do zautomatyzowanego rozpoznawania cech ludzkich** – takich jak cechy twarzy, ale także sposób chodzenia, odciski palców, DNA, głos, sposób uderzania w klawisze klawiatury i inne dane biometryczne lub behawioralne – **w przestrzeni publicznej** i w każdym kontekście⁷. Proponowany akt w sprawie sztucznej inteligencji w obecnej postaci umożliwia stosowanie, w niektórych przypadkach⁸, systemów zdalnej identyfikacji biometrycznej w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw. Europejska Rada Ochrony Danych z zadowoleniem przyjmuje niedawno przyjętą rezolucję PE, w której podkreślono te istotne zagrożenia⁹.

- Europejska Rada Ochrony Danych uważa również, że w akcie o usługach (DSA) należy bardziej restrykcyjnie uregulować **reklamę ukierunkowaną** na korzyść mniej inwazyjnych form reklamy, które nie wymagają śledzenia interakcji użytkownika z treścią, i apeluje do współprawodawców o rozważenie stopniowego wprowadzenia **zakazu stosowania internetowej reklamy ukierunkowanej opierającej się na wszechobecnym śledzeniu**¹⁰ i o całkowite zakazanie profilowania dzieci.
- Europejska Rada Ochrony Danych zaleca wprowadzenie zarówno w akcie o usługach cyfrowych, jak i w akcie o rynkach cyfrowych, **wymogów interoperacyjności** w celu promowania środowiska cyfrowego bardziej otwartego na konkurencję, ułatwiającego osobom fizycznym dokonywanie wyboru usług oferujących lepszą ochronę prywatności i danych¹¹.

2. FRAGMENTARYCZNY NADZÓR

Wszystkie wnioski przewidują ustanowienie organów nadzorczych i nowych europejskich struktur współpracy między tymi organami („europejskie rady”)¹². Mimo że przetwarzanie danych osobowych ma kluczowe znaczenie dla działalności uregulowanej w tych wnioskach, organów nadzorczych ds. ochrony danych nie wyznaczono jako główne właściwe organy. Europejska Rada Ochrony Danych przypomina, że w art. 16 ust. 2 TFUE i art. 8 ust. 3 Karty praw podstawowych UE zawarto wymóg

⁷ Wspólna opinia EROD i EIOD dotycząca aktu w sprawie sztucznej inteligencji, pkt 32.

⁸ Określonych w art. 5 ust. 1 lit. d) pkt (i)–(iii) aktu w sprawie sztucznej inteligencji.

⁹ Rezolucja Parlamentu Europejskiego z dnia 6 października 2021 r. w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych (2020/2016(INI)).

¹⁰ Zob. również pkt 69–70 opinii EIOD w sprawie aktu o usługach cyfrowych oraz rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. zawierająca zalecenia dla Komisji w sprawie aktu o usługach cyfrowych: dostosowanie przepisów prawa handlowego i cywilnego do podmiotów gospodarczych prowadzących działalność internetową (2020/2019(INL)), pkt 15.

¹¹ Zob. również pkt 84–85 opinii EIOD w sprawie aktu o usługach cyfrowych oraz pkt 37–38 opinii EIOD w sprawie aktu o rynkach cyfrowych.

¹² W akcie o rynkach cyfrowych – Komitet Doradczy ds. Rynków Cyfrowych (DMAC); w akcie o usługach cyfrowych – Europejska Rada ds. Usług Cyfrowych (EBDS); w akcie w sprawie sztucznej inteligencji – Europejska Rada ds. Sztucznej Inteligencji (EAIB); w akcie w sprawie zarządzania danymi – Europejska Rada ds. Innowacji w zakresie Danych (EDIB).

w odniesieniu do ochrony i swobodnego przepływu danych osobowych, aby nadzór nad przetwarzaniem danych osobowych został powierzony niezależnym organom ochrony danych¹³.

Ponadto Europejska Rada Ochrony Danych jest bardzo zaniepokojona faktem, że we wnioskach nie określono jasno, w jaki sposób nowe organy nadzorcze (i towarzyszące im europejskie rady) mają współpracować z organami nadzorczymi ds. ochrony danych (i Europejską Radą Ochrony Danych). W szczególności w omawianych wnioskach nie uregulowano odpowiednio sytuacji potencjalnego nakładania się kompetencji ani sytuacji, w których organy powinny konsultować się ze sobą w kwestiach będących przedmiotem wspólnego zainteresowania. Stwarza to **ryzyko istnienia równoległych struktur nadzoru**, w których różne właściwe organy nadzorują te same podmioty w odniesieniu do tych samych czynności (przetwarzania), **nie współpracując ze sobą w zorganizowany sposób**.

Konkretne przykłady:

- Proponowany akt o usługach cyfrowych zobowiązuje właściwe organy do nadzorowania **systemów rekomendacji**¹⁴ bardzo dużych platform internetowych (które często obejmują profilowanie osób, których dane dotyczą, w rozumieniu RODO); a także środków zastosowanych w celu **oceny i ograniczenia ryzyka systemowego, w tym zagrożenia dla prawa do prywatności**¹⁵. Ten sam wniosek zawiera również przepisy dotyczące **kodeksów postępowania**, które mogą dotyczyć przetwarzania danych osobowych¹⁶. Nie wymaga on jednak od właściwych organów formalnych konsultacji ani współpracy z Europejską Radą Ochrony Danych czy też z jej członkami. Stwarza to ryzyko istnienia sprzecznych wytycznych lub nawet różnych wyników działań organów nadzorczych w zakresie egzekwowania prawa.
- W proponowanym akcie o usługach cyfrowych definiuje się **nowe rodzaje dostawców usług i organizacji**, którzy przetwarzaliby duże ilości potencjalnie wrażliwych danych, w szczególności dostawców usług pośrednich w zakresie danych i organizacje o altruistycznym podejściu do danych. System **weryfikacji tych podmiotów ma jednak charakter niemal deklaracyjny i jako taki nie zapewnia wystarczającej ochrony osobom, których dane dotyczą**¹⁷, ponieważ ogranicza się do weryfikacji przez właściwy organ (głównie formalnych) wymogów¹⁸, a termin na taką weryfikację jest bardzo krótki¹⁹.

¹³ Zob. oświadczenie EROD 05/2021 dotyczące aktu w sprawie zarządzania danymi w świetle zmian legislacyjnych, s. 3; wspólna opinia EROD i EIOD dotycząca aktu w sprawie sztucznej inteligencji, pkt 14.

¹⁴ Art. 29 aktu o usługach cyfrowych.

¹⁵ W szczególności w kontekście art. 27 (identyfikacja i ocena najważniejszego i powtarzającego się ryzyka systemowego oraz najlepsze praktyki w zakresie zmniejszania takiego ryzyka), który odnosi się do art. 26, w tym do art. 26 ust. 1 lit. b) oraz art. 35 i 36 aktu o usługach cyfrowych (kodeksy postępowania).

¹⁶ Zob. art. 35–36 aktu o usługach cyfrowych.

¹⁷ Zob. wspólna opinia EROD i EIOD dotycząca aktu w sprawie zarządzania danymi, pkt 136, 140, 151, 155, 175, 180, 191.

¹⁸ Określonych odpowiednio w art. 11 aktu w sprawie zarządzania danymi w odniesieniu do dostawców usług udostępniania danych oraz w art. 16–19 w odniesieniu do organizacji o altruistycznym podejściu do danych.

¹⁹ Tydzień od daty zgłoszenia w przypadku dostawców usług udostępniania danych (art. 10 ust. 7 aktu w sprawie zarządzania danymi); 12 tygodni od daty wniosku w przypadku organizacji o altruistycznym podejściu do danych (art. 17 ust. 5 aktu w sprawie zarządzania danymi).

- W proponowanym akcie w sprawie sztucznej inteligencji określono **system certyfikacji i kodeksy postępowania** dla systemów sztucznej inteligencji wysokiego ryzyka, ale nie jest jasne, czy te certyfikaty i kodeksy mogą współdziałać z wymogami określonymi w RODO, a jeżeli tak, to w jaki sposób²⁰. Mogłoby to prowadzić do sytuacji, w których systemy sztucznej inteligencji, mimo że są certyfikowane (oznaczone znakiem CE) na podstawie aktu w sprawie sztucznej inteligencji jako dopuszczone do wprowadzenia do obrotu lub oddania do użytku, nie byłyby zgodne z przepisami i zasadami ochrony danych (w szczególności z zasadą uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych)²¹. Ponadto w proponowanym akcie w sprawie sztucznej inteligencji brakuje odniesienia do (obowiązkowych) mechanizmów monitorowania kodeksów postępowania mających na celu sprawdzenie, czy dostawcy systemów sztucznej inteligencji nieobarczonych wysokim ryzykiem przestrzegają tych kodeksów²².
- Proponowany akt o rynkach cyfrowych zobowiązuje strażników dostępu do ułatwiania **przenoszenia danych** zgodnie z RODO oraz do zapewnienia, pod pewnymi warunkami, **dostępu do danych**, w tym danych osobowych, na podstawie art. 6 ust. 1 lit. h) oraz i), oraz danych zanonimizowanych, na podstawie art. 6 ust. 1 lit. j), nie zapewniając jasnej podstawy prawnej przetwarzania danych osobowych ani obowiązku konsultacji i współpracy między właściwym organem wyznaczonym na mocy aktu o rynkach cyfrowych a właściwym organem ochrony danych przy nadzorowaniu przestrzegania tych przepisów aktu o rynkach cyfrowych.

Aby zapewnić komplementarność nadzoru i zwiększyć pewność prawa, Europejska Rada Ochrony Danych zdecydowanie zaleca, aby w każdym z wniosków wyraźnie wymienić organy nadzorcze ds. ochrony danych wśród odpowiednich właściwych organów, z którymi ma się odbywać współpraca. Każdy z wniosków powinien prócz tego **przewidywać wyraźną podstawę prawną dla wymiany informacji niezbędnych do skutecznej współpracy oraz określać okoliczności, w których powinna się odbywać współpraca**. Ponadto wnioski powinny umożliwiać organom nadzorczym określonym jako właściwe organy w poszczególnych wnioskach **wymianę informacji** uzyskanych w ramach wszelkich audytów i dochodzeń związanych z przetwarzaniem danych osobowych z właściwymi organami ochrony danych – na ich wniosek lub z własnej inicjatywy²³. Europejska Rada Ochrony Danych pragnie podkreślić potrzebę zapewnienia organom nadzorczym ds. ochrony danych **wystarczających zasobów** pozwalających na wykonywanie tych dodatkowych zadań.

3. RYZYKO WYSTĄPIENIA NIESPÓJNOŚCI

Wszystkie omawiane wnioski mają na celu uregulowanie technologii lub działalności, które wiążą się z przetwarzaniem danych osobowych. W związku z tym zastosowanie do nich mają w pełni istniejące ramy ochrony danych. Tekst normatywny wniosków może jednak **prowadzić do niejasności** odnośnie do tego, czy w pewnych przypadkach ramy ochrony danych faktycznie mają zastosowanie. Współprawodawca powinien rozwiązać wszelkie wątpliwości, **gwarantując** tym samym pewność prawa

²⁰ Zob. wspólna opinia EROD i EIOD dotycząca aktu w sprawie sztucznej inteligencji, pkt 74.

²¹ Zob. wspólna opinia EROD i EIOD dotycząca aktu w sprawie sztucznej inteligencji, pkt 76.

²² Zob. wspólna opinia EROD i EIOD dotycząca aktu w sprawie sztucznej inteligencji, pkt 79.

²³ Zob. również pkt 87–89 opinii EIOD w sprawie aktu o usługach cyfrowych oraz pkt 39–41 opinii EIOD w sprawie aktu o rynkach cyfrowych.

i zwiększając spójność z istniejącymi ramami ochrony danych w celu zapewnienia ich skutecznego stosowania. Niezależnie od wszystkiego we wnioskach **należy wyraźnie wskazać, że nie mają one wpływu na stosowanie obowiązujących przepisów o ochronie danych ani ich nie podważają, a także zapewnić pierwszeństwo stosowania przepisów o ochronie danych** w każdym przypadku przetwarzania danych osobowych²⁴.

Ponadto w niektórych przepisach stosuje się tę samą terminologię co w RODO lub dyrektywie o prywatności i łączności elektronicznej, bez wyraźnego odniesienia do wspomnianych wyżej przepisów. Może to wpłynąć na wykładnię podstawowych pojęć RODO (takich jak kluczowe pojęcia „zgody” lub „osoby, której dane dotyczą”)²⁵. Powoduje to również ryzyko interpretowania niektórych przepisów jako odbiegających od RODO lub dyrektywy o prywatności i łączności elektronicznej. W związku z tym niektóre przepisy **można z łatwością interpretować w sposób niezgodny z obowiązującymi ramami prawnymi, co kolei może przełożyć się na brak pewności prawa.**

Konkretne przykłady:

- Wniosek dotyczący aktu o usługach cyfrowych zawiera wymóg, aby dostawcy usług **oferowali użytkownikom co najmniej jedną opcję rekomendowania treści, która nie wiąże się z korzystaniem z profilowania**²⁶. Jednak zasada ochrony danych w fazie projektowania i domyślnej ochrony danych wymaga, że systemy oferujące te rekomendacje nie powinny się opierać *domyślnie* na profilowaniu²⁷.
- W wielu przypadkach **podstawa prawna** przetwarzania danych osobowych nie wynika jasno z treści normatywnej wniosków. Przykładem zaczerpniętym z proponowanego aktu w sprawie zarządzania danymi jest brak jasności co do ponownego wykorzystywania danych osobowych będących w posiadaniu organów sektora publicznego²⁸. W proponowanym akcie w sprawie sztucznej inteligencji wskazano, że nie stanowi on ogólnej podstawy prawnej przetwarzania danych osobowych, a jednocześnie stwierdzono, że dostawcy systemów sztucznej inteligencji wysokiego ryzyka „mogą przetwarzać szczególne kategorie danych osobowych” w celu zapewnienia monitorowania, wykrywania i korygowania tendencyjności; przewidziano w nim ponadto wymóg stosowania dodatkowych zabezpieczeń w odniesieniu do tego przetwarzania²⁹.
- **Pokrywające się (częściowo) terminy** o wyraźnie odmiennych znaczeniach, takie jak „usługi pośrednictwa internetowego” w proponowanym akcie o rynkach cyfrowych i „usługi pośrednictwa w zakresie danych” w proponowanym akcie w sprawie zarządzania danymi, są mylące i wpływają negatywnie na przejrzystość wniosków.

²⁴ Zgodnie z podstawowymi prawami do prywatności i ochrony danych osobowych przewidzianymi w art. 7 i 8 Karty UE oraz w art. 16 TFUE.

²⁵ EROD z zadowoleniem przyjmuje fakt, że w mandacie Rady dotyczącym aktu w sprawie zarządzania danymi przyjętym 24 września 2021 r. pojęcia zgody i osoby, której dane dotyczą, zostały dostosowane do wymogów dotyczących zgody określonych w RODO.

²⁶ Art. 29 aktu o usługach cyfrowych.

²⁷ Zob. opinia EIOD w sprawie aktu o usługach cyfrowych, pkt 73.

²⁸ Art. 5 ust. 6 aktu w sprawie zarządzania danymi.

²⁹ Art. 10 ust. 5 aktu w sprawie sztucznej inteligencji.

- Jedną z głównych kwestii budzących zastrzeżenia w odniesieniu do proponowanego aktu w sprawie zarządzania danymi jest to, że przepisy nie precyzują w wystarczającym stopniu, **czy odnoszą się do danych nieosobowych, danych osobowych czy obu rodzajów danych**, ani nie precyzują w wystarczającym stopniu, że w przypadku „mieszanych zbiorów danych” zastosowanie ma RODO. W związku z tym nie jest jasne, czy ramy ochrony danych miałyby nadal zastosowanie w każdym przypadku przetwarzania danych osobowych oraz kiedy należy uwzględnić konkretne zagrożenia związane z ponowną identyfikacją zanonimizowanych danych osobowych³⁰. Ten brak rozróżnienia może prowadzić do nieporozumień, na przykład odnośnie do tego, czy wymagana jest podstawa prawna zgodna z RODO (co ma miejsce w przypadku każdego przetwarzania danych osobowych wchodzącego w zakres jego stosowania)³¹.

Perspektywy:

Europejska Rada Ochrony Danych zdaje sobie sprawę, że jedną z kluczowych inicjatyw w ramach europejskiej strategii w zakresie danych jest stworzenie **wspólnych europejskich przestrzeni danych** w strategicznych sektorach i obszarach leżących w interesie publicznym, w tym w obszarze zdrowia („europejska przestrzeń danych dotyczących zdrowia”). EROD i EIOD podkreślili już we wspólnej opinii dotyczącej aktu w sprawie zarządzania danymi, że we wszystkich przyszłych inicjatywach, takich jak **akt w sprawie danych**, które mogą mieć wpływ na przetwarzanie danych osobowych, należy zapewnić i utrzymać poszanowanie i stosowanie dorobku prawnego UE w dziedzinie ochrony danych osobowych³².

W chwili sporządzania niniejszego oświadczenia cel i treść wniosków dotyczących aktu w sprawie danych i europejskiej przestrzeni danych dotyczących zdrowia nie są jeszcze dostępne. Oczywiście jest jednak, że obie inicjatywy będą miały na celu zwiększenie dostępu do danych (osobowych) i ich ponownego wykorzystywania na potrzeby wymiany danych między podmiotami prywatnymi i publicznymi.

W podobnym duchu Europejska Rada Ochrony Danych wzywa zatem Komisję, aby ta unikała niejasności w nowych wnioskach, co pozwoli zagwarantować pewność prawa i spójność z istniejącymi ramami ochrony danych, a tym samym skuteczne stosowanie tych ram. Niezależnie od powyższego we wnioskach tych należy wyraźnie wskazać, **że nie mają one wpływu na stosowanie obowiązujących przepisów o ochronie danych ani ich nie podważają, a także zapewnić pierwszeństwo stosowania przepisów o ochronie danych w każdym przypadku przetwarzania danych osobowych**³³.

Ponadto, mając na uwadze szczególne wyzwania związane ze wzmożoną wymianą danych, Europejska Rada Ochrony Danych wzywa do tego, by w przyszłych wnioskach ustawodawczych dotyczących europejskich przestrzeni danych i w akcie w sprawie danych już na samym wstępie określać **konkretne zabezpieczenia w zakresie ochrony danych**, zapewniając wysoki stopień ochrony danych, z uwzględnieniem, w stosownych przypadkach, przetwarzania szczególnych kategorii danych, takich jak dane dotyczące zdrowia. Dzięki wyraźnemu zdefiniowaniu tych zabezpieczeń już na samym

³⁰ Zob. wspólna opinia EROD i EIOD dotycząca aktu w sprawie zarządzania danymi, pkt 16.

³¹ Zob. również pkt 47–56 wspólnej opinii EROD i EIOD dotyczącej aktu w sprawie zarządzania danymi, w których wskazano brak pewności prawa w odniesieniu do podstawy prawnej przetwarzania danych osobowych.

³² Wspólna opinia EROD i EIOD dotycząca aktu w sprawie zarządzania danymi, pkt 19.

³³ Zgodnie z podstawowymi prawami do prywatności i ochrony danych osobowych przewidzianymi w art. 7 i 8 Karty UE oraz w art. 16 TFUE.

wstępie możemy zapewnić odpowiedni stopień ochrony danych osobowych i uniknąć potencjalnego braku pewności prawa.

Poza wskazanymi powyżej obawami związanymi ze wszystkimi proponowanymi aktami Europejska Rada Ochrony Danych pragnie podkreślić:

(i) **niezbywalny charakter** prawa do ochrony danych osobowych jako prawa odnoszącego się do **każdej osoby fizycznej**, ustanowionego w art. 16 ust. 1 TFUE i art. 8 Karty UE, którego nie można się zrzec³⁴.

(ii) potrzebę wprowadzenia **szczególnych zabezpieczeń w celu zapewnienia zgodności ze wszystkimi zasadami ochrony danych**, a w szczególności z zasadami **minimalizacji danych, ograniczenia celu i przejrzystości**. Odpowiednie zabezpieczenia obejmują między innymi: określenie rodzajów danych, które mogą być przetwarzane, celów, w jakich dane mogą być przetwarzane, osób, których takie dane dotyczą, podmiotów, którym takie dane osobowe mogą być udostępniane, oraz okresów przechowywania. Szczególną uwagę należy zwrócić na zabezpieczenia dotyczące przetwarzania **do celów badań naukowych**, takie jak **wymóg weryfikacji** naukowców, którzy będą mieli dostęp do dużej ilości potencjalnie wrażliwych danych osobowych³⁵. Pomoże to zapewnić **zgodne z prawem, odpowiedzialne i etyczne** zarządzanie danymi.

(iii) znaczenie obowiązku **uwzględniania ochrony danych już w fazie projektowania i domyślnej ochrony danych**, który jest szczególnie istotny w kontekście „**przedmiotów podłączonych do internetu**” (np. internetu rzeczy i internetu ciał³⁶), ze względu na poważne zagrożenia dla podstawowych praw i wolności zainteresowanych osób³⁷.

W imieniu Europejskiej Rady Ochrony Danych

Przewodnicząca

(Andrea Jelinek)

³⁴ Oświadczenie EROD dotyczące aktu w sprawie zarządzania danymi w świetle zmian legislacyjnych, s. 4.

³⁵ Zob. na przykład warunki określone w art. 31 ust. 4 i 5 aktu o usługach cyfrowych.

³⁶ Zob. wstępna ocena skutków aktu w sprawie danych, s. 6, odnosząca się do „inteligentnych urządzeń gospodarstwa domowego, urządzeń do noszenia na ciele i asystentów domowych”, dostępna pod adresem: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en.

³⁷ Zob. opinia Grupy Roboczej Art. 29 nr 8/2014 w sprawie najnowszych osiągnięć w zakresie internetu przedmiotów, s. 6–9, dostępna pod adresem: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_pl.pdf.

ZAŁĄCZNIK: Wykaz wcześniejszych opinii i oświadczeń przyjętych przez EROD i EIOD

-) Wspólna opinia EROD i EIOD 03/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi), przyjęta 11 marca 2021 r., dostępna pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_pl
-) Oświadczenie EROD 05/2021 dotyczące aktu w sprawie zarządzania danymi w świetle zmian legislacyjnych, przyjęte 19 maja 2021 r., dostępne pod adresem: https://edpb.europa.eu/system/files/2021-05/edpb_statementondga_19052021_en_0.pdf
-) Wspólna opinia EROD i EIOD 05/2021 w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji („akt w sprawie sztucznej inteligencji”), przyjęta 18 czerwca 2021 r., dostępna pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_pl
-) Opinia EIOD 01/2021 w sprawie wniosku dotyczącego aktu o usługach cyfrowych, przyjęta 10 lutego 2021 r., dostępna pod adresem: https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en
-) Opinia EIOD 02/2021 w sprawie wniosku dotyczącego aktu o rynkach cyfrowych, przyjęta 10 lutego 2021 r., dostępna pod adresem: https://edps.europa.eu/data-protection/our-work/publications/opinions/digital-services-act_en
-) Opinia EIOD 03/2020 w sprawie europejskiej strategii w zakresie danych, przyjęta 16 czerwca 2020 r., dostępna pod adresem: https://edps.europa.eu/sites/default/files/publication/20-06-16_opinion_data_strategy_en.pdf
-) Wstępna opinia EIOD 8/2020 w sprawie europejskiej przestrzeni danych dotyczących zdrowia, przyjęta 17 listopada 2020 r., dostępna pod adresem: https://edps.europa.eu/sites/default/files/publication/20-11-17_preliminary_opinion_european_health_data_space_en.pdf.