PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 01.09.2025 r.

DPNT.413.39.2025

Pani
Jolanta Sobierańska-Grenda
Minister Zdrowia
Ministerstwo Zdrowia

Pan
Marcin Kulasek
Minister Nauki i Szkolnictwa Wyższego
Ministerstwo Nauki i
Szkolnictwa Wyższego

Szanowna Pani Minister,

Szanowny Panie Ministrze,

w związku z rozwojem nowych technologii przetwarzania danych, w tym danych osobowych, z wykorzystaniem również systemów opartych na algorytmach sztucznej inteligencji, środowiska medyczne i naukowe, jak też Agencja Badań Medycznych, zgłaszają Prezesowi Urzędu Ochrony Danych Osobowych problemy związane ze stosowaniem i wykładnią przepisów ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta[1] oraz ustawy Prawo o szkolnictwie wyższym i nauce[2] w kontekście wykorzystywania zasobów danych medycznych, w tym zindywidualizowanych w celach badań naukowych.

Zważywszy na sygnalizowane problemy, po analizie regulacji prawnych – w szczególności z punktu widzenia unijnych rozporządzeń, w tym rozporządzenia o europejskiej przestrzeni danych dotyczących zdrowia (ang. EHDS)[3], które weszło w życie 26 marca 2025 r., jak również aktu w sprawie zarządzania danymi[4] oraz aktu w

[1] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. z 2024 r. poz. 581; dalej: ustawa o prawach pacjenta i Rzeczniku Praw Pacjenta).
[2] Ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571 ze zm.; dalej: ustawa - Prawo o szkolnictwie wyższym i nauce).
[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/327 z dnia 11 lutego 2025 r. w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847 (dalej: EHDS).
[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi).

sprawie sztucznej inteligencji[5] – **wobec braku w prawie krajowym adekwatnych i proporcjonalnych rozwiązań prawnych w zakresie ochrony danych osobowych w odniesieniu do regulacji dotyczących udostępnienia dokumentacji medycznej w celach naukowych, w ocenie Prezesa UODO, konieczne jest dokonanie przeglądu przepisów krajowych i podjęcie właściwych działań legislacyjnych w tym obszarze**.

Należy przy tym wskazać, że udostępnianie i dalsze wtórne wykorzystywanie danych osobowych oraz danych nieosobowych dotyczących zdrowia ma istotne znaczenie z punktu widzenia zarówno interesów państwa, jak i interesów (także zbiorowych) osób fizycznych (w szczególności pacjentów), których dane dotyczą, w kontekście wynikającego z EHDS obowiązku wtórnego wykorzystania elektronicznych danych dotyczących zdrowia.

W związku z powyższym należy stwierdzić, że podstawą przetwarzania danych w zakresie niezbędnym do prowadzenia badań naukowych i prac rozwojowych może być zasadniczo art. 9 ust. 2 lit. j rozporządzenia 2016/679 w zw. z art. 26 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz w zw. z art. 469b ust. 2-4 ustawy Prawo o szkolnictwie wyższym i nauce (por. także art. 15 ust. 3 i następne ustawy z o Agencji Badań Medycznych)[6]. Niemniej, regulacje te pozostają względem w siebie w relacji budzącej wątpliwości interpretacyjne, jak też ich zakres nie odpowiada potrzebom wynikającym z celu prowadzenia badań naukowych i udzielania świadczeń leczniczych.

Warunki udostępniania dokumentacji medycznej zostały określone w art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Zgodnie z brzmieniem tego przepisu udostępnienie dokumentacji medycznej szkole wyższej lub instytutowi badawczemu w celach naukowych może nastąpić „bez ujawniania nazwiska i innych danych umożliwiających identyfikację osoby, której dokumentacja dotyczy”. Z treści ww. przepisu jednoznacznie wynika, że nie jest dopuszczalne udostępnienie danych osobowych zawartych w dokumentacji medycznej w sposób umożliwiający ustalenie tożsamości osoby, której ta dokumentacja dotyczy. A zatem w odniesieniu do udostępnienia dokumentacji medycznej na podstawie art. 26 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta może nastąpić to w celach naukowych i badawczych pod warunkiem dokonania **anonimizacji danych osobowych** w tej dokumentacji zawartych.

Należy przy tym mieć na względzie, że istotną treścią dokumentacji medycznej są dane osobowe dotyczące najwrażliwszych sfer prywatności każdego człowieka. Oprócz danych o stanie zdrowia mogą to być dane genetyczne, dane o seksualności,

---

[5] Rozporządzenie Parlamentu i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Dz. Urz. UE. L. 2024.1689, dalej jako: akt w sprawie sztucznej inteligencji, lub AI Act).

[6] Ustawa z dnia 21 lutego 2019 r. o Agencji Badań Medycznych (Dz. U. z 2025 r. poz. 259; dalej ustawa o ABM).

o schorzeniach, których źródłem są uzależnienia bądź nałogi, ujawniające pochodzenie rasowe i etniczne czy też dane określające przekonania religijne oraz światopoglądowe, np. gdy dany pacjent z uwagi na przekonania odmawia zgody na wykonanie określonego zabiegu[7]. Dokumentacja medyczna zawiera również dane osobowe osób trzecich, np. członków rodziny.

W tym kontekście istotna jest również treść motywu 35 rozporządzenia 2016/679, zgodnie z którym do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą[8]. Zgodnie z orzecznictwem Trybunału Sprawiedliwości UE (TSUE), pojęcie „danych dotyczących zdrowia" należy rozumieć szeroko. Jak podkreśla Trybunał, szeroka wykładnia pojęć szczególnych kategorii danych osobowych jest zgodna z celem rozporządzenia 2016/679 , jakim jest zagwarantowanie wysokiego poziomu ochrony podstawowych praw i wolności osób fizycznych, a zwłaszcza ich życia prywatnego, w zakresie przetwarzania danych osobowych, które ich dotyczą[9].

Ze względu na wysoce wrażliwy charakter danych dotyczących zdrowia – mających status danych szczególnej kategorii (art. 9 rozporządzenia 2016/679) – należy więc mieć na uwadze konieczność dokonywania, we wskazanych celach naukowych, anonimizacji danych osobowych medycznych, w taki sposób, aby **zapewnić nieodwracalność tego procesu** i jego realizację z poszanowaniem zasady poufności i integralności wynikającej z art. 5 ust. 1 lit. f rozporządzenia 2016/679[10]. Jest to istotne z punktu widzenia poszanowania tajemnic prawnie chronionych, m.in. tajemnicy zawodowej lekarza, przewidzianej w art. 13 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, a także tajemnicy medycznej jaką dokumentacja medyczna jest prawnie chroniona, do czego nawiązuje regulacja rozporządzenia nakładające szczególne wymogi dla przetwarzania danych dotyczących zdrowia (art. 9 ust. 3 rozporządzenia 2016/679).

---

[7] M. Krasińska, *Przetwarzanie danych osobowych w dokumentacji medycznej* [w:] K. Andres, E. Bielak-Jomaa, M. Jagielski, P. Kawczyński, M. Krasińska, P. Litwiński, A. Sieradzka, K. Wojsyk, *Ochrona danych osobowych medycznych*, Warszawa 2018.

[8] Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro

[9] Zob. wyroki: TSUE z 6.11.2013 r. w sprawie C-101/01, Bodil Lindqvist, z 1.08.2022 w sprawie C-184/20, z 4.10.2024 r. w sprawie C-21/23.

[10] Zob. opinię Grupy Roboczej Art. 29 nr 4/2007 w sprawie pojęcia danych osobowych, przyjęta 20 czerwca 2007 r.

W ramach rozwoju nauk medycznych i kształtowania odpowiednich rozwiązań technologicznych sprzyjających ochronie zdrowia przedstawiciele licznych środowisk wskazują na potrzebę pozyskiwania danych z dokumentacji medycznej do wykorzystania w celach naukowych w sposób uniemożliwiający identyfikację pacjenta po stronie odbiorcy danych (szkoła wyższa lub instytut badawczy), jednakże w postaci spseudonimizowanej, tj. zaszyfrowanych danych za pomocą „klucza kodującego" niemożliwego do zwrotnego odkodowania przez odbiorcę danych, ale będącego w posiadaniu podmiotu udostępniającego dane.

Dane speudonimizowane, jak wynika z Wytycznych Europejskiej Rady Ochrony Danych (EROD) nr 01/2025 w sprawie pseudonimizacji, które można przypisać osobie fizycznej za pomocą dodatkowych informacji, **należy uznawać za informacje o możliwej do zidentyfikowania osobie fizycznej, a zatem za dane osobowe**[11]. To stwierdzenie jest również prawdziwe, jeśli spseudonimizowane dane i dodatkowe informacje nie znajdują się we władaniu tej samej osoby czy podmiotu[12]. Jeżeli dane spseudonimizowane i dodatkowe informacje mogłyby zostać połączone z uwzględnieniem środków, które z rozsądnym prawdopodobieństwem mogą zostać wykorzystane przez administratora lub inną osobę, wówczas dane spseudonimizowane są danymi osobowymi. Nawet jeżeli wszystkie dodatkowe informacje przechowywane przez administratora pseudonimizującego zostały usunięte, spseudonimizowane dane stają się anonimowe tylko wtedy, gdy spełnione są warunki anonimowości.

Pseudonimizacja danych stanowi więc formę zabezpieczenia praw i wolności podmiotów danych w kontekście przetwarzania danych osobowych w celach badań naukowych i powinna być ujęta w przepisach prawa regulujących ten obszar przetwarzania danych. Pseudonimizacja jest bowiem zabezpieczeniem, które wykonawcy norm (administratorzy) mogą stosować w celu spełnienia wymogów prawa o ochronie danych, a w szczególności w celu wykazania zgodności z zasadami ochrony danych zgodnie z art. 5 ust. 2 RODO[13].

W art. 26 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta ustawodawca nie przewidział jednak adekwatnych regulacji dotyczących pseudonimizacji, **umożliwił jedynie dokonanie anonimizacji danych podczas udostępniania dokumentacji medycznej w celach naukowych.** Aktualne regulacje nie przewidują zatem żadnych wyjątków w zakresie udostępniania danych medycznych w celach naukowych, umożliwiając udostępnianie wyłącznie danych nieosobowych. **Powoduje to, że wynik badań naukowych, w ramach których np. uzyskuje się informacje, które byłyby istotne z punktu widzenia leczenia konkretnego pacjenta, nie mogą być w takim celu wykorzystane.**

Dla pełnej oceny prawnej wskazać należy, że art. 469b ustawy Prawo o szkolnictwie wyższym i nauce dotyczy przetwarzania danych osobowych w celach

[11] Wytyczne EROD 01/2025 w sprawie pseudonimizacji, przyjęte 16 stycznia 2025 r.
[12] Wyrok TSUE z 19 października 2016 r. w sprawie C-582/14 Breyer.
[13] Zob. Wytyczne 01/2025 w sprawie pseudonimizacji.

naukowych w odniesieniu do podmiotów wskazanych w art. 7 ust. 1 pkt 1, 4-7 tej ustawy[14], przewidując konieczność wdrożenia przez administratora odpowiednich zabezpieczeń technicznych i organizacyjnych praw i wolności osób fizycznych, których dane osobowe są przetwarzane, w szczególności przez pseudonimizację albo szyfrowanie danych (por. też art. 15 ust. 3 i następne ustawy o ABM). Wobec braku adekwatnych gwarancji w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta, przepis ten nie może jednak stanowić podstawy pozyskiwania danych osobowych z dokumentacji medycznej.

Tymczasem zwalniająca z zakazu przetwarzania danych szczególnej kategorii przesłanka z art. 9 ust. 2 lit. j rozporządzenia 2016/679 – **niezbędność przetwarzania** do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, zgodnie z art. 89 ust. 1 rozporządzenia 2016/679 – **musi wynikać z prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą**. Zgodnie z art. 89 ust. 1 rozporządzenia 2016/679 przetwarzanie do celów badań naukowych podlega odpowiednim **zabezpieczeniom** dla praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te polegają na wdrożeniu środków technicznych i organizacyjnych zapewniających poszanowanie zasady minimalizacji danych, a środki te mogą też obejmować pseudonimizację danych, o ile pozwala ona realizować powyższe cele. **Jeżeli cele te można zrealizować w drodze dalszego przetwarzania danych, które nie pozwalają albo przestały pozwalać na zidentyfikowanie osoby, której dane dotyczą, cele należy realizować w ten sposób**.

Tym samym, na gruncie rozporządzenia 2016/679 dopuszczalne jest przetwarzanie danych osobowych do celów badań naukowych, jednakże z zastrzeżeniem zapewnienia odpowiednich warunków, wynikających z art. 9 ust. 2 lit. j rozporządzenia 2016/679 (w tym niezbędności przetwarzania) i zabezpieczeń dla praw i wolności podmiotów danych, o których mowa w art. 89 ust. 1 rozporządzenia 2016/679 (np. poprzez pseudonimizację danych, ale nawet anonimizację danych), przewidzianych w prawie Unii lub w prawie państwa członkowskiego.

[14] Zgodnie z art. 7 ust. 1 pkt 1, 4-7 tej ustawy będą to podmioty: uczelnie; instytuty naukowe PAN; instytuty badawcze, działające na podstawie ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych; międzynarodowe instytuty naukowe utworzone na podstawie odrębnych ustaw działające na terytorium Rzeczypospolitej Polskiej, zwane dalej "instytutami międzynarodowymi"; Centrum Łukasiewicz, działające na podstawie ustawy z dnia 21 lutego 2019 r. o Sieci Badawczej Łukasiewicz; instytuty działające w ramach Sieci Badawczej Łukasiewicz; Centrum Medycznego Kształcenia Podyplomowego, działające na podstawie ustawy z dnia 13 września 2018 r. o Centrum Medycznego Kształcenia Podyplomowego; Polska Akademia Umiejętności.

Należy mieć również na względzie perspektywę przepisów EHDS. Jak wynika z motywu 72 oraz art. 66 ust. 2 i 3 EHDS[15]: „ponieważ elektroniczne dane dotyczące zdrowia stanowią dane wrażliwe, należy ograniczyć ryzyko dotyczące prywatności osób fizycznych poprzez stosowanie zasady minimalizacji danych. W związku z powyższym **elektroniczne dane nieosobowe dotyczące zdrowia powinny być udostępniane we wszystkich przypadkach, gdy dostarczenie takich danych jest wystarczające**. Jeżeli użytkownik danych dotyczących zdrowia musi użyć elektronicznych danych osobowych dotyczących zdrowia, powinien podać we wniosku wyraźne uzasadnienie stosowania tego typu danych, a organ ds. dostępu do danych dotyczących zdrowia powinien ocenić zasadność tego uzasadnienia. **Elektroniczne dane osobowe dotyczące zdrowia należy udostępniać wyłącznie w formacie spseudonimizowanym**. Biorąc pod uwagę konkretne **cele** przetwarzania, elektroniczne dane osobowe dotyczące zdrowia należy **spseudonimizować lub zanonimizować** na jak najwcześniejszym etapie procesu udostępniania danych do wtórnego wykorzystywania".

Przepisy EHDS przewidują zatem możliwość udostępnienia danych dotyczących zdrowia w celu wtórnego wykorzystywania w postaci **zanonimizowanej**, zaś w pewnych przypadkach, **ograniczonych do sytuacji wyraźnie uzasadnionych**, danych również w postaci spseudonimizowanej.

W tym zakresie potrzebne są zatem odpowiednie przepisy krajowe – odpowiadające warunkom przewidzianym we wskazanych rozporządzeniach ogólnych, ale i realizujące *ratio legis* zarówno dla dobra pacjentów, jak i dla celów naukowych.

Rozporządzenie 2016/679 nie stoi zatem na przeszkodzie realizacji przepisów EHDS, ale wyraźnie odwołuje się do konieczności zagwarantowania wysokiego stopnia ochrony danych osobowych – wyważenia równowagi pomiędzy dobrami i prawami podstawowymi oraz istotnymi celami przetwarzania danych – a zatem zapewnienia w przepisach krajowych regulacji, których treść nie będzie budzić wątpliwości co do dopuszczalności przetwarzania danych osobowych. Szybki postęp techniczny i globalizacja przyniosły bowiem nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Przemiany te wymagają zatem stabilnych, spójniejszych ram ochrony danych w Unii oraz zdecydowanego ich egzekwowania, gdyż **ważna jest budowa zaufania, które pozwoli na rozwój**

[15] Zgodnie z art. 66 ust. 2 i 3 EHDS organy ds. dostępu do danych dotyczących zdrowia przekazują elektroniczne dane dotyczące zdrowia w **formacie zanonimizowanym**, jeżeli takie dane umożliwiają osiągnięcie celu przetwarzania przez użytkownika danych dotyczących zdrowia, biorąc pod uwagę informacje przekazane przez użytkownika danych dotyczących zdrowia (ust. 2). Jeżeli użytkownik danych dotyczących zdrowia wykazał w wystarczającym stopniu, że celu przetwarzania nie można osiągnąć za pomocą zanonimizowanych danych, zgodnie z art. 68 ust. 1 lit. c) organy ds. dostępu do danych dotyczących zdrowia udzielają dostępu do elektronicznych danych dotyczących zdrowia w formacie spseudonimizowanym. Informacje niezbędne do odwrócenia procesu pseudonimizacji są dostępne wyłącznie dla organu ds. dostępu do danych dotyczących zdrowia lub podmiotu, który występuje jako zaufana strona trzecia zgodnie z prawem krajowym (ust. 3).

gospodarki cyfrowej na rynku wewnętrznym. Osoby fizyczne powinny więc mieć kontrolę nad własnymi danymi osobowymi. Osoby fizyczne, podmioty gospodarcze i organy publiczne powinny zyskać większe **poczucie pewności prawa i jego stosowania w praktyce** (zob. motyw 6 i 7 rozporządzenia 2016/679).

Zgodnie z art. 5 ust. 1 lit a oraz stosownie do motywu 41 rozporządzenia 2016/679, podstawa prawna lub akt prawny będący podstawą do przetwarzania danych osobowych powinny być **jasne i precyzyjne**, a ich **zastosowanie przewidywalne dla osób im podlegających** – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej i Europejskiego Trybunału Praw Człowieka. Jak stanowi zaś art. 6 ust. 3 rozporządzenia 2016/679 **podstawa przetwarzania**, o której mowa w ust. 1 lit. c) i e), **musi być określona w prawie Unii lub w prawie państwa członkowskiego**, któremu podlega administrator i ma zawierać cel przetwarzania, a dodatkowo także przepisy szczegółowe dostosowujące stosowanie przepisów rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania. Prawo ma służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

Realizacja zasady zgodności z prawem, rzetelności i przejrzystości wynikająca z art. 5 ust. 1 lit. a rozporządzenia 2016/679 w zw. z art. 6 ust. 3 oraz w zw. z art. 9 ust. 2 lit. j w zw. z art. 89 ust.1 rozporządzenia 2016/679, wymaga zatem od prawodawcy krajowego **właściwego wdrożenia unijnych przepisów dotyczących wtórnego wykorzystywania danych dotyczących zdrowia**, poprzez stworzenie adekwatnych rozwiązań prawnych, które **w sposób jasny i precyzyjny będą wskazywały na właściwe gwarancje ochrony danych osobowych dotyczących zdrowia**, w tym wymagające zachowania tajemnicy zawodowej. Jak wynika z art. 9 ust. 3 rozporządzenia 2016/679 obowiązek zachowania tajemnicy zawodowej przy przetwarzaniu szczególnych kategorii danych powinien być nałożony przepisami prawa i dotyczyć osób przetwarzających dane.

Rozwiązania te powinny odpowiadać porządkowi konstytucyjnemu, który przewiduje – w art. 47 oraz art. 51 w zw. z art. 31 ust. 3 Konstytucji RP – wysoki standard ochrony danych osobowych i prawa do prywatności wskazując na konieczność wprowadzenia ograniczeń tych praw w formie ustawowej.

Skoro aktualne regulacje krajowe przewidują w art. 26 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta możliwość udostępnienia w celach naukowych jedynie nieosobowych danych dotyczących zdrowa, to w ocenie Prezesa UODO, **uzasadnionym jest podjęcie właściwych działań legislacyjnych w kierunku określenia właściwej podstawy prawnej dla udostępnienia danych medycznych w formacie również spseudonimizowanym** – co jednak ważne, stosownie do wymagań EHDS – **ograniczonych do sytuacji wyraźnie uzasadnionych** oraz

niezbędnych dla celów badań naukowych a także wskazujących dopuszczalne sposoby przetwarzania takich danych. Prawodawca powinien stworzyć podstawę prawną uwzględniając właściwe gwarancje dla ochrony danych osobowych, jak tego wymagają regulacje rozporządzenia 2016/679 (art. 9 ust. 2 lit. j oraz ust. 3 w zw. z art. 89 ust. 1 rozporządzenia 2016/679) oraz EHDS (66 ust. 2 i 3 EHDS), dotyczące wtórnego wykorzystywania danych dotyczących zdrowia[16].

Podsumowując, **art. 26 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta jest przykładem regulacji, która w kontekście stosowania przepisów EHDS wymaga zmiany.**

Wdrożenie tego rozporządzenia unijnego wymaga jednak dokonania przeglądu regulacji prawnych w szerszym zakresie, w tym obejmującego przepisy ustawy o systemie informacji w ochronie zdrowia[17], ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych[18], które w ocenie Prezesa UODO nie spełniają aktualnie właściwych standardów ochrony danych osobowych, a także wymogów EHDS[19].

W kontekście przepisów aktu o sztucznej inteligencji, w przypadku przetwarzania danych w celach badań naukowych oparcie procesów przetwarzania, zwłaszcza trenowania systemów AI, na danych anonimowych lub syntetycznych, niepowiązanych z osobami fizycznymi, jest jedną ze stosowanych i zalecanych strategii uwzględniania ochrony danych w fazie projektowania (art. 25 rozporządzenia 2016/679)[20].

---

[16] Jak wynika motywu 77 EHDS „przetwarzanie danych osobowych w (…) bezpiecznym środowisku przetwarzania powinno być zgodne z rozporządzeniem (UE) 2016/679, w tym – w przypadku gdy bezpiecznym środowiskiem zarządza strona trzecia – z wymogami określonymi w art. 28 tego rozporządzenia oraz, w stosownych przypadkach, w rozdziale V tego rozporządzenia. Takie bezpieczne środowisko przetwarzania powinno ograniczać ryzyko dla prywatności związane z takimi czynnościami przetwarzania i uniemożliwiać przekazywanie elektronicznych danych dotyczących zdrowia bezpośrednio użytkownikom danych dotyczących zdrowia. Organ ds. dostępu do danych dotyczących zdrowia lub posiadacz danych dotyczących zdrowia świadczący tę usługę powinni przez cały czas sprawować kontrolę nad dostępem do elektronicznych danych dotyczących zdrowia, a dostęp udzielany użytkownikom danych dotyczących zdrowia powinien być obwarowany warunkami określonymi w wydanym zezwoleniu na dostęp do danych. Z takiego bezpiecznego środowiska przetwarzania użytkownicy danych dotyczących zdrowia powinni pobierać jedynie elektroniczne dane nieosobowe dotyczące zdrowia, które nie zawierają żadnych elektronicznych danych osobowych dotyczących zdrowia. Takie bezpieczne środowisko przetwarzania jest zatem podstawowym zabezpieczeniem chroniącym prawa i wolności osób fizycznych w związku z przetwarzaniem ich elektronicznych danych dotyczących zdrowia do celów wtórnego wykorzystywania”.

[17] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2025 r. poz. 302)

[18] Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2024 r. poz. 146)

[19] Por. opinia Prezesa UODO dot. w sprawie projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw (UD 238 (DPNT.401.224.2025).

[20] Jak wynika z opinii EROD nr 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli AI, przyjętej 17 grudnia 2024 r. ustalenie, czy model sztucznej inteligencji jest anonimowy, powinno być oceniane indywidualnie w oparciu o określone kryteria. Jak wskazano w opinii, aby model sztucznej inteligencji można było uznać za anonimowy, przy użyciu rozsądnych środków zarówno (i) prawdopodobieństwo bezpośredniego (w tym probabilistycznego) wyodrębnienia danych osobowych dotyczących osób, których dane osobowe

Akt w sprawie zarządzania danymi, określając warunki ponownego wykorzystywania danych, również przewiduje konieczność zapewnienia przez podmioty sektora publicznego ochrony danych podczas udostępniania danych do celów ponownego wykorzystywania poprzez m.in. anonimizację danych osobowych[21].

Przy podejmowaniu działań legislacyjnych w tym obszarze konieczne jest zachowanie odpowiednich standardów dotyczących przetwarzania danych osobowych, gdyż wskazane akty unijne funkcjonują równolegle do rozporządzenia 2016/679, a celem tego rozporządzenia jest zagwarantowanie wysokiego poziomu ochrony podstawowych praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych (art. 1 ust. 2 oraz motywy 4 i 10 rozporządzenia 2016/679), które to prawo chronione jest mocą art. 8 Karty praw podstawowych UE i jest ściśle związane z prawem do poszanowania życia prywatnego, wyrażonym w art. 7 Karty praw podstawowych UE. Prezes UODO, jako organ stojący na straży ochrony danych osobowych, zobowiązany jest natomiast do dbania o właściwy standard tej ochrony, także poprzez sygnalizowanie potrzeb zmian przepisów prawa krajowego.

Należy przy tym podkreślić, że projektowanie rozwiązań prawnych w tym obszarze wymaga dokonania **oceny skutków dla ochrony danych**. Do jej przeprowadzenia zobowiązuje art. 35, w szczególności w procesie tworzenia prawa art. 35 ust. 10 rozporządzenia 2016/679 oraz art. 25 ust. 1 i 2 rozporządzenia 2016/679. Przeprowadzenie oceny skutków ułatwia także zapewnienie i wykazanie zgodności z dotyczącymi przetwarzania danych osobowych zasadami wynikającymi z art. 5 rozporządzenia 2016/679, a także wykazanie spełnienia warunków przetwarzania danych osobowych określonych w art. 6 ust. 3 i art. 9 ust. 2 i 3. Ocena taka pozwala ocenić czy rozwiązania zawarte w projekcie przewidują jednocześnie odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą, zwłaszcza – jak wymagają wskazane przepisy rozporządzenia 2016/679 – z uwagi na charakter

---

zostały użyte do szkolenia modelu, jak i (ii) prawdopodobieństwo uzyskania takich danych osobowych w wyniku zapytań, celowo lub nie, powinny być znikome dla każdej osoby, której dane dotyczą (https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_pl_0.pdf). Por. D. Lubasz, *RODO dla AI. Zgodność z zasadami godnej zaufania sztucznej inteligencji w modelu data protection by design*, Warszawa 2025. Por. wyrok TSUE z 19 października 2016 r. w sprawie Breyer, C-582/14, wyrok TSUE z 19 października 2016 r. w sprawie Nowak, C-582/14.

[21] Zgodnie z art. 5 aktu w sprawie zarządzania danymi wskazuje warunki ponownego wykorzystywania danych, w tym m.in. konieczność zapewnienia przez podmioty sektora publicznego, zgodnie z prawem Unii i prawem krajowym, aby chroniony charakter danych został zachowany, poprzez możliwość ustanawiania wymagań: a) dostępu do celów ponownego wykorzystywania danych udziela się wyłącznie pod warunkiem, że podmiot sektora publicznego lub właściwy podmiot po otrzymaniu wniosku o ponowne wykorzystywanie zapewniły, by dane te: zostały zanonimizowane - w przypadku danych osobowych; oraz (ii) zostały zmodyfikowane, zagregowane lub przekształcone za pomocą innej metody zapobiegającej ujawnieniu - w przypadku poufnych informacji handlowych, w tym tajemnic handlowych lub treści chronionych prawami własności intelektualnej; b) dostęp do danych i ich ponowne wykorzystywanie odbywa się w sposób zdalny w bezpiecznym środowisku przetwarzania zapewnianym lub kontrolowanym przez podmiot sektora publicznego; c) jeżeli nie można zezwolić na dostęp zdalny bez stwarzania zagrożenia dla praw i interesów osób trzecich, dostęp do danych i ich ponowne wykorzystywanie odbywa się w obrębie obiektów fizycznych, w których panuje bezpieczne środowisko przetwarzania zgodnie z rygorystycznymi normami bezpieczeństwa.

danych, rodzaj (sposób) przetwarzania, w szczególności z użyciem nowych technologii, ze względu na zakres, kontekst i cele oraz z uwzględnieniem prawdopodobieństwa ryzyka naruszenia praw lub wolności osób fizycznych.

W przypadku zatem podjęcia działań legislacyjnych w tym zakresie, Prezes UODO deklaruje swoje wsparcie eksperckie celem zapewnienia ww. standardu dla realizacji tak ważnego celu jakim są badania naukowe w środowisku medycznym, które służą poprawie sytuacji pacjentów.

Uprzejmie proszę Państwa Ministrów o udzielenie odpowiedzi na niniejsze wystąpienie w terminie 30 dni od dnia jego otrzymania.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

Do wiadomości:
Prezes
Agencji Badań Medycznych