



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**

Mirosław Wróblewski

Warszawa, 26 maja 2026

DPNT.060.21.2026.MKS

**Pani
Katarzyna Bis-Płaza
Sekretarz Komitetu do spraw
Cyfryzacji
Ministerstwo Cyfryzacji**

Szanowna Pani Sekretarz,

w związku z przekazaniem do wiadomości organu nadzorczego pismem z 22 maja br. (znak: DPiS-WWKS.002.26.1.2026), dotyczącym opisu założeń projektu informatycznego **„WUM Data Hub - Centrum Doskonałości Danych WUM – cyfrowe udostępnienie i ponowne wykorzystanie zasobów naukowych Warszawskiego Uniwersytetu Medycznego”** (wnioskodawca: Minister Zdrowia, beneficjent: Warszawski Uniwersytet Medyczny; dalej: „opis założeń”), działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ oraz art. 51 ustawy o ochronie danych osobowych², Prezes UODO zgłasza uprzejmie **następujące uwagi**.

Z opisu założeń projektu informatycznego **WUM Data Hub - Centrum Doskonałości Danych WUM** wynika, że tworzony system ma umożliwiać „pozyskiwanie, porządkowanie, anonimizację, standaryzację, archiwizację i udostępnianie danych

¹ 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).

² Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 ze zm.).

naukowych, klinicznych, publikacyjnych oraz dydaktycznych w sposób wspierający ich bezpieczne i ponowne wykorzystanie przez odbiorców wewnętrznych i zewnętrznych”. Jednocześnie wskazuje się, że system ma służyć „uporządkowaniu i zintegrowaniu procesów przetwarzania danych w obszarze nauki, dydaktyki i ochrony zdrowia, tak aby możliwe było ich przekształcanie w informacje i wiedzę użyteczną dla badań, analiz i decyzji”. System ten ma być dodatkowo zintegrowany z innymi publicznymi systemami (dane.gov.pl, eCRF ABM, eCRF UCWBK, EDM, , e-learning WUM, eTMF UCWBK, HealthData@EU, openCARDIO, PPM, PPM WUM, REDCap, SGZ, SSOZ, System CDD, System mObywatel) a uwierzytelnienie użytkownika ma następować za pomocą Węzła Krajowego, a także Węzła transgranicznego.

1. W opisie założeń nie przewidziano jednak dokonania zmian w aktach prawnych (pkt 6, otoczenie prawne).

W opinii Prezesa UODO konieczne jest jednak **podjęcie działań legislacyjnych mających na celu określenie właściwej regulacji ustawowej dla przetwarzania przez podmioty objęte projektem danych osobowych dla tak określonych celów oraz sposobów przetwarzania**, w tym w związku z korzystaniem z nowych technologii w projektowanym systemie, ze względu także na szeroki zakres i charakter przetwarzanych także dotyczących zdrowia (szczególnych kategorii w rozumieniu przepisów rozporządzenia 2016/679).

Przypomnieć trzeba, że Prezes UODO w piśmie z 1 września 2025 r. wystąpił do Ministra Cyfryzacji oraz Ministra Zdrowia z wnioskiem o podjęcie działań legislacyjnych w kierunku określenia właściwej podstawy prawnej dla udostępnienia danych medycznych w celach naukowych i badawczych w formie spseudonimizowanym³. Aktualny stan prawny (art. 26 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta⁴) umożliwia bowiem udostępnienie dokumentacji medycznej **pod warunkiem dokonania anonimizacji danych osobowych w tej dokumentacji zawartych**, a regulacje prawne pozostają względem w sobie w relacji budzącej wątpliwości interpretacyjne, jak też ich zakres nie odpowiada potrzebom wynikającym z celu prowadzenia badań naukowych i udzielania świadczeń leczniczych (art. 26 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta w zw. z art. 469b ust. 2-4 ustawy Prawo o szkolnictwie wyższym i nauce⁵ a także art. 15 ust. 3 i następne ustawy z o Agencji Badań Medycznych⁶).

Konieczne jest natomiast – także dla dobra i komfortu prawnego wykonawców projektu – **dostosowanie prawa krajowego do przepisów EHDS⁷**, które umożliwiają, w sytuacjach wyraźnie uzasadnionych oraz niezbędnych dla celów badań naukowych, przetwarzanie danych spseudonimizowanych.

³ Zob. wystąpienie Prezesa UODO dostępne na stronie internetowej: <https://uodo.gov.pl/pl/138/3880>

⁴ Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2024 r. poz. 581).

⁵ Ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571).

⁶ Ustawa z dnia 21 lutego 2019 r. o Agencji Badań Medycznych (Dz. U. z 2025 r. poz. 259).

⁷ 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).

2. Projektodawca **nie wskazuje podmiotów odpowiedzialnych za przetwarzanie danych w tym systemie** (nie jest jasne, czy administratorem systemu ma być Minister Zdrowia, czy Warszawski Uniwersytet Medyczny), ani **zasad i trybu pozyskiwania danych z systemów publicznych** (w tym, nie jest jasne jak będą kształtować się zasady współpracy i odpowiedzialności za przetwarzanie danych między podmiotami – podmiotami publicznymi odpowiedzialnymi za przetwarzanie danych w rejestrach publicznych), **w szczególności nie jest jasne na jakim etapie będzie następował proces anonimizacji danych szczególnych kategorii**.

Projektodawca **nie wykazał też, że projekt w sposób właściwy będzie wdrażał postanowienia EHDS**, które wprowadzają określone warunki dla przetwarzania danych klinicznych jak również, że projekt **zapewnia zgodność z przepisami o badaniach klinicznych**⁸.

3. W przypadku przetwarzania danych osobowych przez podmioty publiczne, takie przetwarzanie powinno odbywać się **na podstawie przepisów prawa**, które w sposób precyzyjny wskazują cele przetwarzania, jakie dane dla ich realizacji będą przetwarzane, przez jaki okres czasu oraz kto będzie za to przetwarzanie odpowiadał. Przetwarzanie danych niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze lub wykonania zadania realizowanego w interesie publicznym (art. 6 ust. 1 lit. c i e rozporządzenia 2016/679⁹) wymaga określenia w prawie państwa członkowskiego, któremu podlega administrator – w tym w regulacji prawnej kształtującej funkcjonowanie przedmiotowego systemu – elementów, o których mowa w art. 5, 6 ust. 3 ¹⁰, art. 9, art. 22 rozporządzenia 2016/679.

⁸ Zob. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylecia dyrektywy 2001/20/WE (Dz.U. L

158 z 27.5.2014). Por. Opinia EROD nr 3/2019 w sprawie pytań i odpowiedzi dotyczących wzajemnych zależności między rozporządzeniem w sprawie badań klinicznych (RBK) a ogólnym rozporządzeniem o ochronie danych (RODO) (art. 70 ust. 1 lit. b)) Przyjęta w dniu 23 stycznia 2019 r.

⁹ Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków: c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

¹⁰ Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona: a) w prawie Unii; lub b) w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) - musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

4. Sprawy istotne, które muszą zostać uregulowane w przepisach rangi ustawy, obejmują w szczególności warunki dopuszczalności przetwarzania danych osobowych¹¹ (standardy konstytucyjne dotyczące prawa do ochrony danych osobowych wynikającego z art. 51 Konstytucji RP).

5. Kolejnym istotnym zagadnieniem jest to, czy zaproponowany sposób przetwarzania danych w systemie będzie wiązał się z **łączeniem zbiorów danych**, które z punktu widzenia przepisów rozporządzenia 2016/679 jest niedozwolone¹². W poszczególnych rejestrach publicznych można bowiem przetwarzać tylko te dane, które są unikalne w ramach wszystkich rejestrów prowadzonych przez administrację publiczną, a przede wszystkim zgodnie z celami utworzenia rejestru i celami przetwarzania danych. Dane, które już są przetwarzane w innym rejestrze, powinny być pobierane w chwili wystąpienia takiej potrzeby z istniejących rejestrów referencyjnych. Należy bowiem unikać gromadzenia danych, które już są przechowywane w innym rejestrze.

Niedopuszczalny jest więc taki sposób przetwarzania danych osobowych w ramach systemu informatycznego, który prowadziłby do połączenia różnych zbiorów danych (różnych administratorów), a dodatkowo funkcjonował bez ww. podstawy prawnej ze wskazanymi wymaganymi jej elementami.

6. Z uwagi na potencjalne przetwarzanie danych osobowych, w tym szczególnej kategorii, na dużą skalę w projektowanym systemie, z użyciem nowych technologii w ocenie organu nadzorczego, wskazane jest także przeprowadzenie **testu prywatności, w tym oceny skutków dla ochrony danych** (art. 25 ust. 1¹³ oraz 35 ust. 1¹⁴ rozporządzenia 2016/679), które służą ocenie ryzyka naruszenia praw lub wolności podmiotów danych. Przeprowadzenie testu pozwoli na szczegółowe rozeznanie ryzyk

¹¹ Zob. wyroki TK z 19 maja 1998 r., sygn. akt U 5/97, 30 lipca 2014 r., sygn. akt K 23/11 oraz 19 lutego 2002 r., sygn. akt U 3/01.

¹² Zakaz łączenia baz danych wyraźnie podkreślono w treści motywu 31 rozporządzenia 2016/679 zdanie drugie w brzmieniu: „żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych”. Przetwarzając dane osobowe takie organy powinny przestrzegać mających zastosowanie i wiążących je przepisów o ochronie danych, zgodnie z wyznaczonymi im celami przetwarzania. W kontekście łączenia baz danych warto wskazać również na wyrok TSUE z 1 października 2015 r. w sprawie C-201/14

Smaranda Bara i in., z którego treści wynika, że odrębne organy w ramach administracji publicznej należy traktować jako odrębnych administratorów z własnymi przesłankami, co w konsekwencji oznacza, że organ, któremu przekazuje się dane osobowe jest ich odbiorcą.

¹³ „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator - zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą”.

¹⁴ „Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę”.

towarzyszących przetwarzaniu dla praw i wolności podmiotów danych oraz na wprowadzenie gwarancji te ryzyka eliminujące.

Opis założeń odnosi się co prawda do ww. testu prywatności, a także analizy w zakresie zastosowania sztucznej inteligencji zgodnie z opinią Europejskiej Rady Ochrony Danych 28/2024 z 17 grudnia 2024 r.) w zakresie punktu 2.4, pkt 3 opisu założeń (produkty końcowe projektu, kamienie milowe)¹⁵, jednakże nie zwalnia to projektodawcy, już na początkowym etapie przygotowywania założeń projektu, od oceny ryzyk zgodnie z przepisami rozporządzenia 2016/679.

Oceniając natomiast ryzyka związane z przetwarzaniem danych osobowych – np. wyciek PHI (Protected Health Information – chronione informacje zdrowotne) przez błąd anonimizacji; pkt. 5.1 projektu – aktualnie projektodawca określa je jako niskie, co ze względu na cele i sposoby przetwarzania, szeroki zakres i charakter przetwarzanych w tym systemie danych, budzi istotne wątpliwości z punktu widzenia skutków dla ochrony danych. Ponadto, już na obecnym etapie projektodawca zobowiązany jest do przeprowadzenia analizy obowiązujących przepisów prawa w ramach przeprowadzonego testu prywatności (otoczenie prawne). Przegląd regulacji pozwoli zaś na określenie podstawy prawnej przetwarzania, w tym trybu pozyskiwania danych z rejestrów publicznych, gromadzenia i dalszego ewentualnego udostępniania. Należy przy tym zwrócić uwagę, że niepoprawnie projektodawca wskazuje z pkt 6 założeń projektu zapis, „czy zmian wymaga rozporządzenie 2016/679”. W tym zakresie należy usunąć wskazywanie w tabeli (pkt 6 tabeli) odniesienie się do rozporządzenia 2016/679, które – wbrew aktualnemu brzmieniu - powinno być wskazywane jako wyznacznik prawidłowego ukształtowania przepisów krajowych.

Jednocześnie Prezes UODO deklaruje swoje eksperckie wsparcie w zakresie zapewnienia zgodności tej regulacji z rozporządzeniem 2016/679 w przypadku przedstawienia mu do zaopiniowania projektu przepisów ustawy wdrażającej projektowany system informatyczny.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu

Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/

Załącznik 1: Tabela uwag Prezesa UODO dla Projektodawcy.

¹⁵ Zob. uzgodnienia dot. ujęcia kwestii ochrony danych osobowych w dokumencie opisu założeń projektów informatycznych (OZPI) - pismo Prezesa UODO z 14 stycznia br., znak DOL.071.42.2024.

Do wiadomości:

Pan

Tomasz Maciejewski

Podsekretarz Stanu

Ministerstwo Zdrowia