PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 12.01.2026 r.

DPNT.060.2.2026.WL.MKS

Pan
Dariusz Standerski
Sekretarz Stanu
Wiceprzewodniczący Komitetu do spraw Cyfryzacji
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

w związku z przekazanym do wiadomości organu nadzorczego pismem z 2 stycznia br. (znak: DPiS.WWKS.002.69.1.2024), dotyczącym opisu założeń projektu informatycznego „**mLekarz – kompleksowa cyfryzacja procesów obsługi członków Okręgowej Izby Lekarskiej w Warszawie**” (wnioskodawca Minister Zdrowia, beneficjent Okręgowa Izba Lekarska w Warszawie; dalej: „opis założeń”), działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] oraz art. 51 ustawy o ochronie danych osobowych[2], Prezes UODO zgłasza uprzejmie **następujące uwagi**.

Z opisu założeń projektu informatycznego **mLekarz** wynika, że tworzony system będzie przetwarzał szeroki zakres danych osobowych lekarzy / lekarzy dentystów związanych zarówno ze składaniem wniosków administracyjnych (np. dot. przyznania prawa wykonywania zawodu lekarza/lekarza dentysty), jak i socjalnych (zapomogi, becikowe, pożyczki, odprawy pośmiertne, stypendia). Ponadto, system ma umożliwiać używanie innych systemów, takich jak Centralny Wykaz Pracowników Medycznych (CWPM), Centralny Rejestr Lekarzy i Lekarzy Dentystów Rzeczypospolitej Polskiej (FINN), Centralny Rejestr Instytucji ZUS, Rejestr lekarzy upoważnionych do wystawiania zaświadczeń lekarskich (KSI ZUS), Rejestr Asystentów Medycznych (RAM). Dodatkowo, uwierzytelnienie użytkownika systemu ma nastąpić za pomocą Węzła Krajowego i przy wykorzystywaniu zawartości innych

[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).

systemów informatycznych. System ten powinien być zatem zostać oceniony z punktu widzenia przepisów rozporządzenia 2016/679.

W opisie założeń przewidziano dokonanie zmian w uchwałach Naczelnej Rady Lekarskiej[3] i Regulaminach Okręgowej Rady Lekarskiej (pkt 6, otoczenie prawne). Rozważenia wymaga jednak **podjęcie działań legislacyjnych mających na celu określenie właściwej regulacji ustawowej dla przetwarzania danych osobowych w tym systemie** – ze względu na cele przetwarzania, sposoby przetwarzania, w tym korzystanie z nowych technologii, szeroki zakres i charakter przetwarzanych w tym systemie danych, które potencjalnie mogą dotyczyć także danych dotyczących zdrowia, a zatem danych szczególnych kategorii w świetle rozporządzenia 2016/679. System ten ma być dodatkowo zintegrowany z innymi publicznymi systemami, a uwierzytelnienie użytkownika ma następować za pomocą Węzła Krajowego, co powinno znaleźć odzwierciedlenie w przepisami prawa.

Projektodawca **nie wskazuje podmiotów odpowiedzialnych za przetwarzanie danych w tym systemie** (nie jest jasne, czy administratorem systemu ma być Minister Zdrowia, czy Okręgowa Izba Lekarska), 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 miedzy podmiotami - podmiotami publicznymi odpowiedzialnymi za przetwarzanie danych w rejestrach publicznych). Istotne jest także ustalenie, czy zaproponowany sposób przetwarzania danych w systemie będzie wiązał się z **łączeniem zbiorów danych**, które z punktu widzenia przepisów rozporządzenia 2016/679 jest niedozwolone[4] . W poszczególnych rejestrach publicznych można bowiem przechowywać tylko te dane, które są unikalne w ramach wszystkich rejestrów prowadzonych przez administrację publiczną. Dane, które już są przechowywane 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).

W przypadku przetwarzania danych osobowych przez podmioty publiczne, takie przetwarzanie powinno odbywać się **na podstawie przepisów prawa**, które w

---

[3] Uchwała nr 1/17/VII Naczelnej Rady Lekarskiej z dnia 13 stycznia 2017 r. w sprawie szczegółowego trybu postępowania w sprawach przyznawania prawa wykonywania zawodu lekarza i lekarza dentysty oraz prowadzenia rejestru lekarzy i lekarzy dentystów oraz uchwale nr 40/23/IX Naczelnej Rady Lekarskiej z dnia 20 października 2023 r. określającą zasady wykorzystania systemów IT w sprawach PWZ i rejestru lekarzy

[4] 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.

sposób precyzyjny wskazują cele przetwarzania, jakie dane dla ich realizacji będą przetwarzane, przez jaki okres czasu oraz kto będzie za to przetwarzanie odpowiadał. W przypadku wskazanym w art. 6 ust. 1 lit. c i e rozporządzenia 2016/679[5], gdy mamy do czynienia z przetwarzaniem danych niezbędnym do wypełnienia obowiązku prawnego ciążącego na administratorze lub wykonania zadania realizowanego w interesie publicznym, zastosowanie znajduje art. 6 ust. 3 rozporządzenia 2016/679[6], zgodnie z którym podstawa przetwarzania musi być określona w prawie państwa członkowskiego, któremu podlega administrator – regulacja prawna kształtująca funkcjonowanie przedmiotowego systemu powinna uwzględniać elementy, o których mowa w art. 5, 6 ust. 3, 9, ew. 22 rozporządzenia 2016/679.

Z punktu widzenia standardów konstytucyjnych dotyczących prawa do ochrony danych osobowych wynikającego z art. 51 Konstytucji RP należy także podnieść, że sprawy istotne, które muszą zostać uregulowane w przepisach rangi ustawy, obejmują w szczególności warunki dopuszczalności przetwarzania danych osobowych[7].

Jednocześnie organ nadzorczy 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.

Z uwagi na 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**

---

[5] 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.

[6] 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.

[7] 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.

tym oceny skutków dla ochrony danych (art. 25 ust. 1[8] oraz 35 ust. 1[9] rozporządzenia 2016/679), które służą ocenie ryzyka naruszenia praw lub wolności podmiotów danych. Przeprowadzenie testu pozwoli na szczegółowe rozeznanie ryzyk 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 w zakresie punktu 2.4 opisu założeń (produkty końcowe projektu)[10], jednakże nie oznacza to zwolnienia projektodawcy z **przeprowadzenia analizy obowiązujących przepisów prawa w tym zakresie** (otoczenie prawne)**.** Przegląd ten pozwoliłby na określenie podstawy prawnej przetwarzania, w tym trybu pozyskiwania danych z rejestrów publicznych, gromadzenia i dalszego ewentualnego udostępniania. Takie rozwiązanie przyczyni się zaś do tworzenia projektów informatycznych w zgodzie z przepisami rozporządzenia 2016/679.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/

Do wiadomości:

Pan
Tomasz Maciejewski
Podsekretarz Stanu
Ministerstwo Zdrowia

[8] „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”.

[9] „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”.

[10] 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.