PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 28-02-2025

DPNT.060.20.2025.WL.OJ

Pani
Katarzyna Bis-Płaza
Sekretarz Komitetu Rady Ministrów
do spraw Cyfryzacji
Ministerstwo Cyfryzacji

ePUAP**:** /MAiC/SkrytkaESP

Szanowna Pani Sekretarz,

w związku z przekazanym do wiadomości organu nadzorczego pismem z 21 lutego 2025 r. (znak: DPiS.WWKS.002.7.1.2025), dotyczącym opisu założeń projektu informatycznego **„e-Zdrowie KPO”** (dalej: „projekt”) skierowanego do zaopiniowania przez osoby uczestniczące w posiedzeniach Komitetu Rady Ministrów do spraw Cyfryzacji, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] (dalej „rozporządzenie 2016/679”) oraz art. 51 ustawy o ochronie danych osobowych[2], organ nadzorczy zgłasza następujące uwagi.

Zgodnie z deklaracjami zawartymi w załączonym do projektu wniosku o dofinansowanie ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO) opiniowany projekt informatyczny ma na celu dostarczenie nowoczesnych narzędzi wspierających analizę stanu zdrowia pacjentów oraz cyfryzację dokumentacji medycznej z wykorzystaniem zaawansowanych technologii takich, jak sztuczna inteligencja (AI) oraz uczenie maszynowe (ML). Efektem projektu ma być poprawa jakości opieki zdrowotnej, optymalizacja procesów diagnostycznych oraz zwiększenie dostępności usług medycznych, zarówno dla lekarzy, jak i pacjentów. W ocenie

[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 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019, poz. 1781).

wnioskodawcy wdrożenie nowoczesnych technologii cyfrowych usprawni procesy diagnostyczne, terapeutyczne, administracyjne, a także zapewni wyższy poziom bezpieczeństwa danych medycznych i usprawni zarządzanie nimi.

We wniosku o dofinansowanie z KPO podkreślono powody realizacji projektu, wśród których wskazano:

1. poprawę jakości opieki zdrowotnej: dzięki wdrożeniu narzędzi opartych na AI i ML systemy medyczne będą mogły dostarczać lekarzom bardziej precyzyjne informacje o stanie zdrowia pacjentów, co umożliwi szybsze podejmowanie decyzji klinicznych oraz minimalizację ryzyka błędów lekarskich. Rozwiązania te będą wspierały procesy diagnostyczne, oferując lekarzom narzędzia do bardziej efektywnego i dokładnego przeglądania danych pacjentów w systemie SIM (System Informacji Medycznej);
2. zwiększenie efektywności pracy personelu medycznego: W ramach projektu planowane jest wdrożenie intuicyjnych narzędzi analitycznych oraz alertów dla lekarzy, które pomogą w szybszym wykrywaniu nieprawidłowości w historii medycznej pacjentów (np. brak realizacji recept czy brak wyników badań). Systemy te pozwolą na większą dostępność czasową dla pacjentów i optymalizację wykorzystania zasobów medycznych;
3. zwiększenie dostępności opieki zdrowotnej: narzędzia telemedyczne oraz rozwój systemu zdalnego monitorowania pacjentów (IoMT – Internet of Medical Things) pozwolą na monitorowanie stanu zdrowia pacjentów poza tradycyjnymi wizytami w placówkach medycznych. Pacjenci będą mogli korzystać z usług takich, jak teleporady, które zapewnią szybki dostęp do specjalistów, a także umożliwią bardziej kompleksowe podejście do leczenia, oparte na ciągłym zbieraniu danych o ich stanie zdrowia;
4. cyfryzacja dokumentacji medycznej: budowa centralnego repozytorium danych medycznych i cyfryzacja dokumentacji medycznej (w tym dokumentów takich jak karta DILO, opisy badań histopatologicznych, plan leczenia onkologicznego) ma na celu ułatwienie dostępu do informacji medycznych dla lekarzy oraz pacjentów. Umożliwi to szybszy dostęp do historii chorób, co jest kluczowe w diagnostyce i leczeniu pacjentów. Zdigitalizowanie dokumentacji zmniejszy obciążenie pacjentów w zakresie dostarczania fizycznych kopii wyników badań (np. na płytach CD).

Wnioskodawca identyfikuje 4 główne grupy odbiorców końcowych projektu, wskazując: liczącą około 37,6 milionów osób w Polsce grupę docelową pacjentów; 28 tys. podmiotów leczniczych (m.in. szpitale, przychodnie, praktyki lekarskie, pielęgniarskie i Położnicze); 550 tys. pracowników medycznych (w tym lekarzy, pielęgniarki, ratowników medycznych, techników medycznych, farmaceutów oraz innych specjalistów), a także podmioty centralnej administracji publicznej.

Odnosząc się do powyższych informacji, zauważyć należy, że projektowane rozwiązania w przypadku ich wejścia w życie będą miało ogromny wpływ na model przetwarzania danych osobowych w systemie opieki zdrowotnej w Polsce.

W tworzonym na podstawie projektu systemie informatycznym będą bowiem przetwarzane dane, w tym dane osobowe, na wielką skalę związane w szczególności ze

stanem zdrowia, dane genetyczne, dane biometryczne a także inne dane szczególnych kategorii (w rozumieniu w art. 9 ust 1 rozporządzenia 2016/679[3]), podlegające zgodnie ze standardami RODO wzmocnionej ochronie prawnej. W systemie tym będą także przetwarzane numery PESEL, który stanowi krajowy numer identyfikacyjny zgodnie z art. 87 rozporządzenia 2016/679[4], którego przetwarzanie również podlega wzmocnionej ochronie prawnej oraz dane objęte tajemnicą prawnie chronioną zawarte w dokumentacji medycznej. Z projektu nie wynika natomiast jednoznacznie, czy – w związku z informacjami dotyczącymi w szczególności leczenia więźniów w tworzonym systemie – będą też przetwarzane dane dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa objęte dodatkową ochroną z art. 10 rozporządzenia 2016/679[5], niemniej organ nadzorczy zwraca uwagę także na ten aspekt planowanego projektu.

Jednocześnie powyższe dane osobowe podlegające szczególnej ochronie prawnej mają być przetwarzane w projektowanym systemie informatycznym za pomocą nowych technologii, przy użyciu metod wykorzystujących sztuczną inteligencję (AI) oraz uczenie maszynowe (ML). Rozwiązania projektu wskazują też na możliwość profilowania osób fizycznych, a także automatycznego przetwarzania ich danych, w tym także danych szczególnej kategorii w ramach tworzonych rozwiązań.

Należy zwrócić szczególną uwagę, że opiniowany projekt informatyczny zakłada szeroką integrację systemów i stworzenie megabazy w postaci **centralnego repozytorium danych medycznych**. Zamieszczona w opisie założeń projektu informatycznego „Lista systemów wykorzystywanych w projekcie" wskazuje aż 56 takich systemów, w tym m.in. System Gromadzenia Danych Medycznych (SGP); Krajowa Sieć Onkologiczna (KSO); Elektroniczna Dokumentacja Medyczna (EDM); System Domowej Opieki Medycznej (DOM); e-Profl Pacjenta (ePP), czy Kompleksowy System Informatyczny ZUS (KSI ZUS).

Należy wobec tego zauważyć, że w wielu z tych systemów dane osobowe pacjentów i innych osób fizycznych są zbierane w konkretnych celach, które wprost nie odpowiadają założeniom projektowanego systemu. Pozyskiwanie w ramach projektu do tworzonego centralnego repozytorium danych osobowych gromadzonych i przetwarzanych przez podmioty udzielające świadczeń zdrowotnych, a także innych

---

[3] Zgodnie z art. 9 ust. 1 rozporządzenia 2016/679 zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

[4] Państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym. W takim przypadku krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje niniejsze rozporządzenie.

[5] Zgodnie z art. 10 rozporządzenia 2016/679 przetwarzania danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

administratorów w ustawowo określonych, pierwotnie węższych celach, może potencjalnie oznaczać zmianę celów przetwarzania danych osobowych, co powinno zostać wnikliwie rozważone. Zmiana pierwotnego celu przetwarzania danych osobowych – stosownie do art. 6 ust. 4 [6] rozporządzenia 2016/679 – może zachodzić jedynie **na podstawie prawa** państwa członkowskiego, stanowiącego w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu jedynie celów, o których mowa w art. 23 ust. 1[7] rozporządzenia 2016/679 oraz z uwzględnieniem zasad i warunków z tego artykułu wynikających.

Wnioskodawca w pkt 5.1 w opisie założeń projektu informatycznego jako **ryzyko o małej sile odziaływania** i niskim prawdopodobieństwie wystąpienia określił „ Zmiany prawne mające wpływ na realizację Projektu. Ryzyko związane z wdrożeniem, na etapie realizacji projektu, zmian prawnych mających wpływ na zakres projektu”[8].

Biorąc pod uwagę szeroki zakres zmian przepisów prawa z zakresu przetwarzania danych osobowych, jaki będą musiały towarzyszyć wdrożeniu projektowanego rozwiązania, wspomniane ryzyko powinno być poddane ponownej wnikliwej ocenie. Projektodawca, tworząc podstawę prawną dla tworzonego systemu informatycznego i

---

[6] Zgodnie z art 6 ust. 4 rozporządzenia 2016/679 jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator - aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane - bierze pod uwagę między innymi:
a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;
c) 27 charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i czynów zabronionych zgodnie z art. 10;
d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

[7] Zgodnie z art 23 ust. 1 rozporządzenia 2016/679 Prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12-22 i w art. 34, a także w art. 5 - o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12-22 - jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym: a) bezpieczeństwu narodowemu; b) obronie; c) bezpieczeństwu publicznemu; d) zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom; e) innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu; f) ochronie niezależności sądów i postępowania sądowego; g) zapobieganiu naruszeniom zasad etyki w zawodach regulowanych, prowadzeniu postępowań w takich sprawach, ich wykrywaniu oraz ściganiu; h) funkcjom kontrolnym, inspekcyjnym lub regulacyjnym związanym, nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) - e) oraz g); i) ochronie osoby, której dane dotyczą, lub praw i wolności innych osób; j) egzekucji roszczeń cywilnoprawnych.

[8] W pkt 6 opisu założeń projektu informatycznego wskazano jako wymagane zmiany ustawowe na ustawę z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2023 r. poz. 2465, ze. zm.) oraz ustawę z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2024 r. poz. 146, ze zm.). Zgodnie z ww. dokumentem pracę nad nowelizacją tych aktów prawnych są na etapie prac legislacyjnych – konsultacje wewnętrzne.

analizując legalność stosowanych w nim rozwiązań, powinien wziąć pod uwagę w szczególności nie tylko przepisy rozporządzenia 2016/679, ale także wdrażany obecnie do polskiego porządku prawnego Akt w sprawie sztucznej inteligencji[9] oraz rozporządzenie w sprawie europejskiej przestrzeni danych dotyczących zdrowia[10].
W związku z powyższą analizą wysoce pożądane i zasadne jest przeprowadzenie dla projektu **testu prywatności**[11] na jak najwcześniejszym etapie prac. Tymczasem z opisu założeń projektu wynika, że wnioskodawca planuje wykonanie raportu z inicjalnego testu prywatności dopiero na rok 2026 r.

W ocenie Prezesa Urzędu Ochrony Danych waga i zakres tworzonych rozwiązań, zmieniających zasadniczo model przetwarzania danych osobowych w systemie opieki zdrowotnej w Polsce, sprawia, że test prywatności powinien być przeprowadzony znacznie wcześniej. Wnioskodawca na dalszych etapach tworzenia projektu informatycznego musi mieć bowiem pełną i miarodajną informację o ryzykach w sferze ochrony danych osobowych, a także koniecznych kierunkach zmian otoczenia prawnego.

Należy również podkreślić, że z art. 27 Aktu w sprawie sztucznej inteligencji wynika odrębny **obowiązek dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych**. W ocenie organu nadzorczego wnioskodawca powinien więc również uwzględnić dokonanie takiej oceny w dokumencie opisu założeń projektu informatycznego. Co prawda z przedstawionych dokumentów, nie wynika jednoznaczne jaki będzie model przetwarzania danych w systemach AI wykorzystanych w projekcie, jednakże przedstawione informacje wskazują, że systemy te mogą spełniać przesłanki systemów AI wysokiego ryzyka, o których mowa w art. 6 Aktu w sprawie sztucznej inteligencji.

Pragnę jednocześnie zadeklarować, że w przypadku podjęcia prac legislacyjnych nad projektami aktów prawa, które stanowiłyby podstawę dla projektowanego rozwiązania, Urząd Ochrony Danych Osobowych deklaruje swoje eksperckie wsparcie.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany kwalifikowanym podpisem elektronicznym/

[9] Rozporządzenie Parlamentu Europejskiego 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 (akt w sprawie sztucznej inteligencji).
[10] Rozporządzenia parlamentu europejskiego i Rady w sprawie europejskiej przestrzeni danych dotyczących zdrowia oraz zmiany dyrektywy 2011/24/UE i rozporządzenia (UE) 2024/2847, dalej: rozporządzenie w sprawie europejskiej przestrzeni danych dotyczących zdrowia.
[11] Zawierającego ocenę skutków dla ochrony danych i odpowiadającego wymogom art. 25 ust. 1 i art. 35 (w szczególności ust. 1 oraz ust. 10) rozporządzenia 2016/679.