PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, 12-04-2026

DPNT.060.10.2026.WL.PM

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

Szanowny Panie Ministrze,

w związku z pismem z 7 kwietnia 2026 r. znak: DPiS.WWKS.002.37.1.2026, przekazującym do wiadomości Prezesa Urzędu Ochrony Danych Osobowych informację o skierowaniu do zaopiniowania przez osoby uczestniczące w pracach Komitetu do spraw Cyfryzacji **opisu założeń projektu informatycznego pn. „System Monitorowania Kształcenia Pracowników Medycznych – SMK 2.0”** – wnioskodawca: Minister Zdrowia, beneficjent: Centrum e-Zdrowia”, 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 jako organ nadzorczy zgłasza uprzejmie następujące uwagi.

Zgodnie z częścią **4.2. Wykaz poszczególnych pozycji kosztowych** opisu założeń projektu informatycznego (str. 12) infrastrukturę teleinformatyczną SMK 2.0 będzie stanowić chmura obliczeniowa – „Zostanie wykorzystane rozwiązanie chmurowe, w związku z czym w projekcie nie będą ponoszone koszty związane z zakupem ITS, a jedynie koszty usługi wynajmu mocy obliczeniowej.”.

[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.).

Jak wskazano natomiast w części **7.5. Bezpieczeństwo** opisu założeń projektu informatycznego (str. 29) SMK 2.0 będzie zlokalizowany w infrastrukturze technicznej Centrum e-Zdrowia.

Organ nadzorczy zwraca uwagę, że **przekazanie danych do chmury obliczeniowej będzie powierzeniem danych osobowych w rozumieniu art. 28** rozporządzenia 2016/679. Biorąc pod uwagę fakt, że zgodnie z art. 30 ust. 3 i 4 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz. U. z 2026 r. poz. 208 ze zm.) „3. Administratorem danych przetwarzanych w Systemie Monitorowania Kształcenia Pracowników Medycznych jest minister właściwy do spraw zdrowia. 4. Administratorem systemu jest jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia.”, umowa powierzenia z dostawcą usług chmurowych będzie zawierana przez Ministra Zdrowia, choć SMK 2.0 będzie zlokalizowany w infrastrukturze technicznej Centrum e-Zdrowia. Minister Zdrowia będzie więc odpowiadał, za wybór odpowiedniego podmiotu przetwarzającego (dostawcy chmurowego), nie obsługując jednocześnie SMK 2.0. Zgodnie z art. 9a ust. 2 ustawy o systemie informacji w ochronie zdrowia Minister Zdrowia będzie mógł upoważnić Centrum e-Zdrowia do zawarcia umowy powierzenia, dojdzie wtedy jednak do **kaskadowego powierzenia danych osobowych**.

Jak stanowi 9a ust. 2 ustawy o systemie informacji w ochronie zdrowia: „Jeżeli administrator danych przetwarzanych w SIM, dziedzinowych systemach teleinformatycznych lub rejestrach medycznych lub podmiot przez niego upoważniony zawarł umowę o powierzeniu przetwarzania danych osobowych, o której mowa w art. 28 ust. 3 rozporządzenia 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), podmiot, któremu powierzono przetwarzanie tych danych, jest obowiązany do stworzenia warunków organizacyjnych i technicznych zapewniających ochronę przetwarzanych danych, w szczególności zabezpieczenia danych przed nieuprawnionym dostępem, nielegalnym ujawnieniem lub pozyskaniem, a także ich modyfikacją, uszkodzeniem, zniszczeniem lub utratą.”.

Zgodnie z art. 5 ust. 1 pkt 2 lit. i ustawy o systemie informacji w ochronie zdrowia System Monitorowania Kształcenia Pracowników Medycznych zalicza się do dziedzinowych systemów teleinformatycznych.

Należy przy tym zwrócić uwagę, że zgodnie z częścią **2.4. Produkty końcowe projektu** opisu założeń projektu informatycznego (str. 8) SMK 2.0 ma osiągnąć następujące funkcjonalności: „Zmodyfikowany system teleinformatyczny SMK 2.0 dla lekarzy i lekarzy dentystów, diagnostów laboratoryjnych, farmaceutów uwzględniający funkcjonalności: panel wspólny/administracja, profil użytkownika, profil podmiotu, publikacja miejsc szkoleniowych, programy specjalizacji, wnioskowanie o specjalizację, postępowanie kwalifikacyjne, skierowanie na specjalizację i obsługa skierowania, realizację specjalizacji (EKS), weryfikacja specjalizacji, egzamin specjalizacyjny, akredytacja na specjalizację, akredytacja na staż, egzamin zawodowy (wersja pl i wersja ang lekarze i lekarze dentyści), profil użytkownika wersja angielska, doskonalenie zawodowe, rejestr osób w trakcie specjalizacji, RESTApi. CEM, CMKP, web service SIR,

migracja danych.”. W SMK 2.0 będzie więc **przetwarzany szeroki wolumen informacji dotyczących kształcenia podyplomowego pracowników medycznych, który zgodnie założeniami projektu informatycznego będzie przetwarzany w chmurze obliczeniowej**.

Mając na uwadze powyższe, organ nadzorczy wskazuje, że w odniesieniu do planowanego użycia w projekcie rozwiązań chmurowych oraz niewskazania przez projektodawcę w jaki sposób nastąpi powierzenie danych dostawcy usług chmurowych, konieczne jest przeprowadzenie **testu prywatności, w tym oceny skutków dla ochrony danych** (art. 25 ust. 1 [3] oraz 35 ust. 1 [4] rozporządzenia 2016/679). Rozwój SMK 2.0 będzie wiązał się z przetwarzaniem danych na dużą skalę z użyciem nowych technologii (chmura obliczeniowa). Dochodzi do tego **oparcie przetwarzania na nieprecyzyjnym otoczeniu regulacyjnym**, to jest art. 30 ust. 3 i 4 ustawy o systemie informacji w ochronie zdrowia, który opiera się na dualizmie odpowiedzialności „administratora systemu” i „administratora”, wielokrotnie sygnalizowanym przez organ nadzorczy[5]. Ocena skutków dla ochrony danych powinna określać w jaki sposób dojdzie do powierzenia danych oraz czy rozwiązanie oparte na chmurze obliczeniowej nie będzie generować wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Powinna również zawierać analizę, czy nie będzie konieczna **zmiana ustawy o systemie informacji w ochronie zdrowia, w zakresie odpowiedzialności podmiotów publicznych w procesach przetwarzania danych**. Powszechnie obowiązujące przepisy nie powinny pozostawiać wątpliwości co do zakresu odpowiedzialności podmiotów publicznych, gdyż powinny one być związane „instrumentem prawnym” w rozumieniu art. 28 ust. 3 rozporządzenia 2016/679, zgodnie z którym przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora, w tym zakresie, tj. przepisami prawa w zakresie powierzenia obejmującymi wszystkie elementy z art. 28 ust. 3 rozporządzenia 2016/679. Kwestie te powinny zostać odzwierciedlone w opisie założeń projektu informatycznego.

Na marginesie organ nadzorczy wskazuje, że w części **7.4**. **Opis zasobów danych przetwarzanych w planowanym rozwiązaniu** opisu założeń projektu informatycznego

---

[3] „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”.

[4] „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”.

[5] Np. podczas opiniowania projektu ustawy o zmianie niektórych ustaw w związku z rozwojem usług e-zdrowia (UPRO5) – pismo Prezesa UODO z 24 marca 2026 r. z uwagami na KdsC, znak: DPNT.401.43.2026.WL.PM.

(str. 29) jest mowa o Centralnym Wykazie Personelu Medycznego, natomiast art. 17 ustawy o systemie informacji w ochronie zdrowia reguluje funkcjonowanie Centralnego Wykazu Pracowników Medycznych. Jeżeli więc projekt odnosi się do Centralnego Wykazu Pracowników Medycznych, to powyższe postanowienie wymaga korekty.

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
w Ministerstwie Zdrowia