PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, **22 lipca 2026**

DPNT.060.98.2026.WL

Pani
Katarzyna Bis-Płaza
Sekretarz Komitetu do spraw Cyfryzacji

Ministerstwo Cyfryzacji

Szanowna Pani Minister,

w związku z przekazanym do wiadomości organu nadzorczego pismem z 17 lipca 2026 r., znak: DPIS-WWKS.002.132.1.2026, dotyczącym **opisu założeń projektu informatycznego „Rozwój e-usług i optymalizacja procesów zarządczych Śląskiego Uniwersytetu Medycznego w Katowicach poprzez wdrożenie systemów analizy parametrycznej i cyfrowej obsługi studenta”,** dalej: OZPI, (wnioskodawca: Minister Zdrowia, beneficjent: Śląski Uniwersytet Medyczny w Katowicach, 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 Urzędu Ochrony Danych Osobowych zgłasza uprzejmie uwagi.

Celem projektu jest stworzenie **ekosystemu e-usług i optymalizacji procesów zarządczych** - zastępującego dotychczasową analogową (papierową) obsługę (administracyjną, zarządczą, dydaktyczną i naukową) Uczelni – **likwidujących bariery społeczne i administracyjne dla studentów i kadry Uczelni**. Przewidziane rozwiązania obejmują: e-podania, e-zaświadczenia, e-stypendia, e-dyplomy, cyfrowa zapisy na egzaminy, e-listy obecności oraz zautomatyzowane e-ankiety, które **wiążą się z przetwarzaniem danych osobowych**.

[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.).

Wnioskodawca **nie uwzględnił jednak w OZPI wykonania testu prywatności**, który wymagany jest z uwagi na przetwarzanie danych osobowych na **dużą skalę** (ok. 10 000 studentów i doktorantów) **przy zastosowaniu nowych technologii**. W pkt. 1.1 OZPI na wskazano potrzebę predykcji (BI) oraz optymalizacji algorytmicznej a także potrzebę w zakresie automatyzacji procesów. Nie jasne jest czy wskazane rozwiązania wiążą się z procesami przetwarzania danych osobowych, a jeśli tak, to czy będą wykorzystywane jako wspierające te procesy, czy jako samodzielne narzędzia.

Przeprowadzenie **testu prywatności** jest konieczne celem wykonania – dla konkretnego przedsięwzięcia związanego z przetwarzaniem danych osobowych - **oceny skutków dla ochrony danych**. Test ten powinien spełniać wymogi art. 25 ust. 1 [3] i art. 35 (w szczególności ust. 1 [4], ust. 7 [5] oraz ust. 10 [6]) rozporządzenia 2016/679.

W ocenie tej i na jej podstawie wnioskodawca i beneficjent powinni:

- zdiagnozować **ryzyka dla praw i wolności podmiotów danych** wynikające z wdrażanych rozwiązań,
- wypracować **konkretne środki zaradcze oraz techniczno-organizacyjne minimalizujące zidentyfikowane zagrożenia**,
- przeanalizować i dokonać przegląd ukierunkowany na **ustalenie czy pośród danych osobowych przetwarzanych w związku z realizacją przedsięwzięcia informatycznego znajdują się dane osobowe szczególnej kategorii, które podlegają szczególnej ochronie**,
- przeanalizować **zagadania związane z otoczeniem prawnym** – czy na pewno analiza nie prowadzi do potrzeby uzupełnienia podstaw prawnych przetwarzania danych osobowych.

---

[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 zagrożenia 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] Ocena zawiera co najmniej: a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez administratora; b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów; c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

[6] Ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

Jednym z ryzyk wpływających na utrzymanie efektów (**pkt. 5.2 OZPI**) wskazano ryzyko utraty spójności i „niepełnych danych”, określając siłę oddziaływania jako „średnią” oraz prawdopodobieństwo wystąpienia ryzyka ze wskazaniem na „niskie”. Wymieniono również ryzyko naruszenia bezpieczeństwa danych o sile „dużej” oraz prawdopodobieństwu wystąpienia „znikomym”. Biorąc pod uwagę wskazane ryzyka niezbędne jest wdrożenie skutecznych i adekwatnych środków prewencyjnych i ochronnych (po uprzednim przeprowadzeniu testu prywatności i rozpoznaniu zagrożeń) zapewniających integralność, poufność, ale również i prawidłowość danych, w tym odpowiednich środków bezpieczeństwa, szyfrowania, pseudonimizacji i anonimizacji danych osobowych.

Mając powyższe na uwadze, Prezes UODO deklaruje swoje eksperckie wsparcie w zakresie zapewnienia zgodności tej regulacji z rozporządzeniem 2016/679, w tym także w przypadku przedstawienia do zaopiniowania projektu przepisów ustawy wdrażającej projektowane rozwiązania.

Z wyrazami szacunku,

z up. Prezesa Urzędu
Ochrony Danych Osobowych
Zastępczyni Prezesa
Urzędu Ochrony Danych Osobowych
dr hab. Agnieszka Grzelak

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/