



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa, 13-02-2025

DPNT.060.18.2025.WL.OJ

**Pan
Dariusz Standerski
Wiceprzewodniczący Komitetu Rady
Ministrów do spraw Cyfryzacji
Sekretarz Stanu
w Ministerstwie Cyfryzacji**

ePUAP: /MAiC/SkrytkaESP

Szanowny Panie Ministrze,

w związku z przekazaniem do wiadomości organu nadzorczego pismem z 7 lutego 2025 r. (znak: DPiS.WWKS.002.16.1.2024) dotyczącym opisu założeń **projektu informatycznego „System Obsługi Dofinansowań i Refundacji SODiR 3.0”** (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) 2016/679¹ (dalej „rozporządzenie 2016/679”) oraz art. 51 ustawy o ochronie danych osobowych², Prezes UODO jako organ nadzorczy zgłasza uprzejmie następujące uwagi.

Jak wynika z pisma Pani Katarzyny Bis-Płazy, Sekretarza Komitetu Rady Ministrów do spraw Cyfryzacji, w ramach współpracy z beneficjentami przy przygotowaniu dokumentu opisu założeń projektu informatycznego (OZPI) Komitet

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 r. poz. 1781).

rekomenduje włączanie **testu prywatności** (obejmującego m.in. ocenę skutków dla ochrony danych), jako kluczowego dla oceny przetwarzania danych osobowych, do OZPI (w następujących punktach: pkt 2.4 - Produkty końcowe projektu, Pkt 3 – Kamienie milowe, pkt 4.2 - Wykaz poszczególnych pozycji kosztowych, pkt 6 – Otoczenie prawne)³.

Niestety, przekazany do Urzędu Ochrony Danych Osobowych dokument opisu założeń projektu informatycznego „System Obsługi Dofinansowań i Refundacji SODiR 3.0” w, żadnym ze wskazanych punkcie nie zakłada przeprowadzenia **testu prywatności** zawierającego ocenę skutków dla ochrony danych odpowiadającego wymogom art. 25 ust. 1⁴ i art. 35 (w szczególności ust. 1⁵ oraz ust. 10⁶) rozporządzenia 2016/679.

Jednocześnie analiza projektu wskazuje, że wymaga on szczególnie wnikliwej oceny pod kątem przetwarzania i ochrony danych osobowych.

Jak zostało wskazane w jego opisie, celem projektu jest budowa przez PFRON⁷ systemu informatycznego SODiR⁸ 3.0 mającego służyć do świadczenia e-usługi pełnej obsługi procesów wsparcia osób korzystających z systemu oraz integracji z rejestrami publicznymi. System ten ma zastąpić obecnie działający system informatyczny SODiR 2.0, który wspiera osoby z niepełnosprawnościami w obszarze rynku pracy, i który jak wskazano w projekcie jest systemem przestarzałym, kosztownym i trudnym w utrzymaniu, nieodpowiadającym współczesnym standardom dojrzałych systemów informatycznych. System ten jest wykorzystywany do obsługi dofinansowań do wynagrodzeń pracowników niepełnosprawnych i refundacji składek na ubezpieczenia społeczne płaconych przez osoby niepełnosprawne prowadzące działalność gospodarczą, niepełnosprawnych rolników bądź rolników zobowiązanych do opłacania składek za niepełnosprawnego domownika.

W tworzonym na podstawie projektu systemie informatycznym będą więc przetwarzane w znacznej ilości i na dużą skalę dane osób fizycznych związane także ze stanem zdrowia, a zatem dane szczególnych kategorii (w rozumieniu w art. 9 ust 1

³ Pismo Pani Katarzyny Bis-Płazy Sekretarza Komitetu Rady Ministrów do spraw Cyfryzacji z 31 stycznia 2025 r. (znak: DPiS.WWKS.501.1.1.2025).

⁴ 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.

⁵ 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.

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.

⁷ Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych.

⁸ System Obsługi Dofinansowań i Refundacji.

rozporządzenia 2016/679⁹), podlegające zgodnie ze standardami RODO wzmocnionej ochronie prawnej. W systemie tym będą także przetwarzane numery PESEL, dane stanowiące krajowy numer identyfikacyjny zgodnie z art. 87 rozporządzenia 2016/679¹⁰, które również podlegają szczególnej ochronie. Jednocześnie z projektu nie wynika jednoznacznie czy w związku z informacjami dotyczącymi osób niepełnosprawnych w tworzonym systemie będą też przetwarzane informacje objęte tajemnicą prawnie chronioną, zawarte w dokumentacji medycznej.

Także inne przyjęte dla tworzonego systemu rozwiązania wymagają pogłębionej analizy pod kątem ryzyk dla przetwarzanych danych osobowych. W szczególności, jak wynika z opisanej w projekcie „Listy systemów wykorzystywanych w projekcie”, a także „Listy przepływów”, projektowanie systemu informatycznego ma się odbywać z wykorzystaniem szeregu systemów teleinformatycznych, w tym m.in. EZD RP, PESEL, nSIU KRUS, KSI ZUS.

Fakt planowania integracji szeregu rejestrów publicznych i systemów teleinformatycznych z tworzonym systemem daje uzasadnione podstawy do wyrażenia wątpliwości czy istotnie zmiana otoczenia prawnego dla tego projektu informatycznego nie powinna zakładać nowelizacji przepisów ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych¹¹, a nie jedynie rozporządzeń wykonawczych do tego aktu – jak wskazuje wnioskodawca.

Biorąc pod uwagę powyższe, skoro dla realizacji celów projektowanego systemu informatycznego przetwarzane mają być m.in. dane szczególnych kategorii, PESEL, który jako krajowy numer identyfikacyjny podlega szczególnej ochronie, a także mają być pozyskiwane dane osobowe z rejestrów publicznych i innych systemów informatycznych to wysoce pożądane i zasadne jest przeprowadzenie dla projektu **testu prywatności**.

Przeprowadzenie takiego testu zgodnie z wypracowanymi w ramach dotychczasowej korespondencji organu nadzorczego z Komitetem Rady Ministrów do spraw Cyfryzacji standardami pozwoli zweryfikować zasadność wykorzystywania w projekcie tak szerokiego i takiego jak planowany zakresu danych, ocenić ryzyka dla tych danych, a także prawidłowości sporządzonej oceny kierunków zmian otoczenia prawnego przez wnioskodawcę.

Jednocześnie pragnę podkreślić, że w przypadku podjęcia prac legislacyjnych nad projektami aktów prawnych – zwłaszcza takimi, które stanowiłyby źródła powszechnie obowiązującego prawa oraz wymagałyby oceny pod kątem zgodności z ogólnym

⁹ 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.

¹⁰ 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.

¹¹ Ustawa z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (Dz. U. z 2024 r. poz. 44 ze zm.).

rozporządzeniem o ochronie danych – 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/