Warszawa, 10-12-2025

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

sygn. DPNT.060.76.2025.WL.MP

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

ePUAP: /MAiC/SkrytkaESP

Szanowny Panie Ministrze,

w odpowiedzi na pismo z 3 grudnia br., znak DPiS.WWKS.002.172.1.2025, 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], do przedstawionego **opisu założeń projektu informatycznego „Multiportal RP”** (dalej jako „OZPI” lub „projekt”) organ nadzorczy – Prezes Urzędu Ochrony Danych zgłasza następujące uwagi.

Multiportal RP stanowić ma rozwinięcie dotychczas funkcjonującego „Portalu RP”, który jest głównym serwisem internetowym polskich instytucji publicznych („gov.pl” oraz „samorzad.gov.pl”). Jego funkcją jest zapewnienie platformy dla podmiotów administracji publicznej, umożliwiającej projektowanie własnych witryn internetowych oraz zarządzanie i publikację treści, przy jednoczesnym zachowaniu spójności i standaryzacji z innymi witrynami organów państwowych. Założyć należy, że w większości przypadków usługi będą polegały na wspieraniu procesu tworzenia portali internetowych charakteryzujących się dostępem otwartym, nie wymagających

[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.) – dalej jako rozporządzenie 2016/679.
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

Urząd Ochrony
Danych Osobowych
ul. Stanisława Moniuszki 1A
00-014 Warszawa

tel. 22 531-03-88
fax 22 531-03-99

www.uodo.gov.pl

logowania użytkownika. Niemniej jednak, projekt zakłada także integrację z Węzłem Krajowym, umożliwiając uwierzytelnianie użytkowników systemu w przypadku oferowania konkretnych usług. Ponieważ w takich przypadkach będzie dochodzić do przetwarzania danych osobowych, konieczne jest **przeprowadzenie osobnej analizy pod względem zgodności z wymogami przepisów rozporządzenia 2016/679**.

Zgodnie z „Listą systemów wykorzystywanych w projekcie" (pkt. 7.1.) „*system nie przechowuje danych uwierzytelniających się osób fizycznych wykorzystujących środki identyfikacji elektronicznej, jest jedynie pośrednikiem między systemami identyfikacji elektronicznej a systemami udostepniającymi usługi*". Nie kwestionując prawidłowości przyjętego rozwiązania należy mieć na względzie potencjalne trudności z ustaleniem **podziału ról i zakresem odpowiedzialności** poszczególnych administratorów biorących udział w procesach przetwarzania danych. Wymagane jest ustalenie jasnych i przejrzystych reguł określających w jakim zakresie administratorem przetwarzanych danych będzie podmiot publicznych korzystający z platformy i zapewniający usługi dla docelowych odbiorców, a w jakim podmiot odpowiedzialny za funkcjonowanie Multiportalu.

Konieczne jest dokonanie przeglądu obowiązujących przepisów prawa pod względem **ustalenia i wykazania ustawowych podstaw prawnych**, zarówno do funkcjonowania systemu teleinformatycznego jak i do poszczególnych operacji przetwarzania danych osobowych dokonywanych za jego pośrednictwem, uwzględniając różnorodność celów realizowanych przez poszczególne podmioty docelowe. Podstawy przetwarzania muszą spełniać wymogi określone w art. 6 ust. 1 i 3 rozporządzenia 2016/679. W kontekście rozpatrywanego projektu, wykazane musi zostać przede wszystkim kryteriów **niezbędności i proporcjonalności** przetwarzania dla realizacji zadania publicznego.

Zasadniczą rolą systemu teleinformatycznego jest zapewnienie scentralizowanych narzędzi CMS dla poszczególnych organów administracji, w taki sposób, który zapewnieni spójność i prawidłowości treści na poszczególnych witrynach rządowych. Standaryzacji dostępności do informacji powinna towarzyszyć także **standaryzacja pod względem wdrożenia adekwatnych środków organizacyjnych i technicznych** przez odbiorców usługi (podmioty publiczne) pod względem ochrony danych osobowych. Oferowane narzędzia powinny zostać zaprojektowane w taki sposób, aby przewidywać konieczność uwzględnienia zgodności z przepisami dotyczącymi ochrony danych osobowych, wspierając dobre praktyki tworzenia usług gwarantujących przetwarzanie danych zgodnie z wymogami zasad ograniczenia celu, minimalizacji, integralności i poufności, rozliczalności, zgodności z prawem, rzetelności, przejrzystości.

Pozytywnie należy ocenić, że OZPI zakłada przeprowadzenie zarówno inicjalnego jak i końcowego testu prywatności[3]. Test ten powinien obejmować ocenę skutków dla ochrony danych osobowych (art. 35 ust. 1 rozporządzenia 2016/679), która pozwoli na zdiagnozowanie konkretnych ryzyk dla praw i wolności podmiotów danych wynikających z wdrażanych rozwiązań oraz wypracowanie szczegółowych rozwiązań techniczno-organizacyjnych, minimalizujących zidentyfikowane zagrożenia. Ze względu na szeroki zakres oddziaływania planowanego systemu teleinformatycznego rozważyć należy także implementację **testów weryfikacyjnych na poszczególnych etapach** realizacji projektu, które pozwolą na bieżące zbadanie skuteczności planowanych wcześniej środków i konieczne modyfikacje w tym zakresie.

W ocenie organu nadzorczego, ze względu na węzłowy charakter planowanego systemu teleinformatycznego, istotnego dla zapewnienia punktów informacyjnych dla obywateli, OZPI powinien zostać rozszerzony o aspekty zapewniające nie tylko bezpieczeństwo danych, ale i **cyberbezpieczeństwo**. Systemom informatycznym, wykorzystywanym przez organy publiczne, szczególnie jeżeli ich eksploatacja związana jest (przynajmniej pośrednio) z funkcjonowaniem infrastruktury krytycznej, przyporządkowane powinny zostać adekwatne środki ochrony, zwiększające **odporność na zorganizowane cyberataki, ataki hybrydowe, zorganizowane manipulacje treściami i migracją danych**, szczególnie w kontekście planowanego korzystania z **chmur obliczeniowych**.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

[3] To jak ważnym aspektem jest test prywatności towarzyszący wdrażaniu systemów teleinformatycznych Prezes UODO wielokrotnie wskazywał w korespondencji z Komitetem, a potrzeba ta została podzielona w piśmie z 31 stycznia 2025 r., znak DPiS.WWKS.501.1.1.2025.