PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, **03 lipca 2026**

DPNT.060.61.2026.WL.MW

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

Szanowna Pani Sekretarz,

w związku z pismem z 1 lipca 2026 r., (znak: DPIS-WWKS.002.99.1.2026), 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 do opisu założeń projektu informatycznego (dalej OZPI) **„„Tożsamość Cyfrowa i Rozwój Uwierzytelniania oraz Podpisów w Systemach Teleinformatycznych (TRUST)" – wnioskodawca: Minister Cyfryzacji, beneficjent: Ministerstwo Cyfryzacji"** przedstawia **następujące stanowisko**.

Z przedstawionego opisu założeń wnioskować należy, że realizacja przedmiotowego projektu informatycznego **wiązać się będzie z przetwarzaniem danych osobowych w bardzo szerokim zakresie**.

W **punkcie 1.1.** wnioskodawca wskazał, że: „Na gruncie krajowym konieczne są zmiany legislacyjne, stworzenie systemów i rejestrów publicznych oraz dostosowanie istniejących systemów i narzędzi, aby zapewnić zgodność z rozporządzeniem eIDAS2".

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

Organ nadzorczy:

- zgłaszał uwagi do **projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122)**[3], wskazując na konieczność dostosowania polskiego sytemu prawnego do eIDAS2 w celu zminimalizowania ryzyk;

- przyjmuje **wprowadzenie szeregu zmian legislacyjnych** w funkcjonującym obecnie systemie identyfikacji elektronicznej:

  - dotyczy to przede wszystkim **wprowadzenia nowych profili zaufanych** w postaci profilu identyfikującego i opisującego podmiot publiczny oraz profilu identyfikującego i opisującego osobę fizyczną reprezentującą podmiot publiczny - co ograniczy używanie „prywatnych" profili zaufanych do celów służbowych,

  - jako, że głównym celem projektu jest **zmodernizowanie krajowych systemów teleinformatycznych służących do identyfikacji elektronicznej** (profil zaufany 2.0 (PZ 2.0), węzeł krajowy 2.0 (WK 2.0)), składania podpisów elektronicznych (węzeł podpisu (WP)), w celu dostosowania do wymogów rozporządzenia eIDAS2;

- przyjmuje, że:

  - wnioskodawca uwzględnił w **OZPI** wykonanie „**inicjalnego" testu prywatności systemów węzeł krajowy 2.0, profil zaufany 2.0, węzeł podpisu, SIE (e-dowód)**, z którego raport ma być przedstawiony w sierpniu 2026 r., co z pewnością pozwoli zweryfikować zasadność wykorzystywania w projekcie planowanego zakresu danych, ocenić ryzyka dla tych danych, a także prawidłowość sporządzonej oceny kierunków zmian otoczenia prawnego przez wnioskodawcę,

  - do końca 2026 r. mają być **wdrożone produkcyjnie zmiany** w systemach teleinformatycznych cyfrowej tożsamości (węzeł krajowy 2.0, profil zaufany 2.0, węzeł podpisu) dostosowujące je do wejścia w życie krajowych aktów prawnych implementujących rozporządzenie eiDAS2.

[3] Pismo z 25 marca 2026 r. (znak: DPNT.401.60.2026.WL.PM).

Test zawierający ocenę skutków dla ochrony danych powinien spełniać wymogi art. 25 ust. 1 [4] i art. 35 (w szczególności ust. 1 [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 projektu 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 (pkt 6 OZPI), w szczególności biorąc pod uwagę elementy wskazane w art. 6 ust. 3, i art. 9 ust. 2 – 4 rozporządzenia 2016/679.

Z zadowoleniem należy przyjąć, że wnioskodawca w **punkcie 6 „Otoczenie prawne”** dostrzega konieczność zmian następujących aktów prawnych:

- ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz.1557 i 1717),

- ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725),

- ustawy z dnia 19 sierpnia 2024 r. o aplikacji mObywatel (Dz.U. z 2024 r. poz. 1275)

- rozporządzenia Ministra Cyfryzacji z dnia 29 czerwca 2020 r. w sprawie profilu zaufanego i podpisu zaufanego (Dz. U. z 2023 r. poz. 2551),

Wskazano, że ogólne rozporządzenie o ochronie danych **NIE wymaga zmian z uwagi na wdrożenie projektu informatycznego, co jest błędne i niewłaściwe**:

---

[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.

- nigdy nie będzie dochodzić do sytuacji, w której planowane przyjęcie przez polską administrację publiczną projektu informatycznego będzie skutkowało koniecznością zmiany tego typu aktu na poziomie europejskim,

- błędnym i niewłaściwym jest choćby kierunkowe przyjmowanie (odpowiedź TAK/NIE), że projektowane rozwiązanie może mieć wpływ na treść czy na zmianę regulacji rozporządzenia 2016/697,

- ten punkt wymaga usunięcia.

Ze względu na charakter przetwarzania danych i wiążące się z nim ryzyko naruszenia praw i wolności osób fizycznych, poszerzonej analizy wymagają również:

- kwestie związane z podatnością systemu na potencjalne **cyberataki i działania hybrydowe** - rozpoznaniu (w drodze prawidłowo przeprowadzonego testu prywatności) konkretnych zagrożeń, powinno towarzyszyć wdrożenie skutecznych i adekwatnych środków prewencyjnych i ochronnych – technicznych oraz organizacyjnych, skutecznie zapewniających integralność, poufność, ale również i prawidłowość danych, w tym odpowiednich środków bezpieczeństwa, szyfrowania, pseudonimizacji i anonimizacji danych osobowych.

Jeżeli w projektowanym systemie mają być wykorzystywane **systemy sztucznej inteligencji** wnioskodawca powinien wziąć pod uwagę:

- nie tylko przepisy rozporządzenia 2016/679, ale także

- akt w sprawie sztucznej inteligencji[7], którego zapewnienie stosowania w krajowym porządku prawnym jest i będzie niezwykle istotne (art. 27 aktu w sprawie sztucznej inteligencji wynika odrębny obowiązek **dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych** (**FRIA**)) - jeżeli realizacja projektu będzie wiązała się z wykorzystaniem takich systemów sztucznej inteligencji, to wnioskodawca powinien również uwzględnić dokonanie takiej oceny w dokumencie opisu założeń projektu informatycznego.

Wnioskodawca powinien także zidentyfikować ryzyka związane z przetwarzaniem danych osobowych, jakie mogą pojawić się w związku z działaniem projektu informatycznego, zwłaszcza wobec:

- znaczącej liczby **systemów teleinformatycznych wykorzystywanych w projekcie**,

- planowanych **przepływów danych** pomiędzy nimi.

Wdrożeniu rozwiązań technologicznych powinny towarzyszyć stosowne rozwiązania prawne gwarantujące wymagany poziom poszanowania praw podstawowych, w tym konstytucyjnego prawa do prywatności oraz ochrony danych osobowych.

[7] 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).

Wprowadzenie rozwiązań technicznych, organizacyjnych, prawnych, czyniących zadość zarówno zasadom rozporządzenia 2016/679, jak i normom Konstytucji RP (art. 47 i art. 51 Konstytucji RP) ma fundamentalne znaczenie dla prawidłowego funkcjonowania technologii cyfrowych w społeczeństwie demokratycznym.

Jednocześnie podkreślić należy, że przedstawiane uwagi Prezesa Urzędu Ochrony Danych Osobowych mają charakter eksperckich wskazówek dla projektodawcy, który podejmuje decyzję co do ostatecznego kształtu projektowanych rozwiązań i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych. Wyrażam nadzieję, że uwzględnienie niniejszych uwag będzie pomocne w tym procesie i przyczyni się do podwyższenia poziomu ochrony danych osobowych w przedmiotowym projekcie informatycznym.

Jeżeli podjęte zostaną odpowiednie prace legislacyjne we wskazanym obszarze, Prezes Urzędu Ochrony Danych Osobowych, jak zawsze, deklaruje swoje eksperckie wsparcie w analizie propozycji przepisów prawa pod kątem ich zgodności z rozporządzeniem 2016/679.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu

Ochrony Danych Osobowych

/-dokument w postaci elektronicznej

podpisany kwalifikowanym podpisem elektronicznym/