



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**

Mirosław Wróblewski

Warszawa, **06 marca 2026**

DPNT.060.5.2026.WL.TG

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

Szanowny Panie Ministrze,

w odpowiedzi na pismo z 26 lutego 2026 r., znak: DPiS.WWKS.002.36.1.2026, przekazujące do zaopiniowania przez osoby uczestniczące w pracach Komitetu do spraw Cyfryzacji opis założeń projektu informatycznego pod nazwą „**Rozwój Systemów Służących do Identyfikacji Elektronicznej i Składania Podpisów Elektronicznych (RSIEPE)**”, powoływany dalej z zastosowaniem skrótu „opis założeń projektu RSIEPE”, uprzejmie informuję, że z części 6. „OTOCZENIE PRAWNE” opisu założeń projektu RSIEPE wynika, że wdrożenie systemu teleinformatycznego węzeł podpisu (MVP) oraz budowa nowej wersji systemu teleinformatycznego profil zaufany (PZ 2.0) i nowej wersji systemu teleinformatycznego węzeł krajowy (WK 2.0) nie będzie wymagać zmian legislacyjnych. Tym samym przyjęć należy, że zakres danych użytkowników przetwarzanych w ww. systemach teleinformatycznych nie ulegnie zmianie w stosunku do stanu obecnego, a proponowane w opisie założeń projektu RSIEPE zmiany mają jedynie charakter informatyczny (w zakresie stosowanego do przetwarzania software'u). Z uwagi na powyższe Prezes Urzędu Ochrony Danych Osobowych, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE)

2016/679¹, powoływanego dalej z zastosowaniem skrótu „rozporządzenie 2016/679”, oraz art. 51 ustawy o ochronie danych osobowych², jako organ nadzorczy do opisu założeń projektu RSIEPE uwag nie zgłasza.

Wszakże przypominam jednocześnie, że podmiot (organ) budujący lub przebudowujący systemy teleinformatyczne, w których będą przetwarzane dane osobowe, ponosi odpowiedzialność za takie ukształtowanie zasad funkcjonowania tego systemu teleinformatycznego (tych systemów teleinformatycznych), by minimalizować ryzyko dla przetwarzanych w nim (nich) danych osobowych. Na kwestię tę zwrócił też uwagę prawodawca unijny, nakładając w art. 25 ust. 1 rozporządzenia 2016/679³ obowiązek uwzględnienia ochrony danych w fazie projektowania (*privacy by design*), czyli przyjmowania tylko takich rozwiązań technicznych i organizacyjnych odnoszących się do przetwarzania danych osobowych, które zapewniają skuteczną realizację zasad ochrony danych, przy uwzględnieniu ryzyka naruszenia praw i wolności osób fizycznych o różnym stopniu prawdopodobieństwa i wadze.

Organ właściwy w sprawie ochrony danych osobowych sygnalizuje również projektodawcy, by w procesie budowy lub przebudowy systemów teleinformatycznych dedykowanych identyfikacji elektronicznej uwzględnił on unormowania zamieszczone w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2024/1183⁴, zwanym rozporządzeniem eIDAS2.

Łączę wyrazy szacunku,
Miroslaw Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym /

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).

³ Zgodnie z art. 25 ust. 1 rozporządzenia 2016/679: „1. 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 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz. Urz. UE L 2024/1183 z 30.4.2024 ze zm.).