Do druku nr 2670

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, **25 czerwca 2026**

DPNT.401.241.2026.WL.OJ

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L. dz. SPS-III.020.45.14.2026
Data wpływu 26.06.26 r.

Pan
Dariusz Salamończyk
Zastępca Szefa
Kancelarii Sejmu RP
Kancelaria Sejmu RP

Szanowny Panie Ministrze,

w odpowiedzi na pismo z 1 czerwca 2026 r. znak: SPS-III.020.45.10.2026, 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], uprzejmie informuję, że do przedstawionego **senackiego projektu ustawy o zmianie ustawy Kodeks wyborczy oraz ustawy o referendum lokalnym (druk nr 2670)**, dalej: projekt, Prezes Urzędu Ochrony Danych Osobowych zgłasza następujące uwagi.

Jak podkreślono w uzasadnieniu, w ocenie projektodawców każdy obywatel RP przebywający za granicą powinien móc dopisywać się do spisu wyborców oraz podlegać takim samym zasadom weryfikacji tożsamości przy wydawaniu karty do głosowania jak obywatel przebywający na terenie innego państwa członkowskiego Unii Europejskiej.

Zgodnie z projektowanym nowym brzmieniem art. 35 § 2b Kodeksu wyborczego[3]: „§ 2b. W celu weryfikacji danych wyborcy konsul posiada dostęp do danych zawartych w rejestrze PESEL, o którym mowa w ustawie z dnia 24 września 2010 r. o ewidencji ludności, w rejestrze dokumentów paszportowych, o którym mowa w ustawie z dnia 27 stycznia 2022 r. o dokumentach paszportowych (Dz. U. z 2026 r. poz. 196) oraz w

[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.).
[3] Ustawa z dnia 5 stycznia 2011 r. - Kodeks wyborczy (Dz. U. z 2025 r. poz. 365 ze zm.), dalej: Kodeks wyborczy.

rejestrze dowodów osobistych, o którym mowa w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2025 r. poz. 1753).".

Projektowany przepis w porównaniu do obecnej wersji regulacji[4] został rozbudowany o **uprawnienie dla konsulów do dostępu do Rejestru Dowodów Osobistych w celów weryfikacji danych wyborców**.

Wobec powyższego wskazać trzeba, że ustawa o dowodach osobistych[5] w art. 55 ust. 7 przyznaje konsulowi w celu realizacji zadań określonych w ustawie dostęp do Rejestru Dowodów Osobistych.

Z punktu widzenia zasady ograniczenia celu (art. 5 ust. 1 lit. b rozporządzenia 2016/679) i minimalizacji danych (art. 5 ust. 1 lit. c rozporządzenia 2016/679) projektodawca powinien jednak rozważyć:

- czy skoro na podstawie **art. 55 ust. 6a** ustawy o dowodach osobistych dane z Rejestru Dowodów Osobistych przekazywane są do rejestru PESEL, to dostęp do kolejnego rejestru publicznego jest dla konsulów w celu weryfikacji danych wyborcy niezbędny,
- czy nie powoduje to dodatkowych ryzyk dla podmiotów danych w związku potencjalnym przekazywaniem ich danych osobowych do systemów teleinformatycznych placówek dyplomatycznych, które to dane chronione są co prawda prawem i immunitetem dyplomatycznym, ale jednak fizycznie znajdując się na terenie państwa gdzie znajduje się dana placówka.
- czy do celów weryfikacji danych osobowych wyborców konsule nie powinni korzystać jedynie z dedykowanego do tego celu Centralnego Rejestru Wyborców, do którego na podstawie art. 18 § 8 pkt 5 Kodeksu wyborczego mają dostęp.

[4] Zgodnie z art. 35 § 2b Kodeksu wyborczego „W celu weryfikacji danych wyborcy konsul posiada dostęp do danych zawartych w rejestrze PESEL, o którym mowa w ustawie z dnia 24 września 2010 r. o ewidencji ludności, oraz w rejestrze dokumentów paszportowych, o którym mowa w ustawie z dnia 27 stycznia 2022 r. o dokumentach paszportowych (Dz. U. z 2024 r. poz. 1063).".

[5] Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. z 2025 r. poz. 1753), dalej: ustawa o dowodach osobistych.

Pomóc w takiej ocenie może wykonanie dla projektu **testu prywatności wraz z oceną skutków dla ochrony danych** (art. 25 [6] i 35 ust. 1 [7] i ust. 10 [8] rozporządzenia 2016/679). W szczególności w trakcie wykonania powyższego testu projektodawca powinien wykonać analizę podatności systemów wykorzystywanych przez konsulów na potencjalne cyberataki i działania hybrydowe.

Taka analiza i wnioski z niej płynące mogłyby doprowadzić w ramach testu prywatności do:

- rozpoznania konkretnych zagrożeń,
- wdrożenia 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 wyborców.

Pragnę jednocześnie podkreślić, że uwagi organu nadzorczego przedstawiane w toku prac legislacyjnych mają charakter eksperckich wskazówek dla projektodawcy, który podejmuje decyzję co do ostatecznego kształtu przyjmowanych przepisów i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych
/ - dokument w postaci elektronicznej podpisany kwalifikowanym podpisem elektronicznym/

---

[6] Ust. 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.
2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych. 3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 i 2 niniejszego artykułu, można wykazać między innymi poprzez wprowadzenie zatwierdzonego mechanizmu certyfikacji określonego w art. 42.

[7] 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.

[8] 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.