



**PREZES  
URZĘDU OCHRONY  
DANYCH OSOBOWYCH  
Mirosław Wróblewski**

Warszawa, 23-09-2024

DOL.060.18.2024.WL.PM

**Pani**

**Wioletta Zwara  
Sekretarz Komitetu Rady Ministrów  
do spraw Cyfryzacji  
Ministerstwo Cyfryzacji**

elektroniczna skrzynka podawcza  
/MAiC/SkrytkaESP

Szanowna Pani Minister,

w związku z pismem z 12 września 2024 r. (znak: DPiS.WWKS.002.127.1.2024), przekazującym do wiadomości Prezesa UODO informację o skierowaniu do rozpatrzenia przez KRMC założeń projektu informatycznego **Rozbudowa ekosystemu aplikacji mObywatel**, działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679<sup>1</sup> oraz art. 51 ustawy o ochronie danych osobowych<sup>2</sup>, Prezes UODO jako organ nadzorczy zgłasza uprzejmie następujące poniższe uwagi.

Wdrożenie projektu informatycznego zakładającego rozbudowę „ekosystemu aplikacji mObywatel” będzie wiązało się z koniecznością dostosowania stanu prawnego do nowych funkcjonalności aplikacji mObywatel. Ministerstwo Cyfryzacji w pkt 6 „Otoczenie Prawne” Opisu Założeń Projektu Informatycznego wskazało zakres zmian, jaki ma być wprowadzony w poszczególnych aktach prawnych regulujących funkcjonowanie aplikacji mObywatel.

---

<sup>1</sup> 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.).

<sup>2</sup> Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

W ocenie organu nadzorczego przy tej okazji oraz ze względu na ilość, jak i zakres podmiotowy i przedmiotowych nowych e-usług, tj. np. obsługi wniosków paszportowych, usługi Chatbot opartej o mechanizm sztucznej inteligencji, opartej o dane z aplikacji mObywatel oraz serwisu gov.pl, usługi opłat skarbowych, systemu płatności w ramach aplikacji mObywatel oraz usługi Dyżurnet.pl służącej do zgłaszanie nielegalnych treści, **pogłębionej analizie powinien zostać poddany zakres podmiotów uczestniczących w procesach przetwarzania danych w aplikacji mObywatel oraz zakres ról i odpowiedzialności tychże podmiotów**, reprezentujących zarówno sektor publiczny, jak i prywatny (administratorów w rozumieniu rozporządzenia 2016/679). Konieczne jest również **przeprowadzenie oceny skutków dla ochrony danych już w ramach procesu legislacyjnego nowelizacji ustawy o aplikacji mObywatel**, odpowiadającej wymogom art. 25 ust. 1<sup>3</sup> i art. 35 (w szczególności ust. 1<sup>4</sup> i ust. 10<sup>5</sup>) rozporządzenia 2016/679.

Kwestie te były już wskazywane przez organ nadzorczy w ramach opiniowania ustawy o aplikacji mObywatel. W ocenie organu nadzorczego rozszerzenie funkcjonalności aplikacji mObywatel powinno odbyć się po pogłębionej ewaluacji tego narzędzia przez Ministerstwo Cyfryzacji, w kontekście wszystkich problemów z zakresu ochrony danych osobowych jakie pojawiły się w trakcie jego dotychczasowego funkcjonowania i stosowania przedmiotowej ustawy.

Organ nadzorczy deklaruje jednocześnie swoje wsparcie eksperckie w ramach procesu oceny aplikacji mObywatel.

Łączę wyrazy szacunku,

Mirosław Wróblewski  
Prezes Urzędu Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany  
kwalifikowanym podpisem elektronicznym/

---

<sup>3</sup> 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.

<sup>4</sup> 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.

<sup>5</sup> 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.

Do wiadomości:

**Pan**

**Krzysztof Gawkowski**

**Wiceprezes Rady Ministrów**

**Minister Cyfryzacji**

elektroniczna skrzynka podawcza  
/MAiC/SkrytkaESP