



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa, 04-11-2024

DOL.060.36.2024.WL.MWR

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

**ul. Królewska 27
00-060 Warszawa**

ePUAP: /MAiC/SkrytkaESP

Szanowna Pani Sekretarz,

w związku z przekazaniem do wiadomości organu nadzorczego pismem z 29 października br. (znak: DPiS.WWKS.002.140.1.2024) dotyczącym opisu założeń projektu informatycznego **„Rozbudowa Systemu do Obsługi Postępowań Administracyjnych w Budownictwie i Portalu e-Budownictwo oraz wybranych rejestrów GUNB (SOPAB 1.0)** (dalej: „Opis”), działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ oraz art. 51 ustawy o ochronie danych osobowych², Prezes UODO jako organ nadzorczy zgłasza uprzejmie następujące poniższe uwagi.

Należy zwrócić uwagę, że w Opisie nie przewidziano konieczności dokonania zmian w prawie (w pkt 6 pt. „Otoczenie prawne” wymieniono akty prawne związane z realizacją projektu informatycznego i wskazano, że żaden z nich nie wymaga zmian). Jednocześnie w pkt 7.1 Opisu wymieniono szereg systemów wykorzystywanych w projekcie, w szczególności planowane jest wdrożenie systemu „Konto użytkownika”, który „przechowuje dane użytkowników wraz z informacjami o realizowanych

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).

sprawach i dostępem do dokumentów z postępowań”. Ponadto zmodyfikowane mają zostać m. in. system Cyfrowa Książka Obiektu Budowlanego („zbiór podstawowych informacji o obiekcie budowlanym, takich jak dane o właścicielu czy zarządcy; możliwość podglądu książki poprzez integrację z SOPAB”) czy system e-Budownictwo Wnioski („System do generowania i bezpośredniego składania wniosków w procesie budowlanym, z kontem użytkownika, na którym wnioski można gromadzić oraz sprawdzać status swojej sprawy”).

Zważywszy na możliwe przetwarzanie danych osobowych w projektowanym systemie SOPAB 1.0, **niezbędne jest przeprowadzenie analizy obowiązujących przepisów prawa w tym zakresie**. Przegląd ten pozwoli na określenie podstawy prawnej przetwarzania (pozyskiwania, gromadzenia, udostępniania). Podkreślić należy, że przetwarzanie danych osobowych przez podmioty publiczne odbywać powinno się na podstawie przepisów prawa, które w sposób precyzyjny wskazują jakie dane będą przetwarzane, w jakim celu, przez jaki okres czasu oraz kto będzie za to przetwarzanie odpowiadał. W przypadku wskazanym w art. 6 ust. 1 lit. c rozporządzenia 2016/679³, gdy mamy do czynienia z przetwarzaniem danych niezbędnym do wypełnienia obowiązku prawnego ciążącego na administratorze, zastosowanie znajduje art. 6 ust. 3 rozporządzenia 2016/679⁴, zgodnie z którym podstawa przetwarzania musi być określona w prawie państwa członkowskiego, któremu podlega administrator.

Wątpliwości organu nadzorczego budzi również obsługa wniosków składanych przez system informatyczny – w szczególności wyjaśnienia wymaga to, czy dla zrealizowania tego celu wykorzystywane będą dane pochodzące z rejestrów państwowych. Jeżeli tak, to prawodawca powinien pamiętać, że wymiana danych między rejestrami musi być szczegółowo uregulowana w prawie. Należy przypomnieć, że rejestry prowadzone są w konkretnych wskazanych w przepisach prawa celach, w których też przetwarzane są dane osobowe w nich zgromadzone. Pozyskiwanie przez organ publiczny danych z innych baz danych powinno odbywać się z poszanowaniem zasad i gwarancji wynikających z rozporządzenia 2016/679. Przepisy wdrażające tego rodzaju rozwiązania powinny szczegółowo określać procedurę, formę, zakres i tryb udostępniania danych osobowych.

³ Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków: c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

⁴ Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona: a) w prawie Unii; lub b) w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) - musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewnijające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

Wśród ryzyk wpływających na realizację projektu (pkt 5.2 Opisu) zauważono „Ryzyko nieodpowiedniego zabezpieczenia przetwarzanych danych”. Jako sposób zarządzania ryzykiem wskazano na „przeprowadzanie cyklicznych audytów bezpieczeństwa także po zakończeniu realizacji projektu zgodnie z wymaganiami stawianymi jednostkom finansów publicznych”, a także „położenie szczególnego nacisku na przestrzeganie wytycznych w zakresie bezpiecznego przetwarzania danych przez podmioty korzystające z systemu”. Prawdopodobieństwo wystąpienia takiego ryzyka oszacowano na „niskie”, a siłę oddziaływania ryzyka na „średnie”. Należy jednak zwrócić uwagę, że w odniesieniu do procesu przetwarzania danych osobowych ryzyka naruszenia praw lub wolności podmiotów danych określa się w drodze testu prywatności, w tym oceny skutków dla ochrony danych (art. 25 ust. 1⁵ oraz 35 ust. 1⁶ rozporządzenia 2016/679). Przeprowadzenie testu pozwoliłoby na szczegółowe rozeznanie ryzyk towarzyszących przetwarzaniu dla praw i wolności podmiotów danych oraz na wprowadzenie gwarancji te ryzyka eliminujące.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem
elektronicznym/

Do wiadomości:

Pan
Krzysztof Paszyk
Minister Rozwoju i Technologii
Ministerstwo Rozwoju i Technologii
ePUAP

⁵ 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.

⁶ 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.