PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 12 grudnia 2024 r.

DOL.060.52.2024.WL.RB

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 przekazanym do wiadomości organu nadzorczego pismem z 5 grudnia br. (znak: DPiS.WWKS.002.167.1.2024) **opisu założeń projektu informatycznego: System obsługi centralnej ewidencji emisyjności budynków - Faza II (CEEB 2.0)** (dalej: „opis założeń"), 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 projektu Prezes Urzędu Ochrony Danych Osobowych, jako organ nadzorczy, przedstawia następujące uwagi.

W projekcie założeń wskazano, że realizacja projektu wynika z potrzeb związanych z łatwym i rzetelnym ewidencjonowaniem źródeł ciepła, energii elektrycznej i spalania paliw wykorzystywanych w gospodarce komunalnobytowej.

Należy zwrócić uwagę na fakt, że w projekcie założeń **nie przewidziano konieczności dokonania zmian w prawie** (**pkt 6** projektu założeń). W **pkt 2.4** projektu założeń wskazano natomiast powstanie m.in. Centralnego Rejestru Charakterystyki Energetycznej Budynków, a także zmodyfikowanej Bazy danych

[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).

CEEB oraz zmodyfikowanej CEEB pobierania danych, jako produktów końcowych projektu. Z uwagi na możliwe przetwarzanie danych osobowych w powyżej wskazanych rejestrach, niezbędne jest przeprowadzenie analizy obowiązujących przepisów prawa w tym zakresie. Przegląd ten pozwoli na określenie podstawy prawnej przetwarzania danych osobowych (ich pozyskiwania, gromadzenia, udostępniania). Przetwarzanie danych osobowych przez podmioty publiczne – zwłaszcza o ile w wyniku przeprowadzenia projektu informatycznego miałyby powstać nowe zasoby danych osobowych - 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 gdy mamy do czynienia z przetwarzaniem danych niezbędnym do wypełnienia obowiązku prawnego ciążącego na administratorze[3] zastosowanie znajduje art. 6 ust. 3 rozporządzenia 2016/679[4] - podstawa przetwarzania musi być określona w prawie państwa członkowskiego, któremu podlega administrator.

Zgodnie z założeniami projektu, jego realizacja wiązać się będzie z **wykorzystaniem licznych, już istniejących systemów** (**pkt 7.1** projektu założeń), z **przepływem danych z innych systemów** (**pkt 7.1** projektu założeń), a także z **przetwarzaniem zawartości innych rejestrów publicznych** (**pkt 7.4** projektu założeń). Wskazać należy, że rejestry prowadzone są w konkretnych wskazanych w przepisach prawa celach, w których też przetwarzane są dane osobowe w nich zgromadzone. Projektodawca powinien natomiast przeprowadzić stosowną analizę obowiązujących przepisów co do istnienia podstaw prawnych dla zakładanego przetwarzania danych osobowych – ocenę skutków dla ochrony danych (art. 35 ust. 1 rozporządzenia 2016/679[5]), celem określenia podstawy prawnej „wykorzystywania" systemów, „wymiany" oraz „przetwarzania" zawartych w nich 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 zapewniające 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.

[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.

Wśród ryzyk wpływających na utrzymanie efektów (**pkt 5.2** projektu założeń) wskazano na **nieodpowiednie zabezpieczenie przetwarzanych danych**. Siłę oddziaływania tego ryzyka oceniono na „dużą", a prawdopodobieństwo wystąpienia na „średnie". Wśród sposobów zarządzania ryzykiem wskazano na „przeprowadzanie cyklicznych audytów bezpieczeństwa także po zakończeniu realizacji projektu zgodnie z wymaganiami stawianymi jednostkom finansów publicznych. Położenie szczególnego nacisku na przestrzeganie wytycznych w zakresie bezpiecznego przetwarzania danych przez podmioty korzystające z systemu". Ryzyka naruszenia praw lub wolności podmiotów danych określa się w drodze testu prywatności, w tym oceny skutków dla ochrony danych (art. 25 ust. 1[6] oraz 35 ust. 1 rozporządzenia 2016/679). Przeprowadzenie takiego 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 Rozwój i Technologii

e-PUAP

[6] 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.