



Warszawa, 04-12-2024

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

DOL.060.48.2024.MP

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

ePUAP: /MAiC/SkrytkaESP

Szanowna Pani Sekretarz,

w związku z przekazaniem do wiadomości organu nadzorczego pismem z 28 listopada br. (znak DPiS.WWKS.002.151.1.2024) dotyczącym **opisu założeń projektu informatycznego CEZAM – Portal klienta** (dalej jako „CEZAM”), działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹, Prezes UODO jako organ nadzorczy zgłasza uprzejmie następujące uwagi.

System CEZAM zakłada przetwarzanie danych osobowych klientów i interesantów Głównego Urzędu Miar. Zakłada ponadto powiązanie za pomocą protokołów API z rejestrami państwowymi, m. in. CEIDG oraz KRS, z których pobierane mają być dane o przedsiębiorcach czy innych osób.

W tym kontekście istotne jest przeprowadzenie analizy planowanych operacji pod względem podstaw prawnych przetwarzania (pozyskiwania, gromadzenia, udostępniania, wykorzystywania). Przetwarzanie danych osobowych przez podmioty publiczne powinno odbywać się w zgodzie z dyspozycją art. 6 ust. 3 rozporządzenia

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.).

2016/679². W kontekście planowanego systemu szczególnie istotne jest wykazanie zakresu niezbędności przetwarzania do realizacji zadań publicznych wynikających z przepisów rozdziału 4 ustawy Prawo o miarach³.

Przegląd planowanych operacji przetwarzania pozwoli nie tylko na ustalenie czy aktualizują się przesłanki legalizujące przetwarzanie z art. 6 ust. 1, ale czy spełnione zostały zasady określone w art. 5 rozporządzenia 2016/679, w tym zasada zgodności z prawem i rozliczalności. W perspektywie planowanej integracji z innymi rejestrami państwowymi rozpatrzenia wymaga przede wszystkim sposób realizacji zasad minimalizacji danych i ograniczenia celu. Wymagane jest przyjęcie takich rozwiązań organizacyjnych i technicznych, które ograniczą dostęp jedynie do danych w zakresie realnie niezbędnym do wypełnienia obowiązku prawnego ciążącego na administratorze lub wykonania zadania realizowanego w interesie publicznym.

Wprowadzeniu nowych rozwiązań technologicznych towarzyszyć powinna analiza ryzyka pod względem oddziaływania na prawa lub wolności osób fizycznych (art. 25 ust. 1⁴ rozporządzenia 2016/679). Rozważyć należy również przeprowadzenie oceny skutków dla ochrony danych (art. 35 ust. 1⁵ rozporządzenia 2016/679). Umożliwiłoby to szczegółowe rozpoznanie ryzyk towarzyszących przetwarzaniu oraz na wprowadzenie środków minimalizujących te ryzyka.

Łączę wyrazy szacunku,

Z up. Prezesa Urzędu
Ochrony Danych Osobowych

Zastępczyni Prezesa
Dr hab. Agnieszka Grzelak

² 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.

³ Ustawa z dnia 11 maja 2001 r. Prawo o miarach (Dz. U. 2022, poz. 2063).

⁴ 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.

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.

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/