PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 22-11-2024

sygn. DOL.060.38.2024

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

ePUAP: /MAiC/SkrytkaESP

Szanowna Pani Sekretarz,

w związku z otrzymaną korespondencją z 18 listopada br. (znak: DPiS.WWKS.002.154.1.2024) uprzejmie dziękuję za przekazanie do wiadomości Prezesa Urzędu Ochrony Danych Osobowych **opisu założeń projektu informatycznego - „KRONIK@ 2.0”**, skierowanego do zaopiniowania przez osoby uczestniczące w posiedzeniach Komitetu Rady Ministrów do spraw Cyfryzacji. Jednocześnie, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] (dalej „rozporządzenie 2016/679”) oraz art. 51 ustawy o ochronie danych osobowych[2], organ nadzorczy zgłasza następujące uwagi.

Jak zostało wskazane w jego opisie, projekt stanowi kontynuację i rozwinięcie zrealizowanego projektu KRONIK@ - Krajowe Repozytorium Obiektów Nauki i Kultury. Portal KRONIK@ służy do przechowywania, zabezpieczenia i udostępniania w celu ponownego wykorzystywania informacji sektora publicznego z zakresu kultury i nauki. Jednym z systemów wykorzystywanych podczas realizacji ww. projektu ma być Węzeł Krajowy – który jako zaawansowany system organizacyjno-techniczny jest kluczowy w uwierzytelnianiu użytkowników systemów teleinformatycznych korzystających z usług online. Działa jako pośrednik między systemami identyfikacji elektronicznej a systemami udostępniającymi usługi online (str. 18 OZPI). W zakresie wymienianych danych, 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.).
[2] Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019, poz. 1781).

przypadku korzystania z węzła krajowego jako środka identyfikacji, mają się znaleźć: imię i nazwisko, adres poczty elektronicznej, numer telefonu oraz PESEL. W związku z powyższym powstaje pytanie o celowość i konieczność wykorzystywania wskazanego modelu w procesie udostępniania przedmiotowych zasobów, biorąc pod uwagę w szczególności takie zasady przetwarzania danych osobowych wynikające z rozporządzenia 2016/679, jak ograniczenie celu (art. 5 ust. 1 lit. b) czy minimalizacja danych (art. 5 ust. 1 lit. c).

Należy również zwrócić uwagę, że pozyskiwany ma być m.in. PESEL, który jako krajowy numer identyfikacyjny podlega szczególnej ochronie[3]. W związku z powyższym zasadne wydaje się **przeprowadzenie oceny skutków dla ochrony danych** odpowiadającej wymogom art. 25 ust. 1[4] i art. 35 (w szczególności ust. 1[5] oraz ust. 10[6]) rozporządzenia 2016/679. Przeprowadzenie takiej analizy pozwoli zweryfikować zasadność wykorzystywania tak szerokiego zakresu danych, a także potrzebę stworzenia odpowiedniej podstawy prawnej lub/i dokonania nowelizacji obowiązujących aktów prawnych niezbędnych do funkcjonowania przedmiotowego systemu.

W przypadku podjęcia prac legislacyjnych nad projektami aktów, zwłaszcza tymi, które stanowiłyby źródła powszechnie obowiązującego prawa oraz wymagałyby oceny pod kątem zgodności z ogólnym rozporządzeniem o ochronie danych – Urząd Ochrony Danych Osobowych deklaruje swoje eksperckie wsparcie.

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

---

[3] Art. 87 rozporządzenia 2016/679: Państwa członkowskie mogą określić szczególne warunki przetwarzania krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym. W takim przypadku krajowego numeru identyfikacyjnego lub innego identyfikatora o zasięgu ogólnym używa się wyłącznie z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą, które przewiduje niniejsze rozporządzenie.

[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 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.

[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.

[6] 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.

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/