PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 16-12-2024

sygn./znak DOL.060.58.2024

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

ePUAP: /MAiC/SkrytkaESP

Szanowna Pani Sekretarz,

w związku z przekazanym do wiadomości organu nadzorczego pismem z 10 grudnia br. (znak: DPiS.WWKS.002.165.1.2024) dotyczącym opisu założeń projektu informatycznego **- „Digitalizacja i cyfrowe udostępnianie dokumentacji w obszarze ochrony zabytków (w tym dokumentacji archiwalnej) w województwach: lubuskim, małopolskim, mazowieckim, opolskim, podlaskim”** (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], Prezes UODO jako organ nadzorczy zgłasza uprzejmie następujące uwagi.

Jak zostało wskazane w opisie założeń, powyższy projekt zakłada zwiększenie możliwości wykorzystania zasobów kultury poprzez digitalizację i cyfrowe udostępnienie dokumentacji w obszarze ochrony zabytków, co ma nastąpić m. in. poprzez modyfikację istniejącego już Systemu NID. Jednym z systemów wykorzystywanych podczas realizacji ww. projektu (pkt. 7.1 opisu założeń) ma być Węzeł Krajowy, który umożliwia uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za

[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).

pośrednictwem Węzła Transgranicznego”. Wskazano również, że zakres wymienianych danych ma obejmować „weryfikację i pobieranie danych użytkownika. Modyfikacja dotyczy uwzględnienia integracji z nowo budowanymi komponentami”. Jak wynika z art. 21a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725) w zakresie wymienianych danych, w przypadku korzystania z Węzła Krajowego jako środka identyfikacji, znajdują się m. in.: imię i nazwisko, adres zamieszkania, miejsce i data urodzenia oraz numer PESEL. W związku z powyższym powstaje pytanie o celowość i konieczność wykorzystywania wskazanego modelu w przedmiotowym projekcie informatycznym, biorąc pod uwagę w szczególności takie zasady przetwarzania danych osobowych wynikające z rozporządzenia 2016/679, jak ograniczenie celu (art. 5 ust. 1 lit. b)[3] czy minimalizacja danych (art. 5 ust. 1 lit. c)[4].

Należy również zwrócić uwagę, że pozyskiwany ma być m.in. PESEL, który jako krajowy numer identyfikacyjny podlega szczególnej ochronie[5]. W związku z powyższym zasadne wydaje się **przeprowadzenie oceny skutków dla ochrony danych** odpowiadającej wymogom art. 25 ust. 1[6] i art. 35 (w szczególności ust. 1[7] oraz ust. 10[8]) 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 pkt 7.1 opisu założeń wskazano także na system Google jako służący „potwierdzaniu tożsamości – weryfikacji i pobieraniu danych użytkownika”. Jak wskazano

---

[3] „Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami ("ograniczenie celu")”.

[4] „Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych")”.

[5] 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.

[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 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.

[7] 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.

[8] 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.

wyżej, systemem służącym uwierzytelnieniu użytkownika jest Węzeł Krajowy, będący systemem państwowym uregulowanym przepisami prawa. Nie jest jasne, dlaczego w opisie założeń wskazano jednocześnie na system Google, dostarczany przez prywatnego giganta technologicznego przetwarzającego znaczne ilości danych osobowych na dużą skalę, jako służący weryfikacji użytkownika. Z opisu założeń nie wynika także, jakie dane osobowe użytkownika miałyby być przetwarzane w związku z wykorzystaniem systemu Google w przedstawionym projekcie informatycznym. Pod rozwagę twórcy opisu założeń należy poddać zasadność wykorzystania tego systemu w projekcie, co ma szczególne znaczenie z punktu widzenia ww. zasady minimalizacji danych, a także zasady integralności i poufności (art. 5 ust. 1 lit. f rozporządzenia 2016/679)[9].

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

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

[9] „Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność")".