



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa, 02-04-2025

DPNT.060.46.2025.WL.MW

**Pani
Katarzyna Bis-Płaza
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 31 marca 2025 r. (znak: DPiS.WWKS.002.73.1.2025), dotyczącym opisu założeń projektu informatycznego **„Digitalizacja i opracowanie zbiorów Muzeum Powstania Warszawskiego oraz ich upowszechnianie poprzez zaawansowaną, wielofunkcyjną internetową platformę cyfrową”** – wnioskodawca: Minister Kultury i Dziedzictwa Narodowego, beneficjent: Muzeum Powstania Warszawskiego, skierowanym do zaopiniowania przez osoby uczestniczące w posiedzeniach Komitetu Rady Ministrów do spraw Cyfryzacji, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ (dalej: „rozporządzenie 2016/679”) oraz art. 51 ustawy o ochronie danych osobowych², Prezes Urzędu Ochrony Danych Osobowych zgłasza **następujące uwagi**.

Z przedstawionego opisu założeń wnioskować należy, że realizacja przedmiotowego projektu informatycznego wiązać się będzie z przetwarzaniem danych osobowych w szerokim zakresie. W ramach **„Digitalizacji i opracowania zbiorów Muzeum Powstania Warszawskiego oraz ich upowszechniania poprzez zaawansowaną, wielofunkcyjną internetową platformę cyfrową”** została wskazana

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).

obszerna lista systemów wykorzystywanych w projekcie, m.in.: baza danych uczestników powstania, baza grobów Powstania Warszawskiego czy baza nagrań i stenogramów rozmów z uczestnikami wydarzeń 1944 roku. Projekt przewiduje digitalizację dokumentów zawierających informacje sektora publicznego oraz dane prywatne pozyskane z wielu źródeł. W ramach projektu teleinformatycznego będą przetwarzane zarówno dane osób żyjących, jak i zmarłych. Zgodnie z rozporządzeniem 2016/679 ochrona danych osobowych dotyczy wyłącznie osób fizycznych, które posiadają zdolność prawną, a w chwili śmierci osoba traci tę zdolność, co oznacza, że rozporządzenie unijne nie obejmuje bezpośrednio danych osób zmarłych (motyw 27 rozporządzenia 2016/679). Jednakże w przypadku informacji dotyczących osób zmarłych konieczne jest rozważenie wpływu przetwarzania danych tych osób na ich bliskich – zarówno ze względu na ochronę prywatności, jak i ochronę dóbr osobistych żyjących członków rodziny.

Celem projektu jest stworzenie multimedialnej platformy Muzeum Powstania Warszawskiego oraz publikacja ucyfrowionych zasobów. Wnioskodawca uwzględnił w projekcie wykonanie „**inicjalnego**” **testu prywatności**, który ma być przeprowadzony w styczniu 2026 r., co z pewnością pozwoli zweryfikować zasadność wykorzystywania w projekcie planowanego zakresu danych, ocenić ryzyka dla tych danych, a także prawidłowość sporządzonej oceny kierunków zmian otoczenia prawnego przez wnioskodawcę. Test ten zawierający ocenę skutków dla ochrony danych powinien spełniać wymogi art. 25 ust. 1³ i art. 35 (w szczególności ust. 1⁴ oraz ust. 10⁵) rozporządzenia 2016/679. Ocena ta powinna zdiagnozować ryzyka dla praw i wolności podmiotów danych wynikające z wdrażanych rozwiązań. Pozwoli to na wypracowanie konkretnych środków zaradczych oraz techniczno-organizacyjnych minimalizujących zidentyfikowane zagrożenia, ale także na prawidłową analizę zagadnień związanych z otoczeniem prawnym.

Biorąc pod uwagę zakres planowanych operacji przetwarzania danych, projektowany model przetwarzania danych osobowych powinien zostać **zweryfikowany z obecnym stanem prawnym**. Analizując pkt 6 OZPI dedykowany otoczeniu prawnemu

³ 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.

⁴ 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.

⁵ 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.

zwrócić uwagę należy, że **wnioskodawca nie przewiduje zmiany wskazanych w ww. punkcie 13 aktów prawnych związanych z realizacją projektu**, co w ocenie Prezesa Urzędu Ochrony Danych powinno być **ponownie przeanalizowane i zweryfikowane**.

Ze względu na charakter przetwarzania danych i wiążące się z nim ryzyko naruszenia praw i wolności osób fizycznych, poszerzonej analizy wymagają również kwestie związane z podatnością systemu na potencjalne **cyberataki i działania hybrydowe**. Rozpoznaniu – w drodze prawidłowo przeprowadzonego testu prywatności – konkretnych zagrożeń, powinno towarzyszyć wdrożenie skutecznych i adekwatnych środków prewencyjnych i ochronnych – technicznych oraz organizacyjnych, skutecznie zapewniających integralność, poufność, ale również i prawidłowość danych, w tym odpowiednich środków bezpieczeństwa, szyfrowania, pseudonimizacji i anonimizacji danych osobowych.

Jeżeli w projektowanym systemie mają być wykorzystywane **systemy sztucznej inteligencji** wnioskodawca powinien wziąć pod uwagę w szczególności nie tylko przepisy rozporządzenia 2016/679, ale także akt w sprawie sztucznej inteligencji⁶, którego zapewnienie stosowania w krajowym porządku prawnym jest i będzie niezwykle istotne. Należy bowiem podkreślić, że z art. 27 aktu w sprawie sztucznej inteligencji wynika odrębny obowiązek dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych (FRIA). Jeżeli realizacja projektu będzie wiązała się z wykorzystaniem takich systemów sztucznej inteligencji, to w ocenie organu nadzorczego wnioskodawca powinien również uwzględnić dokonanie takiej oceny w dokumencie opisu założeń projektu informatycznego.

Prezes UODO zwraca uprzejmie uwagę, że wdrożeniu rozwiązań technologicznych powinny towarzyszyć stosowne rozwiązania prawne gwarantujące wymagany poziom poszanowania praw podstawowych, w tym konstytucyjnego prawa do prywatności oraz ochrony danych osobowych. Wprowadzenie rozwiązań technicznych, organizacyjnych, prawnych, czyniących zadość zarówno zasadom rozporządzenia 2016/679, jak i normom Konstytucji RP (art. 47 i art. 51 Konstytucji RP) ma fundamentalne znaczenie dla prawidłowego funkcjonowania technologii cyfrowych w społeczeństwie demokratycznym.

W przypadku podjęcia prac legislacyjnych nad projektami aktów prawnych, które stanowiłyby podstawę dla projektowanego rozwiązania UODO deklaruje swoje eksperckie wsparcie.

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji).

/ - dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/