



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski**

Warszawa, 08-04-2025

DPNT.060.50.2025.WL.PM

**Pani
Katarzyna Bis-Płaza
Sekretarz Komitetu Rady Ministrów
do spraw Cyfryzacji
Ministerstwo Cyfryzacji**

elektroniczna skrzynka podawcza
/MAiC/SkrytkaESP

Szanowna Pani Minister,

w związku z pismem z 3 kwietnia 2025 r. (znak: DPiS.WWKS.002.79.1.2025), przekazującym do wiadomości Prezesa UODO informację o skierowaniu do zaopiniowania przez osoby uczestniczące w pracach Komitetu Rady Ministrów do spraw Cyfryzacji **opisu założeń projektu informatycznego: Ocalone dziedzictwo odkryte na nowo. Zabezpieczenie, opracowanie i digitalizacja zbiorów Biblioteki Kórnickiej wpisanych na listy UNESCO oraz kontynuacja procesu cyfryzacji najcenniejszych kolekcji z zasobu – wnioskodawca: Minister Nauki i Szkolnictwa Wyższego, beneficjent: Polska Akademia Nauk Biblioteka Kórnicka**, działając na podstawie art. 57 ust. 1 lit. c rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679¹ oraz art. 51 ustawy o ochronie danych osobowych², Prezes UODO jako organ nadzorczy zgłasza następujące uwagi.

Zgodnie z opisem założeń projektu informatycznego, stworzony ma zostać m. in. „»Asystent Czytelnika«, wykorzystujący AI i zawierający komponent przetwarzania języka naturalnego, (...)”. Dodatkowo w LP. 5 tabeli zawierającej „Listę systemów wykorzystywanych w projekcie” wskazano, że w ramach węzła krajowego przetwarzane będą następujące dane osobowe: imię (tylko pierwsze), nazwisko, PESEL, data urodzenia. W pierwszej kolejności wyjaśnienia wymaga czy dane te będą przetwarzane z wykorzystaniem systemów sztucznej inteligencji. Organ nadzorczy wskazuje również na

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).

konieczność analizy czy dane te są adekwatne z punktu widzenia zasady ograniczenia celu (art. 5 ust. 1 lit. b rozporządzenia 2016/679³) oraz zasady minimalizacji danych (art. 5 ust. 1 lit. c rozporządzenia 2016/679⁴) gdyż data urodzenia osoby wynika bezpośrednio z numeru PESEL. Dodatkowo należy zwrócić uwagę, że numer PESEL na podstawie art. 87 rozporządzenia 2016/679⁵ jest krajowym numerem identyfikacyjnym, którego przetwarzanie powinno odbywać się z zachowaniem odpowiednich zabezpieczeń praw i wolności osoby, której dane dotyczą przewidzianych w rozporządzeniu 2016/679. Dlatego też niezbędność przetwarzania numeru PESEL powinna zostać również poddana analizie przez projektodawcę.

Wykorzystanie narzędzi opartych na sztucznej inteligencji implikuje konieczność przeprowadzenia testu prywatności i oceny skutków dla ochrony danych już w ramach przyjmowania podstawy prawnej przetwarzania, odpowiadającej wymogom art. 25 ust. 1⁶ i art. 35 (w szczególności ust. 1⁷ i ust. 10⁸). Jednocześnie wykorzystanie w ramach projektu technologii sztucznej inteligencji sprawia, że projekt ten powinien zostać także oceniony przez pryzmat zapewnienia stosowania Aktu w sprawie sztucznej inteligencji⁹, z

³ Zgodnie z zasadą ograniczenia celu 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.

⁴ Zgodnie z zasadą minimalizacji danych dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

⁵ Zgodnie z art. 87 RODO: 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.

⁹ 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).

uwzględnieniem jego art. 27, także ust. 4 tej regulacji¹⁰, tj. oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych. W opinii Prezesa UODO wnioskodawca powinien więc rozważyć dokonanie takiej oceny w dokumencie opisu założeń projektu informatycznego, jeżeli uzna, że systemy te będą spełniać przesłanki systemów AI wysokiego ryzyka, o których mowa w art. 6 Aktu w sprawie sztucznej inteligencji.

Organ nadzorczy wskazuje również, że jeśli przy okazji wykorzystywania narzędzi AI będzie dochodziło do przetwarzania danych biometrycznych, konieczne staną się zmiany prawne z uwagi na gwarancje określone w art. 9 rozporządzenia 2016/679.

Organ nadzorczy deklaruje jednocześnie swoje wsparcie eksperckie w związku z wspomnianą wyżej oceną skutków dla ochrony danych.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

¹⁰ Przed wdrożeniem systemu AI wysokiego ryzyka, o którym mowa w art. 6 ust. 2, z wyjątkiem systemów AI wysokiego ryzyka przeznaczonych do stosowania w obszarze wymienionym w załączniku III pkt 2, podmioty stosujące będące podmiotami prawa publicznego lub podmiotami prywatnymi świadczącymi usługi publiczne, oraz podmioty stosujące systemy AI wysokiego ryzyka, o których mowa w załączniku III pkt 5 lit. b) i c), przeprowadzają ocenę skutków w zakresie praw podstawowych, jakie może wywołać wykorzystanie takiego systemu. W tym celu podmioty stosujące przeprowadzają ocenę obejmującą:

- a) opis procesów podmiotu stosującego, w których system AI wysokiego ryzyka będzie wykorzystywany zgodnie z jego przeznaczeniem;
- b) opis okresu, w którym każdy system AI wysokiego ryzyka ma być wykorzystywany i opis częstotliwości tego wykorzystywania;
- c) kategorie osób fizycznych i grup, na które może mieć wpływ wykorzystywanie systemu;
- d) szczególne ryzyko szkody, które może mieć wpływ na kategorie osób fizycznych lub grupy osób zidentyfikowane zgodnie z lit. c) niniejszego ustępu, z uwzględnieniem informacji przekazanych przez dostawcę zgodnie z art. 13;
- e) opis wdrożenia środków nadzoru ze strony człowieka, zgodnie z instrukcją obsługi;
- f) środki, jakie należy podjąć w przypadku urzeczywistnienia się tego ryzyka, w tym ustalenia dotyczące zarządzania wewnętrznego i mechanizmów rozpatrywania skarg.

2. Obowiązek ustanowiony w ust. 1 ma zastosowanie do wykorzystania systemu AI wysokiego ryzyka po raz pierwszy. W podobnych przypadkach podmiot stosujący może polegać na wcześniej przeprowadzonych ocenach skutków dla praw podstawowych lub na istniejących ocenach skutków przeprowadzonych przez dostawcę. Jeżeli w trakcie wykorzystania systemu AI wysokiego ryzyka podmiot stosujący uzna, że którykolwiek z elementów wymienionych w ust. 1 uległ zmianie lub nie jest już aktualny, podmiot ten podejmuje niezbędne kroki w celu aktualizacji informacji.

3. Po przeprowadzeniu oceny, o której mowa w ust. 1 niniejszego artykułu, podmiot stosujący powiadamia organ nadzoru rynku o jej wynikach, przedkładając jako element tego powiadomienia wypełniony wzór, o którym mowa w ust. 5 niniejszego artykułu. W przypadku, o którym mowa w art. 46 ust. 1, podmioty stosujące mogą zostać zwolnione z obowiązku dokonania powiadomienia.

4. Jeżeli którykolwiek z obowiązków ustanowionych w niniejszym artykule został już spełniony w wyniku oceny skutków dla ochrony danych przeprowadzonej zgodnie z art. 35 rozporządzenia (UE) 2016/679 lub art. 27 dyrektywy (UE) 2016/680, ocena skutków w zakresie praw podstawowych, o której mowa w ust. 1 niniejszego artykułu, stanowi uzupełnieniem tej oceny skutków dla ochrony danych.

5. Urząd ds. AI opracowuje wzór kwestionariusza, w tym za pomocą zautomatyzowanego narzędzia, aby ułatwić podmiotom stosującym spełnianie ich obowiązków wynikających z niniejszego artykułu w sposób uproszczony.

/ - dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/