



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**

Mirosław Wróblewski

Warszawa, 12-08-2026

DPNT.060.104.2026.WL.PM

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

Szanowna Pani Sekretarz,

w związku z pismem z 6 sierpnia 2026 r. znak: DPIS-WWKS.002.143.1.2026 przekazującym do wiadomości Prezesa Urzędu Ochrony Danych Osobowych informację o skierowaniu do zaopiniowania przez osoby uczestniczące w pracach Komitetu do spraw Cyfryzacji opisu przedsięwzięcia pn. **„Cyfrowy Bliźniak URE (CBURE) – pilotaż postępowań taryfowych w sektorze ciepłownictwa”** – wnioskodawca: Szef Kancelarii Prezesa Rady Ministrów, beneficjent: Urząd Regulacji Energetyki, 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 uprzejmie przekazuje uwagi do projektu.

Zgodnie z **pkt 1.1** OZPI (str. 1) „Identyfikacja problemu i potrzeb” przedsięwzięcie CBURE „(...) zakłada opracowanie trzech grup produktów: ustandaryzowanego modelu procesowego wspierającego wdrażanie rozwiązań AI, środowiska dydaktyczno-testowego do doskonalenia standardu oraz środowiska do pilotażowego wykorzystania zestandaryzowanego procesu w postępowaniach URE.”. W tabeli na str. 2 OZPI wnioskodawca jako zidentyfikowany problem wskazuje: „Brak wystarczającej liczby zwalidowanych wzorców odpowiedzialnego wykorzystania AI w administracji publicznej.

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.), dalej: „rozporządzenie 2016/679”.

² Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 ze zm.).

Ograniczona możliwość testowania standardów transparentności, audytowalności, interoperacyjności i humanin- the-loop w realnym procesie administracyjnym.”. **Pkt 2 OZPI** (str. 3) Efekty Przedsięwzięcia stanowi natomiast: „Przedsięwzięcie realizuje cele Strategii Cyfryzacji Państwa w obszarze transformacji cyfrowej administracji publicznej poprzez opracowanie i pilotażowe wdrożenie rozwiązania wspierającego prowadzenie postępowań administracyjnych z wykorzystaniem technologii cyfrowych i sztucznej inteligencji (...).”

Organ nadzorczy wskazuje, że:

1) – zgodnie z **art. 22 ust. 1** rozporządzenia 2016/679 „Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.”,

– w polskim systemie prawnym nie uregulowano kwestii tego, na ile systemy sztucznej inteligencji oparte o modele językowe mogą działać autonomicznie, co jest szczególnie istotne w kontekście postępowań prowadzonych przez administrację publiczną,

– wydawanie rozstrzygnięć administracyjnych, nawet potwierdzanych przez człowieka, przy znacznej pomocy systemów sztucznej inteligencji opartych o modele językowe wiąże się z wysokim ryzykiem naruszenia praw i wolności osób fizycznych.

2) Zgodnie z **art. 22 ust. 2 lit. b** rozporządzenia 2016/679 w prawie państwa członkowskiego UE należy przewidzieć właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą w przypadku decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu.

Przepis ten należy interpretować szeroko, gdyż w przeciwieństwie do wcześniejszych narzędzi służących jedynie automatyzacji przetwarzania danych, współczesne systemy AI umożliwiają realizację znacznie bardziej złożonych i zaawansowanych działań o znacznym stopniu komplikacji,

– w naturalny sposób tworzy to tendencję do bezrefleksyjnego wykorzystania tych narzędzi, co w kontekście potencjalnych „halucynacji” i błędnych wnioskowań tych systemów może prowadzić do wydania decyzji np. na podstawie nieistniejących danych, błędnej klasyfikacji obywateli lub spraw oraz tworzenia fałszywych powiązań między informacjami,

– bardzo istotne jest **zastosowanie zasady human-in-the-loop (nadzoru ludzkiego) jako kryterium architektury IT.**

Testowanie tego rozwiązania nie może się jednak odbywać w toku programu pilotażowego oraz poprzez wydawanie decyzji administracyjnych z użyciem systemów sztucznej inteligencji **bez odpowiedniej podstawy prawnej do takich działań.**

3) Opis przedsięwzięcia nie wskazuje *de facto* jaki będzie udział systemu sztucznej inteligencji w wydawaniu decyzji administracyjnych,

4) Opis przedsięwzięcia informatycznego wskazuje, że jego przyjęcie powinno zostać poprzedzone testem prywatności, czyli **oceną skutków dla ochrony danych** (art. 25 ust. 1³ oraz 35 ust. 1 rozporządzenia 2016/679⁴). Zastosowanie sztucznej inteligencji wspierającej decyzje pracowników administracji publicznej implikuje celowość przeprowadzenia tej oceny i jej bieżącej aktualizacji.

Wnioskodawca powinien również rozważyć, czy projekt CBURE nie powinien zostać oceniony również przez pryzmat zapewnienia stosowania Aktu w sprawie sztucznej

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 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”.

inteligencji⁵, z uwzględnieniem jego art. 27 ust. 4, tj. **oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych**⁶.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/

Do wiadomości

Pan Grzegorz Karpiński

Sekretarz stanu

Zastępca Szefa Kancelarii Prezesa Rady Ministrów

⁵ 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) Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689 z późn. zm.).

⁶ 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.