PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, 17-04-2026

DPNT.060.13.2026.WL.PM

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

Szanowna Pani Sekretarz,

w związku z pismem z 13 kwietnia 2026 r. znak: DPiS.WWKS.002.170.1.2025, przekazującym do wiadomości Prezesa Urzędu Ochrony Danych Osobowych informację o skierowaniu do zaopiniowania przez osoby uczestniczące w pracach Komitetu do spraw Cyfryzacji założeń projektu informatycznego pod nazwą **„System Archiwizacji i Bazy Wiedzy dla Wojewódzkiego Inspektora Nadzoru Geodezyjnego i Kartograficznego”** wnioskodawca: Minister Spraw Wewnętrznych i Administracji, beneficjent: Pomorski Urząd Wojewódzki w Gdańsku, 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.

Zgodnie z częścią **1.1. Identyfikacja problemu i potrzeb opisu założeń projektu informatycznego** (str. 1) projekt zakłada wdrożenie dwóch systemów teleinformatycznych: „GeoSafe – system umożliwiający bezpieczne i w pełni elektroniczne przekazywanie kopii baz danych EGiB przez jednostki administracji geodezyjnej i kartograficznej (aGiK) do PWINGiK oraz „**GBase** – wewnętrzna baza wiedzy, która umożliwia pracownikom urzędu szybkie wyszukiwanie i przeglądanie wcześniejszych spraw, decyzji administracyjnych, orzeczeń sądów administracyjnych oraz dokumentów z

[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 ze zm.).

Elektronicznego Zarządzania Dokumentacją (EZD).”. W przypadku GBase, jak wskazuje projektodawca „System wykorzystuje metadane (np. kategorie spraw, przepisy, sygnatury, tezy orzeczeń), oferuje filtrowanie i powiązania pomiędzy sprawami, co przyspiesza proces decyzyjny i ułatwia wdrażanie nowych pracowników. Docelowo rozwijany o funkcje automatycznego tagowania treści z wykorzystaniem technologii NLP (Natural Language Processing – przetwarzania języka naturalnego).”.

W przypadku wykorzystania danych osobowych w ramach wewnętrznej bazy wiedzy organu publicznego konieczne jest odrębne określenie celu oraz ocena dopuszczalności takiego przetwarzania, zwłaszcza gdy ma ono charakter wtórny względem pierwotnego celu zebrania danych (np. analityczny lub szkoleniowy). Art. 6 ust. 4 rozporządzenia 2016/679[3] określa warunki przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane. Jak wskazał Trybunał Sprawiedliwości UE w wyroku z 1 października 2015 r. w sprawie C-201/14 Smaranda Bara i in. przeciwko Presedintele Casei Nationale de Asigurări de Sănătate i in[4], dane zebrane dla jednego, określonego celu nie mogą być wykorzystywane do innych celów bez odpowiedniej podstawy prawnej.

Organ nadzorczy zwraca uwagę na potencjalne zagrożenia związane z użyciem technologii NLP, które powinny zostać ocenione przez wnioskodawcę w ramach **oceny skutków dla ochrony danych**, o której mowa w art. 35 ust. 1 rozporządzenia 2016/679[5], tak aby dla funkcjonowania projektowanego systemu spełnione zostały wymagania uwzględniające ochronę danych w fazie projektowania (art. 25 ust. 1 rozporządzenia 2016/679[6]). Opis funkcjonalności systemu wskazuje na cele o ogólnym charakterze (m.in. filtrowanie i powiązania pomiędzy sprawami, wsparcie procesu decyzyjnego, wdrażanie pracowników, rozwój funkcji NLP), nie przesądzając jednoznacznie, czy mają one służyć

---

[3] Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, ani prawa Unii lub prawa państwa członkowskiego stanowiących w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący zagwarantowaniu celów, o których mowa w art. 23 ust. 1, administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi: a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania; b)kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem; c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10; d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

[4] Wyrok TSUE z 1.10.2015 R., C-201/14, Smaranda Bara i in. v. Pretedintele Casei Nationale De Asigurări De Sănătate i in., Zotsis 2015, Nr 10, Poz. I-638.

[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] 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.

wyłącznie prowadzeniu indywidualnych postępowań administracyjnych, czy także zestawieniom i analizom danych pochodzących z różnych spraw. W konsekwencji cele przetwarzania danych pozostają niedookreślone, co utrudnia ocenę ich adekwatności oraz niezbędności w kontekście konkretnych obowiązków służbowych pracowników. Nawet jeśli projektowany system ma mieć charakter wspomagający, jego wykorzystanie do filtrowania, priorytetyzacji lub sugerowania rozstrzygnięć może w praktyce prowadzić do profilowania osób fizycznych w rozumieniu art. 22 ust. 1 rozporządzenia 2016/679[7]. Należy więc zminimalizować ryzyko wystąpienia sytuacji, w której decyzje wywołujące skutki prawne są podejmowane w sposób zautomatyzowany lub w sposób istotnie oparty na wynikach systemu, bez realnej kontroli człowieka. Istnieje ryzyko, że zestawienie wielu pozornie neutralnych informacji (np. sygnatur, kategorii spraw, dat) umożliwi pośrednią identyfikację osoby fizycznej, zwłaszcza przy łączeniu danych z różnych postępowań lub rejestrów. Należy wskazać, że operacje polegające na filtrowaniu i powiązaniu pomiędzy sprawami nie zawsze są niezbędne do realizacji indywidualnych postępowań administracyjnych i mogą służyć także innym celom, takim jak optymalizacja procesów, wdrażanie pracowników czy rozwój funkcji analitycznych (np. NLP). W takim przypadku dochodzi do przetwarzania danych dla celów innych niż pierwotny, a łączenie informacji pochodzących z różnych spraw, decyzji administracyjnych, orzeczeń sądów administracyjnych oraz dokumentów z systemu EZD stwarza możliwość ich zestawiania, w wyniku czego może dojść do reidentyfikacji osoby. Narusza to zasady ochrony danych osobowych: zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a)[8], ograniczenia celu (art. 5 ust. 1 lit. b)[9], minimalizacji danych (art. 5 ust. 1 lit. c)[10], rozliczalności (art. 5 ust. 2)[11] oraz art. 6 ust. 4 rozporządzenia 2016/679.

Jeżeli projektowany system GBase oparty na technologii NLP wykorzystującej technologie sztucznej inteligencji będzie dodatkowo wspomagany przez inne systemy sztucznej inteligencji o charakterze dużych modeli językowych (ang. Large Language Models, LLM), to może to znacząco rozszerzyć autonomię tego systemu. Nie będzie to co prawda system wysokiego ryzyka w rozumieniu art. 6 Aktu w sprawie sztucznej inteligencji[12], może on natomiast ograniczyć udział czynnika ludzkiego w ostatecznym podejmowaniu rozstrzygnięć administracyjnych. Wiąże się to z ryzykiem przetwarzania danych w sposób nieprzejrzysty oraz trudny do zweryfikowania. W szczególności może to

[7] 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.
[8] Zgodnie z zasadą zgodności z prawem, rzetelności i przejrzystości dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.
[9] 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.
[10] Zgodnie z zasadą minimalizacji danych dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
[11] Zgodnie z zasadą rozliczalności administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie.
[12] 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).

prowadzić do ograniczenia kontroli nad prawidłowością i zakresem przetwarzania danych, zwiększać ryzyko błędów lub nieuprawnionego profilowania, bez możliwości ich skutecznego wychwycenia na etapie podejmowania decyzji.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany kwalifikowanym podpisem elektronicznym/

Do wiadomości:

Pan
Tomasz Szymański
Sekretarz Stanu
Ministerstwo Spraw Wewnętrznych i Administracji