PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, **23 lipca 2026**

DPNT.060.97.2026.WL.NP

Pani
Paulina Hennig-Kloska
Minister Klimatu i Środowiska

Szanowna Pani Minister,

w odpowiedzi na skierowane do wiadomości Prezesa Urzędu Ochrony Danych Osobowych pismo z 17 lipca 2026 r. znak: DPIS-WWKS.002.132.1.2026, przekazujące, w celu zaopiniowania przez osoby uczestniczące w pracach Komitetu do spraw Cyfryzacji, dokumentu **opisu założeń przedsięwzięcia informatycznego „Cyberbezpieczna Platforma eGeologia wykorzystująca technologię AI”**, dalej: projekt, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (dalej „rozporządzenie 2016/679”)[1] oraz art. 51 ustawy o ochronie danych osobowych[2], organ nadzorczy zauważa uprzejmie co następuje.

Z przedstawionego opisu założeń wynika, że celem realizacji przedmiotowego przedsięwzięcia informatycznego jest budowa platformy eGeologia udostępniającej e-usługi świadczone przez PIGPIB. **Platforma ma integrować informację geologiczną Polski z zasobów zgromadzonych w PIG-PIB**.

[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 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019, poz. 1781 ze zm.).

Wnioskodawca uwzględnił w projekcie wykonanie **testu prywatności**, co z pewnością pozwoli zweryfikować zasadność wprowadzanych zmian, ocenić ryzyka, a także prawidłowość projektowanych rozwiązań. Pozwoli również ustalić, czy podejmowane działania będą dotyczyły także przetwarzania danych osobowych.

Informacyjnie wskazuję, że **test ten, zawierający ocenę skutków dla ochrony danych** powinien spełniać wymogi art. 25 ust. 1 [3] i art. 35 (w szczególności ust. 1 [4] oraz ust. 10 [5]) rozporządzenia 2016/679. W ocenie tej i na jej podstawie wnioskodawca i beneficjent powinni:

- zdiagnozować ryzyka dla praw i wolności podmiotów danych wynikające z wdrażanych rozwiązań,

- wypracować konkretne środki zaradcze oraz techniczno-organizacyjne minimalizujące zidentyfikowane zagrożenia,

- przeanalizować i dokonać przegląd ukierunkowany na ustalenie czy pośród danych osobowych przetwarzanych w związku z realizacją przedsięwzięcia informatycznego znajdują się dane osobowe szczególnej kategorii, które podlegają szczególnej ochronie,

- przeanalizować zagadnienia związane z otoczeniem prawnym – czy na pewno analiza nie prowadzi do potrzeby uzupełnienia podstaw prawnych przetwarzania danych osobowych.

Zgodnie z założeniami nowy system będzie tworzył **zasoby danych o charakterze rejestru publicznego**. Powstaną dwa rejestry: **rejestr produkcji i podaży surowców**, **rejestr danych kluczowych w gospodarce surowcowej**.

W opisie założeń wskazano również, że nowy **system będzie wykorzystywał inne** systemy, które są zawarte w tabeli pn.” Lista systemów wykorzystywanych w projekcie” oraz **przetwarzał (używał, zmieniał) zawartość szeregu innych rejestrów,** które zostały wskazane w tabeli w pkt. 7.4 „Opis zasobów danych przetwarzanych w planowanym rozwiązaniu”.

---

[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.

Zważywszy jednak na:

- związek projektowanych e-usług z innymi systemami teleinformatycznymi prowadzonymi w konkretnych celach wyznaczonych przepisami prawa, a także,

- niewystarczająco precyzyjnie wskazane w OZPI jak projekt będzie wpływał - „używał, zmieniał" - zawartość innych systemów sektora publicznego,

niezbędne jest przeprowadzenie analizy obowiązujących przepisów prawa w tym zakresie.

Przegląd ten pozwoli na określenie:

- podstawy prawnej przetwarzania (pozyskiwania, gromadzenia, udostępniania),

- ustalenie celów oraz

- przejrzyste określenie sposobów „używania, zmieniania" systemów (rejestrów).

W opisie założeń w pkt. 6 „Otoczenie prawne" wskazano, że **realizacja przedsięwzięcia wymaga zmiany kilku aktów prawnych**, w tym m.in. ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze. **Niemniej jednak wskazano jedynie hasłowo, że zmiany miałyby dotyczyć zmiany trybu i zakresu gromadzenia danych.**

„Używanie, zmienianie" dotyczyć ma rejestrów publicznych, w których przetwarzane są dane osobowe, zatem podstawa prawna tego przetwarzania – w myśl zasady **zgodności z prawem, rzetelności i przejrzystości** - musi być określona w prawie państwa członkowskiego (art. 6 ust. 3 lit b[6] rozporządzenia 2016/679), a przez wzgląd na konieczność wyposażenia wykonawców przedsięwzięcia w konstytucyjnie prawidłowe regulacje prawne oraz konieczność ochrony danych osobowych zgodnie z przepisami obowiązującymi w tym zakresie regulacja ta musi być precyzyjna i wyczerpująca. **Podmioty publiczne, realizujące zadania publiczne z użyciem danych osobowych nie mogą wykonywać na nich operacji w sposób dowolny** – za niewystarczające uznać trzeba określenie jedynie w założeniach projektu, że: „projekt będzie używał, zmieniał zawartość innych systemów sektora publicznego", zwłaszcza w kontekście **powstawania i funkcjonowania nowych rejestrów, dla realizacji działania których „używane, zmieniane" mają być dane**.

Biorąc pod uwagę, że nowy system będzie „przetwarzał zawartość innych rejestrów" należy wziąć również pod uwagę**, czy rozwiązania te przewidują łączenie**

[6] Podstawa przetwarzania, o którym mowa w ust. 1 lit. c) i e), musi być określona: a) w prawie Unii; lub b) w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e) - musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

zbiorów danych, które z punktu widzenia przepisów rozporządzenia 2016/679 jest niedozwolone[7].

W poszczególnych rejestrach publicznych można bowiem przechowywać tylko te dane, które są unikalne w ramach wszystkich rejestrów prowadzonych przez polską administrację publiczną. Dane, które już są przechowywane w innym rejestrze, powinny być pobierane w chwili wystąpienia takiej potrzeby z istniejących rejestrów referencyjnych. Należy bowiem unikać gromadzenia danych, które już są przechowywane w innym rejestrze[8]. **Niedopuszczalny jest więc taki sposób przetwarzania danych osobowych w ramach systemu informatycznego, który prowadziłby do połączenia różnych zbiorów danych (różnych administratorów).**

Ze względu na charakter proponowanych rozwiązań, które mają na celu również **zapewnienia bezpieczeństwa teleinformatycznego systemu** – poszerzonej analizy wymagają więc kwestie związane z jego podatnością 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.

Zauważyć również należy, że w OZPI dot. przedmiotowego projektu wskazano, że **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) **nie wymaga zmian z uwagi na wdrożenie przedsięwzięcia informatycznego, co jest błędne i niewłaściwe ponieważ**:

- nigdy nie będzie dochodzić do sytuacji, w której planowane przyjęcie przez polską administrację publiczną przedsięwzięcia informatycznego będzie skutkowało koniecznością zmiany tego typu aktu na poziomie europejskim,

---

7 Zakaz łączenia baz danych wyraźnie podkreślono w treści motywu 31 rozporządzenia 2016/679 zdanie drugie w brzmieniu: „żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych". Przetwarzając dane osobowe takie organy powinny przestrzegać mających zastosowanie i wiążących je przepisów o ochronie danych, zgodnie z wyznaczonymi im celami przetwarzania. W kontekście łączenia baz danych warto wskazać również na wyrok TSUE z 1 października 2015 r. w sprawie C-201/14 Smaranda Bara i in., z którego treści wynika, że odrębne organy w ramach administracji publicznej należy traktować jako odrębnych administratorów z własnymi przesłankami, co w konsekwencji oznacza, że organ, któremu przekazuje się dane osobowe jest ich odbiorcą.

8 Zob. też: Dobre praktyki AIP tworzenia rejestrów publicznych. Rekomendacje Ministerstwa Cyfryzacji udostępnione na stronie MC: https://www.gov.pl/web/ia/rejestry-publiczne-dobre-praktykiarchitektoniczne-i-legislacyjne

- błędnym i niewłaściwym jest choćby kierunkowe przyjmowanie (odpowiedź TAK/NIE), że projektowane rozwiązanie może mieć wpływ na treść czy na zmianę regulacji rozporządzenia 2016/697.

Z powyższych względów punkt ten należy usunąć.

Zgodnie z opisem założeń: „System eGeologia — z wykorzystaniem sztucznej inteligencji — przetwarza dane z geologicznych baz danych i dostarcza usługobiorcy raporty, analizy trendów oraz scenariusze decyzyjne w formie elektronicznej. Usługa wspiera zarządzanie kryzysowe na poziomie gminy, powiatu, województwa oraz całego państwa, a także umożliwia definiowanie i monitorowanie realizacji celów strategicznych polityki geologicznej."

W projektowanym systemie mają być wykorzystywane **systemy sztucznej inteligencji**, tak więc wnioskodawca powinien wziąć pod uwagę:

- nie tylko przepisy **rozporządzenia 2016/679, w tym art. 22**, ale także

- **akt w sprawie sztucznej inteligencji**[9], którego zapewnienie stosowania w krajowym porządku prawnym jest i będzie niezwykle istotne (z art. 27 aktu w sprawie sztucznej inteligencji wynika odrębny obowiązek **dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych (FRIA)**), oraz który w aspekcie sposobów i ryzyk przetwarzania stosowany powinien być równolegle i uzupełniająco do rozporządzenia 2016/679.

Jeżeli realizacja projektu będzie wiązała się z wykorzystaniem takich systemów sztucznej inteligencji, to wnioskodawca powinien również uwzględnić dokonanie takiej oceny w dokumencie opisu założeń przedsięwzięcia informatycznego.

W tym kontekście należy uwzględnić gwarancje wynikające z regulacji rozporządzenia 2016/679 w kontekście **zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach, w tym profilowania. Przepisami tymi prawodawca określił warunki jakie muszą być spełnione by do takich działań mogło dochodzić**.

Podmioty publiczne powinny działać na podstawie i w granicach prawa oraz z uwzględnieniem konstytucyjnych źródeł prawa (konstytucyjna zasada praworządności), prawa i wolności osób mogą być ograniczane mocą przepisów prawa z poszanowaniem zasad demokratycznego państwa prawa.

Przepisy prawa dopuszczające podejmowanie decyzji opartych na zautomatyzowanym przetwarzaniu powinny przewidywać odpowiednie środki ochrony praw, wolności i prawnie uzasadnionych interesów osób, których dane dotyczą (art. 22 ust. 2 lit. b rozporządzenia 2016/679) - przepis ten powinien być interpretowany z uwzględnieniem rosnącej roli systemów sztucznej inteligencji w procesach decyzyjnych, także wtedy, gdy nie dochodzi do pełnej automatyzacji procesu.

[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).

Zaznaczyć należy również, 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.

Jednocześnie podkreślić należy, że przedstawiane uwagi Prezesa Urzędu Ochrony Danych Osobowych mają charakter eksperckich wskazówek dla projektodawcy, który podejmuje decyzję co do ostatecznego kształtu projektowanych rozwiązań i odpowiada za zapewnienie ich zgodności z przepisami o ochronie danych osobowych. Wyrażam nadzieję, że uwzględnienie niniejszych uwag będzie pomocne w tym procesie i przyczyni się do podwyższenia poziomu ochrony danych osobowych w przedmiotowym przedsięwzięciu informatycznym.

Z wyrazami szacunku,

z up. Prezesa Urzędu
Ochrony Danych Osobowych
Zastępczyni Prezesa
Urzędu Ochrony Danych Osobowych
dr hab. Agnieszka Grzelak

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

Do wiadomości:

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