



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa, 31-03-2025

DPNT.060.36.2025.WL.EK

**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 26 marca 2025 r. (znak: DPiS.WWKS.002.175.1.2025), dotyczącym opisu założeń projektu informatycznego **„Utworzenie i rozwój wysokiej jakości e-usługi w IERiGŻ PIB”** (dalej: „projekt informatyczny”) skierowanego 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 oraz art. 51 ustawy o ochronie danych osobowych², Prezes Urzędu Ochrony Danych Osobowych zgłasza następujące uwagi.

Opiniowany projekt informatyczny zakłada zbudowanie wysokowydajnych baz danych, nowoczesnych algorytmów do przetwarzania informacji, w tym danych osobowych polegający na utworzeniu e-usług w obszarze kooperacji systemów: „Agrokoszty”, „Narzędzie do oceny ekonomicznej gospodarstwa rolnego”, „Porównywarka gospodarstw”, „e-usługi w zakresie polityki rolnej”, „Zdalna pracownia komputerowa”, „Analizy Rynkowe”, „Biblioteka cyfrowa”. Przedmiotowe przedsięwzięcie ma na celu zwiększenie efektywności realizowanych zadań Instytutu Ekonomiki Rolnictwa i Gospodarki Żywnościowej – Państwowego Instytutu Badawczego (dalej:

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 r. poz. 1781).

IERiGŻ PIB), poprawy możliwości gromadzenia i udostępniania informacji, zarządzania polityką rolną i monitorowanie sytuacji ekonomicznej na obszarach wiejskich. IERiGŻ PIB przetwarza i analizuje różnorodne dane o charakterze ekonomiczno-społecznym (obecnie zbierane prosto z gospodarstw rolnych) i ekonomiczno-finansowym a wyniki ich badań i analiz służą podmiotom krajowym jak i zagranicznym oraz stanowią podstawę do raportów dla Komisji Europejskiej oraz EUROSTAT.

W opisie projektu informatycznego w pkt. 2.2 "Udostępnione usługi" wskazane zostało, że tworzone e-usługi pozwolą na automatyzację raportowania i analiz oraz będą wyposażone w funkcje Chat-IERiGŻ PIN z zaangażowaniem sztucznej inteligencji. Przedmiotowe rozwiązania należy oceniać zarówno przez pryzmat zapewnienia stosowania Aktu w sprawie sztucznej inteligencji³, z uwzględnieniem art. 27, także ust. 4⁴ tej regulacji, tj. oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych, jak również art. 22 rozporządzenia 2016/679 dla pełnego poszanowania tej regulacji, która to nie może stracić na znaczeniu.

³ 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).

⁴ 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.

Termin rozpoczęcia prac przedmiotowego projektu informatycznego zaplanowano na listopad br., natomiast zakończenie budowy tej infrastruktury informatycznej planowane jest na grudzień 2028 r. W pkt. 3 opisu założeń projektu informatycznego uwzględniono przeprowadzenie testu prywatności z terminem wyznaczonym na wrzesień 2028 r., co oznacza, że przeprowadzenie testu zaplanowano jedynie na bardzo zaawansowanym etapie budowy tego projektu informatycznego. **Za zasadne wydaje się również objęcie testem prywatności tego projektu już na jak najwcześniejszym etapie prac**, co pozwoliłoby zweryfikować wykorzystanie w projekcie planowanego zakresu danych, ocenić ryzyka dla tych danych, a także ocenić prawidłowość sporządzonej oceny otoczenia prawnego. Wiązać się to powinno z przeprowadzeniem oceny skutków dla ochrony danych odpowiadającej wymogom art. 25 ust. 1⁵ i art. 35 (w szczególności ust. 1⁶ i ust. 10⁷) rozporządzenia 2016/679.

Nie można również pominąć, że w projekcie informatycznym przewidziano innowacyjne rozwiązania wykorzystujące systemy sztucznej inteligencji, co determinuje również przeprowadzenie oceny zgodnie z Aktem w sprawie sztucznej inteligencji. Z art. 27 tej regulacji wynika bowiem odrębny obowiązek dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych. Omawiany dokument opisu założeń projektu informatycznego powinien zatem, obok wymienionych w pkt. 3 kamieni milowych, uwzględniać dokonanie takiej oceny.

W opisie założeń przedmiotowego projektu wskazane zostało, że obowiązujące przepisy (pkt 6 „Otoczenie prawne”) nie wymagają zmian legislacyjnych. Zważywszy jednak na architekturę projektu informatycznego, niezbędne wydaje się przeprowadzenie analizy obowiązujących przepisów prawa w tym zakresie. Przegląd ten pozwoli na określenie podstawy prawnej przetwarzania (pozyskiwania, gromadzenia, udostępniania) i ustalenie celów oraz sposobów „wymiany danych” projektowanych systemów źródłowych (pkt 7 „Architektura” Lista przepływów). O ile ta „wymiana danych” dotyczyć

⁵ 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.

⁶ 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.

⁷ 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.

ma przetwarzania danych osobowych, to podstawa prawna tego przetwarzania musi być określona w prawie państwa członkowskiego (art. 6 ust. 3 lit b rozporządzenia 2016/679)⁸.

W pkt 7.4 „Opisie zasobów danych przetwarzanych w planowanym rozwiązaniu” przewidziano, że nowy system nie będzie tworzył zasobów danych o charakterze rejestru publicznego. Wątpliwości w powyższym zakresie budzi jednak podniesiona argumentacja w powodach podjęcia projektu (pkt 1) „konieczne jest zbudowanie wysokowydajnych baz danych, nowoczesnych algorytmów do przetwarzania”. Należy zwrócić uwagę, że przypadku tworzenia nowego rejestru wymagane jest przyjęcie kompleksowych i przejrzystych norm prawnych, aby spełnione zostały warunki dla legalnego funkcjonowania nowej struktury oraz jej ukształtowanie nastąpiło z poszanowaniem wszystkich zasad ochrony danych określonych w art. 5 rozporządzenia 2016/679⁹.

W przypadku podjęcia prac legislacyjnych nad projektami aktów prawa, które stanowiłyby podstawę dla projektowanego rozwiązania Urząd Ochrony Danych Osobowych deklaruje swoje eksperckie wsparcie.

⁸ 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.

⁹ 1. Dane osobowe muszą być:

- a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą ("zgodność z prawem, rzetelność i przejrzystość");
- b) 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 ("ograniczenie celu");
- c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych");
- d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("prawidłowość");
- e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania");
- f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwoloną lub niezgodną z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych ("integralność i poufność").

2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie ("rozliczalność").

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych

/ - dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/

Do wiadomości:

Pan

Czesław Siekierski

Minister Rolnictwa i Rozwoju Wsi