PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa,**22 lipca 2026**

DPNT.060.71.2026.WL.KM

Pan
Michał Jaros
Sekretarz Stanu
Ministerstwo Rozwoju i Technologii

Szanowny Panie Ministrze,

w związku z pismem z 13 lipca 2026 r., znak: DPIS-WWKS.002.125.1.2026 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 Urzędu Ochrony Danych Osobowych **do opisu założeń projektu informatycznego** (dalej OZPI) **„e-Złotnik – budowa ogólnokrajowej platformy e-usług probierczych wraz z cyfryzacją procesów back-office i automatyzacją obsługi spraw" – wnioskodawca: Minister Finansów i Gospodarki, beneficjent: Główny Urząd Miar: zgłasza następujące uwagi.**

I. Ogólne założenia projektu.

Stosownie do **pkt 1. „Powody podjęcia przedsięwzięcia" ppkt 1.1. „Identyfikacja problemu i potrzeb"** OZPI planowany projekt informatyczny ma wpłynąć na poprawę bezpieczeństwa przesyłek poprzez weryfikację osoby odbierającej towary 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.), dalej „rozporządzenie 2016/679".
[2] Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 r. poz. 1781 ze zm.).

danymi systemowymi. Z kolei **w pkt 7 „Architektura" ppkt 7.1. „Widok kooperacji aplikacji" – tabela lp. 1. „Opis systemu"** zaznaczono m.in., że system e-Złotnik ma wspierać realizację usług probierczych oraz obsługę procesów administracyjnoprobierczych kierowanych do klientów Okręgowych Urzędów Pobierczych (OUP) w Krakowie i w Warszawie, ich wydziałach zamiejscowych oraz w Głównym Urzędzie Miar (GUM). Celem utworzenia systemu jest cyfryzacja oraz automatyzacja usług probierczych, obejmujących badanie i oznaczanie cechami probierczymi wyrobów z metali szlachetnych, a także optymalizacja procesów administracyjnych dla klientów, służb oraz pracowników backoffice. System zastępuje dotychczasowe, papierowe i rozproszone formy dokumentacji oraz przestarzałe narzędzia teleinformatyczne, co pozwala na skrócenie czasu realizacji zgłoszeń, ujednolicenie procedur, podniesienie jakości świadczonych usług oraz zapewnienia wysokiej dostępności i bezpieczeństwa danych.

II. Przetwarzanie danych osobowych w „e-Złotnik".

W związku z działaniem systemu e-Złotnik dochodzić będzie do przetwarzania danych osobowych np. klientów OUP, pracowników OUP, pracowników Głównego Urzędu Miar. W treści OZPI odnaleźć można liczne odniesienia do tego obszaru. Przykładowo:

- „klient zmuszony jest wprowadzić wszystkie dane do formularzy", „dane o przedsiębiorcach przechowywane są w systemie Złotnik (bez e-) w OUP Warszawa" (**pkt 1 „Powody podjęcia przedsięwzięcia" ppkt 1.1. „Identyfikacja problemu i potrzeb"** OZPI);
- OZPI wskazuje się na rodzaje przetwarzanych danych osobowych np.: „danych kontaktowych – adresu e-mail, nr telefonu klientów" w związku z działaniem modułu powiadomień dedykowanego klientom, czy „imion, nazwisk, stanowisk, adresów mailowych oraz identyfikatorów w stosunku do pracowników OUP (**pkt. 7 „Architektura" ppkt 7.1. „Widok kooperacji aplikacji"** OZPI).

Organ nadzorczy pozytywnie ocenia określone **w pkt 3 „Kamienie milowe"** OZPI przez projektodawcę „przygotowanie raportu z inicjalnego testu prywatności[3]. Rekomendowanym jest, aby na etapie przeprowadzania ww. testu prywatności **projektodawca:**

- na jak najwcześniejszym etapie **dokonał faktycznej i dogłębnej analizy tego jakie kategorie danych osobowych, w jakim zakresie będą przetwarzane;**
- **określił podstawy prawne, na których to przetwarzanie będzie oparte – uwzględnił w przepisach krajowych sposoby przetwarzania danych osobowych na potrzeby „e-Złotnik" zgodnie z normami rozporządzenia 2016/679,**
- **określił „cykl życia" danych osobowych jakie mają być przetwarzane przy wykorzystaniu przedmiotowego projektu (od momentu ich pozyskania do ich usunięcia),**
- **określił role i obowiązki** (w tym też te z obszaru ochrony danych osobowych) **poszczególnych podmiotów, które będą miały realny dostęp do danych**

[3] Prezes UODO w korespondencji z Komitetem ds. Cyfryzacji wielokrotnie podkreślał znaczącą role testu prywatności w procesie wdrażania systemów teleinformatycznych. Zob. pismo DPiS.WWWKS.501.1.2025.

znajdujących się w projektowanym rozwiązaniu (np. będą mogły wprowadzać/modyfikować /usuwać/ przeglądać znajdujące się w niej informacje, w tym dane osobowe).

Przedmiotowy projekt informatyczny powinien zapewniać zachowanie poufności, integralności, autentyczności i kompletności oraz dostępności danych osobowych, które będą w nim przetwarzane.

III. Ryzyka związane z przetwarzaniem danych osobowych w „e-Złotnik"

Na aprobatę zasługuje uwzględnienie przez projektodawcę **w pkt 4 „Koszty" ppkt. 4.2. „Wykaz poszczególnych pozycji kosztowych"** OZPI **nazwa pozycji kosztowej „Bezpieczeństwo" w ramach, której realizowane mają być testy i audyt bezpieczeństwa, w tym testy penetracyjne**. Problematyka bezpieczeństwa, w tym wspominane testy bezpieczeństwa są w kontekście art. 32[4] rozporządzenia 2016/679 – istotnym elementem planowanego projektu informatycznego. Jednocześnie podkreślić należy, że wspomniane w OZPI testy i audyty **nie są jedynymi środkami technicznymi i organizacyjnymi, jakie powinny być brane pod rozwagę. Istotne są także inne aspekty wynikające z przepisów rozporządzenia 2016/679**. Wnioskodawca powinien m.in. rozważyć stworzenie niezbędnej dokumentacji (procedur) z perspektywy ochrony danych osobowych przetwarzanych w projekcie informatycznym.

Z zadowoleniem należy przyjąć ryzyka wyodrębnione przez Wnioskodawcę w **pkt. 5. „Główne ryzyka" ppkt 5.2. Ryzyka wpływające na utrzymanie efektów** OZP np.:

- niestabilność lub niedostępność usługi chmurowej,
- naruszenie bezpieczeństwa danych w wyniku ataku phishingowego
- utrata dostępności danych w wyniku ataku ransomware
- zaszyfrowanie danych w wyniku ataku ransomware

Pamiętać przy tym należy, że **ryzyka (zagrożenia) powinny być szacowane w sposób okresowy (ciągły). Mogą one z czasem ulegać zmianom. Zidentyfikowanie nowych ryzyk przekłada się z kolei na dostosowywanie do nich adekwatnych zabezpieczeń.** Fakt planowania integracji rejestrów publicznych (**pkt 7 „Architektura" ppkt 7.2. „Opis zasobów danych przetwarzanych w planowanym rozwiązaniu"**), jak i wielu istniejących już systemów teleinformatycznych (**pkt. 7 Architektura ppkt. 1 Widok kooperacji aplikacji – Lista systemów wykorzystywanych w projekcie**) w tym planowane przepływy danych między nimi, a projektowanym systemem „e-Złotnik" (**Lista**

[4] Zgodnie z art. 32 ust. 1 rozporządzenia 2016/679 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, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku: a) pseudonimizację i szyfrowanie danych osobowych; b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

przepływów) z pewnością będzie wpływało na powstawanie wielu ryzyk związanych z przetwarzaniem danych osobowych. Dotyczy to zwłaszcza obszarów takich jak nieuprawniony dostęp, wyciek lub nieuprawniona modyfikacja. Jednocześnie powinien on też określić jakie środki techniczne i organizacyjne będą wdrożone w celu ich skutecznego ograniczenia lub minimalizacji ich potencjalnych skutków.

IV. System „e-Złotnik" – rejestr znaków imiennych (rejestr publiczny)

Stosownie do pkt. 7. „Architekutra" ppkt 7.4. „Opis zasobów danych przetwarzanych w planowanym rozwiązaniu" projektodawca przewiduje, **że planowany system „e-Złotnik" będzie tworzył zasoby danych o charakterze rejestru publicznego.** Wskazuje, przy tym na „rejestry jawne znaków imiennych dla OUP Warszawa i OUP Kraków dostępne na wniosek w zakresie pojedynczych wpisów". Wspomnieć wypada, że rejestr jawny znaków imiennych nie jest rejestrem nowym. Założeniem projektu informatycznego jest to, że istniejące rejestry znaków imiennych prowadzone przez OUP Warszawa i Kraków maja być ujednolicone (aktualnie rejestr prowadzony przez OUP Kraków jest niedostępny dla OUP Warszawa i odwrotnie).

Obecnie podstawy prawne (cel, zakres informacji, w tym danych osobowych w nim przetwarzanych, zasad i formy jego funkcjonowania) określają przepisy art. 19-22 ustawy Prawo probiercze[5]. Wpis do tego rejestru wiąże się z podaniem określonych informacji, w tym niekiedy też danych osobowych[6].

Organ nadzorczy przypomina, że funkcjonowanie rejestru publicznego wymaga:

- **umocowania w przepisach rangi ustawowej**,
- **precyzyjnego określenia w przepisach celu/celów jego funkcjonowania, a tym samym celu/celów przetwarzania danych osobowych** (brak regulacji w tym zakresie uchybia art. 6 ust. 3 rozporządzenia 2016/679 wskazującemu niezbędne elementy podstawy prawnej przetwarzania danych oraz zasadzie celowości przetwarzania danych osobowych (art. 5 ust. 1 lit b[7] rozporządzenia 2016/679);
- **określenia w przepisach prawa wyczerpującego katalogu informacji, w danych osobowych, jakie mają znajdować się w tym rejestrze (**powinien on zawierać tylko

[5] Ustawa z 1 kwietnia 2011 r., t.j. Dz. U. z 2023 r., poz. 536, dalej: „ustawa Prawo probiercze".
[6] Zgodnie z art. 20 ust. 1 ustawy Prawo probiercze Wpisowi do rejestru znaków imiennych podlegają: 1) numer ewidencyjny znaku imiennego; 2) data wpisu do rejestru znaków imiennych; 3) oznaczenie podmiotu, o którym mowa w art. 19 ust. 4 pkt 1; 4) **adres do doręczeń lub adres, pod którym jest wykonywana działalność gospodarcza**; 5) numer w rejestrze przedsiębiorców w Krajowym Rejestrze Sądowym oraz numer identyfikacji podatkowej (NIP) - w przypadku podmiotów i wytwórców, o których mowa w art. 18 ust. 2, o ile takie numery posiadają; 6) **numer ewidencyjny Powszechnego Elektronicznego Systemu Ewidencji Ludności (PESEL) lub numer innego dokumentu potwierdzającego tożsamość i obywatelstwo - w przypadku wytwórcy, o którym mowa w art. 19 ust. 2**; 7) informacje o zmianie danych objętych wpisem do rejestru znaków imiennych wraz ze wskazaniem daty powstania tych zmian. 8) (uchylony).
[7] 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 ("ograniczenie celu").

niezbędny, minimalny zakres danych osobowych (art. 5 ust. 1 lit c[8] rozporządzenia 2016/679) niezbędny do realizacji celu/celów działania tego rejestru),
- sprecyzowania, **w jakiej postaci i przy wykorzystaniu jakich narzędzi będzie on prowadzony**,
- **ustalania czy będzie on pozostawał w relacji z innymi rejestrami publicznymi, a jeśli tak to na jakich zasadach będą między nimi realizowane przepływy danych.**
- **określenia okresów retencji zawartych w nich informacji, w tym danych osobowych** – przepisy, które określają jawność danych muszą precyzować konkretny okres retencji (przechowywania), aby dany nie widniały w przestrzeni publicznej bezterminowo (art. 5 ust. 1 lit e rozporządzenia 2016/679)[9],
- **uwzględnienia przepisów ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[10], jak i dobrych praktyk dotyczących tworzenia rejestrów publicznych** opracowanych przez Ministerstwo Cyfryzacji[11].

V. Korzystanie z narzędzi sztucznej inteligencji w związku z planowanym projektem informatycznym.

W kilku miejscach OZPI pojawiają się odwołania do:
- „[…] zastosowanie metod uczenia maszynowego umożliwi automatyzację procesu rejestracji i identyfikacji znaku imiennego wytwórcy" (**pkt 1. „Powody podjęcia przedsięwzięcia" ppkt 1.1. „Identyfikacja problemu i potrzeb"** OZPI);
- „Optymalizacja i automatyzacja procesów administracyjnoprobierczych poprzez wdrożenie nowoczesnego podsystemu pracownika oraz aplikacji mobilnej, opartych na **algorytmach uczenia maszynowego** i zmodernizowanych rejestrach, wdrożonych na bezpiecznej infrastrukturze wysokiej dostępności w celu skrócenia czasu operacji i podniesienia jakości usług". (**pkt. 2 „Cele i korzyści" ppkt 2.1. „Cele i korzyści wynikające z realizacji przedsięwzięcia" – cel 2** OZPI**);**
- „proces wytwarzania oprogramowania dedykowanego systemu eZłotnik dla podsystemu klienta, podsystemu pracownika i aplikacji mobilnej wraz z komponentami procesowości, skrzynki podawczej, **uczenia maszynowego i integracjami**, zakup licencji, usług i baz danych." **(pkt 4 „Koszty" ppkt 4.2. „Wykaz poszczególnych pozycji kosztowych"** OZPI);

---

[8] Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych").
[9] Dane osobowe muszą być 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").
[10] Ustawa z 17 lutego 2005 r., tj. Dz. U. z 2025 r., poz. 1703.
[11] Zob. Zespół Architektury Informacyjnej Państwa Departamentu Projektów i Strategii Ministerstwa Cyfryzacji, *Rejestry publiczne – dobre praktyki architektoniczne i legislacyjne*, strona internetowa: https://www.gov.pl/web/ia/rejestry-publiczne-dobre-praktyki-architektoniczne-i-legislacyjne [dostęp 26.06.2026 r.].

- „[…] moduł identyfikacji znaków imiennych wykorzystujący algorytmy uczenia maszynowego i algorytmy rozpoznawania obrazów do automatycznego wyszukiwania i porównywania nowo rejestrowanych lub badanych znaków imiennych" (**pkt. 7 „Architektura" ppkt 7.1. Widok kooperacji aplikacji – opis systemu „e-Złotnik"** OZPI)

Oznacza to, że projektodawca planuje wykorzystać narzędzia sztucznej inteligencji w związku z realizacją planowanego projektu informatycznego. Mając na uwadze powyższe **zalecanym jest, aby zadbał on o:**

- **doprecyzowanie kwestii planowanego wykorzystania wsparcia AI i jego ewentualnego wpływu na przetwarzanie danych osobowych**,
- **to, aby znalazło to także odzwierciedlenie w osobnej analizie pod względem zgodności planowanych operacji przetwarzania z Aktem w sprawie sztucznej inteligencji[12] (AI Act – art. 27)**. Jednocześnie powinien on też uwzględniać fakt, że de lege lata przepisy ogólne regulujące postępowanie administracyjnego (ustawa Kodeks Postępowania Administracyjnego[13]) nie przewidują możliwości stosowania takich rozwiązań, w szczególności w sprawach kończących się wydaniem decyzji administracyjnej.

W kontekście ewentualnego korzystania ze sztucznej inteligencji zalecanym jest również wzięcie przez projektodawcę pod rozwagę opinię Europejskiej Rady Ochrony Danych (EROD) 28/2024 w sprawie wykorzystania danych osobowych do opracowywania i wdrażania modeli sztucznej inteligencji[14]. Określono w niej kryteria pozwalające ustalić kiedy i w jaki sposób modele sztucznej inteligencji można uznać za realnie anonimowe oraz jakie metody uniemożliwiające identyfikację osób fizycznych można zastosować, aby zapewnić anonimowość.

VI. Otoczenie prawne.

W świetle treści **pkt 6 „Otoczenie prawne" (tabela):**

1) **ppkt 1** OZPI określono, że projekt nie wymaga wprowadzenia zmian w ustawie Prawo probiercze; W kontekście wcześniej wspominanego planowanego ujednolicenia rejestru znaków imiennych **zalecanym jest ponowne przeanalizowanie przez projektodawcę ewentualnej potrzeby doprecyzowania / modyfikacji przepisów ustawy Prawo pobiercze w zakresie regulacji dotyczących ww. rejestru** (m.in. w obszarze doprecyzowania okresu retencji informacji, w tym danych osobowych ujętych w rejestrze);

[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).

[13] Ustawa z 14 czerwca 1960 r., t.j. Dz. U. z 2025 r., poz. 1691.

[14] Wytyczne z 17 grudnia 2024 r., strona internetowa: https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_pl [dostęp 20.07.2026 r.].

2) **ppkt 5** OZPI 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 projektu informatycznego**. W ocenie organu nadzorczego nigdy nie będzie dochodzić do sytuacji, w której planowane przyjęcie przez polską administrację publiczną projektu informatycznego będzie skutkowało koniecznością zmiany tego typu aktu na poziomie europejskim.** 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. Dlatego też w części opisu projektu informatycznego odnoszącym się do otoczenia prawnego nie jest rekomendowanym zamieszczanie informacji o jego wpływie na rozporządzenie 2016/697. Ten punkt wymaga usunięcia. Ta część opisu służy w swojej istocie bardziej wskazaniu aktów na których treść wprowadzenie (i wdrożenie) projektu informatycznego będzie realnie oddziaływało.

Wyrażam nadzieję, że uwzględnienie niniejszych uwag będzie pomocne i przyczyni się do podwyższenia poziomu ochrony danych osobowych w przedmiotowym projekcie 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
Komitet do spraw Cyfryzacji
Ministerstwo Cyfryzacji

Pan
Rafał Kępka
Wiceprezes
Główny Urząd Miar