PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa,**21 lipca 2026**

DPNT.060.71.2026.WL.KM

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

Szanowna Pani Minister,

w związku z pismem z 9 lipca 2026 r., znak: DPIS-WWKS.002.91.1.2026 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) **System Rozliczania Dotacji – SRD, wnioskodawca: Ministerstwo Finansów i Gospodarki, beneficjent: Ministerstwo Finansów zgłasza następujące uwagi.**

I. Założenia ogólne projektu.

Stosownie do **pkt 1. „Powody podjęcia przedsięwzięcia" ppkt 1.1. „Identyfikacja problemu i potrzeb"** OZPI planowany projekt informatyczny ma służyć zwiększeniu efektywności i przejrzystości gospodarowania środkami publicznymi poprzez cyfryzację procesów oceny, zarządzania, kontroli i monitorowania oraz konsolidację

[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.).

wszystkich informacji i dokumentów dotyczących przekazywania, wykorzystania i rozliczania dotacji na realizację zadań publicznym.

Wprowadzenie systemu SRD nierozerwalnie związane jest z przetwarzaniem informacji identyfikujących beneficjentów dotacji.

II. Przetwarzanie danych osobowych w systemie SRD – potrzeba przeprowadzenia inicjalnego testu prywatności.

Z treści zawartych w OZPI wywnioskować można, że w związku z działaniem systemu SRD dochodzić będzie do przetwarzania danych osobowych (np. użytkowników tego systemu, podmiotów: uczestniczących w procesie wnioskowania o dotacje, przypuszczalnie też podmiotów biorących udział w realizacji umówionego i dotowanego zadania). Projektodawca ma tego świadomość, zwłaszcza, że w **pkt. 6 „Otoczenie prawne" OZPI w tabeli lp. 1 kolumna o nazwie „Opis zmian", tiret szóste** dostrzega potrzebę określenie w przepisach ustawy o finansach publicznych[3] „**zasad przetwarzania danych osobowych zawartych w SRD"**

- aspekt ten jest właściwie wspominany tylko w tej części OZPI,
- jak również istotnym jest, że zasady dotyczące przetwarzania danych osobowych wyznaczone są przepisami rozporządzenia 2016/679.

Dlatego też uwzględniając powyższe rekomendowanym jest, aby **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 SRD 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 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.

W **pkt 3. „Kamienie milowe"** OZPI przewiduje się m.in., że: „wykonany system w zakresie udostępniania danych publicznych", „uzyskany pozytywny wynik testów bezpieczeństwa".

[3] Ustawa z 27 sierpnia 2009 r., t.j. Dz.U. z 2025 r., poz. 1483.

Projektodawca nie przewiduje niestety przeprowadzenia inicjalnego testu prywatności[4], czyli oceny skutków dla ochrony danych (art. 25 ust. 1[5] oraz 35 ust. 7[6] rozporządzenia 2016/679), zarówno w aspekcie **funkcjonowania** samego projektu informatycznego jak i stworzenia właściwiej **podstawy prawnej** i **sposobów przetwarzania danych osobowych dla niego**.

Dzięki temu możliwym będzie:

- zidentyfikowanie realnych ryzyk dla praw i wolności podmiotów danych wynikających z planowanego wdrożenia przedmiotowego projektu informatycznego,
- wypracowanie konkretnych rozwiązań techniczno-organizacyjnych, które przyczynią się do minimalizacji zagrożeń jakie płyną z uprzednio zmapowanych ryzyk.

W toku tego testu powinna zostać także przeprowadzona analiza i przegląd ukierunkowany na ustalenie czy pośród danych osobowych przetwarzanych w związku z realizacją projektu informatycznego są dane osobowe szczególnej kategorii (np. dane o stanie zdrowia, jakie mogą pojawić się w związku z realizacją zadań w ramach otrzymanych dotacji), które podlegają szczególnej ochronie oraz przyjęcie w tym zakresie przepisów przewidujących gwarancje ochrony praw osób.

III. Ryzyka związane z przetwarzaniem danych osobowych.

Na aprobatę zasługuje uwzględnienie przez projektodawców w pkt 4 „Koszty" ppkt. 4.2. „Wykaz poszczególnych pozycji kosztowych" OZPI **nazwa pozycji kosztowej „Bezpieczeństwo".** W uzasadnieniu tej pozycji podkreślono potrzebę „wykonania niezbędnych dla bezpieczeństwa analiz, badań i testów oraz zakup specjalistycznego oprogramowania dedykowanego do poprawy bezpieczeństwa". Problematyka bezpieczeństwa, w tym wspominane testy bezpieczeństwa są w kontekście

[4] 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.

[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.

art. 32[7] rozporządzenia 2016/679 – istotnym elementem planowanego projektu informatycznego. Zauważyć jednocześnie należy, że **wspominane w OZPI „przeprowadzenie testów bezpieczeństwa, licencje na rozwiązanie niwelujące ataki z zewnątrz" 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.

W pkt. **5. „Główne ryzyka" 5.1. Ryzyka wpływające na realizację projektu** OZPI ryzyka istotne z perspektywy ochrony danych osobowych w ogóle nie zostały zmapowane. **Wnioskodawca powinien podjąć próbę zidentyfikowania ryzyk związanych z przetwarzaniem danych osobowych, jakie mogą pojawić się w związku z działaniem projektu informatycznego**.

Fakt planowania integracji szeregu 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 nowym systemie SRD (**Lista 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 SRD – planowany nowy rejestr publiczny.

Stosownie do pkt. 7. „Architekutra" ppkt 7.4. „Opis zasobów danych przetwarzanych w planowanym rozwiązaniu" projektodawca przewiduje, **że nowy system będzie tworzył zasoby danych o charakterze rejestru publicznego.** Wskazuje, przy tym, że „do tego rejestru dostęp będzie nieograniczony dla wszystkich, którzy będą chcieli uzyskać informacje o podmiocie lub zadaniu dotowanym ze środków publicznych, będą w nim prezentowane syntetyczne dane o kwotach dotacji, celach na jakie zostały udzielone oraz podmiotach uczestniczących w procesie udzielania dotacji (nazwa, adres siedziby, oznaczenie realizowanego zadania, nazwa zadania, termin jego realizacji, kwota

[7] 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.

przekazanych środków, nazwa i adres dysponenta nadzorującego realizację zadania, dane kontaktowe), itp., itd.”.

Jeżeli planowane jest stworzenie nowego rejestru publicznego to m.in., koniecznym jest, aby:

- jego istnienie znalazło **umocowanie w przepisach rangi ustawowej**,
- **precyzyjnie określono w tworzonych przepisach cel/cele jego funkcjonowania, a tym samym cel/cele 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[8] rozporządzenia 2016/679);
- **ujęty został w przepisach prawa wyczerpujący katalog informacji, w danych osobowych, jakie mają znajdować się w tym rejestrze (**powinien on zawierać tylko niezbędny, minimalny zakres danych osobowych (art. 5 ust. 1 lit c[9] rozporządzenia 2016/679) niezbędny do realizacji celu/celów działania tego rejestru),
- sprecyzowano, **w jakiej postaci i przy wykorzystaniu jakich narzędzi będzie on prowadzony**,
- **ustalano czy będzie on pozostawał w relacji z innymi rejestrami publicznymi, a jeśli tak to na jakich zasadach będą między nimi realizowane przepływy danych, w jaki sposób będą udostępniane dane osobowe celem poszanowania zasady rozliczalności** (art. 5 ust. 2 rozporządzenia 2016/679).
- **określono okresy 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)[10],
- **uwzględniono przepisy ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[11], jak i dobrych praktyk dotyczących tworzenia rejestrów publicznych** opracowanych przez Ministerstwo Cyfryzacji[12].

Na etapie projektowania regulacji prawnych dotyczących tego rejestru przeprowadzony powinien zostać wspominany już wcześniej **test prywatności, w tym** –

[8] 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").

[9] Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane ("minimalizacja danych").

[10] 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").

[11] Ustawa z 17 lutego 2005 r., tj. Dz. U. z 2025 r., poz. 1703.

[12] 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.].

zwłaszcza jeżeli przetwarzane będą dane osobowe szczególnej kategorii – **ocena skutków dla ochrony** (art. 25 ust. 1 oraz art. 35 ust. 1[13] i 10[14] rozporządzenia 2016/679), które służą ocenie ryzyka naruszenia praw lub wolności podmiotów danych. Pozwoli to na:

- szczegółowe rozeznanie przez projektodawcę ryzyk towarzyszących przetwarzaniu dla praw i wolności podmiotów danych oraz na wprowadzenie w przedmiotowych przepisach prawa gwarancji te ryzyka eliminujących,
- określenie jasnej i precyzyjnej podstawy prawnej przetwarzania (m.in. pozyskiwania, gromadzenia, udostępniania).

Takie rozwiązanie przyczyni się więc do tworzenia przepisów w zgodzie z przepisami rozporządzenia 2016/679[15].

V. Otoczenie prawne.

W świetle treści **pkt 6 „Otoczenie prawne" (tabela) ppkt 18** 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

---

[13] 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.

[14] 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.

[15] Zob. wystąpienie PUODO z 29 października 2025 r., skierowane do Ministra Cyfryzacji, dotyczące konieczności dokonania przeglądu przepisów prawa dot. rejestrów publicznych, DOL.413.11.2024. Prezes UODO wskazał na konieczność dokonania przeglądu przepisów prawa regulujących przetwarzanie danych osobowych w rejestrach publicznych celem dostosowania warunków ich przetwarzania do zasad ochrony danych osobowych wynikających z Konstytucji RP oraz rozporządzenia 2016/67920 , które to uwagi, w kontekście analizy przedmiotowej ustawy również wymagają przypomnienia i uwzględnienia przez prawodawcę. Wystąpienie dostępne jest na stronie internetowe: https://uodo.gov.pl/pl/138/3968 [dostęp 13.07.2026 r.].

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:
Pan
Jurand Drop
Podsekretarz Stanu
Ministerstwo Finansów i Gospodarki

wnioskodawca: Minister Finansów i Gospodarki