PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, **04 sierpnia 2026**

DPNT.060.101.2026.WL.NP

Pani
Jolanta Sobierańska-Grenda
Minister Zdrowia

Szanowna Pani Minister,

w odpowiedzi na skierowane do wiadomości Prezesa Urzędu Ochrony Danych Osobowych pismo z 3 sierpnia 2026 r. znak: DPIS-WWKS.002.146.1.2026, przekazujące, w celu zaopiniowania przez osoby uczestniczące w pracach Komitetu do spraw Cyfryzacji, dokumentu **opisu założeń przedsięwzięcia informatycznego „Weryfikacja Publikacji Medycznych (WPM)”**, 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 przedsięwzięcia informatycznego (OZPI) wynika, że celem realizacji przedmiotowego przedsięwzięcia informatycznego jest **opracowanie i wdrożenie modułu weryfikacji publikacji medycznych systemu OpenPBL plus opartego na platformie typu low-code, stanowiącego nowoczesną e-usługę dla lekarzy i administracji publicznej**. Moduł umożliwi automatyczne pobieranie, agregowanie i weryfikację danych o publikacjach oraz generowanie elektronicznych zaświadczeń i zestawień dorobku naukowego wykorzystywanych w procesach administracyjnych. Realizacja przedsięwzięcia zlikwiduje lukę pomiędzy wymaganiami formalnymi a możliwościami ich efektywnej realizacji, tworząc nowoczesny moduł

[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 ze zm.).

OpenPBL plus wspierający lekarzy oraz instytucje odpowiedzialne za ocenę ich dorobku naukowego.

Prezes UODO przekazuje niniejszym wskazówki oraz uwagi dla projektodawcy przedstawionego projektu, które będą pomocne w jego opracowywaniu oraz przyczynią się do podwyższenia poziomu ochrony danych osobowych w projektowanym przedsięwzięciu.

1. Przeprowadzenie testu prywatności

Wnioskodawca uwzględnił w projekcie wykonanie **testów prywatności (inicjalnego oraz weryfikacyjnego)**, 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.

Prezes Urzędu Ochrony Danych Osobowych rekomenduje, aby na etapie przeprowadzania testu prywatności **projektodawca (wnioskodawca / beneficjent):**

- na jak najwcześniejszym etapie **dokonał faktycznej i dogłębnej analizy tego, jakie kategorie danych osobowych, w jakim zakresie będą przetwarzane;**
- **określił (zweryfikował ich istnienie) podstawy prawne, na których to przetwarzanie danych będzie oparte** – uwzględnił w przepisach krajowych sposoby przetwarzania danych osobowych na potrzeby realizacji określonego projektu/przedsięwzięcia 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, aby nie było wątpliwości jaki status mają te podmioty w procesach przetwarzania danych);
- ustalił, określił i zapewnił stosowne **środki techniczne i organizacyjne**, gwarantujące zachowanie poufności, integralności, autentyczności i kompletności oraz dostępności danych osobowych w toku planowanych projektów / przedsięwzięć informatycznych;
- **działał z poszanowaniem zasad dotyczących przetwarzania danych osobowych**, zwłaszcza zważywszy na konieczność rozliczalności przestrzegania obowiązków i

procesów przetwarzania zgodnie z przepisami rozporządzenia ogólnego o ochronie danych (art. 5 rozporządzenia 2016/679[3]).

2. Ryzyka związane z przetwarzaniem danych osobowych.

Problematyka **bezpieczeństwa** – w tym wspominane w przedstawionym opisie założeń **testy bezpieczeństwa** – są w kontekście art. 32 [4] (jak i art. 25 i 35) rozporządzenia 2016/679 istotnym elementem większości planowanych projektów / przedsięwzięć informatycznych.

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 / beneficjent powinien m.in. rozważyć **stworzenie niezbędnej dokumentacji (procedur) z perspektywy ochrony danych osobowych przetwarzanych w projekcie informatycznym**. Działania te powinny opierać się na szczegółowej identyfikacji i konkretyzacji ryzyk w odniesieniu do specyfiki konkretnego projektu, uwzględniając m.in. charakter, zakres, kontekst i cele przetwarzania danych.

Z zadowoleniem należy przyjąć, że **wnioskodawca starał się wyodrębnić ryzyka**, np. podatność systemu czy ryzyko naruszenia bezpieczeństwa danych.

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. Dotyczy to zwłaszcza obszarów takich jak nieuprawniony dostęp, wyciek lub nieuprawniona modyfikacja. Jednocześnie powinien on też określić jakie środki

---

[3] 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 niedozwolonym lub niezgodnym 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").

[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.

techniczne i organizacyjne będą wdrożone w celu ich skutecznego ograniczenia lub minimalizacji ich potencjalnych skutków.

W OZPI w części „Bezpieczeństwo” założono, że w ramach projektu zostaną wdrożone zasady bezpieczeństwa informacji zgodne z wymaganiami KRI i dobrymi praktykami, adekwatne do zakresu przetwarzanych danych bibliograficznych i metadanych naukowych. Wskazano również, że projekt przewiduje:

- kontrolę dostępu do systemu — uwierzytelnianie i autoryzację użytkowników administracyjnych;
- rozdzielenie ról i uprawnień użytkowników systemu;
- zabezpieczenie infrastruktury teleinformatycznej (firewalle, aktualizacje systemów, ochrona antywirusowa);
- regularne wykonywanie kopii zapasowych danych oraz procedury ich odtwarzania;
- monitorowanie i rejestrowanie zdarzeń systemowych (Zabbix);
- **spełnienie wymagań RODO w zakresie przetwarzania danych osobowych (ograniczony zakres).**

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.

3. Wykorzystywanie innych systemów.

W przekazanym OZPI pojawiała się **problematyka planowanego wykorzystywania zasobów, w tym wymiany danych, z innych systemów dla realizacji danego projektu.**

W części „Efekty przedsięwzięcia” wskazano, że: „Projekt wspiera podejście zakładające budowę spójnego środowiska cyfrowego administracji publicznej, opartego na wspólnych zasadach wymiany danych, wykorzystaniu interfejsów integracyjnych oraz możliwości współpracy z innymi systemami publicznymi.” Ponadto opis założeń wskazuje na „Listę systemów wykorzystywanych w przedsięwzięciu” takich jak m.in.: POL-on / PBN, Ludzie Nauki, KRONIK@.

Biorąc pod uwagę, że **nowotworzony system będzie wykorzystywał inne systemy** organ właściwy w sprawie ochrony danych osobowych podkreśla, że należy wziąć również pod uwagę, **czy rozwiązanie te przewiduje łączenie zbiorów danych, co z punktu widzenia przepisów rozporządzenia 2016/679 jest niedozwolone.**

Organ nadzorczy przypomina że dla **funkcjonowania rejestru publicznego i nierozerwalnie z nim związanego przetwarzania gromadzonych w nim danych osobowych wymagane jest:**

- **umocowanie w przepisach rangi ustawowej**,
- **precyzyjne określenie 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 rozporządzenia 2016/679),
- **określenie w przepisach prawa wyczerpującego katalogu 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 rozporządzenia 2016/679 niezbędny do realizacji celu/celów działania tego rejestru),
- sprecyzowanie, **w jakiej postaci i przy wykorzystaniu jakich narzędzi będzie zasób prowadzony**,
- **ustalenie czy zasób będzie pozostawał w relacji z innymi rejestrami publicznymi, a jeśli tak to na jakich zasadach będą między nimi realizowane przepływy danych** (wszelkie niejednoznaczne określenia powinny być wyeliminowane),
- **określenie okresów retencji zawartych w nich informacji, w tym danych osobowych** – przepisy, które określają jawność danych muszą precyzować konkretny okres retencji (przechowywania), aby dane nie widniały w przestrzeni publicznej bezterminowo (art. 5 ust. 1 lit e rozporządzenia 2016/679),
- **uwzględnienie przepisów ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne**[5], **jak i dobrych praktyk dotyczących tworzenia rejestrów publicznych** opracowanych przez Ministerstwo Cyfryzacji[6].

Podmioty publiczne, realizujące zadania publiczne z użyciem danych osobowych nie mogą wykonywać na nich operacji w sposób dowolny.

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[7]. **Niedopuszczalny jest więc taki sposób przetwarzania danych osobowych w ramach systemu informatycznego, który prowadziłby do połączenia różnych zbiorów danych (różnych administratorów), chyba że operacja ta opierałaby się na wyraźnej podstawie prawnej w postaci konkretnego przepisu prawa krajowego lub unijnego, a samo łączenie jest niezbędne i proporcjonalne do realizacji określonego zadania publicznego.** Warunkiem koniecznym jest również **jasne zdefiniowanie ról podmiotów** biorących udział w wykonywaniu operacji na danych osobowych mocą przepisów określających strukturę administratorów, **zapewnienie pełnej realizacji praw osób, których dane dotyczą,** oraz przeprowadzanie i udokumentowanie **oceny skutków**

[5] Dz. U. z 2025 r. poz. 1703.
[6] 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.].
7 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

dla ochrony danych, z wykazaniem i zapewnieniem bezpieczeństwa całego procesu, przy jednoczesnym zachowaniu zasady minimalizacji danych i unikaniu nadmiarowego gromadzenia danych.

4. **Zmiana ogólnego rozporządzenia o ochronie danych.**

Przedstawiony opis założeń przedsięwzięcia informatycznego w odniesieniu do rozporządzenia 2016/679 wskazuje, że NIE wymaga ono 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 OZPI 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.

Mając na uwadze powyższe, 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.

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

/-dokument w postaci elektronicznej
podpisany kwalifikowanym podpisem elektronicznym/

Do wiadomości:
Pani Katarzyna Bis-Płaza
Sekretarz Komitetu do spraw Cyfryzacji
Ministerstwo Cyfryzacji