

Nazwa dokumentu: opisu założeń projektu informatycznego (dalej OZPI) „WIEDZ@ - Węzły Integracji Edukacji i Danych Zasobów Akademickich)” –
wnioskodawca: Minister Nauki i Szkolnictwa Wyższego, **beneficjent:** Ośrodek Przetwarzania Informacji - Państwowy Instytut Badawczy

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
1	Prezes UODO	pkt 1. „Powody podjęcia projektu” w ppkt 1. „Identyfikacja problemu i potrzeb” OZPI w zw. z pkt 2. „Efekty projektu” ppkt. 2.3. „Udostępnione informacje sektora publicznego i zdigitalizowane zasoby” OZPI	Stosownie do treści tego punktu ” OZPI platforma WIEDZ@ zakłada utworzenie krajowego, federacyjnego rozwiązania zapewniającego dostęp do metadanych, zasobów i usług związanych z polską nauką oraz wybranymi zasobami archiwalnymi przy zachowaniu rozproszonego modelu przechowywania danych. Ma on w założeniu ingerować istniejące już systemy na poziomie metadanych, usługi i API, bez zastępowania systemów źródłowych. Planowany projekt informatyczny wiąże się – co potwierdzają treści zawarte m.in. w pkt 2. „Efekty projektu” ppkt. 2.3. „Udostępnione informacje sektora publicznego i zdigitalizowane zasoby” OZPI – z przetwarzaniem danych osobowych, albowiem w opisie wspomina się w szczególności o: „danych użytkowników”, „danych autorów”, „danych badawczych”, „danych prywatnych” (np. udostępnianych w wyniku realizacji projektu). Część z nich będzie miała walor informacji o charakterze powszechnie dostępnym (np. dane autorów publikacji, afiliacje autorów, profile naukowców często mający charakter danych służbowych), z tego też tytułu i przetwarzanie nie będzie budziło		

			wątpliwości. Z uwagi na możliwość pojawienia się w związku z realizacją przedmiotowego projektu informatycznego także innych danych osobowych (np. wspomnianych powyżej danych prywatnych) 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, - określił „cykl życia” danych osobowych jakie mają być przetwarzane przy wykorzystaniu przedmiotowego projektu (od momentu ich pozyskania do ich usunięcia), - określił obowiązki i role (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). Projekt informatyczny powinien zapewniać zachowanie poufności, integralności, kompletności oraz dostępności danych osobowych, które będą w nim przetwarzane.		
2	Prezes UODO	pkt 1 „Powody podjęcia projektu” ppkt 1.1. „Identyfikacja problemu i potrzeb” OPZI	Wspomina się o „mechanizmach AI”, które będą wspierały analizę, interpretację i przygotowanie danych do dalszego użycia. Oznacza to, że planowane jest wykorzystanie narzędzi sztucznej inteligencji dla realizacji projektu informatycznego. Cel/cele wykorzystania AI został/-y wskazany/-e przez		

		projektodawcę, ale: - nie jest do końca jasnym, czy wsparcie AI ma służyć użytkownikom projektu informatycznego, a w konsekwencji czy planowana do wykorzystania sztuczna inteligencja będzie w jakimkolwiek stopniu przetwarzała ich dane osobowe, a jeśli tak to w jakim zakresie, - wnioskodawca powinien zadbać o doprecyzowanie kwestii planowanego wykorzystania wsparcia AI i jego ewentualnego wpływu na przetwarzanie danych osobowych – przy uwzględnieniu zasad przetwarzania danych osobowych, a zwłaszcza zasady zgodności z prawem, przejrzystości oraz rozliczalności (art. 5 rozporządzenia 2016/679) – w toku planowanego testu przeprowadzić także test prywatności, w tym uwzględnić ochronę danych w fazie projektowania oraz domyślną ochronę danych (art. 25 rozporządzenia 2016/679). Stosownie nowoczesnych technologii (planowane wsparcie AI) i związane z tym przetwarzanie danych osobowych wymaga przeprowadzania testu prywatności, w tym uwzględnienia ochrony danych zarówno w toku projektowania jak i wykonywania przedmiotowego projektu (art. 35 rozporządzenia 2016/679). Niezależnie od powyższego niezbędna będzie przypuszczalnie również osobna analiza pod względem zgodności planowanych operacji przetwarzania z Aktem w sprawie sztucznej inteligencji (AI Act) . Ze względu na planowane wykorzystanie w projekcie informatycznym wsparcia AI		
--	--	---	--	--

			zalecanym jest także 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 . 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. Zaznaczyć należy, że odpowiednie środki techniczne i organizacyjne powinny uniemożliwiać stosowanie sztucznej inteligencji w celu niedozwolonego profilowania i zautomatyzowanego podejmowania decyzji (art. 22 ust. 1 rozporządzenia 2016/679). Ważnym jest, aby użytkownicy korzystający z AI byli we właściwy sposób informowani o sposobie jej funkcjonowania. Pozwoli to administratorowi danych na realizację zasad przetwarzania danych osobowych zwłaszcza zasady: rozliczalności, rzetelności i przejrzystości.		
3	Prezes UODO	pkt 3. „Kamienie milowe” OZPI	W wierszu pierwszym tabeli przewidywane jest Przeprowadzenie inicjalnego testu prywatności. Takie działania zasługują na aprobatę organu nadzorczego, albowiem świadczą one o tym, że twórca OPZI jest świadomy tego, że będzie w związku z planowaną realizacją projektu będzie dochodziło do przetwarzania danych osobowych. Wspominany inicjalny test prywatności powinien obejmować ocenę skutków dla ochrony danych osobowych (art.		

			35 rozporządzenia 2016/679). Jej przeprowadzenie umożliwi zidentyfikowanie realnych ryzyk dla praw i wolności podmiotów danych wynikających z planowanego wdrożenia przedmiotowego projektu informatycznego. Jednocześnie pozwoli ona także na wypracowanie konkretnych rozwiązań techniczno-organizacyjnych, które przyczynią się do minimalizacji zagrożeń jakie płyną z uprzednio zmapowanych ryzyk. W ramach wspomnianego testu powinna zostać także przeprowadzona analiza i przegląd ukierunkowany na ustalenie czy pośród danych osobowych przetwarzanych w związku z realizacją projektu informatycznego znajdują się dane osobowe szczególnej kategorii (np. dane o niepełnosprawności, jakie mogą pojawić się w związku z realizacją projektów unijnych), które podlegają szczególnej ochronie.		
4	Prezes UODO	w pkt 4 „Koszty” ppkt. 4.2. „Wykaz poszczególnych pozycji kosztowych” OZPI nazwa pozycji kosztowej Bezpieczeństwo w zw. z pkt 2 „Efekty projektu” ppkt 2.4. „Produkty końcowe projektu”.	Na aprobatę zasługuje uwzględnienie przez projektodawców kosztów obejmujących audyty bezpieczeństwa, testy prywatności, testy podatności systemu oraz badania zgodności rozwiązania z obowiązującymi przepisami prawa (pozycja dotyczy działań niezbędnych do zapewnienia ochrony danych i bezpieczeństwa wdrażanych rozwiązań. Problematyka bezpieczeństwa, w tym wspomniane testy jest w kontekście art. 32 rozporządzenia 2016/679 – istotnym elementem planowanego projektu informatycznego. Zauważyć jednocześnie należy, że raporty z testów penetracyjnych, czy ocena zabezpieczeń IT nie są jedynymi		

			środkami technicznymi i organizacyjnymi, jakie powinny być brane pod rozagę. 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. Niejako przy okazji organ nadzorczy pozytywnie ocenia planowane opracowanie „Polityki zarządzania danymi”, o którym wspomina się w pkt 2 „Efekty projektu” ppkt 2.4. „Produkty końcowe projektu”.		
5	Prezes UODO	pkt. 5. „Główne ryzyka” 5.1. Ryzyka wpływające na realizację projektu oraz 5.2. Ryzyka wpływające na utrzymanie efektów w zw. z 7.5. „Bezpieczeństwo”	Z zadowoleniem należy przyjąć wyodrębnione przez Wnioskodawcę ryzyka m.in.: - ryzyka prawne i regulacje dotyczące ochrony danych, zasad dostępu i ponownego wykorzystania - brak spójnego formatu danych z różnych źródeł; - brak odpowiedniego zabezpieczenia systemu (możliwość włamań, ataków hakerskich i naruszeń bezpieczeństwa). Wnioskodawca powinien: - zidentyfikować ryzyka związane z przetwarzaniem danych osobowych, jakie mogą pojawić się w związku z działaniem projektu informatycznego, zwłaszcza wobec znaczącej liczby systemów teleinformatycznych wykorzystywanych w projekcie, jak i planowanych przepływów danych pomiędzy nimi.		
6	Prezes UODO	pkt 6 „Otoczenie prawne” (tabela) l.p. 19 OZPI	W punkcie tym 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. Błędym i niewłaściwym jest choćby kierunkowe przyjmowanie (odpowiedź TAK/NIE), że projektowane rozwiązanie może mieć wpływ na treść czy na zmianę regulacji rozporządzenia 2016/697 (dotyczy to także innych aktów unijnych wspomnianych w pkt 6 Otoczenie prawne l.p. 16-18). 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.	
--	--	--	--	--