

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 dokonać faktycznej i dogłębnej analizy tego jakie kategorie danych osobowych, w jakim zakresie będą przetwarzane, - określił podstawy prawne, na których to przetwarzanie będzie oparte,		Beneficjent przyjmuje uwagę Prezesa UODO dotyczącą potrzeby faktycznej analizy kategorii danych osobowych, które mogą być przetwarzane w projekcie. Analiza taka zostanie przeprowadzona na etapie realizacji projektu. Obejmie ona w szczególności identyfikację kategorii danych osobowych, które mogą wystąpić w systemie, w tym danych autorów, naukowców, użytkowników, osób występujących w zasobach archiwalnych oraz ewentualnych danych prywatnych. Na tym etapie zostaną również określone cele i podstawy prawne przetwarzania, cykl życia danych, zasady retencji i usuwania, role podmiotów uczestniczących w przetwarzaniu danych oraz zasady nadawania, modyfikowania i odbierania uprawnień. Ustalenia te będą wynikały z docelowego modelu organizacyjnego i technicznego systemu, a nie wyłącznie z ogólnych założeń opisanych w OZPI. Projektowane rozwiązanie będzie realizowane z uwzględnieniem wymagań dotyczących poufności, integralności, dostępności i rozliczalności danych, adekwatnie do zakresu przetwarzania i ryzyk zidentyfikowanych w toku realizacji projektu.

			- 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		Beneficjent przyjmuje uwagę dotyczącą potrzeby oceny wpływu mechanizmów AI na przetwarzanie danych osobowych. Na obecnym etapie zakłada się, że mechanizmy AI będą wykorzystywane przede wszystkim do wspierania wyszukiwania semantycznego, wzbogacania metadanych, analizy zasobów, rekomendacji oraz przygotowania danych do ponownego wykorzystania. Nie zakłada się wykorzystywania AI do podejmowania wobec użytkowników decyzji wywołujących skutki prawne lub podobnie istotnie na nich wpływających. Na etapie realizacji projektu zostanie jednak przeanalizowane, czy i w jakim zakresie planowane mechanizmy AI będą przetwarzały dane osobowe użytkowników lub dane osobowe występujące w zasobach przetwarzanych w projekcie. Jeżeli takie przetwarzanie zostanie zidentyfikowane, określone zostaną odpowiednie podstawy prawne, ograniczenia, środki techniczne i organizacyjne oraz obowiązki informacyjne. W toku realizacji projektu zostanie również przeprowadzona analiza zgodności planowanych rozwiązań AI z właściwymi przepisami, w tym z AI Act oraz zasadami wynikającymi z RODO, w szczególności zasadą zgodności z prawem, rzetelności, przejrzystości, minimalizacji danych, ograniczenia celu i rozliczalności.

			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 rozagę 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		Beneficjent wskazuje, że w projekcie przewidziano dwa etapy weryfikacji zagadnień prywatności i ochrony danych. Pierwszym etapem będzie inicjalny test prywatności, realizowany na wczesnym etapie projektu. Jego celem będzie identyfikacja podstawowych kategorii danych, operacji przetwarzania, ról podmiotów, potencjalnych ryzyk oraz obszarów wymagających dalszej analizy. Drugim etapem będzie test prywatności przeprowadzony ok. 3 miesiące przed wdrożeniem pierwszego systemu lub komponentu. Jego celem będzie weryfikacja przyjętych rozwiązań projektowych, docelowych przepływów danych, mechanizmów dostępu, środków technicznych i organizacyjnych oraz zgodności przetwarzania z wymaganiami RODO. W ramach tych działań zostanie zweryfikowane, czy zachodzą przesłanki do przeprowadzenia oceny skutków dla ochrony danych, o której mowa w art. 35 RODO. Jeżeli analiza ryzyka wykaże, że planowane operacje przetwarzania mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ocena skutków dla ochrony danych zostanie przeprowadzona zgodnie z wymaganiami RODO.

			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 w 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 rozważenie. 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”.		Beneficjent podziela stanowisko Prezesa UODO, że bezpieczeństwo danych osobowych nie powinno być utożsamiane wyłącznie z testami technicznymi, testami podatności lub testami penetracyjnymi. Na etapie realizacji projektu działania w zakresie bezpieczeństwa będą obejmowały zarówno środki techniczne, jak i organizacyjne. Oprócz audytów bezpieczeństwa, testów podatności i weryfikacji zabezpieczeń IT, przewidziane zostaną również działania dotyczące dokumentacji i procedur ochrony danych osobowych, adekwatnie do ustalonego zakresu przetwarzania. Może to obejmować w szczególności zasady zarządzania dostępem, obsługi incydentów, retencji danych, realizacji obowiązków informacyjnych, powierzania przetwarzania danych, realizacji praw osób, których dane dotyczą oraz dokumentowania decyzji projektowych związanych z ochroną danych w fazie projektowania i domyślną ochroną danych.
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		Beneficjent przyjmuje uwagę dotyczącą potrzeby identyfikacji ryzyk związanych z przetwarzaniem danych osobowych. Ryzyka te zostaną przeanalizowane na etapie realizacji projektu, w szczególności w związku z integracją wielu systemów, przepływami danych pomiędzy podmiotami oraz planowanym wykorzystaniem mechanizmów AI. Analiza obejmie m.in. ryzyka związane z przetwarzaniem danych w zakresie szerszym niż niezbędny, nieprawidłowym określeniem podstaw prawnych przetwarzania, nieuprawnionym dostępem do danych, błędną konfiguracją uprawnień, naruszeniem poufności, integralności lub dostępności danych, nieprawidłowym udostępnieniem danych w ramach integracji oraz ewentualnym przetwarzaniem danych przy wykorzystaniu AI. Dla zidentyfikowanych ryzyk zostaną określone działania ograniczające, obejmujące środki organizacyjne, techniczne i proceduralne.

			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. Błędny i niewłaściwym jest choćby kierunkowe przyjmowanie (odpowieź 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.		Beneficjent częściowo przyjmuje uwagę Prezesa UODO dotyczącą sposobu ujęcia RODO i innych aktów prawa UE w tabeli otoczenia prawnego. Beneficjent zgadza się, że realizacja projektu WIEDZ@ nie będzie skutkować zmianą rozporządzenia 2016/679 ani innych aktów prawa Unii Europejskiej. Oczywiście jest, że krajowy projekt informatyczny nie może wpływać na treść rozporządzenia unijnego. Jednocześnie beneficjent wskazuje, że zgodnie z dobrymi praktykami przygotowania OZPI w tabeli otoczenia prawnego wskazuje się akty prawne istotne dla realizacji projektu, także wtedy, gdy projekt nie wymaga ich zmiany. Celem tej części dokumentu jest bowiem identyfikacja aktów prawnych, które dotyczą projektu, oraz wskazanie, czy ich zmiana jest konieczna. Z tego względu RODO oraz inne właściwe akty prawa UE nie zostaną usunięte z tabeli otoczenia prawnego, ponieważ są istotne dla realizacji projektu i określają wymagania, które muszą zostać uwzględnione przy jego projektowaniu, wdrażaniu i eksploatacji. W tabeli pozostanie informacja, że projekt nie wymaga zmiany tych aktów prawnych. Oznacza to wyłącznie, że realizacja projektu nie powoduje potrzeby ich nowelizacji, a nie że akty te są nieistotne dla projektu. Projekt będzie realizowany zgodnie z wymaganiami wynikającymi z RODO oraz innych właściwych aktów prawa UE.