

Nazwa dokumentu: opisu założeń projektu informatycznego (dalej OZPI) „Zintegrowany Obszar Raportowania i Zarządzania ARiMR (ZORZA)” – wnioskodawca: Minister Rolnictwa i Rozwoju Wsi, beneficjent: Agencja Restrukturyzacji i Modernizacji Rolnictwa

| 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 | <p>Planowany projekt informatyczny wiąże się z zarządzaniem danymi. Z treści opisu można wywnioskować, że działania planowanego projektu informatycznego będą wiązać się z przetwarzaniem danych osobowych np. dotyczących użytkowników korzystających z dotychczas funkcjonujących systemów teleinformatycznych, które w założeniu mają zasilać nowy system ZORZA. Tytułem przykładu w pkt 7 „Architektura” ppkt 7.1. „Widok kooperacji aplikacji” w tabeli zawierającej Listę systemów wykorzystywanych w projekcie OZPI wiersz oznaczony:</p> <ul style="list-style-type: none"> - l.p. 13 dotyczący funkcjonującego Portalu Rolnika w opisie systemu pojawia się informacje takie jak np.: „główne funkcjonalności systemu to zarządzanie tożsamością i dostępem użytkowników”, „komunikacja – powiadomienia e-mail, SMS, Push”; - l.p. 18 w odniesieniu do istniejącego aktualnie Rejestru Podmiotów Wykluczonych (RPW), do którego dostęp mają pracownicy ARiMR w opisie systemu wskazuje się na to, że wyszukiwanie podmiotów w rejestrze odbywa się za pośrednictwem: nr identyfikacyjnego producenta, nr PESEL, nr REGON. | | |

| | | | | | |
|---|-------------|-------------------------------|--|--|--|
| | | | <p>Rekomendowanym jest, aby projektodawca:</p> <ul style="list-style-type: none"> - 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 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). <p>Przedmiotowy projekt informatyczny powinien zapewniać zachowanie poufności, integralności, kompletności oraz dostępności danych osobowych, które będą w nim przetwarzane.</p> | | |
| 2 | Prezes UODO | pkt 3. „Kamienie milowe” OZPI | <p>Takie planowane przez projektodawcę działanie należy ocenić pozytywnie. Wspominany inicjalny test prywatności powinien obejmować ocenę skutków dla ochrony danych osobowych (art. 35 rozporządzenia 2016/679). Dzięki jej przeprowadzeniu możliwym będzie:</p> <ul style="list-style-type: none"> 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 | | |

| | | | | | |
|---|-------------|---|--|--|--|
| | | | <p>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.</p> | | |
| 3 | Prezes UODO | <p>pkt 2 „Efekty projektu” ppkt 2.1. „Cele i korzyści wynikające z projektu” OZPI tabela Cel – 1, korzyści w związku z zapewnieniem mechanizmów zaawansowanej analityki predykcyjnej AI oraz uczenia maszynowego. W tym samym punkcie w ppkt 2.2. „Udostępnione e-usługi OZPI” w tabeli w l.p. 4 oraz w związku z pkt 7</p> | <p>Cel wykorzystania AI został wskazany przez projektodawcę, ale:</p> <ul style="list-style-type: none"> - 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 musi zadbać o doprecyzowanie kwestii planowanego wykorzystania wsparcia AI i jego ewentualnego wpływu na przetwarzanie danych osobowych. W tym celu powinien on – przy uwzględnieniu zasad przetwarzania danych osobowych, a zwłaszcza zasady zgodności z prawem, przejrzystości oraz rozliczalności (art. 5 rozporządzenia 2016/679) – w toku planowanego testu prywatności (o którym wspomina się w pkt. 3 „Kamienie milowe” drugi wiersz OZPI) pamiętać o konieczności uwzględnienia ochrony danych w fazie projektowania oraz domyślnej ochroną danych art. 25 rozporządzenia 2016/679). Stosownie nowoczesnych technologii (planowane wsparcie AI) i związane z tym przetwarzanie danych | | |

| | | | | | |
|---|-------------|---|--|--|--|
| | | <p>„Architektura” ppkt 7.1. Lista systemów wykorzystywanych w projekcie OZPI w tabeli w l.p. 1 oraz l.p. 13</p> | <p>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). W związku z planowanym wykorzystaniem 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 uniemożliwić 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.</p> | | |
| 4 | Prezes UODO | <p>pkt 4 „Koszty” ppkt. 4.2. „Wykaz</p> | <p>Na aprobatę zasługuje uwzględnienie przez projektodawców w pkt 4 „Koszty” ppkt. 4.2.</p> | | |

| | | | | | |
|---|-------------|--|--|--|--|
| | | poszczególnych pozycji kosztowych” OZPI nazwa pozycji kosztowej „Bezpieczeństwo” | „Wykaz poszczególnych pozycji kosztowych” OZPI nazwa pozycji kosztowej „Bezpieczeństwo” uzasadnienie tej pozycji, w tym kosztów audytów bezpieczeństwa, analizy statystycznej kodu, testów podatności systemu, badania zgodności systemu z obowiązującymi przepisami prawa, zakupu specjalistycznej infrastruktury i oprogramowania dedykowanych wyłącznie poprawie bezpieczeństwa przetwarzanych informacji. Problematyka bezpieczeństwa, w tym wspomniane testy są w kontekście art. 32 ¹ 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 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. | | |
| 5 | Prezes UODO | pkt. 5. „Główne ryzyka” 5.1. Ryzyka wpływające na realizację projektu | Z zadowoleniem należy przyjąć ryzyka wyodrębnione przez Wnioskodawcę - cyberataków naruszenia bezpieczeństwa danych, przewidując w ramach sposobów | | |

¹ 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.

| | | | | | |
|--|--|-----|--|--|--|
| | | OZP | <p>zarządzania z ryzykiem wyposażenie rozwiązania w zaawansowane mechanizmy bezpieczeństwa; wprowadzony zostanie również system backupów który umożliwi szybkie przywrócenie danych w przypadku incydentu;</p> <ul style="list-style-type: none">- odmienny zakres danych w poszczególnych systemach – przewidując w ramach sposobów zarządzania ryzykiem opracowanie przez Wykonawcę spójnego modelu danych; przygotowanie tabel mapowania i harmonizacji danych;- brak gotowości systemów zewnętrznych do integracji z systemem ZORZA - – przewidując w ramach sposobów zarządzania ryzykiem opracowanie i uzgodnienie harmonogramu integracji systemów; przygotowanie wymagań w zakresie integracji dal systemów, a także ścisłą współpracę z koordynatorami odpowiedzialnymi za wprowadzenie zmian w poszczególnych systemach. <p>Wnioskodawca powinien:</p> <ul style="list-style-type: none">- podjąć próbę zidentyfikowania ryzyk związanych z przetwarzaniem danych osobowych, jakie mogą pojawić się w związku z działaniem projektu informatycznego. <p>Kolejnym istotnym zagadnieniem jest planowana integracja 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 planowanie przepływu danych między nimi a nowym systemem</p> | | |
|--|--|-----|--|--|--|

| | | | | | |
|----|-------------|---|--|--|--|
| | | | <p>teleinformatycznym ZORZA (Lista przepływów). Rozwiązanie takie z pewnością będzie wpływało na powstawanie wielu ryzyk związanych z przetwarzaniem danych osobowych.</p> <ul style="list-style-type: none"> - w pierwszej kolejności istotne jest zapewnienie podstawy prawnej dla takich rozwiązań, zwłaszcza wobec treści aktualnych przepisów dot. przetwarzania danych osobowych w rejestrach i systemach – czy regulacje prawne są w tym zakresie wystarczające i zupełne? - ryzyka dotyczą także obszarów takich jak: nieuprawniony dostęp, wyciek lub nieuprawniona modyfikacja danych – czy wystarczająca są identyfikacja i zapewnienie środków technicznych i organizacyjnych jakie będą wdrożone w celu ich skutecznego ograniczenia lub minimalizacji ich potencjalnych skutków? | | |
| 6. | Prezes UODO | pkt 6 „Otoczenie prawne” (tabela) ppkt 8 OZPI | <p>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. 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</p> | | |

| | | | | | |
|--|--|--|--|--|--|
| | | | bardziej wskazaniu aktów na których treść wprowadzenie (i wdrożenie) projektu informatycznego będzie realnie oddziaływało. | | |
|--|--|--|--|--|--|