

Nazwa dokumentu: opis założeń projektu informatycznego pn.: Zintegrowany Obszar Raportowania i Zarządzania ARiMR (ZORZA) – wnioskodawca: Minister Rolnictwa i Rozwoju Wsi, beneficjent: Agencja Restrukturyzacji i Modernizacji Rolnictwa.

L p.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
1.	MC	Pkt. 5. Główne ryzyka.	W pkt. 5. Główne ryzyka, brakuje wskazanych ryzyk związanych z bezpieczeństwem danych mimo, że z samego projektu wynika, że projekt może mieć wpływ na to bezpieczeństwo i podatności związane z projektowanym systemem. Cyberataki i podatności dotyczących bezpieczeństwa dla powstającego systemu, wykorzystanie AI – mają wpływ na bezpieczeństwo danych w systemie, osób których te dane dotyczą. W ocenie MC konieczne jest wdrożenie procesu zarządzania ryzykami związanymi z bezpieczeństwem danych osobowych np. stosowanie zasady privacy by design na każdym etapie projektu, zaangażowanie w prace nad projektem IOD, identyfikowanie podatności dot. bezpieczeństwa dla systemu oraz prowadzenie regularnych audytów/testów bezpieczeństwa na co projekt wskazuje, że będą przeprowadzane. Kwestie dotyczące identyfikowanych ryzyk związanych z bezpieczeństwem danych powinny znaleźć odzwierciedlenie w pkt. 5.1 i 5.2 opisu założeń projektowych.		<p>W pkt. 5.1 Uzupelniono sposób zarządzania ryzykiem nr. 3 „Cyberataki i naruszenia bezpieczeństwa danych” - „Rozwiązanie zostanie wyposażone w zaawansowane mechanizmy bezpieczeństwa. Wprowadzony zostanie również system backupów, który umożliwi szybkie przywrócenie danych w przypadku incydentu.</p> <p><u>Wdrożenie procesu zarządzania ryzykami związanymi z bezpieczeństwem danych osobowych poprzez stosowanie zasady privacy by design na każdym etapie projektu, zaangażowanie w prace nad projektem IOD, identyfikowanie podatności dot. bezpieczeństwa dla systemu oraz przeprowadzenie testów bezpieczeństwa.”</u></p> <p>Jednocześnie wyjaśniamy, że ARiMR posiada uregulowania wewnętrzne, wynikające z przepisów prawa, w zakresie ochrony i bezpieczeństwa danych, w tym w szczególnym zakresie bezpieczeństwa danych osobowych a także zarządzania ryzykami związanymi z bezpieczeństwem danych. Mechanizmy wynikające z wewnętrznych regulaminów/polityk, stosowane są w ramach budowy i rozwoju systemów teleinformatycznych.</p>
1	MRPiPS	1.1. Identyfikacja problemów i potrzeb	Wymieniono szerokie grupy docelowe: rolników, rybaków (1 270 000 osób), doradców, a także urzędników. W diagnozie problemów nie uwzględniono specyficznych barier, z jakimi mierzą się	Dodanie do grupy docelowej rolników z niepełnosprawnościami oraz	Wyjaśnienia wymaga wskazanie, iż projekt ZORZA jest projektem typu back-office, którego głównym celem jest optymalizacja procesów związanych z analizą danych, przygotowaniem raportów, sprawozdań i prognoz. Jednocześnie, jedna z e-usług kierowana jest do szerokiego

			<p>starsi rolnicy oraz rolnicy z niepełnosprawnościami (np. problemy ze wzrokiem, dysfunkcje ruchowe rąk, wykluczenie cyfrowe) podczas korzystania z e-usług rolniczych. Brak ujęcia perspektywy osób z niepełnosprawnościami na etapie koncepcyjnym może skutkować pominięciem ułatwień dostępu na etapie projektowania interfejsów oraz brakiem dostępu poprzez brak możliwości skorzystania z narzędzi asystujących.</p>	<p>starszych rolników.</p>	<p>grona użytkowników: „Tworzenie raportów umożliwia dostęp do predefiniowanych raportów, generowanie raportów na żądanie z możliwością ich parametryzacji oraz automatyczne tworzenie cyklicznych sprawozdań zgodnych z wymaganiami”.</p> <p>Należy przy tym podkreślić, iż użytkownikami systemu i poszczególnych e-usług będą odpowiednio przedstawiciele wskazanych grup interesariuszy, którzy nie są różnicowani pod względem żadnej z przesłanek dyskryminujących (zgodnie z definicją zawartą w Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021-2027), co oznacza, że identyfikacja problemów i potrzeb, odnosi się do każdego użytkownika, w tym również do rolników i rybaków z niepełnosprawnościami. Szczególne potrzeby użytkowników z niepełnosprawnościami czy osób starszych będą stanowiły ważny obszar prac w zakresie przygotowania i wdrożenia e-usługi.</p> <p>Zgodnie z wykazem poszczególnych pozycji kosztowych (pkt. 4.2) pod poz. „Koszty UX i grafiki” zaplanowano w projekcie „Koszty testowania rozwiązań wśród docelowych użytkowników oraz przeprowadzenia testów WCAG dostarczonych rozwiązań”. Prace w tym zakresie będą realizowane począwszy od etapu analizy aż do testowania i wdrożenia systemu i e-usług. Udział użytkowników w tym procesie pozwoli na zaprojektowanie i wdrożenie rozwiązania dostosowanego do rzeczywistych preferencji osób z niepełnosprawnościami i osób starszych, natomiast ostatecznym potwierdzeniem spełnienia wymagań w zakresie dostępności będą testy UX, w tym potwierdzenie wymagań WCAG.</p> <p>Wobec powyższego nie dokonano zmian w OZPI.</p>
2	MRPiPS	2.1. Cele i korzyści wynikające z projektu	<p>Brak wskaźników jakościowych, w tym mierników dostępności i użyteczności platformy. Brak formalnego pomiaru dostępności, w tym testowania systemu pod kątem potrzeb osób korzystających z asystujących technologii (np. czytniki ekranu) może spowodować brak dostępności platformy.</p>	<p>Zgodnie z uwagą RA IT prośba o korektę założeń.</p>	<p>Wyjaśnienia wymaga wskazanie, iż projekt ZORZA jest projektem typu back-office, którego celem jest optymalizacja procesów związanych z analizą danych, przygotowaniem raportów, sprawozdań i prognoz.</p> <p>Jednocześnie, jedna z e-usług kierowana jest do szerokiego grona użytkowników: „Tworzenie raportów umożliwia dostęp do predefiniowanych raportów, generowanie raportów na żądanie z możliwością ich parametryzacji oraz automatyczne tworzenie cyklicznych</p>

					<p> sprawozdań zgodnych z wymaganiami”.</p> <p>Zgodnie z wykazem poszczególnych pozycji kosztowych (pkt. 4.2) zaplanowano w projekcie realizację testowania rozwiązań wśród docelowych użytkowników oraz przeprowadzenia testów UX, w tym potwierdzenie spełnienia wytycznych WCAG dostarczonych rozwiązań.</p> <p>Jednocześnie zgodnie z tabelą kamieni milowych (pkt. 3) zaplanowano testy badań UX, dla których zgodnie z tabelą produktów (pkt. 2.4) powstanie Raport z testów UX. Testy UX z uwzględnieniem testowania dostępności projektowanych rozwiązań, realizowane będą na podstawie Ustawy o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych, w której zgodnie z załącznikiem „Wytyczne dla dostępności treści internetowych stosowane do stron internetowych i aplikacji mobilnych w zakresie dostępności dla osób niepełnosprawnych” określone zostały kryteria sukcesu dla poszczególnych wytycznych, które z zasady stanowią mierniki dostępności i użyteczności platformy. Wobec powyższego nie dokonano zmian w OZPI.</p>
3	MRPiPS	7.1. Widok kooperacji aplikacji, Lista systemów wykorzystywanych w projekcie, Opis systemu „Portal Rolnika” (lp.13)	Brak zdefiniowanej roli „Wirtualnego Asystenta – asystenta AI” funkcjonującego w ramach modyfikowanego Portalu Rolnika. Asystenci oparci na AI (chatboty/voiceboty) często stanowią poważną barierę – bywają niedostępni dla czytelników ekranu, nie obsługują komend głosowych w sposób przewidywalny lub generują odpowiedzi trudne do zrozumienia dla osób z niepełnosprawnością intelektualną lub poznawczą.	Doprecyzowanie roli asystenta i zapewnienie alternatywnego dostępu dla osób korzystających z narzędzi asystujących.	<p>Portal Rolnika posiada dwie role w systemie ZORZA:</p> <ul style="list-style-type: none"> • przekazywanie danych do systemu ZORZA ze złożonych wniosków oraz danych o zarejestrowanych użytkownikach w celach raportowych i statystycznych • prezentacja zagregowanych danych statystycznych oraz raportów w Portalu Rolnika <p>Wirtualny Asystent (asystent AI) realizowany w systemie Portal Rolnika nie wpływa na zdefiniowaną rolę funkcjonalną Portalu Rolnika w systemie ZORZA oraz nie wpływa na funkcje automatyzacji procesów raportowania i analizy danych w systemie ZORZA, wykorzystujące technologie AI. Są to dwa odrębne rozwiązania.</p> <p>Wirtualny Asystent (asystent AI) Portalu Rolnika nie wpływa na usługi i funkcjonalności systemu ZORZA i pozostaje poza zakresem realizacji projektu ZORZA.</p> <p>Jednocześnie podkreślenia wymaga, iż projekt ZORZA jest projektem typu back-office, którego celem jest optymalizacja</p>

					procesów związanych z analizą danych, przygotowaniem raportów, sprawozdań i prognoz. W związku z tym technologie AI będą wykorzystywane w systemie ZORZA do automatyzacji procesów raportowania i analizy danych.
4	MRPiPS	4.2. Wykaz poszczególnych pozycji kosztowych	W budżecie projektu przewidziano pozycję „Koszty UX i grafiki”, która ma obejmować testy WCAG. Opis wskazuje głównie na przygotowanie „koncepcji wizualnej oraz makiet interfejsu”. Bez wymogu zaangażowania ekspertów od dostępności z certyfikatami oraz realnego udziału rolników z niepełnosprawnościami w testach UX, kontrola ta może mieć jedynie charakter formalny (automatyczne sprawdzanie kodu).	Dodanie wymogu zaangażowania ekspertów od dostępności z certyfikatami oraz udziału rolników z niepełnosprawnościami w testach UX.	<p>Zgodnie z wykazem poszczególnych pozycji kosztowych (pkt. 4.2) pod poz. „Koszty UX i grafiki” zaplanowano w projekcie „Koszty testowania rozwiązań wśród docelowych użytkowników oraz przeprowadzenia testów WCAG dostarczonych rozwiązań”.</p> <p>Użytkownikami systemu i poszczególnych e-usług będą odpowiednio przedstawiciele wskazanych grup interesariuszy, którzy nie są różnicowani pod względem żadnej z przesłanek dyskryminujących (zgodnie z definicją zawartą w Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021-2027), co oznacza, że testowanie rozwiązań wśród docelowych użytkowników, odnosi się do każdego użytkownika, w tym również do rolników i rybaków z niepełnosprawnościami.</p> <p>Istotą testów WCAG, zaplanowanych zgodnie z poz. „Koszty UX i grafiki”, jest potwierdzenie spełnienia kryteriów sukcesu dla poszczególnych wytycznych zgodnie z załącznikiem „Wytyczne dla dostępności treści internetowych stosowane do stron internetowych i aplikacji mobilnych w zakresie dostępności dla osób niepełnosprawnych” do Ustawy o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.</p> <p>Powodzenie testów UX, w tym potwierdzenie spełnienia wymogów WCAG jest wprost uzależnione od zapewnienia analizy potrzeb i zaprojektowania rozwiązań oraz ich przygotowania przez specjalistów, którzy posiadają praktyczną wiedzę i wieloletnie doświadczenie w zakresie dostępności cyfrowej oraz w pracy z użytkownikami. Udział specjalistów ds. dostępności cyfrowej zostanie zatem zapewniony na każdym etapie projektu, od analizy potrzeb po testowanie i wdrażanie rozwiązań.</p> <p>Udział użytkowników w tym procesie pozwoli na zaprojektowanie i wdrożenie rozwiązania dostosowanego do rzeczywistych preferencji osób z niepełnosprawnościami, natomiast ostatecznym potwierdzeniem spełnienia wymagań w zakresie dostępności będą testy UX, w tym potwierdzenie</p>

					wymagań WCAG. Jednocześnie w OZPI uzupełniono uzasadnienie o zapisy wskazane w kolumnie drugiej pod nazwą "Nazwa pozycji kosztowej"
1	Prezes UODO	pkt 1. „Powody podjęcia projektu” w ppkt 1. „Identyfikacja problemu i potrzeb” OZPI	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: 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. Rekomendowanym jest, aby projektodawca: na jak najwcześniejszym etapie dokonał		W pkt. 5.1 OZPI „Ryzyka wpływające na realizację projektu” uzupełniono sposób zarządzania ryzykiem nr. 3 „Cyberataki i naruszenia bezpieczeństwa danych” - „Rozwiązanie zostanie wyposażone w zaawansowane mechanizmy bezpieczeństwa. Wprowadzony zostanie również system backupów, który umożliwi szybkie przywrócenie danych w przypadku incydentu. <u>Wdrożenie procesu zarządzania ryzykami związanymi z bezpieczeństwem danych osobowych poprzez stosowanie zasady privacy by design na każdym etapie projektu, zaangażowanie w prace nad projektem IOD, identyfikowanie podatności dot. bezpieczeństwa dla systemu oraz przeprowadzenie testów bezpieczeństwa.</u> ” Jednocześnie, zgodnie z OZPI, w projekcie zostanie przeprowadzony inicjalny test prywatności, w ramach którego na wczesnym etapie projektu zostanie wykonana analiza w celu określenia jakie kategorie danych osobowych, w jakim zakresie będą przetwarzane, podstawy prawne przetwarzania, na których to przetwarzanie będzie oparte, określony zostanie „cykl życia” danych osobowych jakie mają być przetwarzane przy wykorzystaniu systemu ZORZA (od momentu ich pozyskania do ich usunięcia), role i obowiązki (w tym też te z obszaru ochrony danych osobowych) poszczególnych podmiotów, które będą miały realny dostęp do danych znajdujących się w systemie ZORZA. Jednocześnie wyjaśniamy, że ARiMR posiada uregulowania wewnętrzne, wynikające z przepisów prawa, w zakresie ochrony i bezpieczeństwa danych, w tym w szczególnym zakresie bezpieczeństwa danych osobowych a także zarządzania ryzykami związanymi z bezpieczeństwem danych. Mechanizmy wynikające z wewnętrznych regulaminów/polityk, stosowane są w ramach budowy i rozwoju systemów teleinformatycznych.

			<p>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). 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: 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-</p>		<p>W ramach projektu nie będą przetwarzane dane osobowe szczególnej kategorii (np. dane o niepełnosprawności). Niemniej jednak, zgodnie z OZPI, w projekcie zostanie przeprowadzony inicjalny test prywatności, w ramach którego na wczesnym etapie projektu zostanie wykonana analiza w celu określenia jakie kategorie danych osobowych, w jakim zakresie będą przetwarzane, podstawy prawne przetwarzania, na których to przetwarzanie będzie oparte, określony zostanie „cykl życia” danych osobowych jakie mają być przetwarzane przy wykorzystaniu systemu ZORZA (od momentu ich pozyskania do ich usunięcia), role i obowiązki (w tym też te z obszaru ochrony danych osobowych) poszczególnych podmiotów, które będą miały realny dostęp do danych znajdujących się w systemie ZORZA.</p>

			<p>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 spośród 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 „Architektura” ppkt 7.1. Lista systemów wykorzystywanych</p>	<p>Cel wykorzystania AI został wskazany 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 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</p>		<p>Projekt ZORZA jest projektem typu back-office, którego celem jest optymalizacja procesów związanych z analizą danych, przygotowaniem raportów, sprawozdań i prognoz. Technologie AI będą wykorzystywane w systemie ZORZA do automatyzacji procesów raportowania i analizy danych.</p> <p>Zgodnie z OZPI, w projekcie zostanie przeprowadzony inicjalny test prywatności, w ramach którego na wczesnym etapie projektu zostanie wykonana analiza w celu określenia m.in. jakie kategorie danych osobowych, w jakim zakresie będą przetwarzane, podstawy prawne przetwarzania, na których to przetwarzanie będzie oparte, określony zostanie „cykl życia” danych osobowych jakie mają być przetwarzane przy wykorzystaniu systemu ZORZA (od momentu ich pozyskania do ich usunięcia), role i obowiązki (w tym też te z obszaru ochrony danych osobowych) poszczególnych podmiotów, które będą miały realny dostęp do danych znajdujących się w systemie ZORZA.</p> <p>W ramach analizy zostaną wykorzystane wytyczne i akty prawne, które dotyczą wykorzystania AI w zakresie planowanym do realizacji w projekcie.</p>

	<p>w projekcie OZPI w tabeli w l.p. 1 oraz l.p. 13</p>	<p>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 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</p>		
--	--	--	--	--

			<p>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.</p>		
4	Prezes UODO	<p>pkt 4 „Koszty” ppkt. 4.2. „Wykaz poszczególnych pozycji kosztowych” OZPI nazwa pozycji kosztowej „Bezpieczeństwo”</p>	<p>Na aprobatę zasługuje uwzględnienie przez projektodawców w pkt 4 „Koszty” ppkt. 4.2. „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</p>		<p>Wyjaśniamy, że ARiMR posiada uregulowania wewnętrzne, wynikające z przepisów prawa, w zakresie ochrony i bezpieczeństwa danych, w tym w szczególnym zakresie bezpieczeństwa danych osobowych a także zarządzania ryzykami związanymi z bezpieczeństwem danych. ARiMR posiada Politykę bezpieczeństwa informacji określającą m.in. Regulamin ochrony danych osobowych uwzględniający przepisy prawa krajowego i UE. Dokumenty te wskazują działania do realizacji w ramach budowy i rozwoju systemów teleinformatycznych.</p>

			<p>informacji. Problematyka bezpieczeństwa, w tym wspomniane testy są w kontekście art. 321 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.</p>		
5	Prezes UODO	pkt. 5. „Główne ryzyka” 5.1. Ryzyka wpływające na realizację projektu OZP	<p>Z zadowoleniem należy przyjąć ryzyka wyodrębnione przez Wnioskodawcę - cyberataków naruszenia bezpieczeństwa danych, przewidując w ramach sposobów zarządzania z ryzykiem wyposażenie rozwiązania w zaawansowane mechanizmy bezpieczeństwa; wprowadzony zostanie również system backupów który umożliwi szybkie przywrócenie danych w przypadku incydentu; odmienny zakres danych w poszczególnych systemach – przewidując w ramach sposobów</p>		<p>Wyjaśniamy, że projekt ZORZA jest projektem typu back-office, którego celem jest optymalizacja procesów związanych z analizą danych, przygotowaniem raportów, sprawozdań i prognoz. ARiMR posiada uregulowania wewnętrzne, wynikające z przepisów prawa, w zakresie ochrony i bezpieczeństwa danych, w tym w szczególnym zakresie bezpieczeństwa danych osobowych a także zarządzania ryzykami związanymi z bezpieczeństwem danych. ARiMR posiada Politykę bezpieczeństwa informacji określającą m.in. Regulamin ochrony danych osobowych, Regulamin zarządzania ryzykiem, Regulamin rozwoju aplikacji (w aspekcie bezpieczeństwa informacji) uwzględniające przepisy prawa krajowego i UE w zakresie bezpieczeństwa i zarządzania ryzykiem. Dokumenty te wskazują działania do realizacji w ramach budowy i rozwoju systemów teleinformatycznych.</p>

		<p>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. Wnioskodawca powinien: podjąć próbę zidentyfikowania ryzyk związanych z przetwarzaniem danych osobowych, jakie mogą pojawić się w związku z działaniem projektu informatycznego. 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 teleinformatycznym ZORZA (Lista przepływów). Rozwiązanie takie z pewnością będzie wpływało na</p>	<p>Jednocześnie w pkt. 5.1 Uzupelniono sposób zarządzania ryzykiem nr. 3 „Cyberataki i naruszenia bezpieczeństwa danych” - „Rozwiązanie zostanie wyposażone w zaawansowane mechanizmy bezpieczeństwa. Wprowadzony zostanie również system backupów, który umożliwi szybkie przywrócenie danych w przypadku incydentu. <u>Wdrożenie procesu zarządzania ryzykami związanymi z bezpieczeństwem danych osobowych poprzez stosowanie zasady privacy by design na każdym etapie projektu, zaangażowanie w prace nad projektem IOD, identyfikowanie podatności dot. bezpieczeństwa dla systemu oraz przeprowadzenie testów bezpieczeństwa.</u>”</p>
--	--	--	---

			<p>powstawanie wielu ryzyk związanych z przetwarzaniem danych osobowych.</p> <p>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?</p> <p>ryzyka dotyczą także obszarów takich jak: nieuprawniony dostęp, wyciek lub nieuprawniona modyfikacja danych – czy wystarczająco są identyfikacja i zapewnienie środków technicznych i organizacyjnych jakie będą wdrożone w celu ich skutecznego ograniczenia lub minimalizacji ich potencjalnych skutków?</p>		
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. 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</p>		<p>Usunięto pozycję z aktem prawnym: “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)”</p>

			<p>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.</p>		
--	--	--	--	--	--