|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ***Nazwa dokumentu:*** *opis założeń projektu informatycznego pn.:* ***e-Sanepid*** *– wnioskodawca Minister Zdrowia, beneficjent Główny Inspektorat Sanitarny.* | | | | | |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
| **1** | **MC** | Uwaga ogólna | W wierszu „Źródło finansowania” należy podać:  1. środki programu Fundusze Europejskie na Rozwój Cyfrowy  2021-2027, Działanie FERC.02.01 Wysoka jakość i dostępność e-usług publicznych  2. środki budżetu państwa - **cz. 83 poz. 98.**  Wyjaśnienie: zgodnie z wytycznymi MFiPR, dotyczącymi prac planistycznych do ustawy budżetowej na 2026 r. i na lata 2027-2029, CPPC ujmuje w drukach planistycznych środki na nabory dla projektów planowanych do realizacji m.in. dla PJB, które docelowo będą finansowane z właściwych im części budżetowych. Środki te będą ujęte w rezerwie celowej i będą uruchamiane przez MFiPR do części właściwych dysponentów po rozstrzygnięciu naborów. | Proszę o analizę i ew. korektę opisu założeń. |  |
| **2** | **MC** | 5.1. Ryzyka wpływające na realizację projektu | W ryzykach należy dodać ryzyko wpływu rozwiązania na prywatność osób (test prywatności), poprzez dodanie w 5.1. w tabeli: nazwy ryzyka - Brak zapewnienia zgodności przetwarzania danych osobowych z obowiązującymi regulacjami; Siła oddziaływania- Duża; Prawdopodobieństwo wystąpienia ryzyka - (powinien to określić samodzielnie projektodawca); Sposób zarządzania ryzykiem - Konieczne stosowanie zasady privacy by design na każdym etapie projektu oraz przeprowadzenie oceny skutków dla ochrony danych osobowych dla całego e-Sanepid. | Proszę o analizę i korektę opisu założeń. |  |
| **3** | **MC** | 7.1. Widok kooperacji aplikacji | W „Liście przepływów” wskazano przepływ z systemu SRP do systemu SEPIS, tymczasem na grafice widoku kooperacji nie ma takiego przepływu. Przepływ ten wydaje się być nadmiarowy. | Proszę o analizę i korektę opisu założeń. |  |
| **4** | **MC** | 7.1. Widok kooperacji aplikacji | W liście przepływów projektodawca w pkt. 7.1. wskazał rejestr PESEL oraz RDK jako krytyczne dla sukcesu projektu. Brak jednak określenia precyzyjnego katalogu danych osobowych jakie z rejestru PESEL będą konieczne i wykorzystywane dla tego projektu. Projektodawca wskazał na ogólne określenie: „dane osoby fizycznej” z tego rejestru. Wobec tego przewiduje również dostęp do pełnych danych zgromadzonych w tym rejestrze. Rejestr PESEL zawiera bardzo bogaty zasób danych osobowych, których pozyskiwanie do tego rozwiązania technologicznego niekoniecznie będzie potrzebne. Wobec tego projekt nie powinien zakładać pełnej dostępności lecz tylko dostępność do wybranych, precyzyjnie określonych, ograniczonych do niezbędnego minimum, danych osobowych z rejestrów PESEL i RDK, tj. tylko takich które są niezbędne dla realizacji konkretnych celów projektu (celów ich przetwarzania), w myśl zasady minimalizacji danych oraz zasady ograniczenia celu z art. 5 ust. 1 lit. b i c RODO. Z uwagi na rodzaj, charakter, zakres, kontekst i cele projektowanego przetwarzania danych osobowych, na masową skalę, które z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, należy dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o której mowa w art. 35 RODO. M. in. dla prawidłowego określenia niezbędnego katalogu danych osobowych przetwarzanych w projektowanym e-Sanepid względem jego celów, należy przeprowadzić tę ocenę skutków, zaś jej przeprowadzenie powinno zostać przewidziane i umieszczone w ramach przedstawionego projektu opisu założeń. Dopiero pozytywne wyniki takiej oceny, zawierające co najmniej elementy z art. 35 ust. 7 RODO, powinny determinować zakres niezbędnych i dopuszczalnych kategorii danych osobowych, pozyskiwanych z poszczególnych dla e-Sanepid rejestrów. Stosownie do art. 25 RODO należy także zapewnić uwzględnianie ochrony danych osobowych w fazie projektowania dla każdego rozwiązania/etapu w ramach całego systemu e-Sanepid oraz stosować zasadę domyślnej ochrony danych dla kolejnych przyjmowanych rozwiązań w ramach tego systemu. | Proszę o analizę i korektę opisu założeń. |  |
| **5** | **MC** | 7.5. Bezpieczeństwo | W zakresie pkt 7.5. nie powinno się wykreślać tiret dot. dodatkowych zabezpieczeń powyżej wymogów KRI i proponuje uzupełnić odpowiednio uzasadnienie: Bezpieczeństwo i ochrona danych osobowych zostanie zapewnione w modelu trójwarstwowym – na poziomie organizacji, procesów oraz w warstwie technicznej. Zapewnienie bezpieczeństwa obejmie obszary: integralności, poufności oraz dostępności danych oraz całego systemu. Dla bezpieczeństwa systemu w warstwie organizacyjnej zostały ustalone precyzyjnie role i odpowiedzialności. Role w zakresie bezpieczeństwa dotyczą każdej z grup użytkowników systemu. Na poziomie procesów bezpieczeństwo i ochrona danych osobowych zapewnione jest poprzez określenie spójnych procedur dla takich procesów jak: proces zarządzania zmianami, proces zarządzania uprawnieniami, proces monitorowania bezpieczeństwa, proces zarządzania ciągłością działania. Zasadnym jest także aby projektodawca wskazał informacje czy zgodność z wymaganiami w zakresie bezpieczeństwa przetwarzania danych zweryfikowane zostały w ramach audytu bezpieczeństwa dla tego systemu. Czy w ramach audytu wykonane zostały dodatkowo testy bezpieczeństwa (w tym testy penetracyjne itd.). Dodatkowo czy produktem końcowym testów bezpieczeństwa będzie protokół zaleceń, które będą obligatoryjnie wdrożone. | Proszę o analizę i korektę opisu założeń. |  |