| ***Nazwa dokumentu:***  *opis założeń projektu informatycznego:* [***Rozbudowa systemu zarządzania infrastrukturą teleinformatyczną statystyki publicznej i cyberbezpieczeństwa (CyberStat)***](https://www.gov.pl/web/krmc/rozbudowa-systemu-zarzadzania-infrastruktura-teleinformatyczna-statystyki-publicznej-i-cyberbezpieczenstwa-cyberstat) ***– wnioskodawca: Kancelaria Prezesa Rady Ministrów, beneficjent: Główny Urząd Statystyczny.*** | | | | | |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Organ wnoszący uwagi** | **Jednostka redakcyjna, do której wnoszone są uwagi** | **Treść uwagi** | **Propozycja zmian zapisu** | **Odniesienie do uwagi** |
| **1** | **MSWiA** | 4.2. Wykaz poszczególnych pozycji kosztowych, wiersz: Bezpieczeństwo;  kolumna: Uzasadnienie pozycji  kosztowej (przeznaczenie) | Po zdaniu „*Środki umożliwią zapewnienie*  *optymalnych i bezpiecznych rozwiązań. Zostaną*  *przeznaczone m.in. na przeprowadzenie testów*  *bezpieczeństwa niezbędnych do uruchomienia produkcyjnego rozwiązań dostarczonych w*  *ramach realizacji przedsięwzięcia.*” proponuje się dodać dodatkowe wymaganie dotyczące testów bezpieczeństwa opisane w sąsiedniej kolumnie. Wymaganie to powinno być także wskazane w dokumentach OPZ/umowach z wykonawcami. | Testy bezpieczeństwa przeprowadzi niezależny podmiot zewnętrzny, dysponujący kadrą specjalistów posiadających praktyczne umiejętności i doświadczenie w prowadzeniu testów penetracyjnych oraz co najmniej jeden z certyfikatów wymienionych w rozporządzeniu Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz.U. poz. 131). | Uwaga przyjęta, dokonano modyfikacji opisu założeń projektu informatycznego (zwanego dalej „**OZPI**”) dla projektu CyberStat, gdzie doprecyzowano, że testy bezpieczeństwa zostaną przeprowadzenie przez posiadający odpowiednie kompetencje, niezależny podmiot zewnętrzny. |
| **2** | **UODO** |  | Ze względu na wskazane w projekcie przetwarzanie danych osobowych na  szeroką skalę, za niezbędne należy uznać przeprowadzenie **testu prywatności**  (obejmującego m.in. ocenę skutków dla ochrony danych), odpowiadającego wymogom art. 25 ust. 1 i art. 35 (w szczególności ust. 1 oraz ust. 10) rozporządzenia 2016/679. We wskazanych w piśmie pkt 2.4 – „Produkty końcowe projektu” i pkt 3 – „Kamienie milowe” mowa jest jedynie m. in. o pozytywnych raportach z testów bezpieczeństwa i wydajności oraz o uzyskanych pozytywnych wynikach testów bezpieczeństwa i wydajności. Należy zauważyć, że zgodnie z przepisami rozporządzenia 2016/679 ocena skutków dla ochrony danych powinna być przeprowadzana nie tylko przed rozpoczęciem przetwarzania, ale i wtedy, gdy zmienia się ryzyko wynikające z operacji przetwarzania. Zasadne jest zatem – również w nawiązaniu do ustaleń zawartych w piśmie Pani Sekretarz z 31 stycznia br. – włączenie testu prywatności (obejmującego m.in. ocenę skutków dla ochrony danych), jako kluczowego dla oceny przetwarzania danych osobowych, do opisu założeń, w następujących punktach: pkt 2.4 - Produkty końcowe projektu; pkt 3 – Kamienie milowe; pkt 4.2 - Wykaz poszczególnych pozycji kosztowych; pkt 6 – Otoczenie prawne (w zakresie aktów prawnych umożliwiających przetwarzanie  danych). Odpowiednio przeprowadzona analiza powinna pomóc zdiagnozować ryzyka dla praw i wolności podmiotów danych wynikające z przyjmowanych rozwiązań i pozwolić na wypracowanie konkretnych środków zaradczych oraz techniczno-organizacyjnych minimalizując w ten sposób zidentyfikowane zagrożenie. Nie można również pominąć aspektu otoczenia prawnego. Odpowiednio przeprowadzona analiza obowiązujących aktów prawa w przedmiotowym zakresie pozwoli na określenie podstawy prawnej dla każdego z realizowanych procesów związanych z przetwarzaniem danych osobowych. Przez wzgląd na normę zawartą w art. 6 ust. 3 lit b rozporządzenia 2016/679 – dla każdego procesu przetwarzania danych osobowych musi istnieć odpowiednia podstawa prawna, określona w prawie państwa członkowskiego. |  | Usprawnienia wdrażane w ramach projektu informatycznego przyczynią się do zwiększenia bezpieczeństwa danych osobowych przetwarzanych w statystyce publicznej. Ponieważ projekt nie jest ukierunkowany na przetwarzanie danych osobowych, Wnioskodawca nie widzi potrzeby uwzględniania działań związanych z oceną prywatności w OZPI. Niemniej jednak, wszystkie działania będą realizowane zgodnie z wymogami RODO, w szczególności art. 25 ust. 1 oraz art. 35, zapewniając pełną zgodność z obowiązującymi regulacjami ochrony danych osobowych. Odpowiednie analizy zostaną przeprowadzone na możliwie najwcześniejszym etapie projektu, co umożliwi identyfikację zagrożeń dla prywatności oraz opracowanie odpowiednich rozwiązań organizacyjnych i technicznych w celu ich minimalizacji. |
| **3** | **MRiT** | 6. OTOCZENIE PRAWNE  7.5.Bezpieczeństwo | 1. W punkcie 6 OZPI - Otoczenie prawne - przytoczono błędne nazwy, daty wydania lub publikatory aktów prawa. Uwaga odnosi się do podpunktów (l.P.) 1, 5, 6, 8, 9, 16, 17 poza tym należy ujednolicić sposób przywoływania aktów normatywnych - albo z publikatorami albo bez nich, i tak:  1) publikator - jest: (Dz. U. z 2024 poz.17799) powinno być: (Dz. U. z 2024 poz.1799)  5) publikator - jest: (Dz.U. 2018 r. poz. 1560, z późn. zm.) powinno być: (Dz.U. z 2024 r. poz. 1077)  6) powinna być pełna nazwa rozporządzenia, a nie tylko skrót RODO, który w dalszej części nie jest przywoływany  8) brak pełnej nazwy rozporządzenia  9) brak pełnej nazwy rozporządzenia, a ta przywołana jest nieprawidłowa - jest: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1058 z dnia 24 czerwca 2021 r. ustanawiające wspólne przepisy dotyczące funduszy europejskich, powinno być: (...) w sprawie Europejskiego Funduszu Rozwoju Regionalnego i Funduszu Spójności  16) błędna data wydania - jest: Ustawa z dnia 21 listopada 2024 r. o doręczeniach elektronicznych powinna być: Ustawa z dnia 18 listopada 2024 r. (...)  17) jest: Rozporządzenie Ministra Cyfryzacji z dnia 16 czerwca 2021 r. w sprawie profilu zaufanego i podpisu zaufanego, tymczasem wskazana data wydania dotyczy: Rozporządzenia Ministra Cyfryzacji zmieniającego rozporządzenie w sprawie profilu zaufanego i podpisu zaufanego. Prawidłowa nazwa: Rozporządzenie Ministra Cyfryzacji z dnia 20 czerwca 2020 r. w sprawie profilu zaufanego i podpisu zaufanego (tj.Dz.U. z 2023 r. poz. 2551).  2. W pkt 7.5 jest przywołane nieaktualne rozporządzenie KRI. |  | W przypadku sekcji 6 OTOCZENIE PRAWNE - uwaga przyjęta, dokonano modyfikacji OZPI.  W przypadku sekcji 7.5.Bezpieczeństwo – wyjaśnienie przedstawiono poniżej.  OZPI zostało przygotowane przy pomocy generatora udostępnionego przez KRMC pod adresem: <https://www.gov.pl/web/krmc/formularz#/>  Aby wskazany przez MRiT błąd nie występował w OZPI wymagana jest korekta generatora przez KRMC. |