

Stanowisko SPOIWO nt konkursu na pilotażowe wdrożenia open source

Warszawa, 22.06.2026

SPOIWO (Sojusz Przyjaciół Otwartego i Wolnego Oprogramowania) to oddolna koalicja ekspertów, organizacji obywatelskich, środowisk naukowych oraz przedstawicieli polskiej branży IT. Naszym nadrzędnym celem jest działanie na rzecz cyfrowej suwerenności państwa poprzez powszechne wdrażanie otwartego i wolnego oprogramowania, przeciwdziałanie uzależnieniu technologicznemu oraz promowanie najwyższych standardów cyberbezpieczeństwa w administracji publicznej.

Niniejszy dokument stanowi oficjalne stanowisko Sojuszu SPOIWO, wypracowane w ramach otwartych konsultacji założeń konkursu na pilotażowe wdrożenie oprogramowania open source w jednostkach samorządu terytorialnego (JST), prowadzonych przez Ministerstwo Cyfryzacji.

Rekomendacje przedstawione w tym dokumencie cieszą się oficjalnym poparciem następujących organizacji oraz podmiotów zrzeszonych w ramach Sojuszu Przyjaciół Otwartego i Wolnego Oprogramowania (w kolejności alfabetycznej):

Centrum Cyfrowe, Fundacja Internet. Czas Działać!, Fundacja Moje Podlasie, Fundacja Wolnego Oprogramowania Reszka, Hackerspace Pomorze, Hackerspace Wrocław, Jak Głosują, Knyfyrstel Hackerspace Poznań, Kontrabanda, Koopertywa Sieciowa KoopNet, Linux Professional Institute, Polska Grupa Użytkowników Linuxa, Polska Sieć Ekonomii, PyPolska, QuantLab, Rust Poland, Spółdzielnia PLZ, SUSE, Warszawski Hackerspace.

1. W jaki sposób dobrze zdefiniować open source na potrzeby konkursu? Czy definicja powinna odwoływać się do konkretnych licencji lub zapisów licencyjnych?.....	2
2. Jakie czynniki będą służyły skuteczności wdrożeń?.....	3
3. W jaki sposób zapewnić maksymalną replikowalność wdrażanych rozwiązań w innych jednostkach administracji publicznej?.....	4
4. Jakie czynniki powinny być brane pod uwagę przez podmioty realizujące pilotaże w zakresie bezpieczeństwa wdrażanych rozwiązań?.....	5
5. W jaki sposób najskuteczniej ułatwić pracownikom podmiotów realizujących pilotaże przejście z rozwiązań własnościowych na open source?.....	7
6. Jakie wsparcie techniczne i eksperckie powinno zostać zapewnione podmiotom realizującym pilotaże?.....	8
7. Pozostałe uwagi do konkursu: Kwestie cyberbezpieczeństwa a dedykowanych rozwiązań typu SaaS.....	9
Kontakt.....	10

1. W jaki sposób dobrze zdefiniować open source na potrzeby konkursu? Czy definicja powinna odwoływać się do konkretnych licencji lub zapisów licencyjnych?

Celem pilotażu open source w administracji jest zwiększenie poziomu suwerenności cyfrowej, dlatego pytanie o definicję *open source* należy praktycznie rozumieć jako pytanie:

“Jak zamówić rozwiązanie dające zamawiającemu wolność, w tym brak uzależnienia od konkretnego dostawcy, a jednocześnie gwarantujące odpowiednie wsparcie i utrzymanie?”

Definicja powinna nie tyle wskazywać konkretne licencje lub hasła (“wolne” lub “otwarte”), ale odwoływać się do uprawnień gwarantowanych zamawiającym podmiotom administracji. Bardzo konkretną propozycją w tym zakresie są **“Rekomendacje dotyczące zamówień publicznych na systemy informatyczne”** Prezesa Urzędu Zamówień Publicznych, obowiązujące od 2021 r. W **Tomie II rozdział o przeciwdziałaniu vendor lock-in** wskazuje w kilku rekomendacjach szczegółowych wymagania zamówień takie jak:

- Dostęp do informacji niezbędnych do późniejszej integracji z nowymi rozwiązaniami,
- Zdefiniowanie procedury postępowania w razie zakończenia zamówienia; w tym zasad zwrotu lub usunięcia danych i informacji, w określonym formacie i strukturze,
- Zastrzeżenie na rzecz zamawiającego lub innych podmiotów trzecich (innych wykonawców) możliwości wykonywania swobodnych modyfikacji oprogramowania oraz dokumentacji oprogramowania, w tym zezwalania na wykonywanie praw zależnych w odniesieniu do takiego oprogramowania oraz jej dokumentacji,
- Zastrzeżenie obowiązku wydania kodów źródłowych do oprogramowania zamawiającemu oraz zastrzeżenie możliwości przekazania tych kodów źródłowych także innym wykonawcom, którzy będą modyfikować stworzone przez wykonawcę oprogramowanie,
- Określenie zasad poufności realizacji zamówienia oraz postanowień dot. tajemnicy przedsiębiorstwa wykonawcy, tak, aby nie blokowały one w praktyce uprawnień zamawiającego do udostępniania oprogramowania i jego kodów źródłowych podmiotom trzecim, jeśli jest to niezbędne do modyfikowania takiego oprogramowania i wykonywania uprawnień prawnoautorskich nabytych przez zamawiającego.

Podsumowując, z wymagań konkursu powinno jasno wynikać, że dostarczone rozwiązania mają zapewniać swobodę użytkownika, co w największym skrócie jest możliwe przez **obowiązkowe zapisanie w dokumentacji konkursowej/przetargowej praw wynikających z wytycznych UZP, w tym wymaganie dostarczenia kodu źródłowego na wolnych/otwartych licencjach.**

2. Jakie czynniki będą służyły skuteczności wdrożeń?

Skuteczność wdrożeń, rozumianą przez pryzmat KPIs, należy rozpatrywać przede wszystkim przez stopień adopcji wśród urzędników, ciągłość realizowanych zadań oraz długoterminową stabilność projektu oraz na końcu w kategorii technicznej instalacji oprogramowania. Aby wdrożenie zakończyło się sukcesem, należy zapewnić następujące czynniki:

- **Kompleksowe finansowanie długoterminowe:** Zabezpieczenie środków finansowych nie tylko na proces wdrożenia i pierwszy rok wsparcia, ale również na dalsze wieloletnie funkcjonowanie systemu. Ucięcie budżetów na rozwój i aktualizacje (w tym łatki bezpieczeństwa) bezpośrednio po okresie pilotażu błyskawicznie zniechęci użytkowników i wygeneruje ryzyko powrotu do zamkniętych rozwiązań własnościowych.
- **Wdrażanie rozwiązań zintegrowanych:** Zamiast wdrażania i synchronizowania kolekcji luźnych aplikacji, należy preferować zintegrowane pakiety oprogramowania. Zapewniają one płynną i natywną współpracę komponentów, co oferuje urzędnikom wyższą przystępność, a administracji IT znacząco obniża koszty i zawilości związane z utrzymaniem infrastruktury.
- **Pełna polonizacja interfejsu i dokumentacji:** Bezwzględna dostępność wdrażanego oprogramowania w języku polskim. W ramach pilotażu musi powstać (lub zostać przetłumaczona przy współpracy ze społecznością) profesjonalna, polskojęzyczna dokumentacja techniczna oraz instrukcje dla użytkowników końcowych.
- **Skupienie na ciągłości procesów:** Skuteczne wdrożenie nie powinno opierać się na wymogu stworzenia dokładnej repliki wszystkich pobocznych funkcji dotychczas używanego systemu zamkniętego (co często bywa niemożliwe i jest wykorzystywane przez dostawców własnościowych jako blokada migracji). Czynnikiem sukcesu jest zapewnienie ciągłości kluczowych procesów urzędowych w oparciu o nowe, otwarte i bezpieczne narzędzia.
- **Wewnętrzna interoperacyjność i otwarte standardy:** Nowe systemy wdrażane w ramach pilotażu muszą w pełni wspierać otwarte formaty i protokoły. Ma to na celu zagwarantowanie bezproblemowej integracji i wymiany danych pomiędzy poszczególnymi nowymi komponentami administracji.
- **Partycypacja w rozwoju:** Podmiot wdrażający musi posiadać zdolność do wprowadzania modyfikacji dostosowujących oprogramowanie do specyficznych potrzeb polskich urzędów. Premiowane powinno być podejście pro-aktywnego mapowania procesów i dopasowywania technologii do potrzeb zamawiającego. Jednocześnie, czynnikiem długofalowego sukcesu jest wymóg, aby modyfikacje te (powstające za publiczne środki) nie tworzyły zamkniętych odgałęzień, lecz trafiały z powrotem do oficjalnej, globalnej dystrybucji danego oprogramowania.
- **Profesjonalne zarządzanie zmianą i szkolenia:** Zapewnienie kompleksowych szkoleń zarówno dla administratorów utrzymujących system, jak i użytkowników końcowych. Wykonawca musi wykazać się zdolnością do miękkiego wprowadzania zmiany w kulturze organizacyjnej instytucji.
- **Zaufanie poprzez niezawodność i bezpieczeństwo:** Spełnienie rygorystycznych norm bezpieczeństwa (m.in. wymuszenie uwierzytelniania dwuskładnikowego 2FA, regularne kopie zapasowe, szyfrowanie dysków, terminowe aktualizacje). Poczucie bezpieczeństwa i brak awarii są kluczowymi czynnikami budującymi zaufanie urzędników do nowego oprogramowania.

3. W jaki sposób zapewnić maksymalną replikowalność wdrażanych rozwiązań w innych jednostkach administracji publicznej?

Zapewnienie maksymalnej replikowalności rozwiązań wdrażanych w ramach pilotaży wymaga podejścia dwutorowego. Z jednej strony konieczna jest **standaryzacja**, która pozwoli **zautomatyzować wdrożenia w kolejnych jednostkach**. Równoległe do tego, co stanowi klucz do długoterminowego sukcesu, niezbędne jest **wykreowanie trwałego, międzysektorowego ekosystemu wokół utrzymania wypracowanego stosu technologicznego**. Tylko integracja twardych praktyk zarządzania infrastrukturą z modelem społeczno-gospodarczym pozwoli na bezproblemowe powielanie systemów w jednostkach samorządu terytorialnego o zróżnicowanych budżetach i kompetencjach.

Aby technicznie ułatwić transfer rozwiązań pomiędzy urzędami, podmioty realizujące pilotaże muszą pracować w **paradygmacie Infrastructure as Code**. Wykorzystanie nowoczesnych narzędzi, takich jak Nix, Kubernetes, Docker, Ansible czy Puppet, w połączeniu z przechowywaniem konfiguracji w systemach kontroli wersji, pozwala realizować założenia metodyki GitOps. Dzięki temu możliwe jest zautomatyzowane, szybkie i wolne od błędów ludzkich sklonowanie całego środowiska roboczego w nowej jednostce. Działaniom tym musi towarzyszyć ujednoczenie skryptów instalacyjnych oraz bezwzględny wymóg rygorystycznego wersjonowania wszelkich modyfikacji oprogramowania wprowadzanych na specyficzne potrzeby danej placówki. Fundamentem operacyjnej replikowalności jest również tworzenie kompleksowej, polskojęzycznej dokumentacji technicznej i użytkowej, a także profesjonalizacja procesów wdrożeniowych. Wszelkie modyfikacje muszą być weryfikowane w dedykowanych środowiskach testowych, zanim trafią na środowiska produkcyjne urzędów.

Należy pamiętać, że nawet najlepiej zautomatyzowane wdrożenie nie przetrwa próby czasu bez odpowiedniego zaplecza. Najlepszą gwarancją długofalowej replikowalności jest intencjonalna **integracja organizacji obywatelskich, środowisk naukowych, biznesu open source oraz podmiotów ekonomii społecznej**. Taki model sprzyja sprawnemu transferowi wiedzy i buduje odporność systemów informatycznych państwa na potencjalne kryzysy. Wzorcem dla polskiej administracji powinien być kierunek obrany przez rząd francuski w ramach projektu La Suite, w którym **państwo objęło tam aktywną rolę w rozwoju spółdzielni** komercjalizującej oprogramowanie, m.in. poprzez oferowanie oprogramowania open source jako usługi (SaaS). Osiągnięcie podobnego efektu skali w Polsce umożliwiłoby bezpieczne utrzymanie zaawansowanych systemów open source także w tych JST, które dysponują mniejszymi zdolnościami operacyjnymi i finansowymi. Wymaganie od JST samodzielnego utrzymywania narzędzi cyfrowych w ramach strukturach urzędu („on prem”) prowadzi do obciążenia samorządu większymi kosztami, niepełnego wykorzystania zasobów, oraz braku przepływu wiedzy i praktyk między sektorem publicznym a prywatnym.

Docelowym efektem pilotażu przewidzianym w ramach finansowych powinno być powstanie **międzysektorowych Partnerstw Publiczno-Spółdzielczych**, polegających na integracji lokalnych/regionalnych aktorów gospodarczych w modelu spółdzielni cyfrowej oferującej współdzielone zasoby i usługi dla kolejnych gmin, firm, NGO i obywateli.

4. Jakie czynniki powinny być brane pod uwagę przez podmioty realizujące pilotaże w zakresie bezpieczeństwa wdrażanych rozwiązań?

Zapewnienie bezpieczeństwa wdrożeń pilotażowych musi opierać się na zgodności z obowiązującymi przepisami prawa, w tym m.in. ustawą o dostępności cyfrowej, Krajowymi Ramami Interoperacyjności, ustawą o krajowym systemie cyberbezpieczeństwa oraz wymogami RODO. Ponadto, specyfika wdrażania otwartego oprogramowania wymaga od podmiotów realizujących pilotaże skupienia się na trzech kluczowych obszarach operacyjno-architektonicznych:

1. Zarządzanie podatnościami i łańcuchem dostaw:

- a. **Zgodność z główną gałęzią:** Rozwiązania muszą bazować na oficjalnych, aktywnie rozwijanych wersjach oprogramowania. Niedopuszczalne jest tworzenie odizolowanych, bocznych gałęzi kodu, ponieważ generuje to dług technologiczny i odcina zamawiającego od globalnych poprawek bezpieczeństwa wdrażanych na bieżąco przez społeczność.
- b. **Weryfikacja łańcucha dostaw:** Kod źródłowy oraz komponenty wykorzystywane w urzędzie muszą pochodzić wyłącznie z oficjalnych, zaufanych i podpisanych cyfrowo repozytoriów.
- c. **Ciągle monitorowanie i aplikowanie łat:** Wymagane jest wdrożenie mechanizmów ciągłego monitorowania rejestrów luk bezpieczeństwa i zdolności do natychmiastowego, przedterminowego aplikowania poprawek. Operacje te powinny być ułatwione przez zapewnienie możliwości bezpiecznego, zdalnego zarządzania systemami.

2. Architektura bezpieczeństwa i ciągłość działania:

- a. **Izolacja środowisk:** Bezwzględne oddzielenie środowiska produkcyjnego od testowego. Wszelkie aktualizacje i modyfikacje muszą być weryfikowane przed wdrożeniem na produkcję, a dane produkcyjne urzędu nigdy nie mogą trafiać na środowiska testowe.
- b. **Ochrona tożsamości:** Zunifikowana kontrola dostępu ze wsparciem dla ustandaryzowanych mechanizmów uwierzytelniania, np. LDAP, Węzeł Krajowy, Active Directory oraz obowiązkowe zastosowanie uwierzytelniania wieloskładnikowego.
- c. **Kryptografia:** Pełne szyfrowanie danych zarówno w locie (TLS), jak i w spoczynku (szyfrowanie dysków). Certyfikaty używane do szyfrowania połączeń muszą pochodzić od zaufanych urzędów certyfikacji.
- d. **Ochrona przed ransomware i plany odtworzeniowe:** Wdrożenie rygorystycznej polityki kopii zapasowych, w tym utrzymywanie kopii w lokalizacji niepodłączonej do sieci głównej. Plany odzyskiwania sprawności muszą być testowane minimum raz w roku w pełnym wymiarze, opierając się na sprawdzonych standardach (np. standardach KNF).

3. Audytowanie, wskaźniki SLA i czynnik ludzki:

- a. **Rygorystyczne ramy SLA:** Umowa poziomu usług musi jasno definiować rygorystyczne czasy reakcji na podatności krytyczne, maksymalny budżet błędów (HTTP 4xx, 5xx) oraz wymuszać realizację prac serwisowych wyłącznie poza godzinami pracy urzędów.
- b. **Audyty i scenariusze ryzyka:** Obowiązek regularnego przeprowadzania audytów bezpieczeństwa infrastruktury oraz wykorzystywanych komponentów otwartoźródłowych, wsparty wypracowaniem scenariuszy zarządzania ryzykiem,
- c. **Budżety szkoleniowe:** Projektowanie systemów powinno opierać się na założeniu braku wstępnej wiedzy użytkowników o cyberbezpieczeństwie.

Pilotaż musi przewidywać środki na szkolenia z zakresu bezpiecznego użycia narzędzi (np. przeciwdziałanie phishingowi w nowym systemie pocztowym) oraz techniczne szkolenia dla administratorów z zakresu bezpiecznej konfiguracji systemów.

5. W jaki sposób najskuteczniej ułatwić pracownikom podmiotów realizujących pilotaże przejście z rozwiązań własnościowych na open source?

Przejście jednostek administracji publicznej w otwarty ekosystem technologiczny stanowi głęboką zmianę kulturową. Aby skutecznie ułatwić urzędnikom migrację z dotychczasowych rozwiązań i zapobiec odrzuceniu nowych systemów, konieczne jest wdrożenie kompleksowej strategii opierającej się w pierwszej kolejności na rzetelnym zapleczu szkoleniowym i technicznym. Fundamentem tego procesu musi być zapewnienie dedykowanych **szkoleń** zarówno dla użytkowników końcowych, jak i administracji IT. Równolegle niezbędne jest stworzenie stałego **punktu kontaktowego w formie infolinii lub helpdesku** oraz udostępnienie obszernej **bazy zasobów pomocowych**, takich jak instrukcje i poradniki wideo. Wykonawca musi również świadczyć ciągle wsparcie techniczne polegające na bieżącej i sprawnej reakcji na zgłoszenia dotyczące brakującej konfiguracji czy funkcjonalności.

Zapewnienie stabilnego zaplecza technicznego powinno być następnie poszerzone o mechanizmy ułatwiające współpracę międzyinstytucjonalną. Trwałość wdrożenia wymaga zagwarantowania podmiotom uczestniczącym w pilotażu dedykowanej, **wspólnej przestrzeni służącej wymianie doświadczeń, pomocy wzajemnej** oraz swobodnemu **dzieleniu się kodem źródłowym**. Integracja samorządów w ramach jednego środowiska pozwala urzędom bardziej zaawansowanym cyfrowo wspierać mniejsze jednostki poprzez bezpośrednie dzielenie się dobrymi praktykami. Eliminowane jest w ten sposób ryzyko niezależnego rozwiązywania tożsamyh problemów technologicznych przez poszczególne placówki, co obniża koszty i drastycznie skraca czas adaptacji do nowych rozwiązań.

Dopełnieniem i zwieńczeniem tych działań powinno być wyłonienie wewnątrz urzędów lokalnych liderów i pasjonatów w ramach sformalizowanego **programu ambasadorów open source**. Nadanie im roli naturalnych łączników między Ministerstwem Cyfryzacji a pracownikami urzędów pozwala na znacznie szybsze przełamywanie barier mentalnych i technologicznych. Działanie to trwale zmienia optykę wdrożenia z modelu zakładającego sztuczny podział na urzędników i zewnętrznych dostawców, co bezpośrednio zwiększa zaufanie personelu, ułatwia edukację z zakresu codziennego wykorzystania nowych narzędzi i ostatecznie gwarantuje sukces całego przedsięwzięcia.

6. Jakie wsparcie techniczne i eksperckie powinno zostać zapewnione podmiotom realizującym pilotaże?

Wsparcie dla podmiotów realizujących pilotaże powinno opierać się na połączeniu pomocy technicznej z doradztwem eksperckim na szczeblu strategiczno-prawnym. W wymiarze **technicznym** dostawca musi zagwarantować stałe wsparcie telefoniczne oraz sesje poprzez pulpit zdalny, przy czym sesje te powinny odbywać się bez możliwości bezpośredniego sterowania pulpitem zamawiającego. Uzupełnieniem tych działań operacyjnych muszą być dedykowane szkolenia prowadzone na żywo przez wykwalifikowanego trenera, a także dostarczenie obszernych materiałów wideo i wyczerpującej dokumentacji dla użytkownika końcowego.

Wymiar **eksperski** wymaga natomiast ścisłej współpracy z administracją centralną, w tym bezwzględnej **otwartości instytutu NASK na integrację wdrażanych rozwiązań z systemem EZD RP**. Administracja rządowa powinna jasno komunikować dalsze plany rozwoju kluczowych systemów państwowych, takich jak EZD RP czy aplikacja mObywatel, co pozwoli uniknąć powielania funkcjonalności i nieefektywnego wykorzystywania zasobów finansowych oraz czasowych na poziomie jednostek samorządowych. Należy przy tym wyraźnie zaznaczyć, że mObywatel jest obecnie rozwiązaniem własnościowym, wymuszającym na użytkownikach korzystanie z zamkniętych systemów operacyjnych. Z tego względu postulujemy nałożenie **obowiązku równoległego udostępniania usług państwowych powiązanych z mObywatel w sposób neutralny technologicznie**, wykorzystując do tego otwarte API. Docelowym kierunkiem powinno być oparcie usług publicznych bezpośrednio na wolnych standardach i wolnym oprogramowaniu.

Kluczowym elementem długofalowego wsparcia eksperckiego powinno być również zapewnienie podmiotom realizującym pilotaże dostępu do **prawników ministerialnych**. Profesjonalne doradztwo w tym zakresie ma ułatwić urzędowi poprawne i sprawne wprowadzanie rygorystycznych założeń wynikających z najnowszych aktów prawa unijnego, takich jak **Data Governance Act**, **AI Act** czy ramy tożsamości cyfrowej **EUDI**. Takie podejście umożliwi administracji publicznej nie tylko samo wdrożenie oprogramowania open source, ale również rozwijanie go od podstaw z uwzględnieniem najnowszych regulacji prawnych, co pozwoli na technologiczną i regulacyjną przewagę nad rozwiązaniami dostarczonymi przez największe korporacje technologiczne.

7. Pozostałe uwagi do konkursu: Kwestie cyberbezpieczeństwa a dedykowanych rozwiązań typu SaaS.

Dostawca mógłby chcieć zaoferować instytucji, np. JST, usługę w modelu SaaS (ang. Software as a Service) opartą na oprogramowaniu Open Source zakładającego przetwarzanie w chmurze obliczeniowej. Poza opisywanymi czynnikami w pytaniu *"Jakie czynniki powinny być brane pod uwagę przez podmioty realizujące pilotaże w zakresie bezpieczeństwa wdrażanych rozwiązań?"*, od dostawcy usługi SaaS należałoby bezwzględnie wymagać wymienionych wcześniej czynników bezpieczeństwa. Przetwarzanie w modelach chmur obliczeniowych opiera się na założeniu wysokiego poziomu standaryzacji sprzętu, oprogramowania i usług, których szczegółów implementacyjnych odbiorca zwykle nie zna. W związku z tym wymagany jest szczególnie wysoki poziom zaufania do dostawców usług w chmurach obliczeniowych, taki dostawca:

- Powinien oferować wyższy (np. 99.9%) wskaźnik SLA w porównaniu do oferentów on-premise,
- Tworzy automatyczne, regularne tworzenie kopii zapasowych, szyfrowanie oraz przechowywanie w odizolowanej lokalizacji; w każdej chwili umożliwia migrację swoich danych do własnej infrastruktury urzędu lub do innego dostawcy bez sztucznych barier technologicznych,
- Oferuje ochronę przed atakami DDoS np. przez zaawansowane mechanizmy filtrowania ruchu sieciowego, przez dedykowane urządzenia sieciowe typu firewall,
- Musi stale monitorować publiczne bazy podatności dla utrzymywanego oprogramowania i gwarantować bezzwłoczne wdrażanie poprawek bezpieczeństwa w oferowanej usłudze,
- Zapewnia zgodność ze Standardami Krajowych Ram Interoperacyjności,
- Spełnia obowiązki zawarte w ustawie o Krajowym Systemie Cyberbezpieczeństwa,
- Zapewnia zgodność z RODO; przetwarza dane na terenie Europejskiego Obszaru Gospodarczego i w żaden sposób, w tym jako część grupy kapitałowej nie podlega pod jurysdykcję państwa spoza EOG;
- Spełnia Standard Cyberbezpieczeństwa Chmur Obliczeniowych na poziomie SCCO2; zapewnia JST pełną kontrolę nad kluczami szyfrującymi.

Wielu dostawców infrastruktury na rynku posiada certyfikaty ISO/IEC 27001 (system zarządzania bezpieczeństwem informacji), ISO/IEC 27017 (bezpieczeństwo w chmurze obliczeniowej) oraz oficjalne deklaracje zgodności z SCCO, dzięki czemu dostawca usługi SaaS mógłby postawić na model hybrydowy, wybrać partnera, który certyfikacje już posiada a skupić się na bezpiecznym wdrożeniu samego oprogramowania, wzmocnieniu konfiguracji (hardening), zarządzania kopiami zapasowymi, aktualizacjami, szyfrowaniem.

Konkurs nie powinien jednoznacznie wskazywać w jakiej formule dostawca lub partnerstwo dostawców realizuje usługę, ale postawić na konkretne wymagania jakościowe wskazane powyżej.

Kontakt

Jako koalicja zrzeszająca ekspertów, praktyków branży IT oraz organizacje społeczne, deklarujemy pełną gotowość do dalszej, merytorycznej współpracy z Ministerstwem Cyfryzacji na kolejnych etapach przygotowywania i realizacji pilotaży. Chętnie rozwiniemy i uszczegółowimy każdy z przedstawionych w niniejszym stanowisku postulatów podczas bezpośredniego spotkania lub dalszych konsultacji.

W sprawach związanych z niniejszym dokumentem, w imieniu Sojuszu SPOIWO do dyspozycji pozostaje:

[REDAKTOWANE], Koordynator Sojuszu Przyjaciół Otwartego i Wolnego Oprogramowania

E-mail: [REDAKTOWANE]

Telefon: [REDAKTOWANE]