

Warszawa, 20.07.2026

Biuro Ministra
Ministerstwo Cyfryzacji

Szanowni Państwo,

Działając w imieniu Sojuszu Otwartego i Wolnego Oprogramowania - SPOIWO, z satysfakcją przyjmujemy ogłoszenie przez Komisję Europejską pakietu na rzecz suwerenności technologicznej (COM(2026) 503 final), w tym w szczególności dedykowanej Strategii dla europejskich otwartych ekosystemów cyfrowych (Open Source Strategy) oraz zapowiedzi aktu o rozwoju chmury i AI (*Cloud and AI Development Act – CADA*).

Zgadza się z diagnozą KE, że strukturalne uzależnienie UE od dostawców z państw trzecich stanowi krytyczne zagrożenie dla naszej podmiotowości geopolitycznej i gospodarczej. Jako organizacja stojąca na straży suwerenności cyfrowej i otwartych standardów, pragniemy przedstawić kluczowe postulaty i rekomendacje wdrożeniowe. Opierają się one między innymi na najnowszych badaniach krajowych (raport Centrum Cyfrowego „*Architektura współpracy. Open source jako siła napędowa polskiej innowacji i suwerenności technologicznej*”, 2026) oraz europejskich analizach prawno-autorskich (raport „*Copyright challenges in open-source AI development in the European Union*” stowarzyszenia Communia, 2026).

Poniżej przedstawiamy nasze priorytety, oczekując ich aktywnego uwzględnienia w stanowisku Rządu RP na forum unijnym oraz w krajowych strategiach wdrożeniowych. **Postulaty cieszą się oficjalnym poparciem następujących organizacji oraz podmiotów zrzeszonych w ramach Sojuszu Przyjaciół Otwartego i Wolnego Oprogramowania (w kolejności alfabetycznej):** Ajax, Fundacja Centrum Cyfrowe, Coop Tech Hub, Fundacja Kuźnia Rdzeni, Fundacja Moje Podl@sie, Fundacja Open Source Polska, Hackerspace Pomorze, Hackerspace Wrocław, Fundacja Internet. Czas Działać!, Inicjatywa Jak Głosują, Knyfyrteł, Kontrabanda, Kooperatywa Sieciowa KoopNet, Linux Professional Institute, Polska Grupa Użytkowników Linuxa, Polska Sieć Ekonomii, PyPolska, Quantlab, Fundacja Wolnego Oprogramowania Reszka, Rust Poland, SUSE, Warszawski Hackerspace, Fundacja Wolne Lektury.

Reformy polityki zakupowej i zasada domyślnej otwartości

Fundamentem cyfryzacji państwa musi stać się zasada „publiczne pieniądze, publiczny kod”. Oprogramowanie zamawiane przez instytucje publiczne i finansowane ze środków budżetowych wymaga domyślnego udostępniania na wolnych licencjach. To klucz do budowania odporności i optymalizacji kosztów całkowitych. Konieczne jest wdrożenie mechanizmu „comply-or-explain” (Open Source First), co oznacza kategoryczne zaprzestanie publikacji specyfikacji warunków zamówienia dopuszczających dostarczanie rozwiązań zamkniętych. Suwerenność cyfrową administracji należy weryfikować rynkowymi wskaźnikami: szybkością wyjścia oraz zdolnością do

zmiany kierunku podczas ewentualnej zmiany dostawcy. Aby zminimalizować obawy urzędników przed naruszeniem dyscypliny finansów publicznych, administracja centralna musi uruchomić Centralną Platformę Wdrożeniową. Platforma ta powinna dostarczać udokumentowane modele kalkulacji całkowitego kosztu posiadania oraz państwową bazę zweryfikowanych szablonów przetargowych, uniemożliwiających wykluczanie rozwiązań otwartoźródłowych na etapie postępowań zakupowych.

Przeciwdziałanie open-washingowi

Należy stanowczo przeciwdziałać zjawisku open-washingu, definiowanemu jako nadużywanie pojęcia otwartości dla technologii obwarowanych restrykcyjnymi modelami dystrybucji. Należy odwoływać się do formalnych definicji i list wolnych i otwartych licencji utrzymywanych przez takie organizacje jak Free Software Foundation czy Open Source Initiative. Jednocześnie należy weryfikować oferty określane jako "otwarte", pod kątem tego, czy faktycznie oznaczają one udzielenie wolnej licencji bez zastrzeżeń wraz z przekazaniem kodu źródłowego i korzystanie z oprogramowania w sposób gwarantujący kontrolę użytkownika nad tym oprogramowaniem. Zjawisko "open-washingu" widoczne jest ostatnio szczególnie w obszarze technologii uczenia maszynowego, gdzie termin "otwarty" używany jest szczególnie często bez pokrycia - używane w odniesieniu do modeli licencje zawierają niezgodne z ww. formalnymi definicjami ograniczenia (np. licencja Llama czy licencje zakazujące korzystania komercyjnego) a użytkownikom nie przekazuje się materiałów koniecznych do swobodnego analizowania, uruchamiania, modyfikowania i dzielenia się tymi technologiami.

Architektura bezpieczeństwa i struktury instytucjonalne

Rozproszone inicjatywy wymagają konsolidacji poprzez powołanie w pełni funkcjonalnego Krajowego Repozytorium Kodu. Scentralizowanie i usystematyzowanie projektów open source realizowanych w sektorze publicznym i naukowym zapobiegnie powielaniu wydatków i ułatwi audyty bezpieczeństwa. System ten musi pełnić funkcję ustrukturyzowanego katalogu rozwiązań audytowalnych i posiadających zdefiniowaną ścieżkę wsparcia komercyjnego, gotowych do zaimplementowania przez jednostki krytyczne, z zachowaniem integracji z unijnym Katalogiem Rozwiązań Open Source. Operacjonalizacja tych celów wymaga nadania stałego charakteru operacyjnego oraz realnych uprawnień weryfikacyjnych Zespołowi ds. rozwiązań typu open source, celem przekształcenia go w pełnoprawne biuro OSPO (*Open Source Program Office*). Niezbędne jest także natychmiastowe przejście Polski ze statusu obserwatora do pełnego członkostwa w konsorcjum Digital Commons EDIC, umożliwiające aktywny udział w kształtowaniu europejskich regulacji architektonicznych. Bezpieczeństwo teleinformatyczne musi bazować na modelu Security by Openness, nakazującym włączenie niezależnych audytów publicznego kodu źródłowego do obligatoryjnych standardów cyberbezpieczeństwa administracji.

Optymalizacja makroekonomiczna, utrzymanie kapitału i ekologia cyfrowa

Utrzymanie stabilności infrastruktury wymaga uruchomienia państwowych funduszy dedykowanych ciągłości cyfrowych dóbr wspólnych, wspierających niezależne społeczności deweloperskie dbające o krytyczną infrastrukturę otwartego kodu. Środki te powinny pochodzić z przekierowania kapitału transferowanego dotychczas za granicę w postaci opłat za zamknięte licencje. Alokacja tych funduszy na usługi wdrożeniowe i serwisowe realizowane przez polskie MŚP oraz spółdzielnie cyfrowe stymuluje lokalny rynek IT i stanowi systemowe narzędzie powstrzymujące drenaż specjalistycznych

talentów. Migracja technologiczna przynosi również wymierne korzyści infrastrukturalne. Zoptymalizowany, pozbawiony narzuconej telemetrii kod otwarty drastycznie redukuje użycie zasobów obliczeniowych i zapotrzebowanie energetyczne systemów, co efektywnie zapobiega zjawisku planowanego postarzenia sprzętu i wydłuża cykl życia infrastruktury sprzętowej administracji publicznej.

Niezależność edukacyjna

Zabezpieczenie kadr inżynierskich państwa wymaga systemowej rewizji podstaw programowych na każdym szczeblu edukacji informatycznej. Edukacja cyfrowa musi zostać uniezależniona od zamkniętych ekosystemów platformowych Big Tech na rzecz kształcenia w oparciu o uniwersalne i otwarte standardy inżynierii oprogramowania. Przebudowa programów kształcenia informatycznego w Polsce musi iść w kierunku wzmacniania kompetencji w obszarze technologii open source, zamiast bezkrytycznego promowania zamkniętych ekosystemów monopoli korporacyjnych. Strategia UE Open Source to ważna szansa na zbudowanie pełnego, europejskiego stosu technologicznego (*European technology stack*). Polska może być liderem tych zmian, pod warunkiem, że odejdzie od deklaratywnego poparcia na rzecz odważnych wdrożeń instytucjonalnych.

Zwracamy się z prośbą o uwzględnienie powyższych uwag w oficjalnym stanowisku Rzeczypospolitej Polskiej oraz deklarujemy pełną gotowość do udziału w dalszych pracach eksperckich i warsztatach konsultacyjnych organizowanych przez Ministerstwo.

Z wyrazami szacunku,

Spółeczność Sojuszu Przyjaciół Otwartego i Wolnego Oprogramowania