

Uwagi do strategii Unii Europejskiej dotyczącej otwartego oprogramowania

Szanowni Państwo,

przedstawiona przez Komisję Europejską strategia dotycząca otwartego oprogramowania zasługuje na poparcie. Trafnie wskazuje znaczenie otwartych technologii dla zwiększania interoperacyjności, ograniczania zależności od pojedynczych dostawców oraz wzmacniania europejskich zdolności do utrzymywania kluczowych elementów infrastruktury cyfrowej. Pozytywnie należy ocenić zapowiedzi dotyczące finansowania krytycznych komponentów, dostosowania zamówień publicznych, rozwoju biur programów open source oraz stosowania zasady „public money, public code”.

Skuteczność strategii będzie jednak zależała od sposobu wdrożenia poszczególnych instrumentów. Sama dostępność kodu źródłowego nie przesądza o bezpieczeństwie, trwałości projektu ani o rzeczywistym ograniczeniu zależności technologicznych. Zasadne jest zatem uzupełnienie strategii o jednoznaczne kryteria oceny rozwiązań, standardy wdrożeniowe i mierniki rezultatów.

1. Ocena wkładu rozwiązań open source w suwerenność technologiczną

Ocena rozwiązania nie powinna opierać się przede wszystkim na siedzibie producenta, narodowości twórców ani miejscu utrzymywania repozytorium. Istotniejsza jest zdolność podmiotów europejskich do kontrolowania, utrzymywania, rozwijania i bezpiecznego wykorzystywania danego rozwiązania.

Ramy oceny powinny uwzględniać w szczególności strukturę zarządzania projektem, dostęp do kodu i dokumentacji, możliwość samodzielnego zbudowania oprogramowania, przeniesienia infrastruktury oraz utworzenia rozwidlenia projektu. Ważne są również interoperacyjność, zgodność z otwartymi standardami, warunki licencyjne, dojrzałość procesów bezpieczeństwa oraz dostępność niezależnych podmiotów zdolnych do przejęcia wdrożenia i utrzymania. Takie podejście pozwoli odróżnić formalną otwartość kodu od rzeczywistej odporności operacyjnej.

2. Otwarte oprogramowanie w zamówieniach publicznych

Zapowiedziane wytyczne dotyczące zamówień publicznych powinny promować otwartość za pomocą neutralnych technologicznie wymagań odnoszących się do interoperacyjności, przenośności danych, dokumentacji, możliwości zmiany wykonawcy oraz kosztów całego cyklu życia systemu. Należy przy tym zachować zasady równego traktowania wykonawców, proporcjonalności i uczciwej konkurencji.

Ocena ofert powinna uwzględniać całkowity koszt posiadania rozwiązania, w tym koszty integracji, dostosowania, utrzymania, aktualizacji, szkoleń, audytów, migracji danych oraz zakończenia eksploatacji. Istotna jest również możliwość przejęcia utrzymania przez inny podmiot lub przez samą instytucję.

Warto promować modułową konstrukcję zamówień i ich podział na części, jeżeli pozwala na to architektura rozwiązania. Może to zwiększyć udział małych i średnich przedsiębiorstw oraz podmiotów specjalizujących się w integracji, cyberbezpieczeństwie i utrzymaniu. Jednocześnie konieczne jest jednoznaczne określenie odpowiedzialności za integrację i funkcjonowanie całego systemu.

3. Finansowanie i bezpieczeństwo krytycznych komponentów

Instrument utrzymania otwartego oprogramowania powinien zapewniać finansowanie wieloletnie. Wsparcie powinno obejmować bieżące utrzymanie, aktualizacje, reagowanie na podatności, przeglądy kodu, testy regresji, rozwój dokumentacji oraz utrzymanie infrastruktury budowania i dystrybucji oprogramowania. Warto finansować także przygotowanie nowych opiekunów projektu oraz plany ciągłości na wypadek wycofania się kluczowych osób.

Przy wyborze projektów należy brać pod uwagę ich znaczenie systemowe, liczbę zależnych systemów, wykorzystanie w administracji i infrastrukturze krytycznej, brak łatwo dostępnych zamienników oraz skutki przerwania utrzymania. Liczba użytkowników końcowych nie powinna stanowić głównego kryterium, ponieważ mało rozpoznawalna biblioteka może być podstawową zależnością licznych usług.

Wymagania bezpieczeństwa powinny być proporcjonalne do ryzyka. Dla systemów istotnych z perspektywy administracji należy przewidzieć wykaz komponentów oprogramowania, monitorowanie zależności, procedury zgłaszania podatności, zabezpieczenie kont deweloperskich, podpisywanie artefaktów, kontrolę integralności pakietów oraz plan zastąpienia krytycznych zależności. Obowiązki powinny dotyczyć przede wszystkim podmiotów wdrażających, integrujących lub komercyjnie utrzymujących rozwiązania, tak aby nie obciążać nieproporcjonalnie indywidualnych twórców i społeczności wolontariuszy.

4. Rola biur programów open source

Wzmocnienie biur programów open source (Open Source Programme Office, OSPO) jest właściwym kierunkiem. Powinny one zapewniać doradztwo licencyjne, wspierać zamówienia publiczne, tworzyć wzorcowe wymagania techniczne, identyfikować rozwiązania możliwe do ponownego wykorzystania oraz koordynować szkolenia i analizy ryzyka.

OSPO powinny pełnić głównie funkcję koordynacyjną i doradczą. Nie powinny zastępować zespołów prawnych, architektów systemów ani jednostek cyberbezpieczeństwa. Dla mniejszych instytucji i samorządów warto stworzyć model usług współdzielonych, realizowanych przez krajowe lub regionalne centra kompetencji.

5. Oprogramowanie finansowane ze środków publicznych

Zasadę „public money, public code” należy wdrażać stopniowo również na poziomie państw członkowskich. Odstępstwa od publikacji powinny być uzasadniane i dokumentowane. Mogą dotyczyć informacji niejawnych, prawnie chronionych, praw własności intelektualnej osób trzecich lub konkretnego ryzyka bezpieczeństwa, którego nie da się ograniczyć przez usunięcie danych, kluczy, konfiguracji albo czasowe odroczenie publikacji.

Dane osobowe nie powinny stanowić samodzielnej podstawy do rezygnacji z publikacji całego rozwiązania. Kod i historia repozytorium powinny zostać odpowiednio oczyszczone. Publikacji powinny towarzyszyć licencja open source, dokumentacja wdrożeniowa i architektoniczna, wykaz zależności, instrukcje budowania, zasady zgłaszania podatności oraz informacja o statusie projektu i zapewnianym poziomie wsparcia.

6. Otwarte modele sztucznej inteligencji

W odniesieniu do modeli AI potrzebna jest wielowymiarowa klasyfikacja otwartości. Należy odrębnie oceniać dostępność kodu, wag modelu, dokumentacji technicznej, informacji o danych, kodu treningowego oraz możliwość modyfikacji i redystrybucji.

Samo udostępnienie wag nie powinno być utożsamiane z modelem open source. Warto rozróżnić modele open source, modele z otwartymi wagami oraz modele dostępne źródłowo, lecz objęte dodatkowymi ograniczeniami licencyjnymi. Dla modeli stosowanych w administracji szczególne znaczenie mają wersjonowanie, walidacja przed wdrożeniem, audytowalność, monitorowanie jakości, możliwość uruchamiania w kontrolowanej infrastrukturze oraz procedura wycofania lub zastąpienia modelu.

7. Kompetencje i monitorowanie rezultatów

Szkolenia dla administracji powinny być dostosowane do ról zawodowych. Innego przygotowania wymagają osoby zarządzające, pracownicy zamówień publicznych, prawnicy, architekci, administratorzy i zespoły cyberbezpieczeństwa. Oprócz szkoleń potrzebne są listy kontrolne, wzorcowe klauzule, procedury przejmowania utrzymania oraz scenariusze migracji.

System monitorowania powinien obejmować wskaźniki bezpieczeństwa, konkurencji, trwałości projektów i ograniczania zależności. Należy mierzyć między innymi liczbę ponownie wykorzystywanych rozwiązań, udział zamówień uwzględniających otwarte standardy, liczbę krytycznych komponentów objętych finansowaniem, czas usuwania podatności oraz dostępność alternatywnych podmiotów utrzymujących systemy. Każdy wskaźnik powinien mieć określoną definicję, wartość bazową, źródło danych i podmiot odpowiedzialny za pomiar.

Podsumowanie

Ogólny kierunek strategii należy poprzeć. Warunkiem jej powodzenia jest powiązanie otwartości kodu z bezpieczeństwem, trwałym finansowaniem, dokumentacją, rozwojem kompetencji oraz rzeczywistą możliwością zmiany wykonawcy lub przejęcia utrzymania. Z perspektywy Polski szczególne znaczenie mają rozwój krajowego rynku usług open source, udział małych i średnich przedsiębiorstw w zamówieniach, wsparcie otwartych modeli AI oraz budowa wspólnego zaplecza OSPO dla administracji centralnej i samorządowej.