

## Wkład ZPP w konsultacje zainicjowane przez europoła Axela Vossa na temat rozporządzenia w sprawie sztucznej inteligencji

Związek Przedsiębiorców i Pracodawców z zadowoleniem przyjmuje konsultacje na temat rozporządzenia w sprawie sztucznej inteligencji (ang. *Artificial Intelligence Act*, AIA) zorganizowane przez europoła Axela Vossa. Poniżej przedstawiamy najbardziej istotne kwestie, które według nas mają zasadnicze znaczenie dla wykorzystania potencjału europejskiej gospodarki cyfrowej w nadchodzących latach.

### 1. Jaka jest najlepsza definicja sztucznej inteligencji?

Według nas definicja proponowana obecnie w ramach AIA jest zbyt szeroka. W rezultacie AIA może objąć szereg rozwiązań, które z punktu widzenia praktyki przemysłowej i handlowej nie stanowią sztucznej inteligencji (AI). Na przykład aneks I lit. a) wymienia metody uczenia maszynowego, podczas gdy aneks I lit. c) zawiera podejścia statystyczne, estymację bayesowską, jak również metody wyszukiwania i optymalizacji. Gdyby AIA zostało uchwalone w obecnym brzmieniu, zaliczałoby niemalże każdy algorytm, metodę optymalizacji czy kalkulację statystyczną do sztucznej inteligencji. Dlatego właśnie w ocenie ZPP tak ważne jest pominięcie aneksu I lit. c) w ostatecznej wersji rozporządzenia.

### 2. Co obejmuje wysokie ryzyko?

ZPP od początku brał udział w procesie konsultacji AIA i konsekwentnie opowiadał się za wprowadzeniem podejścia opartego na ocenie ryzyka. Z zadowoleniem przyjmujemy wniosek Komisji dotyczący nałożenia obowiązkowych wymogów. Naszym zdaniem poprzez przyjęcie proporcjonalnego podejścia opartego na analizie ryzyka Komisja zapewniła odpowiednie zrównoważenie między zachowaniem miejsca dla innowacji a ochroną obywateli.

Jednocześnie wierzymy, że pewne postanowienia AIA wymagają dodatkowego objaśnienia. Obszary, które trzeba dopracować to na przykład rozróżnienie między zobowiązaniami poszczególnych podmiotów działających na rzecz sztucznej inteligencji w łańcuchu wartości a konkretnymi wymogami w zakresie zastosowań sztucznej inteligencji wysokiego ryzyka.

### 3. Jak to pogodzić ze standardami etycznymi?

Naszym zdaniem Karta praw podstawowych Unii Europejskiej, a także *acquis communautaire* stanowią fundamentalne źródła standardów etycznych w UE i jako takie są uznawane za wiążące. W związku z tym wszelkie ograniczenia w korzystaniu ze sztucznej inteligencji powinny opierać się na potencjalnym naruszeniu zasad, które już dziś tworzą prawo wspólnotowe. Poszerzenie tej grupy źródeł stworzyłoby ryzyko dla spójności ram prawnych UE i stanowiłoby uszczerbek dla zasady pewności prawa.

### 4. Jak możemy zapewnić skuteczność podejścia do zarządzania AI?

Sformułowaliśmy szereg konkretnych zaleceń w perspektywie wdrożenia i egzekwowania AIA.

Po pierwsze, rozporządzenie powinno doprecyzować zakres obowiązków, którym mają podlegać dostawcy, operatorzy i użytkownicy AI. Szczególną uwagę należy poświęcić kwestii obowiązków użytkowników AI działających w charakterze operatorów oraz kwestii obowiązków dostawców wobec ich klientów. Obecnie AIA nie zawiera definicji operatora. Naszym zdaniem zdefiniowanie go jako podmiotu udostępniającego sztuczną inteligencję użytkownikom w konkretnej sytuacji zwiększyłoby spójność i przejrzystość ogólnych ram regulacyjnych.

Po drugie, powodzenie AIA zależy od tego czy planowane obowiązki będą uzasadnione i wykonalne. Aby to osiągnąć, należy dopracować brzmienie niektórych przepisów tak, by nie wyznaczać niemożliwych do zrealizowania standardów. Przykładowo, wymogi nałożone na sztuczną inteligencję wysokiego ryzyka są zasadniczo proporcjonalne. Niemniej jednak brzmienie przepisów należy zweryfikować, aby upewnić się, że dadzą się one zastosować w praktyce. Przykładem obowiązku niemożliwego do realizacji w praktyce jest art. 10 ust. 3, w którym mowa, że „Zbiory danych dotyczących szkolenia, walidacji i testowania muszą być odpowiednie, reprezentatywne, pozbawione błędów i kompletne”. Jakkolwiek cel jest słuszny, to w praktyce nie da się tego zagwarantować. Ponadto, warto zwrócić uwagę, że niektóre techniki mające na celu poprawę prywatności użytkowników celowo wprowadzają błędy (zaszumienia) do zbiorów danych.

Podobnie, AIA powinno unikać nieproporcjonalnych wymogów. Jednym z przykładów powyższego jest art. 64 lit. a), który stanowi, że „...na uzasadniony wniosek organom nadzoru rynku przyznaje się dostęp do kodu źródłowego systemu AI”. Z jednej strony, przepis ten jest sprzeczny z dyrektywą unijną o tajemnicy przedsiębiorstwa. Z drugiej strony, istnieją mniej inwazyjne, aczkolwiek skuteczne sposoby weryfikacji działania systemu AI. Dlatego naszym zdaniem należałoby zmienić ten przepis, aby zobowiązać dostawców i operatorów AI do skutecznego wspierania organów nadzoru rynku w przeprowadzaniu dokładnych testów (kontrola danych wejściowych/wyjściowych).