Warszawa, dnia 10 czerwca 2021 r.

Szanowna Pani
Anna Sidor
Departament Rozwiązań Innowacyjnych
Cyfryzacja KPRM

Szanowni Państwo,

w nawiązaniu do prowadzonych konsultacji publicznych pakietu projektów przepisów dotyczących sztucznej inteligencji, przesyłam uwagi Związku Cyfrowa Polska do przedmiotowych projektów.

KLUCZOWE PROBLEMY/ OBSZARY DO WYJAŚNIENIA

1. **Zbyt szeroka definicja sztucznej inteligencji:** Jeśli utrzymamy taką definicję, to obawiamy się, że rozszerzająca interpretacja AI może doprowadzić do objęcia nią np. konwencjonalne funkcje informatyczne oparte na formule „jeśli to".

2. **Wyjaśnienia dotyczące art. 5 (zabronione praktyki sztucznej inteligencji)** w szczególności litery a) i b) - zaproponowany język jest wciąż niejasny – jaka jest definicja technik podprogowych? Co to jest „szkoda psychiczna"? Co oznacza sformułowanie: „wykorzystuje dowolną lukę w zabezpieczeniach określonej grupy osób"?

3. **Wyjaśnienia dotyczące obowiązków przejrzystości (art. 52):** czym są „interakcje z osobami fizycznymi"?

- Art. 52 nakłada obowiązek powiadomienia użytkownika, że wchodzi on w interakcję z systemem AI, jeśli nie jest to oczywiste. KE podaje przykład chatbota, który miałby na przykładzie wyjaśnić ten obowiązek. Jednak język w obecnym brzmieniu jest zbyt

niejasny, biorąc pod uwagę, że sztuczna inteligencja jest zintegrowana z wieloma systemami skierowanymi do użytkownika używanymi w celu uzyskania rekomendacji, wyszukiwania informacji, udzielania wskazówek, prognoz — jak zdefiniować „interakcję z osobami fizycznymi" i jak szeroko/wąsko należy to postrzegać?

4. Zaburzona równowaga obowiązków między dostawcami, wdrażającymi i użytkownikami sztucznej inteligencji wysokiego ryzyka

- W obecnym brzmieniu przepisy nie rozróżniają między obowiązkami nakładanymi na użytkownika sztucznej inteligencji, jeśli pełni on rolę wdrażającego dane zastosowanie AI, a obowiązkami „dostawcy AI" wobec klienta.

- Wdrażający zastosowania AI powinni ostatecznie być głównym podmiotem oceny, ponieważ przedsiębiorstwa oferujące narzędzia AI ostatecznie nie są w stanie zweryfikować zastosowań końcowych, do których wykorzystywane są ich systemy, ani dodatkowych danych, które mogą być wprowadzane do systemu. Dostawcy rozwiązań AI mogą i powinni dostarczać wszystkie informacje niezbędne wdrażającym do przeprowadzenia samooceny. Jest to bardzo ważne dla dostawcy rozwiązań/interfejsów API, nad którymi dostawca rozwiązań AI nie przejmuje kontroli, gdy użytkownik wyraża zgodę na umożliwienie klientom/użytkownikom dostępu do rozwiązania według własnego uznania.

5. Zwolnienia dotyczące wielozadaniowych systemów/narzędzi typu open source:

- obowiązki przestrzegania wymogów dotyczących systemów AI powinny spoczywać na podmiotach prawnych lub osobach fizycznych korzystających z narzędzi typu open source, takich jak TensorFlow, czy AutoML, ponieważ mają one ostateczną kontrolę nad celem i wykorzystaniem zastosowań sztucznej inteligencji. Nałożenie obowiązków na dostawcę narzędzi open source w dużej mierze zniechęciłoby do udostępniania takich technologii, które wspierają całe ekosystemy innowacji.

- Zwolnienie z obowiązku publikacji badań podstawowych: wyjaśnienie, że publikacja badań podstawowych nie kwalifikuje się jako „wprowadzanie na rynek" lub

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214

„oddawanie do użytku”.

- Wymagane wyjaśnienia/zabezpieczenia np. zagwarantowanie wolnych od błędów zbiorów danych, lub publikacja kodu źródłowego w celu nadzoru rynku, nie zawsze mogą być możliwe i mogą doprowadzić do tzw. efektu mrożącego. Zasadnym może się wydawać wprowadzenie takich obowiązków dla zastosowań wysokiego ryzyka, jednak nie widzimy racjonalności dla innego rodzaju zastosowań. Czy np. błędne tłumaczenie wynikające z niepełnej/niereprezetatywnej bazy danych ma taki sam negatywny efekt jak np. interpretacja badania medycznego?

- Niejasne, czym jest „element zabezpieczający” (safety component) z art. 3 ust. 14, zwłaszcza w związku z dyrektywą w sprawie urządzeń radiowych. Czy np. system Android jest “elementem bezpieczeństwa” urządzenia mobilnego? Czy obowiązek oznacza, że samo urządzenie lub jej system musi spełniać jakąś funkcję krytyczną dla bezpieczeństwa?

W razie dodatkowych pytań, pozostajemy do dyspozycji na dalszym etapie konsultacji.

Z wyrazami szacunku,

Michał Kanownik

Prezes Zarządu

Związek Cyfrowa Polska

www.zipsee.pl
Związek Cyfrowa Polska
ul. Ogrodowa 58
00-876 Warszawa
Tel. +48 (22) 666 22 46
Fax: +48 (22) 666 22 47
biuro@zipsee.pl
KRS: 0000250359
NIP: 522-280-25-18
REGON 140463214