Ministerstwo Funduszy
i Polityki Regionalnej

Podsekretarz Stanu
Konrad Wojnarowski

Warszawa, data: 7 sierpnia 2024 r.

znak sprawy: DRC-IVa.0221.146.2024.IT

identyfikator koszulki:

telefon: 22 273 85 36

e-mail: ignacy.turowiecki@mfipr.gov.pl

Pani Wioletta Zwara
Sekretarz Komitetu Rady Ministrów do spraw Cyfryzacji

Dotyczy: Uwag Ministerstwa Funduszy i Polityki Regionalnej do projektu dokumentu zawierającego rekomendacje użycia generatywnej sztucznej inteligencji w urzędach.

Szanowna Pani Sekretarz,

w załączeniu przesyłam tabelę z uwagami MFiPR do przedmiotowego projektu dokumentu.

Z poważaniem

Konrad Wojnarowski

/podpisano elektronicznie/

Nazwa dokumentu: Projekt dokumentu zawierającego rekomendacje użycia generatywnej sztucznej inteligencji w urzędach **[REKOMENDACJE]**					
Lp.	**Organ wnoszący uwagi**	**Jednostka redakcyjna, do której wnoszone są uwagi**	**Treść uwagi**	**Propozycja zmian zapisu**	**Odniesienie do uwagi**
1	**MFiPR DI**	Podrozdział: „W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych”	„Za każdym razem weryfikować ich rezultaty - narzędzia GenAI są podatne na stronniczość i dezinformację (tzw. *Halucynacje*)”	„Za każdym razem weryfikować ich rezultaty - narzędzia GenAI są podatne na stronniczość, dezinformację, halucynacje, manipulację, naruszenia własności intelektualnej oraz na ataki typu jailbreaking i wstrzyknięcia złośliwego kodu”. Wszystkie wymienione zagrożenia powinny być krótko scharakteryzowane w podrozdziale „O czym należy pamiętać, gdy wchodzi się w interakcję z GenAI - zwłaszcza w celach służbowych? na str. 7”	
2	**MFiPR DI**	Pkt: „GenAI w chmurze bez dedykowanego dostępu”	„2. Nie należy wpisywać do takich narzędzi żadnych informacji niejawnych, kontrolowanych wrażliwych danych urzędowych ani kontrolowanych danych urzędowych (np. objętych RODO).”	Sformułowanie „kontrolowanych wrażliwych danych urzędowych ani kontrolowanych danych urzędowych” wymaga doprecyzowania.	
3	**MFiPR DI**	Pkt „GenAI w chmurze z dedykowanym dostępem”	„2. Należy wpisywać tam tylko informacje jawne i nieobjęte kontrolą.” - podobnie jak to miało miejsce w poprzedniej uwadze doprecyzowania wymaga pojęcie „”informacji nieobjętych kontrolą. Wydaje się, że właściwym w tym przypadku sformułowanie będzie „informacje nieobjęte mechanizmami ochrony, klasyfikacja informacji, etykietowanie, itp.”	Wydaje się, że właściwym w tym przypadku sformułowaniem będzie „informacje nieobjęte mechanizmami ochrony, np. klasyfikacja informacji, etykietowanie, itp.”	

4	**MFiPR DI**	Pkt „Cyberbezpieczeństwo”	„Wszystkie systemy sztucznej inteligencji wykorzystujące dane osobowe lub inne dane zawierające informacje o istotnym znaczeniu dla sektora publicznego powinny mieć zapewnione warunki: a) solidności technicznej i najwyższego poziomu cyberbezpieczeństwa,”	Zapis wymaga doprecyzowania chociażby z faktu powołania się na dobre praktyki w zakresie modeli AI.	
5	**MFiPR DI**	Pkt „Cyberbezpieczeństwo”	„3. Retrenowanie modelu powinno odbywać się tylko na uporządkowanych danych zweryfikowanych statystycznie.	Sformułowanie wymaga doprecyzowania chociażby z faktu powołania się na dobre praktyki w zakresie modeli AI.	
6	**MFiPR DI**	Pkt „System godny zaufania ”	W przywołanym punkcie nie wiadomo do końca – bez dodatkowego wyjaśnienia - czy wymienione tu wymagania są kryteriami stanowiącymi o systemie godnym zaufania?	Zapis wymaga dodatkowego wyjaśnienia.	
7	**MFiPR DI**	Pkt „System godny zaufania ”	„4. Decyzje modelu powinny być szczegółowo wyjaśniane i powszechnie dostępne.”	Zapis wymaga dodatkowego wyjaśnienia co do celu takiego działania.	
8	**MFiPR BPB**	Uwaga ogólna	Proponujemy dopisanie informacji o wykorzystywaniu możliwości (nie we wszystkich przypadkach) skorzystania wyłącznie ze stron należących do administracji publicznej. Zastosowanie takiego modelu daje pewną gwarancję, iż tekst nie będzie stronniczy i nie będzie zawierał dezinformacji.		