Ministerstwo
Cyfryzacji

Sekretarz Stanu
Dariusz Standerski

BM.WP.057.37.2025
Warszawa, 13 września 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 19 lutego br. Posła na Sejm RP Pana Janusza Cieszyńskiego w sprawie bezpieczeństwa danych użytkowników DeepSeek (interpelacja nr 8083)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Czy Ministerstwo Cyfryzacji przeprowadziło analizę funkcjonowania modelu DeepSeek, która pozwoliła ocenić, czy decyzje rządów Włoch, Australii i Tajwanu o zakazie korzystania z DeepSeek na urządzeniach rządowych są uzasadnione, oraz jakie wnioski zostały wyciągnięte z tych działań?

Prezes Urzędu Ochrony Danych Osobowych 6 lutego 2025 r. wydał komunikat, w którym zalecił ostrożność w wykorzystywaniu przedmiotowego modelu. Biorąc pod uwagę wstępne ustalenia związane z informacjami dostarczonymi przez dostawcę w jego polityce prywatności, Prezes UODO zaleca daleko idącą ostrożność w korzystaniu z aplikacji oraz innych usług oferowanych w ramach DeepSeek. Z informacji w niej zawartych wynika m.in., że dane użytkowników mogą być przechowywane na serwerach zlokalizowanych w Chinach.

Urząd Ochrony Danych Osobowych przypomina również, że technologie oparte na generatywnej sztucznej inteligencji w założeniu opierają się na przetwarzaniu ogromnej ilości danych, które mogą być wykorzystywane do celów niezgodnych z pierwotnym życzeniem użytkownika, np. do dalszego trenowania modelu lub w celach marketingowych.

UODO pozostaje w kontakcie z pozostałymi organami nadzorczymi, będącymi członkami Europejskiej Rady Ochrony Danych, w celu badania działań DeepSeek w UE i ich wpływu na ochronę osób fizycznych w związku z przetwarzaniem ich danych. UODO wymienia się z organami nadzorczymi informacjami o podejmowanych działaniach krajowych.

Ministerstwo Cyfryzacji współpracuje z UODO w zakresie bezpieczeństwa danych osobowych i jest gotowe podjąć wszystkie konieczne działania w przypadku odpowiednich zaleceń UODO lub innych organów.

Ministerstwo Cyfryzacji we wrześniu 2024 r. przygotowało rekomendacje „Generatywna sztuczna inteligencja w służbie pracowników administracji publicznej - pierwsze kroki", odnoszące się do uniwersalnych zasad bezpiecznego korzystania z modeli językowych. Należy ponadto zauważyć, że

Działania Ministerstwa koncentrują się również na tworzeniu i promowaniu suwerennych rozwiązań, które są bezpieczne i mogą być wykorzystane również na urządzeniach rządowych. Model PLLuM, który powstał ze środków publicznych i nad którego stworzeniem pracowali polscy specjaliści zarówno z obszaru IT, jak i obszaru nauk o języku, został upubliczniony i może być wdrażany[1]. Tym samym można przetwarzać dane lokalnie, w granicach kraju, zgodnie z regulacjami wprowadzanymi w Unii Europejskiej w

[1] https://huggingface.co/CYFRAGOVPL

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

odniesieniu do wykorzystania danych w systemach informatycznych oraz zastosowań sztucznej inteligencji (w tym AI ACT, DSA i DMA).

Ad 2) Jakie działania podejmuje Ministerstwo Cyfryzacji w związku z rosnącymi obawami dotyczącymi bezpieczeństwa danych użytkowników w związku z używaniem chińskiego modelu sztucznej inteligencji DeepSeek w Polsce?

Ministerstwo Cyfryzacji prowadzi szkolenia dla pracowników administracji rządowej w celu podniesienia ich kompetencji i świadomości w zakresie technologii AI. Urzędnicy byli zapoznawani z najnowszymi standardami i regulacjami dotyczącymi wprowadzania technologii sztucznej inteligencji w instytucjach publicznych. W IV kwartale 2024 r. przeszkolono ponad 2 tys. pracowników wszystkich resortów. Ministerstwo na bieżąco monitoruje sytuację w zakresie trendów wykorzystywania modeli dostępnych na rynku i będzie podejmować stosowne działania w przypadku wzrostu zagrożenia dla bezpieczeństwa danych użytkowników.

Ad 3) Czy w Polsce zostały podjęte jakiekolwiek kroki mające na celu ograniczenie lub zakazanie korzystania z DeepSeek na urządzeniach rządowych lub w instytucjach publicznych?

Ministerstwo Cyfryzacji opracowało rekomendacje bezpiecznego korzystania z GenAI w administracji publicznej. Wskazówki te są dostępne na portalu sztucznej inteligencji. Wskazujemy, aby do narzędzi GenAI nie wpisywać informacji, które np. zawierają wewnętrzne informacje urzędowe, będące w fazie przygotowawczej, a tym samym nie przeznaczone do upublicznienia lub zawierają dane osobowe, których ujawnienie narusza przepisy o ochronie danych osobowych.

Ponadto, w ramach obowiązujących w Polsce przepisów prawa tego rodzaju działanie umożliwia mechanizm rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, o których mowa w art. 33 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[2] (ustawa o KSC). Pełnomocnik podejmie stosowne działanie niezwłocznie po spełnieniu przez urządzenia informatyczne lub oprogramowanie ustawowych warunków.

Ad 4) Jakie procedury zostały wdrożone w celu monitorowania i zapewnienia, że technologie sztucznej inteligencji, takie jak DeepSeek, nie stanowią zagrożenia dla bezpieczeństwa danych obywateli Polski?

Koordynacja działań dotyczących cyberbezpieczeństwa na poziomie krajowym, w tym wymiana informacji o wynikach szacowania ryzyka związanego z ujawnionymi cyberzagrożeniami oraz zaistniałymi incydentami jest realizowana w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa. Działania te odbywają się w trybie niejawnym.

Ponadto, należy zaznaczyć, że monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym, jak również szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, należy do zadań zespołów reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego (CSIRT NASK, CSIRT GOV i CSIRT MON), o których mowa w art. 26 ust. 3 pkt 1-2 ustawy o KSC.

Ministerstwo Cyfryzacji podejmuje wiele inicjatyw mających na celu podnoszenie świadomości cyberbezpieczeństwa i higieny cyfrowej, w tym zakresie ochrony danych.

[2] Dz.U. z 2018 r. poz. 1560

Przykładowo, w ostatnim czasie, dla przybliżenia wiedzy i możliwości zgłoszenia incydentów, w aplikacji mObywatel powstała zakładka Bezpiecznie w sieci.

Ad 5) Czy Ministerstwo Cyfryzacji planuje przeprowadzenie audytu lub kontrolę technologiczną dotyczącą potencjalnych zagrożeń związanych z wykorzystaniem DeepSeek w Polsce? Jeśli tak, jakie kroki będą podejmowane w celu zabezpieczenia danych użytkowników?

Obowiązujące w Polsce przepisy prawa nie dają ministrowi właściwemu do spraw informatyzacji uprawnień do przeprowadzenia tego rodzaju „audytu lub kontroli technologicznej".

Ad 6) Jakie stanowisko zajmuje Ministerstwo w sprawie cenzurowania informacji i potencjalnych wpływów politycznych w technologii DeepSeek, szczególnie w kontekście bezpieczeństwa narodowego?

Wskazane zagadnienie pozostaje poza zakresem właściwości Ministerstwa Cyfryzacji. Ministerstwo koncentruje swoje działania na zapewnieniu bezpieczeństwa danych obywateli oraz rozwijaniu rodzimych rozwiązań w obszarze sztucznej inteligencji.

Z wyrazami szacunku
Dariusz Standerski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości
Kancelaria Prezesa Rady Ministrów – Departament Spraw Parlamentarnych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa