PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, *06-08-2024*

DOL.401.300.2024.WL.MW

Pani
Wioletta Zwara
Sekretarz Komitetu Rady Ministrów
do spraw Cyfryzacji
Ministerstwo Cyfryzacji

ul. Królewska 27
00-060 Warszawa
elektroniczna skrzynka podawcza
/MAiC/SkrytkaESP

Szanowna Pani Minister,

nawiązując do pisma z 30 lipca 2024 r. znak: DPiS.WWKS.002.112.1.2024, przekazanego do wiadomości Prezesa Urzędu Ochrony Danych Osobowych, działając na podstawie art. 57 ust. 1 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679[1] oraz art. 51 ustawy o ochronie danych osobowych[2], uprzejmie informuję, że do przedstawionego projektu dokumentu zawierającego **rekomendacje użycia generatywnej sztucznej inteligencji w urzędach**, Prezes Urzędu Ochrony Danych Osobowych (dalej jako: organ nadzorczy), przedstawia uprzejmie następujące uwagi.

Projekt dokumentu w części „W skrócie: o czym pamiętać korzystając z GenAI w celach służbowych" opiera się na założeniu, że to użytkownik będzie odpowiadał za sposób oraz skutki wykorzystania narzędzi z zakresu sztucznej inteligencji. Dokument nie definiuje natomiast najważniejszej kwestii: czy będzie to pracownik czy pracodawca. Wskazać należy, że odpowiedzialność za ocenę pozyskiwanych danych osobowych przez pracownika do celów służbowych powinna być przypisana pracodawcy jako administratorowi danych osobowych. Powinno to być wyraźnie określone w przedmiotowych rekomendacjach. Administrator odpowiada za zapewnienie

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.).
[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

poszanowania przepisów dotyczących przetwarzania danych osobowych, w tym ogólnego rozporządzenia o ochronie danych, i wynikających z nich zasad ochrony danych osobowych. Ma on obowiązek zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.

W ocenie Prezesa UODO przyjęcie przez pracodawcę określonego narzędzia usprawniającego pracę (opartego na generatywnej sztucznej inteligencji) powinno zostać poprzedzone przeprowadzoną **oceną skutków dla ochrony danych**[3]. Przeprowadzenie takiej analizy powinno prowadzić do wykazania niezbędności przetwarzania danych osobowych w określony sposób, we wskazanym konkretnie celu (celach) i zakresie oraz oceny ryzyka projektowanych (przyjmowanych) rozwiązań w zakresie przetwarzania danych osobowych. Projektowane założenia ze względu na zakładaną skalę, zakres i sposoby przetwarzania danych osobowych powodować mogę szeroki wachlarz ryzyk dla prywatności i danych osobowych. Do tej materii odnosi się motyw 91 rozporządzenia 2016/679 wskazujący w odniesieniu do operacji przetwarzania o dużej skali, że są to operacje, które „służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, na przykład (ze względu na swój szczególny charakter) gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia – oraz do innych operacji przetwarzania powodujących wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności gdy operacje te utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw”. Przyjęte w dniu 4 kwietnia 2017 r. Wytyczne Grupy Roboczej Art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679 (WP248 rev.01) wskazują na konieczność wybrania metodyki dokonywania oceny skutków dla ochrony danych, która spełnia kryteria określone w załączniku 2 do wytycznych.

Niezależnie od niezbędności dokonania oceny skutków dla ochrony danych **tworzone rozwiązania muszą uwzględniać zasady przetwarzania danych osobowych wynikające z art. 5 RODO**. Należy zwrócić uwagę na zakres danych, których nie należy wprowadzać do narzędzi AI (wzgląd na zasadę minimalizacji danych – art. 5 ust. 1 lit. c RODO). Z projektu wynika, że: „Nie należy wprowadzać do takich narzędzi informacji lub dokumentów, które: są niejawne lub zawierają dane wrażliwe; zawierają informacje urzędowe będące w fazie przygotowawczej, a tym samym nie przeznaczone do upublicznienia; naruszają przepisy o ochronie danych osobowych (strona 3 dokumentu). W tym miejscu należy zaakcentować ryzyka, jakie wiążą się z wykorzystywaniem danych osobowych w narzędziach AI w treściach tzw. krytycznych. Narzędzia AI usprawniające pracę powinny być wykorzystywane nie w generowaniu

[3] Uzasadnionym jest dokonanie oceny skutków dla ochrony danych – zgodnie z art. 35 ust. 10 rozporządzenia 2016/679 – już w ramach oceny skutków regulacji w związku z przyjmowaniem określonej podstawy prawnej przetwarzania danych, co przy dokonaniu prawidłowej oceny i wypracowaniu przepisów szczególnych uwzględniających stosowanie ogólnego rozporządzenia o ochronie danych może zastąpić dokonywanie takiej oceny przez podmioty stosujące / wykonujące następnie tak ustalone przepisy.

całych materiałów bez udziału nadzoru człowieka, lecz mogą stanowić uzupełnienie pracy ludzkiej. Powinny być wykorzystywane w obszarach „mniej twórczych”, gdzie ewentualne ryzyko nie będzie odczuwalne tak, jak w kluczowych projektach (np. zawierających duże bazy danych, w tym danych o charakterze osobowym). Wszelkie obszary pracy związane z wykorzystywaniem narzędzi AI powinny być uprzednio zidentyfikowane przez administratora i poddane szczególnej analizie, w tym pod kątem zakresu danych osobowych. Zwrócić uwagę należy, że narzędzia AI usprawniające pracę nie powinny być wykorzystywane w sprawach skomplikowanych, wymagających indywidualnego podejścia. Ich rola to przede wszystkim pomoc w sprawach rutynowych (np. związanych m.in. z automatyczną obsługą spraw w urzędach). Należy pamiętać, że narzędzie to nie jest nieomylne, bowiem opiera się przede wszystkim na prawdopodobieństwie, a generowane treści mogą zawierać błędy, co może wywoływać negatywne konsekwencje dla osoby, której dane są przetwarzane przez generatywną sztuczną inteligencję.

W analizie zagrożeń dla ochrony danych przy ostatecznym wypracowywaniu przedmiotowego dokumentu na pewno pomocne będzie wsparcie specjalistów z zakresu ochrony danych jakimi są inspektorzy ochrony danych, których zadaniem jest m.in. monitoring i kontrola stosowanych u administratora procedur, oświadczeń woli, sposobu realizacji uprawnień podmiotów danych. Należy mieć na uwadze, że administratorzy są przede wszystkim związani przepisami obowiązującego prawa. Powstaje zatem pytanie czy oprócz opiniowanych rekomendacji planowane są prace legislacyjne w przedmiotowym zakresie. Jeśli tak, Prezes UODO deklaruje swoje wsparcie w tym zakresie.

Łączę wyrazy szacunku,
Mirosław Wróblewski
Prezes Urzędu Ochrony Danych Osobowych
/ - dokument w postaci elektronicznej podpisany
kwalifikowanym podpisem elektronicznym/