Warszawa, dn. 07.05.2025 r.

Korzystanie z narzędzi AI – gdzie w tym dane osobowe?

Wstęp

Stosowanie rozwiązań sztucznej inteligencji (AI) wiąże się z wieloma wyzwaniami w kontekście ochrony danych osobowych, co sprawia, że przepisy GDPR (Ogólne Rozporządzenie o Ochronie Danych Osobowych) wymagają szczególnej uwagi. Oto kilka kluczowych powodów, dlaczego AI wymaga szczególnej ochrony pod kątem przepisów GDPR:

1. **Przetwarzanie dużych ilości danych osobowych**: AI, szczególnie w kontekście uczenia maszynowego często opiera się na ogromnych zbiorach danych. Te informacje mogą zawierać dane osobowe, a ich przetwarzanie na dużą skalę wymaga zapewnienia zgodności z przepisami GDPR, zwłaszcza w zakresie przechowywania, przetwarzania i wykorzystywania danych.
2. **Brak transparentności:** Sztuczna inteligencja, zwłaszcza algorytmy i sposoby ich uczenia mogą być trudne do zrozumienia i wyjaśnienia. Zgodnie z RODO osoby, których dane są przetwarzane, mają prawo do informacji o tym, w jaki sposób ich dane są wykorzystywane, a także do zrozumienia decyzji podejmowanych przez systemy automatyczne. W przypadku AI może to stanowić wyzwanie, ponieważ algorytmy często działają w sposób trudny do zrozumienia dla człowieka.
3. **Zautomatyzowane podejmowanie decyzji**: AI jest wykorzystywana do podejmowania decyzji zautomatyzowanych bez ingerencji ludzkiej, które mogą mieć istotny wpływ na życie osób, np. w obszarze kredytów, rekrutacji, czy decyzji administracyjnych. Zgodnie z RODO osoby te mają prawo do zautomatyzowanego podejmowania decyzji, w tym do niepodlegania decyzjom opartym wyłącznie na automatycznym przetwarzaniu, które wywołują skutki prawne lub w podobny sposób istotnie na nie wpływają. To wymaga stosowania specjalnych środków ochrony, takich jak możliwość interwencji człowieka, złożenie sprzeciwu.
4. **Zasada minimalizacji danych**: RODO wymaga, aby administratorzy i podmioty przetwarzające zbierały i przetwarzały tylko te dane, które są niezbędne do realizacji celu. AI, zwłaszcza w kontekście analizy danych, może generować lub wymagać gromadzenia danych, które mogą wykraczać poza zakres tego, co jest konieczne do realizacji celów przetwarzania. Istnieje więc ryzyko nadmiarowego gromadzenia danych osobowych, co może naruszać zasadę minimalizacji danych.
5. **Różnorodność i stereotypy w danych**: AI może nieświadomie utrwalać uprzedzenia lub dyskryminację, jeśli dane, na których jest szkolona, zawierają niezamierzone uprzedzenia - zwłaszcza jeśli system AI podejmuje decyzje, które mogą prowadzić do nierównego traktowania osób na podstawie danych osobowych, takich jak rasa, płeć czy wiek.
6. **Bezpieczeństwo danych**: Przetwarzanie danych osobowych przez systemy AI wiąże się z koniecznością zapewnienia wysokiego poziomu bezpieczeństwa. RODO nakłada

na organizacje obowiązek stosowania odpowiednich środków technicznych i organizacyjnych w celu ochrony danych przed nieuprawnionym dostępem, utratą lub zniszczeniem. AI, ze względu na swoją złożoność i zależność od danych, stanowi szczególne wyzwanie w tym zakresie.

7. **Prawa osób, których dane dotyczą**: Zgodnie z RODO, osoby, których dane są przetwarzane, mają szereg praw, w tym prawo dostępu, sprostowania, usunięcia, a także prawo do przenoszenia danych i sprzeciwu wobec przetwarzania. Zastosowanie AI do przetwarzania danych osobowych wymaga, aby organizacje miały odpowiednie mechanizmy umożliwiające realizację tych praw, co może być skomplikowane w kontekście dużych zbiorów danych przetwarzanych przez AI.

W tym kontekście, prawnicy, działy prawne, Inspektorzy Ochrony Danych mają coraz więcej pytań i wątpliwości w zakresie stosowania narzędzi AI przez organizacje, w których pracują. W związku z powyższym Prezes Urzędu Ochrony Danych przygotował nieoficjalne tłumaczenie opinii Europejskiej Rady Ochrony Danych w sprawie wykorzystania danych osobowych do opracowania i wdrażania modeli sztucznej inteligencji.

Spojrzenie EROD na modele AI

Opinia ta szczegółowo analizuje kwestie związane z anonimowością modeli AI, wykorzystywaniem prawnie uzasadnionego interesu jako podstawy prawnej do przetwarzania danych oraz skutkami przetwarzania danych osobowych niezgodnie z prawem. Dokument stanowi istotny wkład w dyskusję na temat regulacji dotyczących sztucznej inteligencji, szczególnie w kontekście ochrony danych osobowych i dostarcza wskazówek dla organów ochrony danych oraz innych zainteresowanych stron.

Wskazana opinii skupia się na kilku aspektów dotyczących zgodności z GDPR, w niniejszym artykule chciałbym skupić się wskazówkach EROD dla organów nadzorczych w zakresie oceny przez organy nadzorcze zgodności modelu AI z przepisami GDPR.

Europejska Rada Ochrony Danych (EROD) w swojej najnowszej opinii[1] analizuje, jak powinny wyglądać procesy oceny anonimowości modeli sztucznej inteligencji (AI), szczególnie w kontekście ochrony danych osobowych. Zdaniem EROD-u, kluczowe jest, aby administratorzy wykazali, że projekt AI został rzetelnie zaprojektowany, udokumentowany i przetestowany pod kątem odporności na identyfikację danych. Organy nadzorcze powinny sprawdzać, czy model powstał zgodnie z zaplanowanymi zasadami inżynieryjnymi i czy przeprowadzono odpowiednie audyty, w tym analizy kodu i oceny ryzyka ponownej identyfikacji. Równie istotne są testy odporności na współczesne ataki.

Zgodnie z RODO, każda operacja przetwarzania – także szkolenie modeli AI – musi być należycie udokumentowana. Brak takiej dokumentacji może świadczyć o niespełnieniu wymogów rozliczalności wynikających z art. 5 ust. 2 RODO. Europejska Rada Ochrony Danych (EROD) w swojej opinii jasno wskazuje, że kompletna i przejrzysta dokumentacja modeli sztucznej inteligencji (AI) jest niezbędna do wykazania zgodności z RODO, zwłaszcza gdy twierdzi się, że dane zostały skutecznie zanonimizowane. Organy nadzorcze powinny

[1] https://uodo.gov.pl/pl/138/3657

szczegółowo weryfikować, czy administratorzy gromadzą i przechowują wszystkie wymagane informacje dotyczące projektowania, testowania oraz oceny ryzyk związanych z modelem AI.
Przede wszystkim dokumentacja powinna zawierać wyniki ocen skutków dla ochrony danych (DPIA), opinie inspektora ochrony danych (IOD), jeśli został wyznaczony, oraz szczegóły środków technicznych i organizacyjnych zastosowanych w celu ograniczenia możliwości identyfikacji osób.
Co istotne, EROD oczekuje, że dokumentacja ta obejmie cały cykl życia modelu — od projektowania po wdrożenie — oraz będzie dostępna nie tylko dla organów nadzorczych, ale także dla osób, których dane mogą być przetwarzane.
Opinia EROD podkreśla, że sama deklaracja o anonimowości modelu AI nie wystarcza. Niezbędne są rzetelne testy, solidne zarządzanie projektem i kompletna dokumentacja potwierdzająca, że dane osobowe zostały skutecznie zabezpieczone lub usunięte. To kolejny sygnał, że ochrona danych osobowych musi być integralnym elementem rozwoju sztucznej inteligencji.

Wnioski dla administratorów danych korzystających z narzędzi AI
Na podstawie powyższego można pokusić się o pewne wnioski dla administratorów/organizacji/spółek, które w swojej codziennej pracy chcą wykorzystywać narzędzia AI – niekoniecznie będąc odpowiedzialnym za projektowanie i wdrożenie narzędzia. Przed wyborem narzędzia lub dostawcy narzędzi AI warto zweryfikować u potencjalnego dostawcy:

a) Skąd dostawca pozyskał dane użyte do trenowania modelu AI,
b) Czy zostały przeprowadzone testy bezpieczeństwa mające na celu uniknięcie zewnętrznych lub wewnętrznych ataków na model i dane, które stanowią przedmiot trenowania modelu.
c) Czy została przeprowadzona ocena skutków przetwarzania dla danych osobowych.
d) Jeżeli narzędzie AI może prowadzić do istotnego wpływu na prawa osób (np. profilowanie, decyzje automatyczne), powinieneś rozważyć przeprowadzenie własnej oceny skutków dla ochrony danych – nawet jeśli dostawca zapewnia, że jego model jest bezpieczny.

Samo zapewnienie, że „model jest zanonimizowany" lub „zgodny z RODO" nie zwalnia Cię z odpowiedzialności. EROD podkreśla, że organy nadzorcze mogą zakwestionować takie twierdzenia, jeśli nie są poparte rzetelną dokumentacją. W razie kontroli to Ty – jako administrator – musisz być w stanie udowodnić zgodność z przepisami.

Maciej Łukaszewicz – radca prawny, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.