

Warszawa, dn. 22.10.2025 r.

Rekrutacja pod nadzorem algorytmów AI: obowiązki i ryzyka dla działów HR

Wstęp

Wyobraź sobie scenariusz: wysyłasz CV do wymarzonej firmy. Po kilku minutach chatbot zaprasza Cię na wideorozmowę kwalifikacyjną. Przez 20 minut odpowiadasz na pytania automatu, który analizuje nie tylko Twoje odpowiedzi, ale także ton głosu i mimikę twarzy. Kilka dni później otrzymujesz automatyczną wiadomość z podziękowaniem za udział. Co jeśli powiem Ci, że o Twoim odrzuceniu zdecydował algorytm, a Ty nawet nie zostałeś o tym poinformowany? Brzmi jak science fiction? To codzienność wielu procesów rekrutacyjnych. Tyle że taka praktyka właśnie stała się nie tylko nieetyczna, ale przede wszystkim – nielegalna.

Wymogi dla systemu wysokiego ryzyka na gruncie AI Act

Działy HR toną w CV. Selekcja kandydatów to żmudny proces, dlatego narzędzia oparte na sztucznej inteligencji (AI) – automatycznie skanujące aplikacje, oceniające kompetencje czy nawet prowadzące wstępne rozmowy – wydają się zbawieniem.

Unijny Akt o Sztucznej Inteligencji (AI Act)¹, którego zapisy zaczynają obowiązywać, formalnie klasyfikuje systemy AI używane do rekrutacji i zarządzania pracownikami jako „systemy wysokiego ryzyka” (high-risk). To już dawno przestał być problem wyłącznie działu IT. Stało się to strategicznym wyzwaniem dla HR, zarządu i Inspektora Ochrony Danych (IOD). Załącznik nr III do AI Actu w punkcie 4 wskazuje, że za system wysokiego ryzyka mogą zostać uznane: systemy AI przeznaczone do wykorzystywania do celów rekrutacji lub wyboru osób fizycznych, w szczególności do celów umieszczania ukierunkowanych ogłoszeń o pracę, analizowania i filtrowania podań o pracę oraz do oceny kandydatów. W zależności od tego, czy jest się producentem, dostawcą czy podmiotem stosującym system wysokiego ryzyka AI obowiązków zapewnienia zgodności jest wiele.

Aby zapewnić zgodność z prawem i bezpieczeństwo, podmioty te muszą przestrzegać kilku kluczowych zasad. Przede wszystkim, użytkownicy są zobowiązani do eksploataowania systemu ściśle według instrukcji i dokumentacji dostarczonej przez dostawcę. Jeśli podmiot stosujący ma kontrolę nad danymi wejściowymi wprowadzanymi do systemu, spoczywa na nim odpowiedzialność za zapewnienie, że dane te są adekwatne i odpowiednie do zamierzonego celu systemu.

Nieodzownym elementem jest bieżące monitorowanie działania systemu oraz zapewnienie skutecznego nadzoru ludzkiego nad jego pracą, aby móc interweniować lub korygować ewentualne błędy. Wiąże się z tym również obowiązek przechowywania automatycznie generowanych rejestrów zdarzeń (logów), o ile użytkownik ma nad nimi kontrolę, co pozwala na śledzenie operacji i analizę incydentów.

¹ https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202401689

W przypadku podejrzenia wystąpienia poważnego incydentu związanego z działaniem AI, użytkownik musi niezwłocznie poinformować o tym fakcie dostawcę lub dystrybutora systemu.

Należy również pamiętać, że w sytuacji, gdy system wysokiego ryzyka przetwarza dane osobowe, na podmiocie stosującym ciąży dodatkowy wymóg przeprowadzenia oceny skutków dla ochrony danych (DPIA), zgodnie z regulacjami RODO (GDPR).

Przykład niewłaściwego zastosowania systemów AI w procesie rekrutacyjnym

Wyobraźmy sobie firmę, która kupuje nowoczesne narzędzie AI do selekcji CV. Aby je "nauczyć", dział HR zasila system danymi historycznymi – profilami pracowników, którzy najlepiej sprawdzili się w firmie w ciągu ostatnich 10 lat. Problem? Przez ostatnią dekadę firma (świadomie lub nie) zatrudniała głównie mężczyzn po 30. roku życia, absolwentów dwóch konkretnych uczelni. Co robi AI? Algorytm to potężne narzędzie statystyczne. Błyskawicznie "odkrywa" wzorzec i uczy się, że "dobry" kandydat to mężczyzna w określonym wieku, z konkretnym dyplomem. W rezultacie system zaczyna automatycznie odrzucać aplikacje wybitnie kompetentnych kobiet, osób młodszych lub absolwentów innych, równie dobrych uczelni.

Algorytm nie stał się "zły" – on po prostu perfekcyjnie powielił błędy i uprzedzenia ludzi, którzy go karmili danymi. Jakie potencjalne ryzyka powoduje taki stan faktyczny:

- Naruszenie RODO: Przetwarzanie danych bez podstawy prawnej i w sposób nadmiarowy.
- Naruszenie AI Act: Używanie systemu wysokiego ryzyka, który łamie prawa podstawowe (zakaz dyskryminacji).
- Naruszenie Kodeksu Pracy: Złamanie fundamentalnej zasady równego traktowania w zatrudnieniu.

Wstępny plan działania zgodności

Aby dostosować się do nowych regulacji, dział HR musi przede wszystkim przeprowadzić gruntowny audyt używanych narzędzi. Kluczowe jest sprawdzenie, które z posiadanych systemów – czy to platformy ATS do zarządzania kandydatami, chatboty rekrutacyjne, czy narzędzia do analizy wideorozmów – faktycznie wykorzystują komponenty AI do automatycznej oceny lub selekcji kandydatów.

Po zidentyfikowaniu tych systemów kolejnym krokiem jest natychmiastowy kontakt z ich dostawcami. Należy zadać im wprost fundamentalne pytanie: "Czy ten system jest systemem wysokiego ryzyka w rozumieniu AI Act?". Firma jako użytkownik musi bezwzględnie zażądać od partnera technologicznego pełnej dokumentacji technicznej oraz deklaracji zgodności, aby potwierdzić legalność narzędzia.

Posiadanie dokumentacji od dostawcy to jednak dopiero początek. Kluczową odpowiedzialnością użytkownika, czyli działu HR, jest przeprowadzenie własnych, dogłębnych analiz ryzyka, najlepiej we współpracy z Inspektorem Ochrony Danych (IOD). Nie wystarczy już tylko ocena skutków dla ochrony danych (DPIA) wymagana przez RODO, która skupia się na prywatności.

AI Act wymusza dodatkowo przeprowadzenie oceny wpływu na prawa podstawowe (FRIA), która bada, czy system nie dyskryminuje i nie narusza godności kandydatów. Obie analizy muszą dokumentować ryzyka i opracowywać konkretne sposoby ich mitygacji (zmniejszania). Warto przy tym doprecyzować, że nie każdy system AI do rekrutacji będzie uznany za system wysokiego ryzyka. Sam AI Act (Akt o Sztucznej Inteligencji) jest tu bardzo precyzyjny: system nie zostanie tak sklasyfikowany, jeśli pełni on jedynie funkcje pomocnicze, administracyjne lub przygotowawcze i nie ma realnego wpływu na ostateczną decyzję. Systemy stają się „wysokiego ryzyka” (zgodnie z Załącznikiem III, pkt 4) dopiero wtedy, gdy są przeznaczone do filtrowania aplikacji, oceny kandydatów lub podejmowania decyzji (bądź istotnego wpływania na nie).

Równie istotna staje się pełna transparentność wobec kandydatów. Działy HR muszą dokonać natychmiastowego przeglądu i aktualizacji wszystkich klauzul informacyjnych RODO stosowanych w procesach rekrutacji. Nie wystarczy już ogólny zapis. Nowe klauzule muszą zawierać jasne, proste i zrozumiałe informacje o fakcie stosowania sztucznej inteligencji, wyjaśniać podstawową logikę jej działania oraz informować o prawie kandydata do uzyskania interwencji ludzkiej.

To prawo do interwencji ludzkiej jest absolutną podstawą zgodności i etyki całego procesu. Konieczne jest wdrożenie mechanizmów realnego nadzoru ludzkiego. Oznacza to, że żadna kluczowa decyzja, a w szczególności decyzja o odrzuceniu kandydata, nie może zapadać w pełni automatycznie. Każdy taki werdykt wygenerowany przez system AI musi podlegać rzeczywistej weryfikacji i ostatecznej akceptacji przez człowieka-rekrutera.

Sztuczna inteligencja pozostaje potężnym narzędziem, które może znacząco usprawnić rekrutację, ale musi pozostać tylko narzędziem – pomocnikiem, a nie autonomicznym sędzią. AI Act definitywnie kończy erę "Dzikiego Zachodu" w technologiach HR i głośno przypomina, że w centrum każdego procesu musi stać człowiek i jego niezbywalne prawa.

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