



**PREZES  
URZĘDU OCHRONY  
DANYCH OSOBOWYCH**

**Mirosław Wróblewski**

Warszawa,

**DPNT.0623.18.2026**

**Pani  
dr Agnieszka Dziemianowicz-Bąk  
Ministra Rodziny, Pracy i Polityki  
Społecznej**

**Ministerstwo Rodziny, Pracy i  
Polityki Społecznej**

Szanowna Pani Ministro,

w ostatnim czasie do Urzędu Ochrony Danych Osobowych wpływają sygnały dotyczące **wprowadzania przez pracodawców różnych rozwiązań związanych z wykorzystywaniem sztucznej inteligencji w procesach rekrutacyjnych, w tym wykorzystywania w tym celu danych szczególnych kategorii** (art. 9 rozporządzenia 2016/679<sup>1</sup>)<sup>2</sup>.

---

<sup>1</sup> 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.), dalej: „rozporządzenie 2016/679”.

<sup>2</sup> W przypadku przetwarzania szczególnych kategorii danych przepisy prawa powinny być konstruowane z uwzględnieniem konstytucyjnych zasad praworządności i źródeł prawa (art. 7 i art. 87 Konstytucji RP), jak i art. 6 ust. 2 – 3 oraz art. 9, w tym jego ust. 4 rozporządzenia 2016/679. Innymi słowy - przepisy prawa regulujące tego rodzaju przetwarzanie danych osobowych – zgodnie ze wskazanymi przepisami rozporządzenia 2016/679 – wymagają odpowiedniego zakresu regulacji co do określenia praw i obowiązków związanych z przetwarzaniem danych osobowych w przepisach powszechnie obowiązujących oraz co do celu i sposobu przetwarzania danych. Uzasadnionym jest zapewnienie zupełności regulacji poprzez wskazanie w przepisach: ogólnych warunków zgodności z prawem przetwarzania przez administratora; rodzaju danych podlegających przetwarzaniu; osób, których dane dotyczą; podmiotów, którym można ujawnić dane osobowe; celów, w których można je ujawnić; ograniczenia celu; okresów przechowywania oraz operacji i procedur przetwarzania, w tym środków zapewniających zgodność z prawem i rzetelność przetwarzania - prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu (art. 6 ust. 3 rozporządzenia 2016/679). Przetwarzanie danych z kategorii szczególnie chronionych wymaga natomiast spełnienia warunków wynikających z art. 9 ust. 2-4 rozporządzenia 2016/679.

Dlatego też, zwracam się do Pani Ministry z uprzejmą prośbą o informacje **czy w resorcie planowane/przygotowywane są zmiany legislacyjne związane z wprowadzeniem dodatkowych gwarancji w przepisach krajowych z zakresu prawa pracy** (mając na względzie **art. 88 oraz art. 9 ust. 3 i 4 rozporządzenia 2016/679**), z uwagi na ryzyka nie tylko związane z ochroną danych osobowych, ale i naruszeniem innych praw podstawowych, w tym z **dyskryminacją kandydatów do pracy oraz pracowników**.

1. Zgodnie z art. 18<sup>3a</sup> ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2025 r. poz. 277) pracownicy powinni być traktowani równo niezależnie od płci, wieku, niepełnosprawności, pochodzenia, wyznania, przekonań politycznych czy orientacji seksualnej. Natomiast istnieje wysokie prawdopodobieństwo, że **systemy sztucznej inteligencji w sektorze zatrudnienia** mogą utrzymywać istniejące uprzedzenia obecne w danych treningowych, co w praktyce będzie powodować dyskryminację algorytmiczną. **Art. 22 Kodeksu pracy** zawiera zamknięty katalog danych, których pracodawca może żądać od kandydata do pracy, ale istnieje poważne ryzyko, że systemy sztucznej inteligencji mogą analizować znacznie więcej informacji/danych, w tym danych szczególnej kategorii.

2. W kontekście powyższego, szczególne znaczenie z punktu widzenia ochrony danych osobowych ma **art. 22 rozporządzenia 2016/679**, który stanowi, że – co do zasady – osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na **zautomatyzowanym przetwarzaniu, w tym profilowaniu**, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. Odstępstwa od tej zasady są możliwe po spełnieniu jednego z warunków ustanowionych w art. 22 ust. 2 rozporządzenia 2016/679, **m. in. gdy decyzja ta jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą**. Z przepisu tego jasno wynika, że jeżeli profilowanie ma być stosowane czy dozwolone na podstawie przepisów prawa, to **przepisy te powinny gwarantować właściwe środki ochrony praw osób, których dane dotyczą**.

Szczególna regulacja w kontekście profilowania została przyjęta np. w art. 105a ust. 1a ustawy Prawo bankowe (Dz. U. z 2026 r. poz. 38 ze zm.). Przepis ten określa **cele przetwarzania danych, zakres danych oraz zawiera gwarancje ochrony praw i wolności osób fizycznych**, wobec których ma zostać wydana decyzja oparta wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu i stanowi o: prawie do otrzymania stosownych wyjaśnień co do podstaw podjętej decyzji, prawie do uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji oraz prawie do wyrażenia własnego stanowiska.

3. **Zasady klasyfikacji systemów wysokiego ryzyka** ujęte w art. 6 oraz w Załączniku III aktu w sprawie sztucznej inteligencji<sup>3</sup> (AI Act) sprawiają, że **systemy**

---

<sup>3</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144

**sztucznej inteligencji stosowane w rekrutacji zostały ujęte jako systemy wysokiego ryzyka.** Oznacza to, że ich wdrożenie i wykorzystywanie wymaga spełnienia szeregu wymogów prawnych dotyczących bezpieczeństwa, przejrzystości, nadzoru ludzkiego oraz ochrony praw podstawowych, w tym danych osobowych kandydatów do pracy, w celu zapobiegania dyskryminacji i błędnym decyzjom podejmowanym przez algorytmy. Zgodnie z **art. 86 ust. 1 AI Act**: „Każda osoba, na którą AI ma wpływ, będąca przedmiotem decyzji podjętej przez podmiot stosujący na podstawie wyników systemu AI wysokiego ryzyka wymienionego w załączniku III, z wyjątkiem systemów wymienionych w pkt 2 tego załącznika, która to decyzja wywołuje skutki prawne lub w podobny sposób oddziałuje na tę osobę na tyle znacząco, że uważa ona, iż ma to niepożądany wpływ na jej zdrowie, bezpieczeństwo lub prawa podstawowe, ma prawo uzyskania od podmiotu stosującego jasnego i merytorycznego wyjaśnienia roli tego systemu AI w procedurze podejmowania decyzji oraz głównych elementów podjętej decyzji”.

4. Wprowadzenie przez projektodawcę rozwiązań uwzględniających wykorzystywanie systemów sztucznej inteligencji w sektorze zatrudnienia powinno być poprzedzone przeprowadzoną **oceną skutków dla ochrony danych**<sup>4</sup> ze względu na rodzaj przetwarzania, w szczególności z użyciem nowych technologii, którego charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować **wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, co uzasadnia również **przeprowadzenie testu prywatności**<sup>5</sup>.

Przeprowadzenie przez projektodawcę oceny skutków dla ochrony danych ułatwia zbadanie ryzyk oraz wykazanie zgodności z zasadami dotyczącymi przetwarzania danych osobowych wynikającymi z art. 5 rozporządzenia 2016/679 oraz spełnienia warunków przetwarzania danych osobowych określonych w art. 6 ust. 3 tego rozporządzenia, a także pozwala ocenić czy przyjmowane rozwiązania przewidują jednocześnie odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą.

Należy podkreślić, że z **art. 27 aktu w sprawie sztucznej inteligencji wynika odrębny obowiązek dokonania oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych (FRIA)**. Motyw 96 AI Act podkreśla, że taka ocena ma na celu uzupełnienie oceny ochrony danych, a nie jej zastąpienie. Transparentne systemy AI

---

oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) Tekst mający znaczenie dla EOG (Dz. U. UE. L. z 2024 r. poz. 1689).

<sup>4</sup> Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

<sup>5</sup> Zgodnie z art. 25 ust. 1 RODO uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

działające w oparciu o szczegółowe przepisy wypracowane przez projektodawcę gwarantować powinny dostęp do dokładnych informacji o działaniu modelu sztucznej inteligencji oraz do rzetelnego wyjaśnienia, obejmującego zarówno procesy techniczne systemu, jak i uzasadnienie decyzji dokonywanej przez system sztucznej inteligencji czy przy jego wsparciu. Wykonawcy norm powinni być bowiem świadomi, że dana interakcja odbywa się ze sztuczną inteligencją, a regulacja o odpowiedniej randze (ustawa) powinna określać cele, których realizacji służy, jakim podmiotom przypisany zostanie status administratora danych, jak również jakie gwarancje ochrony praw i wolności osób zostaną określone jej przepisami.

**5. Obowiązki podmiotów stosujących systemy AI wysokiego ryzyka zostały określone w art. 26 aktu w sprawie sztucznej inteligencji.**

Systemy AI wysokiego ryzyka muszą spełnić wymogi prawne dotyczące m.in.:

- utrzymywania systemu zarządzania ryzykiem (art. 9),
- danych i zarządzania danymi (art. 10),
- dokumentacji technicznej (art. 11),
- rejestrowania zdarzeń podczas działania systemów sztucznej inteligencji (art. 12),
- przejrzystości i dostarczania informacji użytkownikom (art. 13),
- nadzoru ze strony człowieka (art. 14),
- solidności, dokładności i cyberbezpieczeństwa (art. 15 aktu w sprawie sztucznej inteligencji).

**Te wszystkie gwarancje powinny mieć odzwierciedlenie w przepisach ustawowych.**

Jeżeli podjęte zostaną odpowiednie prace legislacyjne we wskazanym obszarze, Prezes Urzędu Ochrony Danych Osobowych deklaruje swoje eksperckie wsparcie w analizie propozycji przepisów prawa pod kątem ich zgodności z rozporządzeniem 2016/679.

Łączę wyrazy szacunku,

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych

/-dokument w postaci elektronicznej  
podpisany kwalifikowanym  
podpisem elektronicznym/