

AI Act a polska kancelaria

Co nowe unijne rozporządzenie o sztucznej inteligencji realnie oznacza dla prawnika korzystającego z narzędzi AI

Materiał dla adwokatów i radców prawnych — kancelarie solo, małe i średnie

Wstęp: kancelaria jako podmiot stosujący — własna rola w nowym porządku prawnym

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r., powszechnie nazywane Aktem o sztucznej inteligencji lub AI Act, obowiązuje już jako prawo unijne — a jego kolejne warstwy wchodzi w życie etapami. Prawnicy, do których docierają skróty „AI Act”, często reagują jednym z dwóch sposobów: albo uznają, że to regulacja adresowana do dużych firm technologicznych i ich nie dotyczy, albo obawiają się, że nowe obowiązki są nieproporcjonalne do faktycznego korzystania z AI w codziennej pracy.

Oba podejścia mijają się z prawdą.

Teza tego przewodnika jest prosta: **dla zdecydowanej większości polskich kancelarii korzystających z narzędzi AI najcięższe obowiązki Aktu o AI spoczywają na dostawcach systemów AI — nie na kancelarii**. Kancelaria, która kupuje dostęp do narzędzia AI i stosuje je w swojej pracy, działa w roli **podmiotu stosującego** (*deployer*), nie **dostawcy** (*provider*). To rozróżnienie jest fundamentalne: inny jest zakres obowiązków, inna odpowiedzialność, inne terminy.

Ale kancelaria nie jest bez obowiązków. Ma własne — mniejsze, lecz realne. I ma silny interes w tym, żeby dostawca, którego wybiera, sam spełniał wymogi Aktu: gdy dostawca ich nie spełnia, ryzyko ostatecznie łąduje na biurku prawnika — przez RODO, tajemnicę zawodową i odpowiedzialność dyscyplinarną.

Co to jest AI Act i jak wchodzi w życie

Rozporządzenie (UE) 2024/1689 zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej w lipcu 2024 r. i weszło w życie dnia 1 sierpnia 2024 r. Jako rozporządzenie unijne obowiązuje bezpośrednio we wszystkich państwach członkowskich — bez potrzeby implementacji do prawa krajowego.

Akt o AI nie stosuje się jednak w całości od razu. Zgodnie z art. 113 Rozporządzenia (UE) 2024/1689 przewidziano **etapowe wejście w życie poszczególnych przepisów**, liczone od daty wejścia w życie rozporządzenia. Mechanizm jest następujący:

- **Najwcześniej** zaczęły obowiązywać przepisy dotyczące **zakazanych praktyk AI** — Rozdział II, w tym art. 5 — około sześciu miesięcy od dnia wejścia w życie. To zakazy absolutne: systemy AI

spełniające kryteria tego rozdziału nie mogą być wdrażane ani stosowane na terytorium UE od tego momentu.

- **W dalszej kolejności** weszły w życie przepisy dotyczące **modeli AI ogólnego przeznaczenia** (*General Purpose AI models*, GPAI) — stosownie do art. 113 około dwunastu miesięcy od wejścia w życie.
- **Zasadnicze przepisy** — obejmujące klasyfikację systemów wysokiego ryzyka, obowiązki dostawców i podmiotów stosujących, wymóg kompetencji w zakresie AI oraz transparentności — stosuje się od około **dwudziestu czterech miesięcy** od daty wejścia w życie, tj. zasadniczo od połowy 2026 r.
- Dla określonych kategorii systemów AI ujętych w Załączniku I (m.in. urządzenia medyczne, systemy bezpieczeństwa stanowiące elementy produktów objętych unijnymi przepisami harmonizacyjnymi) przewidziano **wydlużony termin trzydziestu sześciu miesięcy**.

Dla kancelarii praktyczne znaczenie ma przede wszystkim etap dwudziestoczteromiesięczny, który obejmuje obowiązki podmiotu stosującego, wymóg kompetencji w zakresie AI i większość reguł klasyfikacji ryzyka. Kancelarie korzystające z narzędzi AI już teraz powinny traktować ten moment jako datę, do której wdrożenie wewnętrznych procedur musi być zakończone.

Cztery poziomy ryzyka — mapa dla prawnika

Akt o AI klasyfikuje systemy AI według czterech poziomów ryzyka. Klasyfikacja decyduje o tym, jakie obowiązki ciążą na dostawcy — a pośrednio, czego kancelaria może oczekiwać od dostawcy, którego narzędzia używa.

Poziom 1: Praktyki zakazane (art. 5 Rozporządzenia (UE) 2024/1689)

Absolutne zakazy, niezależne od woli stron. Dotyczą m.in. systemów AI manipulujących ludźmi metodami podprogowymi wpływającymi na ich zachowanie wbrew ich woli, systemów masowego nadzoru biometrycznego w przestrzeni publicznej do celów egzekwowania prawa, systemów oceniania obywateli przez organy publiczne na podstawie ich zachowań społecznych, a także systemów identyfikacji emocji w miejscu pracy lub placówkach edukacyjnych.

Dla kancelarii: korzystanie z systemu AI spełniającego kryteria z art. 5 jest zabronione niezależnie od roli podmiotu. Przed wdrożeniem każdego narzędzia warto sprawdzić, czy nie zawiera ono funkcjonalności mieszczących się w tych zakazach.

Poziom 2: Systemy wysokiego ryzyka (art. 6 i Załącznik III)

Systemy AI, których zastosowanie może istotnie wpływać na prawa i interesy ludzi. Załącznik III wymienia konkretne kategorie, spośród których dla pracy prawniczej szczególne znaczenie mogą mieć: systemy AI używane w wymiarze sprawiedliwości do oceny dowodów lub pomocniczo przy wyrokowaniu, systemy oceny zdolności kredytowej, systemy decydujące o dostępie do usług lub zasobów o kluczowym znaczeniu, systemy oceny ryzyka recydywy stosowane przez organy wymiaru sprawiedliwości.

Dla kancelarii: użycie systemu wpadającego w którąś z tych kategorii — np. narzędzia scoringowego oceniającego ryzyko procesowe klienta w sposób wywierający bezpośredni skutek dla jego sprawy — uruchamia rozbudowany reżim obowiązków z art. 26 Rozporządzenia (UE) 2024/1689. W praktyce zdecydowana większość narzędzi do redagowania pism, badania orzecznictwa czy streszczania dokumentów nie spełnia kryteriów systemów wysokiego ryzyka — ale każde konkretne zastosowanie wymaga odrębnej oceny.

Poziom 3: Systemy ograniczonego ryzyka (art. 50)

Systemy, przy których kluczowe jest zapewnienie przejrzystości wobec użytkownika. Obowiązek informowania dotyczy przede wszystkim chatbotów konwersacyjnych oraz systemów generujących treść audiowizualną (*deepfake*). Osoba kontaktująca się z systemem musi wiedzieć, że ma do czynienia z AI.

Dla kancelarii: jeżeli kancelaria wdraża chatbota AI w kontakcie z klientem (np. formularz wstępnej konsultacji lub automatyczna obsługa korespondencji), podmiot stosujący jest zobowiązany do wyraźnego poinformowania o charakterze AI. Obowiązek ten wynika z art. 50 i nie można go uchylić regulaminem ani domniemaną świadomością klienta.

Poziom 4: Minimalne ryzyko

Zdecydowana większość narzędzi AI dla profesjonalistów — narzędzia do analizy tekstu, redagowania dokumentów, tłumaczeń, wyszukiwania orzecznictwa, transkrypcji nagrań. Brak szczegółowych obowiązków z samego Aktu poza wymogiem kompetencji z art. 4. W pełni obowiązują RODO i tajemnica zawodowa.

Gdzie w tym wszystkim jest kancelaria

Dostawca czy podmiot stosujący?

Kluczowe rozróżnienie Aktu o AI przebiega między dwiema rolami.

Dostawca (art. 3 pkt 3 Rozporządzenia (UE) 2024/1689) to podmiot, który opracowuje system AI lub model AI ogólnego przeznaczenia i wprowadza go do obrotu lub oddaje do użytku pod własną nazwą lub znakiem towarowym. Dostawca ponosi ciężar rejestracji systemu, dokumentacji technicznej, testów, zarządzania ryzykiem i — dla systemów wysokiego ryzyka — oznakowań CE.

Podmiot stosujący (art. 3 pkt 4) to podmiot — osoba fizyczna lub prawna, organ publiczny, agencja lub inny podmiot — który stosuje system AI pod własnym zwierzchnictwem w celach innych niż osobiste i niekomercyjne.

Kancelaria prawna, która kupuje dostęp do narzędzia AI i korzysta z niego w pracy zawodowej, jest podmiotem stosującym. Nie jest dostawcą. To zasadniczo ogranicza zakres jej obowiązków wynikających wprost z Aktu — dokumentacja techniczna, testy bezpieczeństwa, rejestracja to domena dostawcy.

Kiedy kancelaria może wejść w zakres wysokiego ryzyka?

Mimo że kancelaria jest podmiotem stosującym, klasyfikacja ryzyka zależy od **zastosowania** systemu — nie od samej technologii. Ten sam model AI może być narzędziem minimalnego ryzyka do redagowania korespondencji i systemem wysokiego ryzyka, gdy jest używany do oceny ryzyka procesowego klienta w sposób determinujący decyzje o jego prawach.

Zasada operacyjna: im bardziej wynik systemu AI bezpośrednio wpływa na decyzje istotne dla praw lub interesów klienta — ocenę jego wiarygodności, dostęp do usług, rekomendację procesową traktowaną jako ostateczną — tym większe prawdopodobieństwo, że zastosowanie wchodzi w zakres wysokiego ryzyka z Załącznika III. Im bardziej AI jest narzędziem wspomagającym, weryfikowanym na każdym kroku przez prawnika, tym bliżej minimalnego ryzyka.

Obowiązki, które realnie dotyczą kancelarii

Kompetencje w zakresie AI — art. 4 Rozporządzenia (UE) 2024/1689

Art. 4 Aktu o AI nakłada na dostawców i podmioty stosujące systemy AI obowiązek podejmowania działań w celu zapewnienia **wystarczającego poziomu kompetencji w zakresie AI** (*AI literacy*) wśród pracowników obsługujących te systemy lub z nich korzystających — stosownie do roli i kontekstu danego podmiotu.

Dla kancelarii oznacza to konieczność przeszkolenia zespołu co najmniej w zakresie: jak działa używane narzędzie AI na poziomie funkcjonalnym (nie technicznym), jakie są ograniczenia modeli językowych i generatywnych, jakie ryzyka niesie bezkrytyczne korzystanie z wyników AI, i jak oceniać, kiedy wynik wymaga weryfikacji zewnętrznej. Spełnienie tego wymogu warto udokumentować.

Dla kancelarii, która już poważnie traktuje tajemnicę zawodową i RODO, kompetencje w zakresie AI są naturalnym przedłużeniem istniejącej kultury zarządzania informacją.

Nadzór człowieka

Akt o AI konsekwentnie zakłada, że systemy AI — zwłaszcza wysokiego ryzyka — muszą pozostawać pod **aktywnym nadzorem człowieka**. Podmiot stosujący systemy wysokiego ryzyka jest odpowiedzialny za zapewnienie tego nadzoru na podstawie art. 26 Rozporządzenia (UE) 2024/1689. Dla systemów minimalnego ryzyka brak sformalizowanego wymogu z Aktu, lecz nadzór człowieka wynika wprost z zasad odpowiedzialności zawodowej. Kancelaria nie może tłumaczyć błędu w piśmie procesowym tym, że „AI tak wygenerowało” — odpowiedzialność zawodowa za każdy dokument leży po stronie prawnika, niezależnie od użytych narzędzi.

Przejrzystość wobec klienta

Dla systemów objętych art. 50 Rozporządzenia (UE) 2024/1689 podmiot stosujący jest zobowiązany do poinformowania osoby kontaktującej się z systemem AI, że ma do czynienia ze sztuczną inteligencją. Obowiązek ten jest bezwzględny i nie podlega wyłączeniu regulaminem.

Niezależnie od tego formalnego obowiązku — informowanie klienta o stosowaniu narzędzi AI w jego sprawie jest dobrą praktyką zawodową, spójną z zasadą rzetelności i lojalności wobec mocodawcy.

Dwa równoległe reżimy: AI Act i RODO

Akt o AI i RODO (Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., dalej: RODO) działają równolegle — żaden nie zastępuje drugiego.

Kluczowe punkty styku dla kancelarii:

Art. 22 RODO — prawo do niepodlegania wyłącznie zautomatyzowanemu podejmowaniu decyzji: jeżeli wynik systemu AI wywołuje skutki prawne lub w podobny sposób istotnie wpływa na klienta, klient ma prawo żądać, by ostateczna decyzja była podjęta przez człowieka. Wymóg nadzoru człowieka z Aktu o AI zmierza w tym samym kierunku.

Art. 5 RODO — zasady przetwarzania: zasada minimalizacji ogranicza zakres danych o kliencie przesyłanych do zewnętrznego systemu AI; zasada rozliczalności wymaga, by kancelaria potrafiła wykazać zgodność przyjętego modelu pracy.

Art. 28 RODO — przetwarzanie powierzone: każde zewnętrzne narzędzie AI, do którego trafiają dane osobowe klientów, wymaga pisemnej umowy powierzenia. Brak tej umowy to naruszenie RODO — i sygnał, że dostawca nie spełnia obowiązków z Aktu o AI w zakresie transparentności łańcucha przetwarzania.

Tajemnica zawodowa — obowiązek bezwzględny, równoległy do AI Act

Polska tajemnica adwokacka (art. 6 ustawy z dnia 26 maja 1982 r. — Prawo o adwokaturze) i tajemnica radcy prawnego (art. 3 ust. 3–6 ustawy z dnia 6 lipca 1982 r. o radcach prawnych) są bezwzględne i bezterminowe — nie ma w tych przepisach wyjątku dla korzystania z technologii AI.

Akt o AI nie zawiera przepisu, który zwalniałby prawnika z tajemnicy zawodowej w związku z używaniem narzędzi AI. Są to dwa niezależne reżimy: Akt o AI określa wymagania wobec systemów AI i ról uczestników rynku; tajemnica zawodowa określa, co prawnik może ujawnić i komu — niezależnie od narzędzia i medium.

Spójność między nimi jest możliwa i praktyczna: narzędzie AI spełniające wymogi Aktu — z dokumentacją, transparentnym łańcuchem przetwarzania, umową powierzenia zgodną z art. 28 RODO — to narzędzie, z którym kancelaria może zbudować model pracy zgodny z tajemnicą zawodową. Narzędzie bez tej dokumentacji to narzędzie, przy którym tajemnica zawodowa jest realnie zagrożona, a ryzyko odpowiedzialności dyscyplinarnej jest realne.

Lista kontrolna: co kancelaria powinna zrobić

1. Zinwentaryzuj narzędzia AI stosowane w kancelarii

Uwzględnij wszystko: narzędzia do redagowania pism, systemy transkrypcji głosu, asystentów wbudowanych w przeglądarkę lub edytor tekstu, narzędzia do streszczania dokumentów PDF, systemy

zarządzania sprawami z elementami automatyzacji i AI. Niejednokrotnie okazuje się, że kancelaria korzysta z kilku narzędzi AI, z których część nie jest formalnie rozpoznawana jako „AI” — transkrypcja, odpowiedzi w edytorze, automatyczne kategoryzowanie korespondencji.

2. Ustal rolę kancelarii wobec każdego narzędzia

Czy kancelaria jest podmiotem stosującym (co jest typowe) czy dostawcą (przypadek wyjątkowy — np. kancelaria buduje własne narzędzie AI i udostępnia je swoim klientom)? Ustalenie roli determinuje zakres obowiązków wynikających z Rozporządzenia (UE) 2024/1689.

3. Oceń, czy dane narzędzie wchodzi w zakres systemów wysokiego ryzyka

Kategorie z Załącznika III do Rozporządzenia (UE) 2024/1689. Kluczowe pytanie: czy zastosowanie tego narzędzia w konkretnym kontekście kancelarii może istotnie wpłynąć na prawa lub interesy klienta — ocenę jego wiarygodności, dostęp do usług, wynik postępowania? Jeżeli tak: sprawdź, czy dostawca posiada wymaganą dokumentację techniczną i czy przeprowadził wymaganą ocenę zgodności.

4. Zweryfikuj, czy dostawca spełnia obowiązki Aktu

Dla systemów wysokiego ryzyka: czy dostawca posiada dokumentację techniczną? Czy kancelaria jako podmiot stosujący otrzymała od dostawcy wystarczające instrukcje obsługi, informacje o ograniczeniach i zasadach nadzoru człowieka? Dla systemów minimalnego ryzyka: czy dostawca transparentnie informuje o sposobie działania systemu, miejscu przetwarzania danych i łańcuchu podprocesorów?

5. Zapewnij i udokumentuj nadzór człowieka nad każdym istotnym wynikiem

Każde pismo, analiza lub rekomendacja procesowa generowana lub współtworzona przez AI powinna przejść przez weryfikację prawnika przed użyciem. Prosta adnotacja w aktach sprawy: „wynik AI zweryfikowany przez [inicjały], [data]” — spełnia wymóg rozliczalności z art. 5 ust. 2 RODO i odpowiada wymogowi nadzoru człowieka z Aktu o AI.

6. Przeszkól zespół w zakresie kompetencji AI

Szkolenie nie musi być certyfikowanym kursem technicznym. Wystarczy, że każdy pracownik kancelarii obsługujący narzędzia AI rozumie: jak dane narzędzie działa funkcjonalnie, jakie są jego znane ograniczenia (błędne cytaty, nieaktualne dane, tzw. halucynacje), kiedy wynik AI wymaga weryfikacji zewnętrznej — i jak postąpić w razie wątpliwości. Spełnienie art. 4 Rozporządzenia (UE) 2024/1689 warto udokumentować: lista szkolonych osób, data, zakres tematyczny.

7. Powiąż z RODO: zweryfikuj umowy powierzenia i klauzule informacyjne

Każde narzędzie AI, do którego trafiają dane osobowe klientów, wymaga pisemnej umowy powierzenia przetwarzania zgodnej z art. 28 RODO. Klauzule informacyjne przekazywane klientom kancelarii

powinny odzwierciedlać faktyczny zakres przetwarzania — w tym korzystanie z zewnętrznych systemów AI jako podmiotów przetwarzających.

8. Sporządź wewnętrzną politykę korzystania z AI

Krótki dokument opisujący: które narzędzia są dopuszczone do użycia, w jakim zakresie, z jakimi ograniczeniami i jak zapewniony jest nadzór człowieka. Jest to jednocześnie dowód rozliczalności z RODO i dowód wdrożenia wymogów z art. 4 Aktu o AI. W razie kontroli Prezesa UODO lub postępowania przed właściwym sądem dyscyplinarnym NRA albo KIRP — pierwszym dokumentem, który wykaże przemyślaną postawę kancelarii, a nie improwizację.

Podsumowanie: AI Act i tajemnica zawodowa zmierzają w tę samą stronę

Akt o AI i polska tajemnica zawodowa mają różne źródła, różne procedury egzekwowania i różne sankcje. Ale ich wspólny kierunek jest ten sam: **człowiek odpowiada, narzędzie wspiera.**

Kancelaria, która korzysta z narzędzi AI z zachowaniem aktywnego nadzoru prawnika, z udokumentowaną weryfikacją wyników, z przeszkolonym zespołem i z dostawcami spełniającymi obowiązki Aktu o AI — ta kancelaria nie tylko spełnia regulacje. Buduje model pracy, w którym AI realnie zwiększa efektywność, bez przenoszenia ryzyka na klientów i bez narażania prawnika na odpowiedzialność zawodową.

Punktem wyjścia pozostaje zasada niezmienną od dziesięcioleci: odpowiedzialność jest niezbywalnie po stronie prawnika. Technologia zmienia narzędzia — nie zmienia tej zasady.

Materiał edukacyjny. Nie stanowi porady prawnej. Przepisy Aktu o AI wchodzi w życie etapami — weryfikuj aktualny harmonogram stosowania poszczególnych przepisów, komunikaty Prezesa UODO oraz stanowiska samorządów zawodowych NRA i KIRP przed podjęciem decyzji w indywidualnej sprawie.

■ Avantwerk Legal AI

Budujemy narzędzia AI dla kancelarii, w których treść sprawy zostaje na urządzeniu prawnika — nie na naszym serwerze.

Operator: Bennovate sp. z o.o. · KRS 0000597272 · Łódź · prawnik.avantwerk.pl