

Zanim wpuścisz AI do kancelarii

10 pytań, które każdy adwokat i radca prawny musi zadać przed wyborem narzędzia

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

Wstęp: Architektura ma znaczenie, regulamin nie

Rozmowy o AI w kancelarii zwykle kończą się jednym z dwóch błędnych wniosków. Albo: „to zbyt ryzykowne, nie dotykamy” — i kancelaria rezygnuje z realnych korzyści produktywnościowych. Albo: „oni mają politykę prywatności, więc jest bezpiecznie” — i prawnik wpuszcza do spraw narzędzie, którego architektury nigdy nie ocenił.

Teza tej listy kontrolnej jest prosta i techniczna: **o zgodności z tajemnicą zawodową i RODO decyduje architektura narzędzia — fizyczna droga danych — a nie treść regulaminu dostawcy**. Regulamin to deklaracja intencji; umowa to zobowiązanie; architektura to fakt.

Polska tajemnica adwokacka (art. 6 ustawy z dnia 26 maja 1982 r. — Prawo o advokaturze) i tajemnica radcy prawnego (art. 3 ust. 3–6 ustawy z dnia 6 lipca 1982 r. o radcach prawnych) są bezwzględne, bezterminowe i nie podlegają uchyleniu przez mocodawcę. Nie ma w tych przepisach wyjątku dla „nowoczesnych narzędzi cyfrowych”. Oznacza to jedno: **to prawnik odpowiada za każdą decyzję o wpuszczeniu treści sprawy do dowolnego systemu** — włącznie z systemem AI.

Poniższe pytania są narzędziem oceny. Można je zastosować wobec każdego produktu AI dostępnego na rynku. Cel jest jeden: zanim podpiszesz umowę, wiedz, gdzie fizycznie trafiają dane Twoich klientów.

Ramy prawne w pigułce

Trzy reżimy prawne działają równolegle — i żaden nie zastępuje pozostałych.

Tajemnica zawodowa — obowiązek bezwzględny. Art. 6 Prawa o advokaturze zobowiązuje adwokata do zachowania w tajemnicy wszystkiego, o czym dowiedział się w związku z udzielaniem pomocy prawnej. Art. 3 ust. 3 ustawy o radcach prawnych nakłada analogiczny obowiązek na radcę prawnego. Obowiązek ten jest bezterminowy — trwa po zakończeniu stosunku zlecenia. Nie ma wyjątku technologicznego: treść sprawy wysłana do zewnętrznego serwera to treść sprawy, która opuściła dyspozycję prawnika.

RODO — rozliczalność administratora. Kancelaria jako administrator danych osobowych (art. 4 pkt 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., dalej: RODO) ponosi odpowiedzialność za każdy krok przetwarzania, w tym za przetwarzanie powierzone podmiotowi zewnętrznemu. Kluczowe przepisy w kontekście AI:

- **Art. 5 ust. 1–2 RODO** — zasady przetwarzania (minimalizacja danych, integralność i poufność) oraz obowiązek rozliczalności: kancelaria musi być w stanie wykazać zgodność z tymi zasadami.

- **Art. 28 RODO** — przetwarzanie powierzone: każde korzystanie z zewnętrznego narzędzia AI, do którego trafiają dane osobowe, wymaga zawarcia umowy powierzenia przetwarzania.
- **Art. 32 RODO** — bezpieczeństwo przetwarzania: środki techniczne i organizacyjne adekwatne do ryzyka, uwzględniające charakter przetwarzanych danych.
- **Rozdział V RODO (art. 44–49)** — transfer danych do państw trzecich poza Europejski Obszar Gospodarczy: dozwolony wyłącznie na enumeratywnie wskazanych podstawach.
- **Art. 22 RODO** — prawo do niepodlegania wyłącznie zautomatyzowanemu podejmowaniu decyzji wywołującemu skutki prawne lub w podobny sposób istotnie wpływającemu na podmiot danych.

Odpowiedzialność zawodowa i dyscyplinarna. Korzystanie z narzędzi AI w sposób naruszający tajemnicę zawodową może być podstawą postępowania dyscyplinarnego przed właściwym sądem dyscyplinarnym (Naczelny Sąd Dyscyplinarny NRA / sądy dyscyplinarne KIRP) i odpowiedzialności majątkowej z obowiązkowego ubezpieczenia OC. Samorządy zawodowe adwokatury i radców prawnych wydają własne wytyczne i stanowiska dotyczące stosowania AI — ich znajomość i przestrzeganie należy do podstawowych obowiązków zawodowych.

Dwa światy architektury

Zanim przejdziesz do listy kontrolnej, warto zrozumieć fundamentalną różnicę między dwoma modelami technicznymi, bo to ona determinuje odpowiedzi na poniższe pytania.

Model chmurowy (dane wychodzą z kancelarii). Prawnik wpisuje tekst w interfejsie przeglądarki lub aplikacji. Tekst jest wysyłany przez internet na serwery dostawcy narzędzia, a stamtąd — potencjalnie dalej — do serwerów operatora modelu AI (który może być podmiotem trzecim, w tym spoza EOG). Odpowiedź wraca tą samą drogą. Dane klienta opuściły urządzenie prawnika i trafiły do co najmniej dwóch podmiotów zewnętrznych. Tego faktu nie zmienia regulamin.

Model lokalny / browser-first (dane zostają na urządzeniu). Narzędzie przetwarza treść sprawy wyłącznie na urządzeniu prawnika — w przeglądarce, na lokalnym serwerze kancelarii lub na urządzeniu end-to-end. Do zewnętrznego systemu AI trafia wyłącznie to, co prawnik świadomie zdecyduje się wysłać, lub nic — jeśli model AI działa lokalnie. Ryzyko naruszenia tajemnicy zawodowej jest minimalne, ponieważ dane nie opuszczają kontrolowanego środowiska.

Większość dostępnych na rynku narzędzi AI dla prawników działa w modelu chmurowym. Nie oznacza to automatycznej niezgodności — oznacza, że pytania z poniższej listy stają się tym bardziej kluczowe.

Lista kontrolna: 10 pytań przed podpisaniem umowy

1. Gdzie fizycznie są przechowywane i przetwarzane dane sprawy?

Pytanie do dostawcy: W którym kraju i na czyich serwerach fizycznie przetwarza się treść, którą wpisuję? Czy dane w ogóle opuszczają terytorium EOG?

Dlaczego to ważne prawnie: Art. 44 RODO wyraźnie zakazuje transferu danych do państw trzecich poza enumeratywnymi wyjątkami z art. 45–49 RODO. Transfer do serwera w USA, na którym

przetwarza się treść sprawy, to transfer danych osobowych poza EOG — niezależnie od tego, czy o tym wiemy. Art. 32 RODO wymaga, by środki bezpieczeństwa uwzględniały m.in. ryzyko związane z lokalizacją przetwarzania.

Dobra odpowiedź: Dostawca podaje konkretną lokalizację centrów danych (kraj, operator), nie ogólnikowe „bezpieczne środowisko chmurowe”. Przetwarzanie odbywa się na terytorium EOG. Kancelaria o najwyższych standardach powinna preferować przetwarzanie wyłącznie lokalne lub z gwarancją EOG.

2. Czy treść sprawy w ogóle opuszcza kancelarię lub urządzenie prawnika?

Pytanie do dostawcy: Czy cokolwiek, co wpisuję — fragment pisma, pytanie do AI, dane klienta — opuszcza fizycznie mój komputer lub serwer kancelarii?

Dlaczego to ważne prawnie: Art. 6 Prawa o adwokaturze i art. 3 ust. 3 ustawy o radcach prawnych chronią „wszystko, o czym prawnik dowiedział się w związku z udzielaniem pomocy prawnej” — bez wyjątku technologicznego. Każde wysłanie treści sprawy poza urządzenie bez upoważnienia klienta i bez odpowiednich zabezpieczeń prawnych jest potencjalnym naruszeniem tajemnicy zawodowej, niezależnie od intencji dostawcy.

Dobra odpowiedź: Narzędzie działa w architekturze lokalnej (przetwarzanie wyłącznie na urządzeniu kancelarii) albo — jeżeli dane opuszczają urządzenie — kancelaria ma podpisaną umowę powierzenia przetwarzania (art. 28 RODO) i klient jest poinformowany o zakresie przetwarzania w klauzuli informacyjnej.

3. Kto jest podprocesorem i czy istnieje umowa powierzenia?

Pytanie do dostawcy: Kto faktycznie przetwarza dane — sam dostawca narzędzia, jego podwykonawca technologiczny, operator modelu AI? Czy mam z dostawcą zawartą umowę powierzenia przetwarzania danych w rozumieniu art. 28 RODO?

Dlaczego to ważne prawnie: Art. 28 ust. 1 RODO: korzystanie z podmiotu przetwarzającego, który nie zapewnia wystarczających gwarancji, jest naruszeniem RODO przez administratora (kancelarię). Art. 28 ust. 2 RODO: procesor może korzystać z podprocesora wyłącznie za uprzednią zgodą administratora. Art. 28 ust. 3 RODO wymaga, by umowa powierzenia miała formę pisemną (w tym elektroniczną) i zawierała enumeratywnie wskazane elementy. Brak umowy powierzenia = bezprawne przetwarzanie.

Dobra odpowiedź: Dostawca udostępnia wzorzec DPA (Data Processing Agreement / Umowa powierzenia przetwarzania danych) zgodny z art. 28 RODO, wskazuje kompletną listę podprocesorów — w tym operatora modelu AI i infrastruktury chmurowej — oraz informuje z wyprzedzeniem o każdej zmianie tej listy.

4. Czy dochodzi do transferu poza EOG i na jakiej podstawie?

Pytanie do dostawcy: Czy dane klientów kancelarii trafiają do państw spoza Europejskiego Obszaru Gospodarczego? Jeżeli tak — na jakiej konkretnej podstawie z art. 44–49 RODO?

Dlaczego to ważne prawnie: Rozdział V RODO (art. 44–49) ustanawia zamknięty katalog podstaw legalnego transferu poza EOG. Art. 44 RODO *expressis verbis* zakazuje transferu bez spełnienia jednej z tych podstaw. Dane sprawy mogą zawierać dane wrażliwe (kategoria szczególna w rozumieniu art. 9 RODO — dane zdrowotne, przekonania religijne, dane biometryczne), dla których standard ochrony jest jeszcze wyższy. Wyrok TSUE w sprawie Schrems II (C-311/18) utrwalił zasadę, że samo wdrożenie standardowych klauzul umownych nie wystarczy bez oceny faktycznego poziomu ochrony w państwie docelowym.

Dobra odpowiedź: Dostawca jasno wskazuje, czy transfer poza EOG w ogóle następuje. Jeżeli tak — podaje konkretną podstawę prawną (np. standardowe klauzule umowne zatwierdzone decyzją Komisji Europejskiej 2021/914) i oświadcza o jej ważności. Optymalnym rozwiązaniem dla kancelarii jest architektura gwarantująca przetwarzanie wyłącznie w granicach EOG.

5. Czy treść klienta jest wykorzystywana do trenowania modelu?

Pytanie do dostawcy: Czy treść, którą wpisuję do narzędzia, może być użyta do trenowania, fine-tuningu lub ulepszania modelu AI — czy to przez samego dostawcę, czy przez któregośkolwiek z jego podprocesorów?

Dlaczego to ważne prawnie: Wykorzystanie treści sprawy do trenowania modelu oznacza *de facto* ujawnienie tych informacji podmiotom zaangażowanym w proces trenowania — co stanowi naruszenie tajemnicy zawodowej. Z perspektywy RODO: cel „trening modelu” jest innym celem niż cel pierwotnego przetwarzania (obsługa kancelarii), co wymaga odrębnej, legalnej podstawy przetwarzania (art. 6 ust. 1 RODO). Kancelaria nie jest w stanie legalnie zapewnić takiej podstawy dla danych objętych tajemnicą zawodową.

Dobra odpowiedź: Umowa z dostawcą zawiera wiążące postanowienie umowne (nie tylko deklarację regulaminową), że dane klientów kancelarii nie są i nie będą wykorzystywane do trenowania, fine-tuningu ani ulepszania jakiegokolwiek modelu AI — przez dostawcę ani żadnego z jego podprocesorów.

6. Czy każdy istotny krok zatwierdza człowiek?

Pytanie do dostawcy: Czy narzędzie może samodzielnie — bez aktywnej decyzji prawnika — podjąć czynność mającą wpływ na sprawę klienta? Czy istnieje techniczny mechanizm wymuszający zatwierdzenie przez człowieka?

Dlaczego to ważne prawnie: Art. 22 ust. 1 RODO przyznaje podmiotom danych prawo do niepodlegania decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, jeżeli wywołuje ona skutki prawne lub w podobny sposób istotnie na nie wpływa. Niezależnie od RODO: adwokat i radca prawny ponoszą osobistą odpowiedzialność zawodową za każdą czynność w sprawie klienta (Kodeks Etyki Adwokackiej, Kodeks Etyki Radcy Prawnego). Tej odpowiedzialności nie można scedować na system AI — „narzędzie tak wygenerowało” nie jest okolicznością wyłączającą winę.

Dobra odpowiedź: Architektura narzędzia wymusza zatwierdzenie przez prawnika każdego wyniku AI przed jego użyciem. AI generuje propozycje i analizy — prawnik zatwierdza, modyfikuje i podpisuje. Brak mechanizmu wymuszającego tę kontrolę to wada produktu, nie kwestia regulaminowa.

7. Czy mogę zweryfikować źródła i cytaty generowane przez narzędzie?

Pytanie do dostawcy: Gdy narzędzie powołuje się na wyrok, przepis lub orzeczenie — czy dostarcza sygnaturę i odniesienie pozwalające mi samodzielnie sprawdzić to źródło przed użyciem w sprawie?

Dlaczego to ważne prawnie: Modele językowe generują treść statystycznie spójną, nie faktograficznie prawdziwą. Powołanie się w piśmie procesowym na nieistniejący wyrok sądu lub błędnie przywołany przepis to błąd w sztuce skutkujący odpowiedzialnością zawodową i cywilną. Prawnik nie może proceduralnie „przerzucić” obowiązku weryfikacji na klienta ani na system AI — jest zobowiązany samodzielnie ocenić każde twierdzenie faktyczne i prawne przed jego użyciem.

Dobra odpowiedź: Narzędzie dostarcza weryfikowalnych odniesień do źródeł (sygnatury wyroków z SAOS, numery ustaw z ISAP, artykuły z Dz.U.) lub — jeżeli ich nie dostarcza — jawnie komunikuje użytkownikowi, że cytaty wymagają weryfikacji zewnętrznej przed użyciem. Idealny model: wbudowana weryfikacja cytowań przed eksportem dokumentu.

8. Kto kontroluje klucz dostępu do modelu AI i logi zapytań?

Pytanie do dostawcy: Kto fizycznie posiada dane uwierzytelniające (klucz API, token dostępu) do modelu AI użytego w narzędziu? Czy kancelaria może samodzielnie cofnąć ten dostęp? Kto ma wgląd w logi zapytań?

Dlaczego to ważne prawnie: Klucz dostępu do modelu AI to faktyczna możliwość wysyłania treści do zewnętrznego systemu. Jeżeli klucz kontroluje wyłącznie dostawca SaaS, kancelaria nie sprawuje pełnej kontroli nad zakresem przetwarzania — co może stać w sprzeczności z obowiązkiem rozliczalności z art. 5 ust. 2 RODO. W modelu BYOK (Bring Your Own Key — kancelaria dysponuje własnym kluczem dostępu) kancelaria może cofnąć uprawnienie w dowolnym momencie, a dostawca narzędzia nie ma własnego dostępu do modelu w imieniu kancelarii.

Dobra odpowiedź: Kancelaria ma możliwość korzystania z własnego klucza dostępu do modelu AI, co daje jej pełną kontrolę nad uprawnieniem do przetwarzania i możliwość jego natychmiastowego cofnięcia. W modelu zarządzanym (klucz po stronie dostawcy): dostawca jasno określa, kto ma dostęp do logów zapytań, w jakim zakresie i na jakiej podstawie prawnej, oraz zapewnia kancelarii możliwość audytu.

9. Czy istnieje ślad audytowy i rejestr czynności AI?

Pytanie do dostawcy: Czy narzędzie prowadzi rejestr — kto, kiedy, w ramach jakiej sprawy, co wygenerował przy użyciu AI? Czy ten rejestr jest dostępny dla kancelarii i możliwy do wyeksportowania?

Dlaczego to ważne prawnie: Art. 5 ust. 2 RODO nakłada na administratora (kancelarię) obowiązek rozliczalności: wykazania, że przetwarzanie odbywa się zgodnie z zasadami z art. 5 ust. 1. W razie kontroli Prezesa UODO lub postępowania dyscyplinarnego kancelaria musi być w stanie udokumentować, że AI działało jako narzędzie wspomagające pod kontrolą człowieka, a treść klienta była chroniona. Rejestr czynności AI jest dowodem tej kontroli — jego brak utrudnia wykazanie rozliczalności.

Dobra odpowiedź: Narzędzie prowadzi rejestr operacji AI przypisanych do spraw i użytkowników, dostępny dla kancelarii i możliwy do wyeksportowania na potrzeby audytu. Optymalne rozwiązanie: rejestr jest zabezpieczony kryptograficznie (np. podpisany cyfrowo) i nie może być jednostronnie zmodyfikowany ani przez dostawcę, ani przez użytkownika po fakcie.

10. Czy rozwiązanie jest zgodne ze stanowiskami samorządu zawodowego?

Pytanie do dostawcy: Czy dostawca zna i może wskazać stanowiska Naczelnej Rady Adwokackiej lub Krajowej Izby Radców Prawnych dotyczące stosowania AI? Czy może wykazać, w jaki sposób architektura jego produktu jest zgodna z tymi stanowiskami?

Dlaczego to ważne prawnie: Samorządy zawodowe adwokatury i radców prawnych wydają stanowiska i wytyczne interpretujące obowiązek tajemnicy zawodowej w kontekście nowych technologii. Naruszenie tych wytycznych może stanowić podstawę odpowiedzialności dyscyplinarnej — niezależnie od technicznej zgodności z RODO. Prawnik korzystający z narzędzia AI działającego wbrew wytycznym swojego samorządu nie może zasłaniać się nieznajomością tych dokumentów.

Dobra odpowiedź: Dostawca zna aktualne stanowiska NRA i KIRP, powołuje się na nie i potrafi wykazać, że architektura i zasady działania jego produktu są z nimi zgodne. Jeżeli samorząd nie wydał jeszcze szczegółowego stanowiska w danej kwestii — dostawca wskazuje obszar niepewności wprost, nie ukrywa go za ogólnymi zapewnieniami.

Podsumowanie: co możesz zrobić od jutra

Lista kontrolna powyżej to narzędzie kupującego, nie certyfikat. Żadna odpowiedź dostawcy nie zwalnia prawnika z własnej oceny. Trzy kroki, które możesz podjąć niezwłocznie:

1. Zidentyfikuj, które narzędzia AI już używasz w kancelarii. Wyszukiwarka AI w przeglądarce, diktafon z transkrypcją, narzędzie do streszczania plików PDF — każde z nich podlega tym samym pytaniom. Zacznij od inwentaryzacji faktycznego stanu, nie od teorii.

2. Zadaj każdemu dostawcy te 10 pytań na piśmie. Forma pisemna ma znaczenie: jeżeli dostawca nie chce odpowiedzieć na piśmie, odpowiedź sama w sobie jest informacją. Umowa powierzenia przetwarzania musi mieć formę pisemną zgodnie z art. 28 ust. 9 RODO — żaden regulamin nie zastępuje umowy.

3. Zanim wpiszesz treść sprawy — sprawdź, dokąd idą dane. Zasada operacyjna: jeżeli nie znasz odpowiedzi na pytania 1 i 2 z tej listy, nie wpisujesz treści sprawy. Wpisujesz anonimizowane pytania ogólne lub nie korzystasz z narzędzia w tym zakresie.

Tajemnica zawodowa jest bezwzględna. Narzędzia AI mogą być wartościowe. Te dwa fakty da się pogodzić — pod warunkiem, że ocena zaczyna się od architektury, nie od cennika.

Materiał edukacyjny. Nie stanowi porady prawnej. Przepisy i stanowiska samorządowe mogą ulegać zmianom — weryfikuj aktualny stan przed podjęciem decyzji w indywidualnej sprawie.

■ Avantwerk Legal AI

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

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