Zanim wpuścisz AI do kancelarii

Wersja 2026-11, zastępująca wydanie 2026-07. Stan prawny i przegląd źródeł: 8 listopada 2026 r.

10 pytań o tajemnicę zawodową, dane i kontrolę nad narzędziem

Dla adwokatów i radców prawnych — kancelarie solo, małe i średnie

Ocena narzędzia wymaga sprawdzenia zarówno jego działania, jak i warunków prawnych korzystania z usługi. Miejsce przetwarzania jest ważne, ale sama architektura nie rozstrzyga zgodności. Liczą się też cel użycia, role stron, dostęp do danych, umowy, bezpieczeństwo i codzienna praktyka kancelarii.

Tajemnica adwokacka i radcowska chronią informacje uzyskane w związku z pomocą prawną bez ograniczenia w czasie (art. 6 ust. 1–3 Prawa o adwokaturze; art. 3 ust. 3–5 ustawy o radcach prawnych). Nie należy opisywać ich jako ochrony pozbawionej jakichkolwiek ustawowych wyjątków: art. 6 ust. 4 i odpowiednio art. 3 ust. 6 odnoszą się do informacji udostępnianych w zakresie przepisów AML. Zgoda klienta, umowa z dostawcą i obowiązki z RODO nie zastępują odrębnej oceny tajemnicy zawodowej.

Najpierw ustal, co faktycznie robi narzędzie

Interfejs w przeglądarce nie oznacza lokalnego przetwarzania. Aplikacja może przechowywać dokument na urządzeniu, a jednocześnie wysyłać zapytania do zewnętrznego modelu. Również przy wdrożeniu lokalnym trzeba sprawdzić zdalny serwis, kopie zapasowe, telemetrię i logi.

Przy chmurze ustal wszystkich odbiorców, zamiast zakładać z góry liczbę dostawców lub miejsce serwerów. Dane na serwerze w EOG i dostęp z państwa trzeciego wymagają odrębnego rozpoznania. Żaden model nie otrzymuje automatycznie etykiety zgodności albo niezgodności.

1. Gdzie dane są przetwarzane, przechowywane i udostępniane?

Zapytaj: W jakich państwach działają serwery, kopie zapasowe i wsparcie? Kto może uzyskać dostęp do dokumentów, zapytań, odpowiedzi i logów? Jak długo są przechowywane?

Dlaczego: Minimalizacja, bezpieczeństwo i rozliczalność wymagają oceny rzeczywistego przetwarzania (art. 5 i 32 RODO). Sama informacja o lokalizacji głównego centrum danych nie opisuje całego przepływu.

Szukaj odpowiedzi: Konkretna mapa danych i odbiorców, okresy przechowywania oraz udokumentowane uprawnienia dostępu. Twierdzenie „dane zostają lokalnie" powinno obejmować także funkcje pomocnicze.

2. W jakiej roli działa dostawca i czego dotyczy umowa?

Zapytaj: Czy dostawca przetwarza dane w imieniu kancelarii, ustala własne cele przetwarzania, czy w określonym zakresie nie otrzymuje danych osobowych?

Dlaczego: Rola podmiotu przetwarzającego wynika z art. 4 pkt 8 RODO i faktycznych czynności. Art. 28 dotyczy powierzenia, nie każdego zakupu oprogramowania. Inne role wymagają odrębnej oceny podstaw i obowiązków.

Szukaj odpowiedzi: Umowa odpowiadająca rzeczywistym rolom i zakresowi usługi. Gdy występuje powierzenie, treść powinna spełniać art. 28. Może stanowić część skutecznie uzgodnionych warunków usługi, również elektronicznych; osobny plik nazwany „DPA" nie jest jedyną dopuszczalną formą.

3. Kto uczestniczy w dalszym przetwarzaniu?

Zapytaj: Jakie podmioty przetwarzają dane na rzecz dostawcy? Czy lista obejmuje operatora modelu, hosting i wsparcie, o ile rzeczywiście otrzymują dane?

Dlaczego: Art. 28 ust. 2 i 4 RODO określa zasady dalszego powierzenia. Upoważnienie może być szczegółowe albo ogólne; przy ogólnym trzeba zapewnić informację o planowanych zmianach i możliwość sprzeciwu.

Szukaj odpowiedzi: Aktualna lista, opis czynności i lokalizacji, mechanizm zgłaszania zmian oraz zasady nakładania obowiązków na podprocesorów.

4. Czy występuje transfer poza EOG?

Zapytaj: Jakie dane i do kogo są przekazywane? Jaki mechanizm z rozdziału V RODO ma zastosowanie i jakie zabezpieczenia go uzupełniają?

Dlaczego: Samo zawarcie umowy powierzenia nie legalizuje każdego transferu. Trzeba ustalić właściwy mechanizm, jego warunki i zakres, zamiast poprzestawać na nazwie „SCC" albo obietnicy „zgodności z RODO".

Szukaj odpowiedzi: Wskazanie państwa, odbiorcy, mechanizmu, dokumentacji jego zastosowania i oceny potrzebnych dodatkowych zabezpieczeń. Wyjątków z art. 49 nie należy traktować jako domyślnego rozwiązania dla rutynowego przetwarzania.

5. Czy dane mogą służyć trenowaniu lub ulepszaniu modeli?

Zapytaj: Czy dostawca lub inny odbiorca wykorzystuje treść, logi albo oceny wyników we własnych celach? Czy wyłączenie treningu obejmuje cały łańcuch usługi i jakie pozostają okresy retencji?

Dlaczego: Własny cel dostawcy wymaga osobnej oceny roli, podstawy przetwarzania i tajemnicy zawodowej. Sama zgoda kancelarii na trening nie rozwiązuje tych kwestii. Wyłączenie treningu także nie oznacza automatycznie braku przechowywania lub dostępu ludzi.

Zalecana zasada kancelarii: Nie dopuszczaj wykorzystania informacji ze spraw do treningu lub ulepszania modeli na rzecz dostawcy. Ewentualny odrębny projekt wymaga osobnej oceny; nie powinien wynikać z domyślnej opcji konta ani ogólnej zgody administratora.

6. Kto sprawdza wynik przed użyciem?

Zapytaj: Jak kancelaria zapewnia weryfikację faktów, prawa i dokumentu przed wysłaniem, podpisaniem albo wniesieniem? Jak reaguje na wynik niepewny?

Dlaczego: Art. 22 RODO dotyczy określonych decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu; zawiera przesłanki, wyjątki i zabezpieczenia. Nie ustanawia technicznego przycisku zatwierdzania każdego tekstu AI.

Zalecenie organizacyjne: Ustal odpowiedzialnego prawnika i rzeczywisty zakres sprawdzenia. Techniczne zatwierdzanie może wspierać kontrolę, ale samo kliknięcie lub adnotacja nie dowodzą poprawności wyniku ani pełnej zgodności.

7. Czy można sprawdzić źródła i aktualność informacji?

Zapytaj: Czy narzędzie wskazuje źródło, sygnaturę lub oznaczenie aktu oraz datę, do której odnosi się wynik? Czy ujawnia brak dostępu do źródła?

Dlaczego: Wynik modelu może zawierać nieistniejący wyrok, błędny cytat albo nieaktualne prawo. Weryfikacja wymaga otwarcia właściwego źródła i porównania go z twierdzeniem.

Szukaj odpowiedzi: Weryfikowalne odniesienia i czytelna informacja o granicach wyniku. Automatyczna kontrola cytatu jest pomocą, a nie gwarancją trafnej interpretacji.

8. Jak można cofnąć dostęp i sprawdzić logi?

Zapytaj: Kto zarządza uprawnieniami, kluczami, kontami i logami? Co dzieje się po cofnięciu dostępu, usunięciu użytkownika lub zakończeniu umowy?

Dlaczego: Własny klucz do modelu może ułatwić zarządzanie dostępem, ale nie gwarantuje kontroli nad kopiami, logami i wcześniejszym przetwarzaniem. Zarządzany dostęp nie jest sam w sobie naruszeniem RODO.

Szukaj odpowiedzi: Udokumentowane role, ograniczenia dostępu, procedura cofnięcia uprawnień, retencja oraz zasady usuwania i audytu — niezależnie od sposobu rozliczania modelu.

9. Jaka dokumentacja jest potrzebna i proporcjonalna?

Zapytaj: Jak wykazać dopuszczenie narzędzia, ocenę ryzyka, szkolenie i kontrolę istotnych wyników? Jakie dane zawierają logi i kto może je odczytać?

Dlaczego: Rozliczalność z art. 5 ust. 2 RODO nie oznacza obowiązku nieograniczonego zapisywania całej treści każdej operacji AI. Logi również mogą zawierać dane osobowe i tajemnicę zawodową.

Zalecenie organizacyjne: Zachowuj potrzebny ślad decyzji i weryfikacji, z kontrolą dostępu i okresem przechowywania. Podpis kryptograficzny może chronić integralność zapisu; nie jest uniwersalnym wymogiem dla każdego narzędzia.

10. Jak uwzględniono obowiązki zawodowe?

Zapytaj: Jak kancelaria oceniła dopuszczalność ujawnienia informacji, poufność i odpowiedzialność za użycie wyniku? Jakie aktualne przepisy i właściwe zasady etyki uwzględniono?

Dlaczego: Tajemnica zawodowa wymaga osobnej analizy. Nie można traktować oświadczenia dostawcy, zgody klienta lub umowy powierzenia jako certyfikatu zgodności z obowiązkami zawodowymi.

Szukaj odpowiedzi: Własna udokumentowana ocena kancelarii, odnosząca się do konkretnej usługi i zastosowania. Stanowiska lub wytyczne samorządu należy identyfikować przez tytuł, datę i zakres; nie wolno przypisywać wszystkim identycznej mocy prawnej.

Trzy działania na początek

1. Zinwentaryzuj narzędzia i przepływy informacji, także funkcje wbudowane w edytory i przeglądarki.
2. Ustal role, warunki umowne i zabezpieczenia przed dopuszczeniem danych ze sprawy.
3. Gdy droga danych pozostaje nieustalona, ogranicz próbę do materiału publicznego lub rzeczywiście anonimowego, bez informacji objętych tajemnicą. Pseudonimizacja ogranicza ryzyko, ale nie wyłącza automatycznie RODO ani tajemnicy.

Źródła i zakres przeglądu

Sprawdzono wskazane przepisy RODO oraz art. 6 i 16b Prawa o adwokaturze i art. 3 ust. 3–6 i art. 5b ustawy o radcach prawnych. Przegląd dotyczy twierdzeń w tym materiale; nie jest oceną zgodności konkretnej kancelarii, systemu ani całości prawa zawodowego. Terminy i rozwiązania organizacyjne proponowane we wzorze są propozycjami do dostosowania, chyba że wyraźnie wskazano przepis.

- RODO — tekst w EUR-Lex.
- Prawo o adwokaturze — tekst ujednolicony Sejmu z 19 października 2026 r..
- Ustawa o radcach prawnych — tekst ujednolicony Sejmu z 8 października 2026 r..

Teksty ujednolicone ułatwiają odczytanie zmian; autentyczne brzmienie ustaw wynika z ogłoszonych aktów.

Historia zmian — 2026-11 względem 2026-07: Usunięto twierdzenia o wyłącznej roli architektury, automatycznym powierzeniu, zgodności wynikającej z lokalnego działania lub własnego klucza oraz o braku jakichkolwiek wyjątków od tajemnicy. Doprecyzowano umowy elektroniczne, trening, art. 22 i proporcjonalną dokumentację.

Materiał edukacyjny i poglądowy. Nie stanowi porady prawnej ani gwarancji zgodności. Przed użyciem należy ocenić aktualne prawo, rzeczywiste przetwarzanie i dokumentację konkretnego wdrożenia.