AI w chmurze czy lokalnie?

Gdzie trafiają dane klienta — porównanie dla kancelarii

Materiał edukacyjny dla adwokatów i radców prawnych

Wstęp: o zgodności decyduje droga danych, nie regulamin

Wybierając narzędzie AI, prawnicy zazwyczaj pytają o cenę, funkcje i interfejs. Pytanie, które zadaje się rzadziej — a które ma największe znaczenie prawne — brzmi: **gdzie fizycznie trafia treść, którą wpisuję do narzędzia?**

Odpowiedź na to pytanie determinuje trzy odrębne reżimy obowiązków: tajemnicę zawodową wynikającą z art. 6 ustawy z dnia 26 maja 1982 r. — Prawo o adwokaturze (Pr.adw.) oraz art. 3 ust. 3–6 ustawy z dnia 6 lipca 1982 r. o radcach prawnych (u.r.p.); obowiązki administratora danych osobowych z art. 5 ust. 1–2, art. 28 i art. 32 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. — ogólnego rozporządzenia o ochronie danych (RODO); wreszcie przepisy o transferze danych poza Europejski Obszar Gospodarczy z rozdziału V RODO (art. 44–49). Żaden z tych reżimów nie zależy od treści regulaminu dostawcy — zależy od architektury technicznej. Regulamin to deklaracja intencji. Architektura to fakt.

Dwa modele — czym się różnią

Narzędzia AI dostępne dla kancelarii różnią się pod względem jednego zasadniczego parametru: **gdzie odbywa się przetwarzanie danych**.

Model chmurowy oznacza, że tekst wpisany przez prawnika — fragmenty pism, fakty sprawy, dane klienta — opuszcza urządzenie i jest przesyłany do serwerów zewnętrznego dostawcy. Przetwarzanie (generowanie odpowiedzi przez model AI) zachodzi na infrastrukturze dostawcy, nie na infrastrukturze kancelarii.

Model lokalny oznacza, że model AI działa na urządzeniu lub serwerze pozostającym w kontroli kancelarii. Tekst nie opuszcza tej infrastruktury — nie jest przesyłany do żadnego zewnętrznego serwera.

Między tymi modelami istnieją warianty pośrednie — chmura prywatna kancelarii, serwer wewnętrzny podmiotu zewnętrznego na wyłączność, przetwarzanie na danych zanonimizowanych lub pseudonimizowanych — których ocena wymaga analizy konkretnej architektury wdrożenia.

Tabela porównawcza

Kryterium	AI w chmurze dostawcy	AI lokalne / na urządzeniu
Gdzie przetwarzane są dane	Serwery dostawcy (lokalizacja zależy od umowy i infrastruktury dostawcy)	Urządzenie lub serwer kancelarii
Czy dane opuszczają kancelarię	Tak — każde zapytanie jest przesyłane do zewnętrznej infrastruktury	Nie — przetwarzanie odbywa się wyłącznie lokalnie
Wymóg umowy powierzenia (art. 28 RODO)	Tak — obowiązkowa umowa powierzenia przetwarzania danych osobowych z dostawcą	Nie dotyczy — kancelaria pozostaje jedynym podmiotem przetwarzającym
Ryzyko transferu poza EOG (art. 44–49 RODO)	Możliwe — serwery mogą znajdować się poza EOG; wymaga weryfikacji podstawy prawnej transferu	Zasadniczo brak — dane nie opuszczają infrastruktury kancelarii
Ekspozycja tajemnicy zawodowej (art. 6 Pr.adw. / art. 3 ust. 3–6 u.r.p.)	Wyższa — treść sprawy jest przekazywana podmiotowi zewnętrznemu; wymaga indywidualnej oceny dopuszczalności	Niższa — treść sprawy pozostaje w infrastrukturze kancelarii
Kto kontroluje dostęp do danych	Dostawca (zakres dostępu zależy od umowy i architektury systemu)	Kancelaria — pełna kontrola techniczna i organizacyjna
Ślad audytowy	Zależny od funkcjonalności dostawcy; może być trudny do niezależnej weryfikacji przez kancelarię	Kancelaria może prowadzić własne logi niezależnie od jakiegokolwiek dostawcy

Co to oznacza w praktyce

> **Model chmurowy — nie jest automatycznie niezgodny, ale wymaga spełnienia warunków**

Korzystanie z narzędzia AI działającego w chmurze dostawcy nie jest automatycznie sprzeczne z RODO ani z tajemnicą zawodową. Jest jednak **obarczone warunkami, których spełnienie wymaga aktywnego działania kancelarii — przed wdrożeniem, nie po fakcie.**

Umowa powierzenia przetwarzania (art. 28 RODO). Kancelaria jako administrator danych osobowych jest obowiązana do zawarcia z dostawcą AI umowy powierzenia przetwarzania, obejmującej co najmniej: przedmiot i czas trwania przetwarzania, jego charakter i cel, rodzaj danych osobowych, kategorie osób, których dane dotyczą, oraz obowiązki i prawa administratora. Brak takiej umowy stanowi naruszenie art. 28 RODO — niezależnie od treści ogólnych warunków świadczenia usług dostawcy.

Transfer danych poza EOG (art. 44–49 RODO). Jeżeli serwery dostawcy lub serwery jego podwykonawców znajdują się poza EOG, przekazywanie danych osobowych wymaga odpowiedniej

podstawy prawnej. Może nią być decyzja Komisji Europejskiej stwierdzająca odpowiedni stopień ochrony danych w danym państwie trzecim (art. 45 RODO), standardowe klauzule umowne (art. 46 ust. 2 lit. c RODO) lub inne mechanizmy określone w art. 46–49 RODO. Sam regulamin dostawcy — nawet redagowany zgodnie z prawem EOG — nie jest podstawą prawną transferu w rozumieniu rozdziału V RODO.

Zasada minimalizacji danych (art. 5 ust. 1 lit. c RODO). Prawnik korzystający z narzędzia chmurowego powinien każdorazowo ocenić, czy treść przekazywana do narzędzia jest adekwatna i ograniczona do tego, co niezbędne do osiągnięcia celu przetwarzania. Przekazywanie pełnej treści akt sprawy — wraz z danymi identyfikacyjnymi klienta i stron — w sytuacji, gdy cel mógłby zostać osiągnięty na podstawie streszczenia pozbawionym takich danych, może naruszać tę zasadę.

Tajemnica zawodowa. Art. 6 Pr.adw. zobowiązuje adwokata do zachowania w tajemnicy wszystkiego, o czym dowiedział się w związku z udzielaniem pomocy prawnej. Art. 3 ust. 3 u.r.p. nakłada analogiczny, bezwzględny i bezterminowy obowiązek na radcę prawnego. Obowiązek ten nie podlega uchyleniu przez mocodawcę i nie zawiera wyjątku technologicznego. Wysłanie treści sprawy na serwery zewnętrznego dostawcy oznacza, że treść ta opuściła wyłączną dyspozycję prawnika i znalazła się w infrastrukturze podmiotu trzeciego. Ocena, czy jest to zgodne z tajemnicą zawodową, musi uwzględniać konkretne warunki umowy, zastosowane środki techniczne i organizacyjne (art. 32 RODO) oraz architekturę przetwarzania — a nie wyłącznie renomę rynkową dostawcy.

> **Model lokalny — mniejsza ekspozycja zewnętrzna, pełna odpowiedzialność własna**

Narzędzie AI działające lokalnie eliminuje część opisanych ryzyk: dane nie opuszczają kancelarii, obowiązek zawarcia umowy powierzenia z dostawcą AI odpada, ryzyko transferu poza EOG jest zasadniczo wyłączone. **Nie oznacza to braku jakichkolwiek obowiązków.** Kancelaria staje się odpowiedzialna za bezpieczeństwo infrastruktury, na której działa model (art. 32 RODO), za kontrolę dostępu do urządzenia lub serwera, za aktualizacje oprogramowania i podatności bezpieczeństwa modelu. Obowiązek dokumentowania i rozliczalności (art. 5 ust. 2 RODO) pozostaje — ślad audytowy musi być prowadzony przez kancelarię we własnym zakresie.

> **Podsumowanie**

Żaden z omawianych modeli nie jest automatycznie „bezpieczny" ani automatycznie „niezgodny z prawem". Model chmurowy wymaga spełnienia zestawu warunków formalnych i technicznych przed wdrożeniem. Model lokalny przenosi ciężar odpowiedzialności za bezpieczeństwo infrastruktury na kancelarię. Decyzja powinna opierać się na analizie konkretnego narzędzia, indywidualnych ryzyk i możliwości organizacyjnych kancelarii — nie na założeniu, że jedno z rozwiązań jest z definicji bezpieczniejsze.

Jak sprawdzić, w którym modelu działa Twoje narzędzie

Przed wdrożeniem dowolnego narzędzia AI warto zadać dostawcy cztery pytania:

1. **Gdzie fizycznie przetwarzane są dane wpisywane do narzędzia?** Odpowiedź powinna wskazywać konkretną lokalizację serwerów (kraj, region, informacja o tym, czy lokalizacja mieści się w EOG) oraz nazwę podmiotu faktycznie przetwarzającego.

2. **Czy dostawca oferuje umowę powierzenia przetwarzania danych osobowych w rozumieniu art. 28 RODO?** Jeśli nie — kancelaria nie może legalnie przekazywać danych osobowych klientów za pośrednictwem tego narzędzia.
3. **Czy dane wpisane przez użytkownika są wykorzystywane do trenowania modelu lub ulepszania produktu?** Jeśli tak — kancelaria powinna ocenić, czy jest to zgodne z celem powierzenia, z zakresem zgody klienta (jeśli stanowi ona podstawę przetwarzania) i z obowiązkiem zachowania tajemnicy zawodowej.
4. **Czy możliwe jest korzystanie z narzędzia bez przesyłania danych poza infrastrukturę kancelarii?** Jeśli dostawca nie potrafi udzielić jednoznacznej odpowiedzi na to pytanie — odpowiedź praktyczna brzmi: nie.

Nota

Niniejszy materiał ma charakter wyłącznie informacyjny i edukacyjny. Nie stanowi porady prawnej ani opinii prawnej w rozumieniu właściwych przepisów. Ocena zgodności konkretnego narzędzia z obowiązującym prawem wymaga analizy prawnej uwzględniającej indywidualną sytuację kancelarii, charakter przetwarzanych danych osobowych i warunki konkretnej umowy z dostawcą. Przywołane przepisy prawa powszechnie obowiązującego cytowane są w brzmieniu aktualnym na datę publikacji niniejszego materiału.

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