Avantwerk | LEGAL AI

BEZPŁATNY MATERIAŁ · DLA KANCELARII

Kontrola UODO a korzystanie z AI w kancelarii

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

Lista kontrolna gotowości

Zasada rozliczalności z art. 5 ust. 2 RODO wymaga przestrzegania zasad ochrony danych i możliwości wykazania tego. Potrzebne dowody zależą od przetwarzania i ryzyka. Poniższa lista porządkuje przygotowanie; nie przedstawia statystyki ustaleń ani kar UODO i nie gwarantuje wyniku kontroli.

Ochrona tajemnicy zawodowej wymaga osobnej uwagi. Art. 16b Prawa o adwokaturze i art. 5b ustawy o radcach prawnych zachowują obowiązek tajemnicy przy żądaniu właściwego organu nadzorczego. Przed udostępnieniem materiału należy ocenić zakres żądania, właściwe przepisy i sposób ochrony tajemnicy. Nie należy przekazywać pełnych akt wyłącznie dlatego, że lista kontrolna wymienia dokumentację do okazania.

A. Dokumentacja i role

A.1 Czynności przetwarzania — art. 30 RODO

☐ Oceniono obowiązek prowadzenia rejestru, w tym warunki art. 30 ust. 5; mała liczba pracowników nie stanowi automatycznego zwolnienia.

☐ Rejestr opisuje aktualne czynności i istotne zmiany po wdrożeniu AI: cele, kategorie danych i osób, odbiorców, transfery, retencję i zabezpieczenia w wymaganym zakresie.

☐ Nowe narzędzie przypisano do odpowiedniej czynności lub zmieniono jej opis. Nie zakłada się, że każda aplikacja musi oznaczać odrębny wiersz.

Przygotuj: Aktualny rejestr albo uzasadnienie zakresu obowiązku; odrębnie można prowadzić pomocniczą listę narzędzi.

A.2 Dostawcy i umowy — art. 28 RODO

☐ Ustalono rzeczywiste role każdego podmiotu. Dostawca AI nie jest automatycznie procesorem.

☐ Gdy dane są przetwarzane w imieniu kancelarii jako administratora, uzgodnione postanowienia powierzenia obejmują wymagania art. 28 ust. 3 oraz dalszego powierzenia.

☐ Zachowano wersję i dowód uzgodnienia warunków. Umowa może być częścią warunków usługi i mieć formę elektroniczną; liczy się jej skuteczność i treść.

Przygotuj: Opis ról, umowy, wykaz podprocesorów, tryb informowania o zmianach i ocena wystarczających gwarancji.

A.3 Zasady pracy i odpowiedzialność

☐ Określono dopuszczone zastosowania, kategorie informacji, kontrolę dostępu, weryfikację wyników i reakcję na incydent.

☐ Wskazano osobę odpowiedzialną i terminy przeglądu.

☐ Jeżeli wyznaczono IOD, zapewniono jego udział i możliwość doradzania. Politykę przyjmuje osoba właściwa w kancelarii; funkcja doradcza i monitorująca IOD nie jest ustawowym obowiązkiem zatwierdzenia polityki.

Przygotuj: Przyjęte zasady, przypisanie odpowiedzialności oraz ewentualne zalecenia IOD i sposób ich rozpatrzenia.

A.4 Informacje dla osób — art. 13 i 14 RODO

☐ Informacje odpowiadają rzeczywistym celom, podstawom, odbiorcom, retencji i transferom. Sama nazwa technologii nie jest kategorią odbiorcy.

☐ Rozróżniono dane zbierane od osoby i pozyskane z innych źródeł. Dla art. 14 oceniono także mające zastosowanie wyjątki, w tym przewidziane w jego ust. 5.

Przygotuj: Właściwe klauzule, sposób ich przekazania albo udokumentowaną ocenę konkretnego wyjątku. Nowa wersja klauzuli jest potrzebna przy zmianie objętych nią informacji; samo dodanie aplikacji nie przesądza automatycznie o naruszeniu poprzedniej klauzuli.

B. Ryzyko i bezpieczeństwo — art. 5, 24, 25, 32 i 35 RODO

☐ Rozpoznano przepływy danych: model, interfejs, logi, wsparcie, kopie i odbiorców. Lokalizacja głównego serwera nie opisuje całego przetwarzania.

☐ Ograniczono dane do potrzebnego zakresu, a dostęp do osób uprawnionych; określono retencję i usuwanie.

☐ Oceniono potrzebę DPIA z art. 35. Gdy przetwarzanie z dużym prawdopodobieństwem powoduje wysokie ryzyko, ocenę wykonuje się przed jego rozpoczęciem, z konsultacją IOD, jeśli

został wyznaczony. Sama obecność AI nie przesądza ani o obowiązku DPIA, ani o zwolnieniu z niego.

☐ Zweryfikowano, czy informacje ze spraw są wykorzystywane do treningu lub własnych celów dostawcy. Zgoda kancelarii nie jest uniwersalną podstawą takiego użycia.

Przygotuj: Ocenę ryzyka, wynik analizy potrzeby DPIA i — jeśli wymagana — DPIA, dokumentację zabezpieczeń oraz warunków wykorzystania danych. Logi także wymagają minimalizacji, ochrony i retencji.

C. Weryfikacja wyników i naruszenia

☐ Ustalono kontrolę istotnych wyników przez prawnika i proporcjonalny sposób jej dokumentowania. Adnotacja nie zastępuje wykonanej weryfikacji.

☐ Procedura rozróżnia incydent bezpieczeństwa i naruszenie ochrony danych oraz role kancelarii i procesora.

☐ Dla naruszenia wymagającego zgłoszenia administrator działa bez zbędnej zwłoki, w miarę możliwości do 72 godzin po jego stwierdzeniu (art. 33 ust. 1 RODO). Ocenia także wyjątek, gdy ryzyko naruszenia praw lub wolności jest mało prawdopodobne; dokumentuje naruszenia zgodnie z ust. 5 i przyczyny decyzji.

☐ Ocenia się zawiadomienie osób przy wysokim ryzyku, z uwzględnieniem art. 34 i jego wyjątków. Procesor zgłasza naruszenie administratorowi bez zbędnej zwłoki; umowny termin operacyjny nie zastępuje tej zasady.

Przygotuj: Role, kontakty, ocenę ryzyka naruszenia, ewidencję zdarzeń, uzasadnienie zgłoszenia lub jego braku i dokumentację działań. Pusty formularz jest pomocą organizacyjną, nie samodzielnym ustawowym dowodem zgodności.

D. Transfer poza EOG — rozdział V RODO

☐ Ustalono odbiorców, państwa i dostęp zewnętrzny, także w usługach pomocniczych.

☐ Jeśli występuje transfer, określono właściwy mechanizm i spełnienie jego warunków. Sam podpis pod umową powierzenia lub deklaracja dostawcy nie wystarczają.

☐ Przy odpowiednich zabezpieczeniach oceniono ich skuteczność w konkretnym transferze oraz potrzebę dodatkowych środków. Wyjątków z art. 49 nie traktuje się jako rutynowej podstawy każdego przepływu.

Przygotuj: Opis przepływu, podstawę transferu i odpowiednią ocenę oraz dokumentację zabezpieczeń. Gdy transferu brak, zachowaj ustalenia dotyczące całego przepływu, a nie

wyłącznie lokalizacji modelu.

E. Kompetencje AI i właściwe terminy

☐ Przyjęto działania wspierające rozwój kompetencji AI zgodnie z aktualnym art. 4 AI Act, uwzględniające zespół, kontekst i odbiorców. Przepis nie wymaga zagwarantowania określonego poziomu każdej osoby.

☐ Oddzielono obowiązki już stosowane od przyszłego reżimu wysokiego ryzyka. Art. 4 jest stosowany od 2 lutego 2025 r. Rozdział III sekcje 1–3, z wyjątkiem art. 6 ust. 5, stosuje się do właściwych systemów z Załącznika III od 2 grudnia 2027 r., a z Załącznika I od 2 sierpnia 2028 r.; należy sprawdzić art. 111.

☐ Monitorowanie zmian obejmuje przepisy i źródła właściwe zastosowaniu, a przegląd jest uruchamiany także po zmianie narzędzia lub incydencie.

Przygotuj: Informację o działaniach szkoleniowych i instrukcjach, przypisaniu odpowiedzialności oraz przyjętej ocenie systemu i terminów. Nie przedstawiaj nadzoru z art. 26 jako obowiązku stosowanego już do wszystkich systemów od sierpnia 2026 r.

Źródła i zakres przeglądu

Sprawdzono wskazane przepisy RODO, art. 4, 26, 111 i 113 AI Act oraz art. 16b Prawa o adwokaturze 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..
- AI Act — art. 4, 26, 111 i 113, aktualny tekst skonsolidowany. Teksty ujednolicone ułatwiają odczytanie zmian; autentyczne brzmienie ustaw wynika z ogłoszonych aktów.

Historia zmian — 2026-11 względem 2026-07: Poprawiono terminy AI Act, rolę IOD, zakres powierzenia i rejestru, brakujący opis DPIA, warunki zgłaszania naruszeń oraz ochronę tajemnicy przy kontroli. Usunięto nieudokumentowane twierdzenia o najczęstszych karach i ustaleniach kontroli.

Materiał edukacyjny, nie porada prawna ani ocena zgodności konkretnego wdrożenia. Przed decyzją sprawdź aktualne prawo, źródła zawodowe i działanie narzędzia.