

Kontrola UODO a korzystanie z AI w kancelarii — lista kontrolna gotowości

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

Wstęp: Rozliczalność to nie stan — to dowód

Artykuł 5 ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (dalej: RODO) formułuje zasadę rozliczalności jednym zdaniem: administrator danych **odpowiada za przestrzeganie** zasad przetwarzania danych i **jest w stanie wykazać ich przestrzeganie**. Drugi człon tego zdania jest najczęściej pomijanym — i najczęściej karanym — elementem. Nie wystarczy działać zgodnie z prawem. Trzeba mieć dokumenty, które to udowadniają, i trzeba umieć je przedstawić na żądanie.

Gdy Prezes Urzędu Ochrony Danych Osobowych wszczyna kontrolę, na stole pojawia się pytanie nie o przekonania prawnika, lecz o dowody. Kontrolerzy działający na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000) mogą wejść do pomieszczeń, żądać wglądu w dokumentację, przesłuchać pracowników i zbadać systemy informatyczne. Kancelaria, która działa poprawnie, ale nie ma dokumentów, działa tak samo bez skutku jak kancelaria, która nie działa poprawnie w ogóle.

Korzystanie z narzędzi AI dodaje do tego obrazu warstwy ryzyka, których tradycyjna praktyka ochrony danych nie przewidywała: dane klientów mogą opuszczać kancelarię, trafiać do podmiotów zewnętrznych — niekiedy poza Europejskim Obszarem Gospodarczym — i być przetwarzane przez algorytmy, których mechanizmów decyzyjnych prawnik bezpośrednio nie kontroluje.

Dodatkową, bezwzględną warstwą nałożoną specyficznie na kancelarie adwokackie i radcowskie jest **tajemnica zawodowa** — art. 6 ustawy z dnia 26 maja 1982 r. — Prawo o adwokaturze (Dz.U. 1982 nr 16 poz. 124 ze zm.) oraz art. 3 ust. 3–6 ustawy z dnia 6 lipca 1982 r. o radcach prawnych (Dz.U. 1982 nr 19 poz. 145 ze zm.). Tajemnica ta jest bezterminowa, bezwzględna i nie podlega uchyleniu przez mocodawcę. Nie ma w tych przepisach wyjątku technologicznego: treść sprawy skierowana do zewnętrznego narzędzia AI to treść sprawy, która opuściła dyspozycję prawnika. Wykazanie zgodności z RODO nie zwalnia z wykazania zgodności z tajemnicą zawodową — i odwrotnie.

Poniższa lista kontrolna porządkuje kluczowe obszary. Każda pozycja wskazuje, czego Prezes UODO może szukać podczas kontroli oraz co kancelaria powinna mieć przygotowane, żeby wykazać zgodność.

Lista kontrolna

A. Dokumentacja

A.1 Rejestr czynności przetwarzania — art. 30 RODO

- ☐ Rejestr czynności przetwarzania zawiera wpis lub wiersze opisujące czynności przetwarzania danych z udziałem narzędzia AI.
- ☐ Wpis obejmuje: cel przetwarzania, kategorie danych osobowych, kategorie osób, których dane dotyczą, odbiorców danych (w tym dostawcę narzędzia AI jako podmiot przetwarzający), planowane terminy usunięcia danych oraz opis środków technicznych i organizacyjnych.
- ☐ Rejestr jest aktualny — uwzględnia narzędzia faktycznie używane, nie narzędzia historyczne ani planowane.

Co mieć gotowe: Aktualny rejestr z datą ostatniej aktualizacji, w formie pisemnej lub elektronicznej, dostępny do okazania kontrolerom bez zwłoki.

A.2 Umowa powierzenia przetwarzania z dostawcą AI — art. 28 RODO

- ☐ Dla każdego narzędzia AI, do którego trafiają dane osobowe klientów lub stron postępowania, kancelaria dysponuje zawartą na piśmie (lub w trwałej formie elektronicznej) umową powierzenia przetwarzania danych.
- ☐ Umowa spełnia wymogi art. 28 ust. 3 RODO: precyzuje przedmiot, czas trwania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa administratora.
- ☐ Umowa zawiera klauzulę dotyczącą dalszego powierzenia przetwarzania (podprocesora) — dotyczy to w szczególności sytuacji, gdy dostawca narzędzia AI korzysta z modelu językowego będącego usługą zewnętrznego operatora.

Co mieć gotowe: Podpisana umowa powierzenia lub — jeśli dostawca stosuje standardowe warunki — dokumentacja ich zaakceptowania z datą i wersją warunków. Uwaga: dostawca AI, który nie oferuje umowy powierzenia zgodnej z art. 28 RODO, nie może przetwarzać danych osobowych klientów kancelarii.

A.3 Wewnętrzna polityka korzystania z AI

- ☐ Kancelaria posiada wewnętrzny dokument (politykę, procedurę lub instrukcję) określający zasady korzystania z narzędzi AI przez prawników i pracowników.
- ☐ Dokument opisuje, jakie kategorie danych mogą być kierowane do narzędzia AI, a jakie są wyłączone — w szczególności dane szczególnych kategorii w rozumieniu art. 9 RODO (m.in. dane o zdrowiu, przekonaniach religijnych, przynależności związkowej) oraz dane objęte tajemnicą zawodową w zakresie uniemożliwiającym ich zewnętrzne przetwarzanie.
- ☐ Polityka wskazuje osobę odpowiedzialną za jej przestrzeganie i datę ostatniego przeglądu.

Co mieć gotowe: Aktualny dokument polityki z datą wejścia w życie, zatwierdzony — jeśli kancelaria wyznacza IOD — przez inspektora ochrony danych.

A.4 Klauzule informacyjne — art. 13–14 RODO

- ☐ Klauzula informacyjna przekazywana klientom przy nawiązaniu współpracy (art. 13 RODO) zawiera informację o ewentualnym korzystaniu z narzędzi AI jako podmiotów przetwarzających lub odbiorców danych, w tym — jeśli dotyczy — o transferze danych poza EOG.
- ☐ Jeśli kancelaria przetwarza z użyciem AI dane pozyskane nie od osoby, której dane dotyczą bezpośrednio (np. dane stron przeciwnych, świadków, kontrahentów), kancelaria dysponuje procedurą realizacji obowiązku informacyjnego z art. 14 RODO.

Co mieć gotowe: Aktualne wzory klauzul informacyjnych uwzględniające AI jako kategorię odbiorcy, z datą ostatniej aktualizacji następującej po wdrożeniu narzędzia AI.

B. Techniczne i organizacyjne środki bezpieczeństwa — art. 32 RODO

- ☐ Kancelaria przeprowadziła i udokumentowała ocenę ryzyka dla czynności przetwarzania danych z użyciem AI — uwzględniając ryzyko nieuprawnionego dostępu, ryzyko transferu danych poza EOG i ryzyko naruszenia tajemnicy zawodowej.
- ☐ Kancelaria wie, **gdzie fizycznie przetwarzane są dane** kierowane do narzędzia AI: w jakim kraju, na czyich serwerach, jak długo dane są tam przechowywane.
- ☐ Stosowana jest zasada minimalizacji danych (art. 5 ust. 1 lit. c RODO): do narzędzia AI kierowane są wyłącznie dane niezbędne do konkretnego zadania; tam, gdzie możliwa jest pseudonimizacja zapytań przed przekazaniem do AI — jest ona stosowana.
- ☐ Kontrola dostępu: dostęp do narzędzia AI mają wyłącznie osoby upoważnione; dane logowania nie są współdzielone między użytkownikami.
- ☐ Kancelaria potwierdziła — w umowie powierzenia lub w pisemnej polityce dostawcy — że dane klientów **nie są używane do trenowania modeli AI** bez uprzedniej zgody kancelarii jako administratora.

Co mieć gotowe: Udokumentowana ocena ryzyka (może być zintegrowana z DPIA — patrz sekcja D) + rejestr upoważnień do systemu AI + pisemne potwierdzenie polityki dostawcy w zakresie trenowania modeli.

C. Nadzór, ślad i procedura naruszeniowa — art. 33–34 RODO

- ☐ Kancelaria prowadzi lub jest w stanie odtworzyć ewidencję, kiedy i w jakim celu narzędzie AI było użyte w danej sprawie — ślad użycia AI umożliwiający weryfikację post factum.
- ☐ Kancelaria stosuje i dokumentuje zasadę nadzoru człowieka: wyniki generowane przez AI są każdorazowo weryfikowane przez prawnika przed przekazaniem klientowi lub sądowi. Zasada ta jest odzwierciedlona w polityce AI (sekcja A.3).
- ☐ Kancelaria posiada pisemną procedurę postępowania w przypadku naruszenia ochrony danych osobowych, uwzględniającą scenariusz: „dostawca narzędzia AI lub jego podprocesor doznał incydentu bezpieczeństwa dotyczącego danych kancelarii”.

☐ Procedura przewiduje 72-godzinny termin zgłoszenia naruszenia do Prezesa UODO (art. 33 ust. 1 RODO) — liczony od momentu uzyskania wiedzy o naruszeniu — oraz procedurę zawiadamiania osób, których dane dotyczą (art. 34 RODO), jeśli naruszenie niesie wysokie ryzyko dla praw i wolności tych osób.

☐ Kancelaria prowadzi rejestr naruszeń (art. 33 ust. 5 RODO) — nawet jeśli do tej pory nie odnotowano żadnego naruszenia, rejestr powinien istnieć i być gotowy do uzupełnienia.

Co mieć gotowe: Pisemna procedura naruszeniowa z przypisanymi rolami i terminami + pusty lub wypełniony rejestr naruszeń + dokumentacja zasady nadzoru człowieka nad wynikami AI.

D. Transfer danych poza Europejski Obszar Gospodarczy — Rozdział V RODO (art. 44–49)

☐ Kancelaria ustaliła, czy dostawca narzędzia AI lub operator modelu językowego przetwarza dane poza EOG (np. na serwerach w Stanach Zjednoczonych, Kanadzie lub innym państwie trzecim).

☐ Jeśli transfer poza EOG ma miejsce: kancelaria zidentyfikowała i udokumentowała podstawę prawną transferu zgodnie z art. 44–49 RODO — decyzję Komisji Europejskiej stwierdzającą odpowiedni stopień ochrony (adequacy decision), standardowe klauzule umowne (SCC) lub inną enumeratywnie wskazaną podstawę.

☐ Jeśli transfer opiera się na standardowych klauzulach umownych: kancelaria przeprowadziła lub uzyskała od dostawcy ocenę skutków transferu (Transfer Impact Assessment) wymaganą po wyroku Trybunału Sprawiedliwości UE z dnia 16 lipca 2020 r. w sprawie C-311/18 (Schrems II).

☐ Jeśli transfer poza EOG nie może być zalegalizowany na żadnej z dostępnych podstaw: kancelaria nie kieruje danych osobowych do tego narzędzia.

Co mieć gotowe: Pisemna dokumentacja podstawy prawnej transferu i — jeśli zastosowane są SCC — ocena skutków transferu. Alternatywnie: pisemne potwierdzenie od dostawcy, że dane nie opuszczają EOG.

E. Kompetencje i szkolenie

☐ Prawnicy i pracownicy kancelarii mający dostęp do narzędzia AI zostali poinformowani o zasadach jego użycia, ograniczeniach wynikających z tajemnicy zawodowej i treści polityki AI kancelarii.

☐ Kancelaria śledzi komunikaty Prezesa UODO oraz bieżące wytyczne Europejskiej Rady Ochrony Danych (EROD) dotyczące przetwarzania danych w kontekście systemów AI.

☐ Jeśli kancelaria wyznaczyła IOD: inspektor był konsultowany przy wdrożeniu narzędzia AI i zaopiniował politykę AI (sekcja A.3).

Co mieć gotowe: Potwierdzenie przeprowadzenia szkolenia lub poinformowania personelu (lista uczestników, e-mail informacyjny lub notatka służbowa). Notatka z konsultacji z IOD, jeśli dotyczy.

Najczęstsze braki stwierdzane przy kontroli

- 1. Brak aktualizacji rejestru czynności przetwarzania po wdrożeniu AI.** Kancelarie często dysponują rejestrem sporządzonym przed wdrożeniem narzędzia AI i nigdy go nie zaktualizowały. Nowe narzędzie = nowy wpis lub nowy wiersz. Naruszenie art. 30 RODO.
 - 2. Brak umowy powierzenia lub niedostateczna jej treść.** Kancelaria zaakceptowała ogólne warunki korzystania z usługi dostawcy, nie weryfikując, czy spełniają one wymogi art. 28 ust. 3 RODO — w szczególności czy zawierają klauzulę dotyczącą podprocesora (operatora modelu AI), który może znajdować się w państwie trzecim.
 - 3. Nieaktualne klauzule informacyjne dla klientów.** Klientom przekazywano klauzule sprzed wdrożenia narzędzia AI — bez wzmianki o dostawcy AI jako odbiorcy danych. Naruszenie art. 13 RODO.
 - 4. Brak dokumentacji zasady nadzoru człowieka.** Prawnik każdorazowo weryfikuje wyniki AI — ale nigdzie tego nie zapisał. Sama deklaracja nie wystarcza. Brak dokumentacji utrudnia wykazanie zgodności z zasadą rozliczalności z art. 5 ust. 2 RODO, a — począwszy od 2 sierpnia 2026 r. — również z obowiązkami wynikającymi z Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie sztucznej inteligencji (Akt o AI) w zakresie nadzoru nad systemami AI wysokiego ryzyka.
-

Disclaimer

Niniejszy materiał ma charakter wyłącznie edukacyjny i informacyjny. Nie stanowi porady prawnej ani opinii prawnej w rozumieniu obowiązujących przepisów prawa. Każda kancelaria powinna ocenić swoją indywidualną sytuację, uwzględniając specyfikę prowadzonej działalności, stosowane narzędzia oraz aktualny stan prawny. W przypadku wątpliwości zalecamy konsultację z adwokatem, radcą prawnym lub inspektorem ochrony danych specjalizującym się w tej dziedzinie.

Stan prawny: lipiec 2026 r. Materiał nie uwzględnia ewentualnych zmian legislacyjnych po dacie publikacji.

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