AI W PRACY RADCY PRAWNEGO

KRAJOWA IZBA
RADCÓW PRAWNYCH

WARSZAWA 2026

AI W PRACY RADCY PRAWNEGO

REKOMENDACJE DOTYCZĄCE KORZYSTANIA PRZEZ RADCÓW PRAWNYCH Z NARZĘDZI OPARTYCH NA SZTUCZNEJ INTELIGENCJI

Wydanie 2
Warszawa 2026



KRAJOWA IZBA
RADCÓW PRAWNYCH



SK&S

Wydawca: Krajowa Izba Radców Prawnych,
ul. Powązkowska 15, 01–797 Warszawa

© Copyright by Microsoft sp. z o.o., 2026

ISBN 978-83-980593-1-2

Redakcja: Klara Szczęsnowicz

Korekta: Aleksandra Sachanowicz-Wrzal

Skład i łamanie: Aleksandra Snitsaruk

Druk: Wiedza i Praktyka sp. z o.o.

Słowo wstępne



Jeszcze nigdy prawnik nie miał pod ręką tak wielu narzędzi, które obiecują mu oszczędność czasu. I chyba nigdy nie musiał z taką uwagą sprawdzać, czy rzeczywiście można na nich polegać. Sztuczna inteligencja potrafi imponować, zaskakiwać, pomagać, ale też popełniać błędy z niezwykłą pewnością siebie. W zawodzie radcy prawnego ta ostatnia cecha może okazać się szczególnie kosztowna.

Dlatego najważniejsze pytanie na dziś brzmi: jak korzystać z AI mądrze, bezpiecznie i z rzeczywistą korzyścią dla siebie i swoich klientów? Jak odróżnić przydatne narzędzie od efektownej obietnicy? Jak wykorzystać nowe możliwości, nie tracąc z oczu zasad wykonywania zawodu? I wreszcie – jak nadążyć za technologią, która zmienia się szybciej niż nasze przyzwyczajenia?

Wierzę, że znacznie łatwiej odpowiedzieć na te pytania po lekturze drugiego wydania poradnika „AI w pracy radcy prawnego", które z satysfakcją oddajemy właśnie w Państwa ręce. Sam fakt, że tak szybko wracamy do tej publikacji, jest wymowny. W świecie AI wiedza wymaga uzupełniania niemal ciągle, pojawiają się nowe możliwości, wyzwania i kolejne pytania dotyczące granic odpowiedzialnego wykorzystywania technologii. Nie wystarczy raz rozeznać tematu – trzeba stale rozwijać kompetencje, sprawdzać przyjęte rozwiązania i być gotowym do uczenia się na nowo.

Jako samorząd zawodowy aktywnie wspieramy radców prawnych w tym procesie. Dlatego Krajowa Izba Radców Prawnych rozwija działania edukacyjne poświęcone sztucznej inteligencji na wielu polach. Organizujemy konferencje, udostępniamy szkolenia na platformie e-KIRP, współpracujemy z zewnętrznymi firmami technologicznymi oraz ekspertami, dzięki którym radcowie prawni mogą korzystać ze specjalistycznej wiedzy, zdobywać praktyczne umiejętności, a także potwierdzać nowe kompetencje odpowiednimi certyfikatami. Zależy nam, aby dostęp do rzetelnej edukacji technologicznej nie był przywilejem nielicznych, lecz realną możliwością dla każdego członka naszego samorządu, niezależnie od wielkości kancelarii, miejsca wykonywania zawodu czy dotychczasowego doświadczenia z AI.

Niniejszy poradnik jest ważną częścią tych działań. Łączy wiedzę o technologii z tym, co dla nas szczególnie istotne – praktyką wykonywania zawodu radcy prawnego. Autorzy prowadzą czytelnika od podstaw funkcjonowania sztucznej inteligencji przez regulacje prawne, kwestie ochrony danych i odpowiedzialności zawodowej aż po konkretne zastosowania narzędzi AI w codziennej pracy. Zrozumiale i interesująco.

W tym miejscu chcę podziękować Autorom poradnika za ich wiedzę, zaangażowanie i wysiłek włożony w przygotowanie kolejnego wydania. Dzięki ich pracy otrzymujemy publikację, która jednocześnie porządkuje wiedzę i pomaga podejmować świadome decyzje.

Zależy nam, by ta publikacja była przede wszystkim zachętą do samodzielnego odkrywania możliwości AI – z ciekawością, ale i zdrowym krytycyzmem. Technologia może pomóc nam pracować szybciej i sprawniej, jednak nie zwalnia z myślenia, weryfikowania informacji ani podejmowania odpowiedzialnych decyzji. Przyszłość naszego zawodu nie zależy od tego, jak wiele potrafi sztuczna inteligencja. Zależy od tego, jak dobrze my nauczymy się wykorzystywać jej możliwości.

Dlatego zachęcam Państwa do lektury i dalszego rozwijania kompetencji. Warto wykorzystać tę szansę – na własnych zasadach, z właściwą nam odpowiedzialnością i profesjonalizmem.

Włodzimierz Chróścik
Prezes Krajowej Rady Radców Prawnych

1. EDYCJA REKOMENDACJI PRZYGOTOWANA WE WSPÓŁPRACY Z:



Krajowa Izba Radców Prawnych

- dr Damian Flisak – radca prawny, KIRP
- dr Paweł Kowalski – radca prawny, pełnomocnik Prezesa Krajowej Rady Radców Prawnych ds. nowych technologii, KIRP



Microsoft sp. z o.o.

- Renata Zalewska – radca prawny, head of legal
- Tomek Kasprzyk – legal program manager
- Paweł Wróbel – technical architect innovation hub | Central Europe



Sołtysiński Kawecki & Szlęzak Kancelaria Radców Prawnych i Adwokatów Spółka Komandytowa

- Agata Szeliga – partner
- Sylwia Macura-Targosz – starszy prawnik
- Katarzyna Paziewska-Młodawska – starszy prawnik
- Anna Tujakowska – senior counsel, head of legaltech & innovation

2. EDYCJA REKOMENDACJI PRZYGOTOWANA WE WSPÓŁPRACY Z:

KRAJOWA IZBA RADCÓW PRAWNYCH

Krajowa Izba Radców Prawnych

- dr hab. Dominik Lubasz – radca prawny, prof. Uniwersytetu Łódzkiego, członek Komisji Nowych Technologii, KIRP
- dr Paweł Kowalski – radca prawny, pełnomocnik Prezesa Krajowej Rady Radców Prawnych ds. nowych technologii, KIRP
- dr Maciej Tąkiel, dyrektor innowacji, Greenberg Traurig, Uniwersytet Warszawski, KIRP

Microsoft

Microsoft sp. z o.o.

- Renata Zalewska – radca prawny, head of legal
- Paweł Wróbel – technical architect innovation hub | Central Europe

SK&S

Sołtysiński Kawecki & Szlęzak Kancelaria Radców Prawnych i Adwokatów Spółka Komandytowa

- Agata Szeliga – partner
- Sylwia Macura-Targosz – senior counsel
- Agnieszka Jurcewicz-Androsz – starszy prawnik
- Katarzyna Wnuk – starszy prawnik
- Sandra Słowik – prawnik
- Anna Tujakowska – senior counsel, head of legaltech & innovation

WSTĘP

Po roku od opublikowania „Rekomendacji" nie zadajemy sobie już pytania, czy prawnicy będą wykorzystywać rozwiązania oparte na AI. Korzystanie z AI stało się codziennością dla większości radców prawnych. Mają oni do swojej dyspozycji zarówno rozwiązania uniwersalne, jak i narzędzia przeznaczone tylko dla prawników. Sama technologia AI rozwija się bardzo dynamicznie. Od nowych modeli AI po nowe sposoby pracy, w tym obejmujące agentów. Pojawiły się też nowe regulacje, czyli przede wszystkim Akt w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji czy Cyfrowy Omnibus, zmieniający te przepisy.

AI daje możliwość zbudowania lepszej relacji z klientami i poprawy jakości pracy – od poprawienia języka porady na bardziej zrozumiały dla biznesu po szybszą identyfikację potencjalnych ryzyk dla klientów i sposobów ich ograniczenia.

Ciągle pozostaje jednak aktualne pytanie, jak radcowie prawni powinni korzystać z tej technologii bez naruszania zasad etyki zawodowej i zachowując bezpieczeństwo prawne klientów. Coraz większe znaczenie mają również kompetencje nie tylko samego używania AI, lecz także odpowiedzialnego dostosowywania się do tych szybkich zmian prawnych i technologicznych. To spowodowało, że postanowiliśmy przygotować dla Państwa aktualizację rekomendacji.

W kolejnej edycji rekomendacji zachowaliśmy wcześniejszy układ. Pierwsza część zawiera podstawowe pojęcia i ogólne informacje o regulacjach dotyczących korzystania ze sztucznej inteligencji. Druga zawiera uaktualnione rekomendacje podzielone na trzy grupy:

- rekomendacje dotyczące przygotowania do korzystania z narzędzi AI,
- rekomendacje dotyczące wdrażania narzędzi AI,
- rekomendacje dotyczące stosowania narzędzi AI.

Wśród nowych rekomendacji znajdą Państwo zalecenia dotyczące uwzględniania AI w szkoleniach aplikantów radcowskich oraz młodych prawników, korzystania z agentów AI w pracy prawników, zasad informowania o korzystaniu z AI (w tym także oznaczania treści wygenerowanych przez AI), a także kwalifikacji narzędzi AI w świetle Aktu o AI.

Uaktualniony został też załącznik nr 2 z przykładami zastosowań AI.

Dodane zostały nowe załączniki: lista sprawdzająca wspierająca analizę zagadnień wynikających z RODO i Aktu o AI przed wdrożeniem narzędzia AI oraz wzór rejestru wykorzystywanych narzędzi AI. Rekomendacje pozostają neutralne wobec dostawców narzędzi AI. Nazwy produktów, w szczególności w załącznikach nr 1 i 2, służą wyłącznie ilustracji i nie są rekomendacją wyboru określonego narzędzia przez samorząd radcowski. Opisy funkcji, warunków licencyjnych i zasad przetwarzania danych odpowiadają stanowi prawnemu na dzień przygotowania niniejszego wydania (22.10.2026 r.) i mogą ulec zmianie; przed wdrożeniem narzędzia radca prawny powinien sprawdzić je w aktualnej dokumentacji i w umowie z dostawcą.

SPIS TREŚCI

Rozdział I 10
SZTUCZNA INTELIGENCJA – PODSTAWOWE ZAGADNIENIA
1. Czym jest AI? 10
2. Przykładowe dostępne narzędzia AI 17
3. Podstawowe pojęcia – generowanie i używanie (trenowanie) danych 20
4. AI a chmura obliczeniowa 23
5. Przykładowe zastosowania narzędzi generatywnej AI w pracy radcy prawnego 24

Rozdział II 26
PRZEPISY PRAWA – PODSTAWOWE REGULACJE
1. Dane osobowe 26
2. Akt o AI 31
3. Prawo autorskie 34
4. Ogólne regulacje dotyczące stosunków umownych 36
5. Odpowiedzialność za produkty wadliwe 36
6. Cyberbezpieczeństwo 37
7. Regulacje dotyczące radców prawnych 38
8. Postępowanie karne 39

Rozdział III 40
KORZYSTANIE Z NARZĘDZI AI PRZEZ PRAWNIKÓW – KORZYŚCI, WYZWANIA I RYZYKA
1. Korzyści 40
2. Wyzwania 42
3. Ryzyka 44

Rozdział IV 50
WYTYCZNE ZAGRANICZNYCH STOWARZYSZEŃ PRAWNIKÓW CO DO STOSOWANIA NARZĘDZI AI

Rozdział V 53
REKOMENDACJE

Załączniki 92
1. Wskazówki dotyczące optymalnego promptowania 92
2. Przykłady zastosowań AI (przy użyciu Microsoft 365 Copilot) 95
3. Obowiązek informacyjny dla radcy prawnego (art. 13 i 14 RODO) 126
4. Wdrożeniowa lista sprawdzająca AI (RODO & Akt o AI) 127
5. Rejestr wykorzystywanych narzędzi AI 138

Rozdział I

SZTUCZNA INTELIGENCJA – PODSTAWOWE ZAGADNIENIA

1. Czym jest AI?

1.1. *STATUS QUO*

AI, zwłaszcza generatywna sztuczna inteligencja, jest szeroko stosowana w wielu branżach, w tym w medycynie, e-commerce, finansach czy przemyśle. Obecnie pozwala przede wszystkim na zwiększenie efektywności organizacji wykorzystujących narzędzia AI, ale ma też potencjał w zakresie przyspieszenia lub rozwoju innowacji.

Rozwiązania korzystające z AI są również przydatne w zawodzie radcy prawnego. Mogą służyć wykonywaniu różnych zadań, takich jak analiza dokumentów, generowanie umów czy przeszukiwanie dużych zbiorów danych. To pozwala radcom prawnym oszczędzać czas oraz koncentrować się na bardziej złożonych aspektach pracy, wymagających ludzkiej oceny i kreatywności. Rozwój AI jest bardzo dynamiczny i zmienia też sposób wykonywania zawodu. Wraz z pojawieniem się tzw. agentów AI możemy samodzielnie tworzyć bardziej skomplikowane procesy (*workflow*) i automatyzować część pracy prawniczej, wykorzystując agenta AI posiadającego pewien poziom autonomii w działaniu. Dla przykładu agent AI może wykonywać działania składające się z wielu etapów, np. wyszukać właściwe przepisy lub wymogi umowne, zastosować je przy analizie dokumentu, wprowadzić zmiany do dokumentu wynikające z analizy, bez konieczności angażowania człowieka na każdym etapie pracy.

Dynamiczny rozwój i upowszechnienie AI przyspieszyły prace nad określeniem prawnych ram korzystania z tej technologii. W dniu 13 czerwca 2024 r. przyjęte zostało rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (Akt w sprawie sztucznej

inteligencji; „**Akt o AI**"). Przepisy Aktu o AI dotyczące zakazanych praktyk oraz kompetencji w zakresie AI już obowiązują. Akt o AI został następnie zmieniony przez rozporządzenie Parlamentu Europejskiego i Rady zmieniające rozporządzenia (UE) 2024/1689 i (UE) 2018/1139 w odniesieniu do uproszczenia wdrażania zharmonizowanych przepisów dotyczących sztucznej inteligencji (akt zbiorczy prawa cyfrowego dotyczący AI; „**rozporządzenie Omnibus dotyczące AI**"). Rozporządzenie Omnibus dotyczące AI wprowadza m.in. nowe terminy stosowania pozostałych przepisów Aktu o AI. Przepisom unijnym towarzyszą również regulacje krajowe mające zapewnić właściwe wdrożenie i nadzór nad AI w państwach członkowskich UE (w Polsce ustawa z dnia 3 lipca 2026 r. o systemach sztucznej inteligencji, Dz.U. z 2026 r. poz. 1003)[1]. Komisja Europejska wydała też pierwsze wytyczne i wskazówki.

1.2. PREDYKCYJNA I GENERATYWNA AI

AI to dziedzina nauki, której celem jest budowanie systemów mających działać inteligentnie.

AI można podzielić na predykcyjną i generatywną, różniące się przede wszystkim sposobem, w jaki przetwarzają dane i generują wyniki. Systemy AI mogą przy tym łączyć oba te podejścia.

Predykcyjna AI (*Predictive AI*) to rodzaj sztucznej inteligencji, która analizuje dane historyczne, aby przewidywać przyszłe wydarzenia lub wyniki. Najistotniejszym elementem predykcyjnej AI są uczenie maszynowe (*machine learning*) i modele statystyczne. Uczenie maszynowe polega na tworzeniu algorytmów umożliwiających systemom komputerowym wykonywanie zadań bez instrukcji, opierając się na wzorcach i wnioskowaniu, a następnie pozwala wykorzystywać te informacje do przewidywania przyszłych zdarzeń lub wyników. Celem uczenia maszynowego jest analiza danych w celu znalezienia wzorców i dokonywania prognoz. To podejście jest obecnie wykorzystywane np. do prognozowania pogody, przewidywania awarii maszyn czy oceny ryzyka kredytowego.

Generatywna AI (GenAI; *Generative AI*) to rodzaj sztucznej inteligencji mogącej tworzyć nowe treści (takie jak tekst, obrazy, muzyka, kod komputerowy) na podstawie danych treningowych. Głównym elementem generatywnej AI są duże modele językowe (LLM; *large language models*), sieci neuronowe czy

[1] Ustawa: https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20260001003 [dostęp: 21.10.2026 r.].

transformery, które przetwarzają i generują tekst przypominający tekst ludzki na podstawie nauczonych wzorców. Przykładem rozwiązania bazującego na generatywnej AI są: ChatGPT, który generuje teksty na podstawie dostarczonych mu danych, DALL-E, który służy do generowania obrazów, czy GitHub Copilot – generujący kod komputerowy lub weryfikujący taki kod.

1.3. JAK DZIAŁA AI?

Końcowym celem badaczy jest stworzenie ogólnej sztucznej inteligencji (*general AI*), to jest systemu, który ma być zdolny do rozumowania i wyciągania wniosków na poziomie takim samym lub nawet lepszym niż człowiek. Taka ogólna AI będzie sama się uczyła, jak wyciągać wnioski, rozwiązywać złożone problemy i rozwijać się, nawet bez udziału człowieka. W tej chwili trwa dyskusja, czy należy dopuścić do trenowania i rozwoju AI przez samą AI (*recursive self-improvement*), czy też przejście do tego etapu będzie oznaczało, że ludzie nie będą wiedzieli, na czym opiera się, jak została zbudowana i jak działają takie systemy i modele AI.

Na obecnym etapie rozwoju AI możemy wyróżnić następujące etapy w działaniu AI:

- zbieranie danych i ich przygotowywanie do dalszego wykorzystania,
- przetwarzanie danych i uczenie się (trenowanie modelu),
- budowa modelu,
- testowanie, walidacja i doskonalenie modelu AI,
- tworzenie systemu AI.

Pierwszym krokiem jest zbieranie dużych zbiorów danych, które mogą pochodzić z różnych źródeł, w tym z Internetu, zasobów własnych czy określonych podmiotów (np. z dokumentów, książek, archiwów prasowych), lub stworzenie danych syntetycznych. Dane te są podstawą, na której AI będzie się uczyć i później podejmować dalsze działania. Na tym etapie dane powinny być też weryfikowane pod kątem ich poprawności lub ryzyka dyskryminacji (np. przez usuwanie błędnych danych).

Kolejnym krokiem jest przetwarzanie i analizowanie zebranych danych oraz uczenie się. Główne techniki uczenia modeli AI obejmują techniki oparte na uczeniu maszynowym, które uczą się z danych, jak osiągać określone cele, oraz techniki oparte na logice i wiedzy, które wnioskują na podstawie zakodowanej wiedzy lub symbolicznej reprezentacji zadania do rozwiązania.

Uczenie maszynowe obejmuje różne podejścia, takie jak uczenie nadzorowane, nienadzorowane, samonadzorowane i uczenie przez wzmocnienie (nagradzanie i karanie w celu wypracowania optymalnego rozwiązania). Przykłady modeli AI opartych na uczeniu nadzorowanym to systemy klasyfikacji obrazów, systemy diagnostyczne urządzeń medycznych oraz systemy wykrywania oszustw. W przypadku uczenia nienadzorowanego model AI uczy się z danych, które nie są oznaczone, wykorzystując techniki takie jak klasteryzacja, redukcja wymiarów, uczenie reguł asocjacyjnych, wykrywanie anomalii czy modele generatywne.

Podejście oparte na logice i wiedzy obejmuje modele, które wnioskują na podstawie zakodowanej wiedzy lub symbolicznej reprezentacji zadania. Przykłady to systemy do diagnozy medycznej, które są rozwijane przez kodowanie wiedzy, którą dysponuje wielu ekspertów medycznych.

Następnym krokiem jest budowa modelu na podstawie wypracowanych wzorców. Najczęściej wykorzystuje się do tego zaawansowane algorytmy (w tym sieci neuronowe) czy metody głębokiego uczenia (które wykorzystują wielowarstwowe sieci neuronowe i mają zdolność do samodzielnego pozyskiwania informacji z danych), tak aby model rozpoznawał złożone wzorce i zależności.

Kolejnym krokiem jest doskonalenie modelu – modele AI są stale doskonalone m.in. na podstawie nowych danych i informacji zwrotnych. Na tym etapie dokonywana też jest walidacja i testowanie modelu AI, tj. sprawdzenie jego dokładności.

Ostatnim krokiem jest wykorzystanie modelu AI do tworzenia systemu AI.

1.4. SYSTEM AI VS. MODEL AI

Zgodnie z art. 3 pkt 1 Aktu o AI **system AI** jest definiowany jako „system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który – na potrzeby wyraźnych lub dorozumianych celów – wnioskuje, jak generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne".

Aby wyjaśnić to pojęcie, Komisja Europejska zatwierdziła Wytyczne dotyczące definicji systemu AI[2]. Wytyczne wskazują w szczególności przypadki, kiedy

[2] Wytyczne Komisji Europejskiej (dalej: KE), https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application [dostęp: 21.10.2026 r.].

określone rozwiązanie informatyczne nie będzie systemem AI. Wytyczne KE mają charakter niewiążący i mają być aktualizowane w razie potrzeby, w szczególności w świetle doświadczeń praktycznych, nowych pytań i pojawiających się przypadków użycia.

Od pojęcia systemu AI należy odróżnić pojęcie **modelu AI**. Akt o AI nie zawiera definicji modelu AI, ale zgodnie z motywem 97 Aktu o AI „modele AI są zasadniczymi elementami systemów AI, nie stanowią same w sobie systemów AI. Aby model AI mógł stać się systemem AI, należy dodać do niego dodatkowe elementy, takie jak na przykład interfejs użytkownika. Modele AI są zwykle zintegrowane z systemami AI i stanowią ich część". System AI to bardziej złożona struktura, która może zawierać jeden lub więcej modeli AI, jak również dodatkowe elementy, takie jak interfejs użytkownika czy bazy danych. Akt o AI nie zawiera też definicji „agenta" czy „agentycznego AI". Przyjmuje się, że agent AI będzie stanowił system AI.

Akt o AI wyróżnia przy tym **model AI ogólnego przeznaczenia**, który jest modelem AI zdolnym do wykonywania szerokiego zakresu różnych zadań (art. 3 pkt 63 Aktu o AI). Zgodnie z motywem 99 Aktu o AI „duże generatywne modele AI są typowym przykładem modeli ogólnego przeznaczenia".

Przez **system AI ogólnego przeznaczenia** należy natomiast rozumieć „system AI oparty na modelu AI ogólnego przeznaczenia, który to system może służyć różnym celom, nadający się zarówno do bezpośredniego wykorzystania, jak i do integracji z innymi systemami AI"[3]. Przykładem systemu AI ogólnego przeznaczenia jest np. ChatGPT.

Komisja Europejska opublikowała Wytyczne w sprawie zakresu obowiązków dostawców modeli AI ogólnego przeznaczenia na mocy Aktu o AI[4]. W wytycznych KE wskazała cztery kryteria wyróżniające modele AI ogólnego przeznaczenia: (i) liczba obliczeń przy trenowaniu modelu przekroczyła 10^{23} FLOP; (ii) model może generować język w formie tekstu lub dźwięku (w tym mowy) albo przetwarzać tekst na obraz lub materiał wideo; (iii) model wykazuje znaczącą ogólność; (iv) model jest w stanie kompetentnie wykonywać szeroki zakres różnych zadań. Decydujące jest przy tym łączne spełnienie wszystkich czterech kryteriów – model, który przekracza próg obliczeniowy i generuje tekst lub mowę, lecz został wytrenowany wyłącznie do wąskiego zestawu zadań (np. wyłącznie do transkrypcji

[3] Art. 3 pkt 66 Aktu o AI.

[4] Wytyczne KE, https://digital-strategy.ec.europa.eu/en/library/guidelines-scope-obligations-providers-general-purpose-ai-models-under-ai-act [dostęp: 21.10.2026 r.].

mowy na tekst), nie kwalifikuje się jako model AI ogólnego przeznaczenia. Natomiast narzędzia AI powszechnie wykorzystywane przez prawników, takie jak Microsoft 365 Copilot, Legora czy Harvey, spełniają wskazane kryteria – są trenowane z wykorzystaniem bardzo dużych zasobów obliczeniowych, generują tekst i kompetentnie realizują szeroki wachlarz zadań.

Komisja Europejska opublikowała również Kodeks postępowania dla modeli AI ogólnego przeznaczenia (art. 56 Aktu o AI)[5]. Kodeks postępowania to najważniejsze narzędzie zapewnienia zgodności z Aktem o AI przez dostawców w okresie przejściowym między wejściem w życie obowiązków dostawców (sierpień 2025 r.) a przyjęciem standardów.

Warto też podkreślić, że nie każdy zautomatyzowany, predykcyjny lub „inteligentny" system będzie mieścił się w definicji „systemu AI" z Aktu o AI. Systemem AI nie będzie system IT oparty na zasadach określonych wyłącznie przez osoby fizyczne w celu automatycznego wykonywania operacji (np. automatycznego dodawania określonej informacji prawnej w generowanym dokumencie), czy systemy mające zdolność do wnioskowania w wąskim zakresie, które mają ograniczoną zdolność do analizowania wzorców i autonomicznego dostosowania wyników[6]. Jest to istotne z punktu widzenia kwalifikacji ryzyk podmiotu korzystającego ze sztucznej inteligencji (zob. rekomendacja nr 11A).

1.5. PODZIAŁ SYSTEMÓW AI WEDŁUG AKTU O AI

Zgodnie z Aktem o AI systemy AI są podzielone na cztery kategorie w oparciu o poziom ryzyka dla użytkowników.

1.5.1. SYSTEMY AI NIEDOPUSZCZALNEGO RYZYKA

Systemy, których użycie jest zakazane. Obejmują one technologie wskazane w art. 5 Aktu o AI, które mogą np. manipulować lub wprowadzać w błąd osoby, wykorzystywać ich słabości (*vulnerabilities*), stosować scoring społeczny lub rozpoznawanie emocji (*inference of emotions*) w miejscach pracy i placówkach edukacyjnych (z pewnymi wyjątkami). Komisja Europejska zatwierdziła szczegółowe

[5] Kodeks postępowania, https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai [dostęp: 17.06.2026 r.].

[6] Wytyczne KE, pkt 41, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application [dostęp: 21.10.2026 r.].

wytyczne dotyczące zakazanych praktyk w zakresie sztucznej inteligencji[7]. Wytyczne nie mają charakteru wiążącego.

1.5.2. SYSTEMY AI WYSOKIEGO RYZYKA

Systemy, które mogą stwarzać znaczące ryzyko dla zdrowia, bezpieczeństwa lub praw podstawowych. Systemy wysokiego ryzyka zostały wskazane w art. 6 i załączniku III do Aktu o AI. Obejmują systemy używane w opiece zdrowotnej, transporcie, edukacji i zatrudnieniu. Wymagają one wdrożenia i utrzymania systemu ocen i ograniczania ryzyka (*risk management systems*), wysokiej jakości danych treningowych w celu zminimalizowania ryzyka dyskryminacji wyników, przejrzystości działania oraz stosowania odpowiednich środków nadzoru ze strony człowieka (*human oversight*), a także wysokiego poziomu solidności, bezpieczeństwa i dokładności (*accuracy, robustness and cybersecurity*). Komisja Europejska przyjęła projekt wytycznych dotyczących klasyfikacji systemów AI wysokiego ryzyka[8]. Wytyczne mają służyć dostawcom, podmiotom stosującym systemy AI oraz właściwym organom nadzoru rynku jako pomoc w ocenie, czy dany system sztucznej inteligencji podlega klasyfikacji jako system wysokiego ryzyka. Projekt zawiera dużo praktycznych przykładów systemów będących systemami wysokiego ryzyka oraz niemieszczących się w tej kategorii. Przykładowo Komisja Europejska nie uznała za systemy AI wysokiego ryzyka narzędzi AI do badań prawnych i wyszukiwania orzecznictwa (systemy semantycznego przeszukiwania baz prawnych, generowanie streszczeń wyroków, wyszukiwanie na podstawie języka naturalnego). W ocenie Komisji Europejskiej pełnią one pomocniczą funkcję informacyjną i nie angażują się w rozumowanie prawnicze. Podobnie narzędzia do redakcji i korekty pism nie zostały uznane za systemy AI wysokiego ryzyka jako będące jedynie narzędziem ulepszającym wynik uprzednio zakończonej działalności człowieka. Natomiast zaawansowane systemy wyszukiwania orzecznictwa z funkcją wnioskowania prawnego stosowane przez organy sądowe, które analizują przedstawione okoliczności sprawy (lub ich streszczenie), a następnie pomagają sędziom w identyfikacji odpowiednich przepisów i orzecznictwa oraz sugerują, w jaki sposób należy je zastosować do okoliczności danej sprawy, zostały uznane przez Komisję Europejską za systemy AI wysokiego ryzyka.

[7] Wytyczne KE, https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act [dostęp: 21.10.2026 r.].

[8] Projekt wytycznych KE, https://digital-strategy.ec.europa.eu/pl/library/draft-commission-guidelines-classification-high-risk-ai-systems [dostęp: 21.10.2026 r.].

1.5.3. SYSTEMY AI OGRANICZONEGO RYZYKA

Obejmują technologie mogące wpływać na użytkowników, ale niestanowiące poważnego zagrożenia, np. czatboty i systemy rekomendacji. Wymagają one jedynie minimalnych środków przejrzystości, takich jak informowanie użytkowników, że mają do czynienia z AI.

1.5.4. SYSTEMY AI MINIMALNEGO RYZYKA

Systemy niestanowiące praktycznie żadnego ryzyka dla użytkowników. Obejmują one większość aplikacji AI, takich jak filtry antyspamowe. Nie wymagają one specjalnych regulacji ani środków ostrożności[9]. Akt o AI nie nakłada na nie szczególnych wymogów (poza m.in. art. 4), co nie zwalnia z obowiązków wynikających z innych przepisów, w tym RODO, oraz z zasad wykonywania zawodu.

2. Przykładowe dostępne narzędzia AI

Dostępne narzędzia AI można podzielić na kilka kategorii w zależności od ich funkcji i zastosowań.

2.1. STANDARDOWE

Standardowe narzędzia AI to systemy AI, które nie wymagają specjalnej konfiguracji i są dostępne od ręki. Wykorzystują sztuczną inteligencję do wspierania użytkowników w różnych codziennych zadaniach, zwiększając kreatywność i produktywność użytkownika. Narzędzia te pomagają w generowaniu i edytowaniu treści, automatyzacji zadań, analizie danych, tworzeniu prezentacji oraz zarządzaniu pocztą e-mail i kalendarzem. Przykładem takiego narzędzia jest Microsoft 365 Copilot, który współpracuje z aplikacjami Microsoft 365, takimi jak Word, Excel, PowerPoint, Outlook i Teams.

2.2. PRZEZNACZONE DLA PRAWNIKÓW

Narzędzia AI przeznaczone dla prawników to rozwiązania dostosowane do specyficznych potrzeb prawników, które pomagają w analizie dokumentów prawnych,

[9] Więcej informacji na temat podziału systemów AI zob. https://digital-strategy.ec.europa.eu/pl/policies/regulatory-framework-ai [dostęp: 21.10.2026 r.].

zarządzaniu sprawami, badaniach prawnych i automatyzacji procesów biurowych. Przykładami takich narzędzi są Legora i Harvey.

Narzędzia dla prawników mogą być też tworzone z wykorzystaniem standardowych aplikacji, np. Microsoft Power Apps lub Copilot Studio pozwalają na budowanie narzędzi pozwalających na wbudowanie modeli AI lub tworzenie własnych agentów.

Przykładowe zastosowania: ułatwianie korzystania przez pracowników firmy z informacji udostępnionych przez dział prawny, automatyczne przygotowywanie pierwszej wersji biuletynu dotyczącego zmian w przepisach i dyskusjach parlamentarnych z poprzedniego tygodnia, identyfikacja i ocena określonych klauzul w umowach, tworzenie agentów wyspecjalizowanych w konkretnym zagadnieniu używanych do pogłębienia wiedzy pracowników i przygotowania do spotkań[10].

2.3. ASYSTENCI BAZUJĄCY NA UDOSTĘPNIONYCH MODELACH AI

Asystenci AI to narzędzia oparte na sztucznej inteligencji, które wykorzystują duże modele językowe do interpretowania języka naturalnego, prowadzenia rozmów i wykonywania zadań. Są wykorzystywani w różnych aplikacjach i systemach do wsparcia użytkowników w zadaniach związanych z przetwarzaniem języka naturalnego. Przykładami są czatboty na stronach internetowych.

2.4. AGENCI AI I AGENTYCZNA AI

Agenci AI to systemy wykorzystujące modele AI do autonomicznego planowania i realizowania czynności, w tym podejmowania określonych decyzji w celu osiągnięcia zdefiniowanych przez człowieka celów (a nie konkretnych zadań). Agent może korzystać z dokumentów dołączonych do agenta, dostępnych na stronach internetowych czy w innych systemach IT, w zależności od jego konfiguracji. Agentyczna AI (*agentic AI*) to pewna cecha lub architektura systemu AI polegająca na zdolności do samodzielnego planowania, podejmowania decyzji

[10] Przykłady zastosowania agentów M365 Copilot w dziale prawnym Microsoftu: agent wyspecjalizowany w materiałach dotyczących regulacji: https://www.linkedin.com/posts/jeff-bullwinkel-a01a259_microsoftcopilot-genai-dora-activity-7285213763962568705-7LYv [dostęp: 26.10.2026 r.]; ułatwianie wglądu do informacji udostępnionych przez dział prawny: https://www.microsoft.com/insidetrack/blog/boosting-efficiency-with-sharepoint-agents-how-our-microsoft-legal-team-is-helping-clients-find-answers-faster/ [dostęp: 21.10.2026 r.].

i realizacji złożonych zadań dla realizacji określonego celu (a nie konkretnego zadania), przy ograniczonym nadzorze człowieka. Agentyczna AI może koordynować wielu agentów, zarządzać ich komunikacją i rozdzielać zadania w celu realizacji większych, bardziej złożonych celów[11].

W odróżnieniu od generatywnej AI, której działanie co do zasady polega na wygenerowaniu treści w odpowiedzi na pytanie użytkownika, agent AI może samodzielnie podejmować działania, dostosowywać się do nowych informacji oraz wchodzić w interakcje z innymi agentami AI i systemami w celu autonomicznego wykonywania pracy. Poziom autonomii agenta AI może być różny, od wymagającego pewnego udziału użytkownika do pełnej samodzielności. To użytkownik decyduje o zakresie tej autonomii, a tym samym ponosi odpowiedzialność za określenie granic samodzielnego działania agenta AI.

Tworzenie agentów AI możliwe jest już przy pomocy standardowych narzędzi, np. M365 Copilot. W zależności od potrzeb agenci M365 Copilot pozwalają na dokładne zdefiniowanie materiałów źródłowych, skonfigurowanie agenta przy pomocy promptu, dodanie akcji oraz funkcji autonomicznych.

Przykładowo generatywna AI działa jak bardzo sprawny researcher, któremu za każdym razem trzeba dać precyzyjne polecenie (prompt), co ma zrobić. Po wykonaniu zadania AI zatrzyma się. Natomiast agent AI przypomina osobę, której można przekazać cały szereg zadań do wykonania, wyznaczając konkretny cel (np. zrób research, przeanalizuj wyniki pod kątem danych dokumentów, na podstawie tej analizy przygotuj wsad do pisma na podstawie załączonego wzoru etc.).

Ciągły rozwój narzędzi AI powoduje zatarcie różnicy między standardowymi i agentycznymi AI. Coraz więcej standardowych narzędzi (ChatGPT, Claude czy Copilot Cowork) ma wbudowane możliwości agentyczne umożliwiające użytkownikom (w zależności od planu, regionu i ustawień organizacji) automatyzacje zaawansowanych procesów, tworzenie i dzielenie się tzw. umiejętnościami oraz używanie narzędzi łączących się z zewnętrznymi systemami.

2.5. *FINE-TUNED MODELS* (MODELE DOSTOSOWANE)

Fine-tuned models to zaawansowane narzędzia AI, które są dostosowywane do specyficznych potrzeb klienta dzięki dodatkowym treningom na jego danych.

[11] Więcej: European Data Protection Supervisor, https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/agentic-ai_en [dostęp: 21.10.2026 r.].

Fine-tuning polega na dostosowywaniu wcześniej wytrenowanego modelu AI do specyficznych zadań lub nowych zbiorów danych (np. umów). Dzięki temu model staje się bardziej precyzyjny i dostosowany do konkretnych wymagań klienta.

3. Podstawowe pojęcia – generowanie i używanie (trenowanie) danych

3.1. GENEROWANIE DANYCH

Najistotniejsze pojęcia w tym zakresie:

- **prompt** – polecenie kierowane przez użytkownika, aby zainicjować tworzenie zawartości wyjściowej w dużych modelach językowych i generatywnej AI;
- **metaprompt** – stosowany systemowo prompt (zakodowane instrukcje), który ma zastosowanie do każdego wysłanego promptu („prompt dla prompta"). Wskazówki do usługi w celu generowania danych wyjściowych, np. „bądź kreatywny" lub „bądź ścisły";
- **grounding** – dodawanie kontekstu do danych wejściowych w celu zwiększenia adekwatności danych wyjściowych (np. pobierając dodatkowe informacje z zasobów klienta, z Internetu, z innych usług);
- **dane wejściowe / zawartość wejściowa (input)** – wejściowa informacja dla systemu generatywnej AI (np. tekstu, obrazu czy dźwięku). Jest to polecenie, które użytkownik dostarcza do systemu generatywnej AI w celu wygenerowania odpowiedzi (danych wyjściowych). Prompt jest specyficznym przykładem danych wejściowych, który dotyczy dużych modeli językowych i generatywnej AI;
- **dane wyjściowe / zawartość wyjściowa (output)** – rezultat działania systemu AI w wyniku przetworzenia danych wejściowych. Może przybierać różne formy, np. tekstu, obrazu, dźwięku czy decyzji.

3.2. TRENOWANIE MODELI AI

Jak wskazaliśmy, tworzenie modelu AI wymaga wyuczenia go na danych. Korzystając z rozwiązań standardowych, radca prawny zwykle nie będzie brał udziału w procesie trenowania modeli AI. Jednak w przypadku tworzenia tzw. modeli dostosowanych (*fine-tuned models*) radca prawny może już być zaangażowany w ten proces, w tym udostępniając dane, które pozwolą na lepsze dotrenowanie

modelu. Należy też pamiętać, że treści udostępniane przez radców prawnych i aplikantów radcowskich w Internecie mogą być wykorzystywane do trenowania modeli. Odnośniki do źródeł w zawartości wyjściowej świadczą jednak przeważnie o pobraniu treści w czasie generowania odpowiedzi (wyszukiwanie w internecie lub w bazie dokumentów, tzw. RAG), a nie wyłącznie o wykorzystaniu jej do trenowania modelu.

Możliwość trenowania modeli, zwłaszcza na danych objętych ochroną prawnoautorską, budzi kontrowersje. Wskazuje się jednak następujące podstawy prawne dla takich działań:

- **Eksploracja tekstów i danych (TDM, *text and data mining*)** oznacza zautomatyzowaną technikę analityczną służącą do analizowania tekstów i danych w postaci cyfrowej w celu wygenerowania informacji obejmujących między innymi wzorce, tendencje i korelacje.

  W ramach nowelizacji prawa autorskiego, stanowiącej implementację art. 4 ust. 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE, wprowadzono – w art. 263 ust. 1 ustawy o prawie autorskim i prawach pokrewnych – **nowy rodzaj dozwolonego użytku w postaci eksploracji tekstów i danych (TDM)**. Przepis ten pozwala użytkownikom na zwielokrotnianie już rozpowszechnionych utworów w celu analizowania treści i danych, chyba że uprawniony zastrzegł inaczej (klauzula opt-out). W przypadku utworów publicznie udostępnionych w taki sposób, aby każdy mógł mieć do nich dostęp w miejscu i czasie przez siebie wybranym, zastrzeżenia dokonuje się w formacie przeznaczonym do odczytu maszynowego. Jednak brak jednoznacznych wytycznych dotyczących metod i sposobów zgłaszania zastrzeżenia oraz brak technicznego standardu dokonywania zastrzeżenia powoduje obecnie poczucie braku możliwości realnego skorzystania z klauzuli opt-out. Niejasny jest w szczególności moment, w którym można zgłosić zastrzeżenie (przed rozpoczęciem eksploracji czy np. już w trakcie funkcjonowania modelu AI), oraz sposób, w jaki należy to zrobić, żeby było to skuteczne.

  Zgodnie z art. 53 ust. 1 lit. c) Aktu o AI dostawcy modeli AI ogólnego przeznaczenia zobowiązani są wprowadzić politykę służącą zapewnieniu zgodności z prawem Unii dotyczącym prawa autorskiego i praw pokrewnych, w tym identyfikować zastrzeżenia praw wyrażone zgodnie z art. 4 ust. 3 dyrektywy (UE) 2019/790 (opt-out), i stosować się do nich także podczas

trenowania modeli. Praktyczne rozwiązania mające pomóc dostawcom modeli AI ogólnego przeznaczenia w spełnieniu tego obowiązku zostały zawarte w rozdziale dotyczącym praw autorskich (*Copyright Chapter*) Kodeksu postępowania dla modeli AI ogólnego przeznaczenia[12]. Komisja Europejska prowadzi obecnie prace nad dwoma uzupełniającymi się inicjatywami dotyczącymi ochrony praw autorskich w kontekście TDM. Pierwsza obejmuje listę ogólnie uzgodnionych protokołów opt-out w formacie przeznaczonym do odczytu maszynowego, które dostawcy modeli AI ogólnego przeznaczenia będą zobowiązani respektować na podstawie Aktu o AI i Kodeksu praktyk dla modeli AI ogólnego przeznaczenia[13]. Druga to unijny rejestr zastrzeżeń praw – narzędzie umożliwiające uprawnionym zgłaszanie zastrzeżeń z TDM, a dostawcom modeli AI ogólnego przeznaczenia ich skuteczną identyfikację[14].

Realne znaczenie klauzuli opt-out waży się obecnie w sprawie *Like Company v. Google Ireland* (C-250/25). Jest to pierwsza tego typu sprawa, w której TSUE bada, czy trenowanie modeli AI na chronionych treściach narusza unijne prawo autorskie.

- ***Fair use principle* (zasada dozwolonego użytku)** to koncepcja wypracowana na gruncie prawa amerykańskiego, która umożliwia korzystanie z utworu chronionego prawami autorskimi bez konieczności uzyskiwania zgody podmiotu uprawnionego (autora, wydawcy/producenta) w określonych warunkach, np. w badaniach naukowych, edukacji czy na potrzeby krytyki. Możliwość skorzystania z tego wyjątku do trenowania modeli AI jest obecnie przedmiotem sporów w USA. Pierwsze wyroki już zapadły, lecz nie przesądzają sprawy i nadal brak jednolitego stanowiska. Przykładowo w sprawie *Bartz v. Anthropic* sąd uznał trenowanie modelu za mieszczące się w ramach zasady dozwolonego użytku, ale jednocześnie obciążył spółkę odpowiedzialnością za pozyskanie utworów z pirackich źródeł, co doprowadziło do ugody na 1,5 mld dol.[15]

[12] Rozdział „Prawa autorskie", Kodeks postępowania w zakresie AI ogólnego przeznaczenia | Kształtowanie cyfrowej przyszłości Europy, https://digital-strategy.ec.europa.eu/pl/policies/contents-code-gpai [dostęp: 24.07.2026 r.].

[13] https://digital-strategy.ec.europa.eu/en/consultations/commission-launches-consultation-protocols-reserving-rights-text-and-data-mining-under-ai-act-and [dostęp: 20.10.2026 r.].

[14] https://digital-strategy.ec.europa.eu/en/library/new-feasibility-study-introducing-eu-level-registry-text-and-data-mining-opt-out [dostęp: 20.10.2026 r.].

[15] *Bartz et al. v. Anthropic PBC*, No. 3:2024cv05417 – Document 437 (N.D. Cal. 2025) z dnia 23 czerwca 2025 r., https://copyrightalliance.org/wp-content/uploads/2025/06/Bartz-v.-Anthropic-Order.pdf oraz memorandum dotyczące zatwierdzenia ugody z dnia 17 października

3.3. WSKAZÓWKI DOTYCZĄCE PROMPTOWANIA

ZAŁĄCZNIK NR 1

W **załączniku nr 1** do rekomendacji znajdują się praktyczne wskazówki dotyczące prawidłowego promptowania, w tym personalizacji promptów.

4. AI a chmura obliczeniowa

Chmura obliczeniowa *(cloud computing)* to świadczona na rzecz klienta usługa cyfrowa umożliwiająca wszechobecny sieciowy dostęp na żądanie do wspólnego zbioru konfigurowalnych, skalowalnych i elastycznych zasobów obliczeniowych o charakterze scentralizowanym, rozproszonym lub wysoce rozproszonym, które mogą być szybko przydzielone i uwolnione przy minimalnym wysiłku pod względem zarządzania lub interakcji z dostawcą usług („usługa przetwarzania danych" w Akcie w sprawie danych)[16].

Chmura obliczeniowa pozwala zatem na dostęp za pomocą Internetu przy minimalnej interakcji z dostawcą usługi do określonych zasobów obliczeniowych. Podstawowe modele usług chmurowych to: platforma jako usługa (PaaS), infrastruktura jako usługa (IaaS) czy oprogramowanie jako usługa (SaaS).

Chmura obliczeniowa odgrywa kluczową rolę w rozwoju i wdrażaniu narzędzi AI. Dzięki chmurze obliczeniowej organizacje mogą testować zaawansowane narzędzia AI i korzystać z nich bez konieczności inwestowania w kosztowną infrastrukturę (w celu instalowania czy trenowania modeli we własnych centrach danych) i bez długotrwałych wdrożeń. W przypadku standardowych narzędzi (np. M365 Copilot) techniczne uruchomienie usługi może nastąpić w kilka godzin; nie oznacza to jednak gotowości do pracy na danych klientów, która wymaga wcześniejszej oceny umowy, konfiguracji i uprawnień (zob. rekomendacje nr 2–8).

Usługa chmury obliczeniowej ułatwia też proces trenowania lub dostosowywania modeli (*fine-tuning*) AI, które często wymagają znacznej mocy obliczeniowej do przetwarzania i analizy dużych ilości danych.

2025 r., https://law.justia.com/cases/federal/district-courts/california/candce/3:2024cv05417/434709/437/ [dostęp: 20.10.2026 r.].

[16] Art. 2 pkt 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. (Akt w sprawie danych), https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=OJ:L_202302854 [dostęp: 20.10.2026 r.].

Wykonane przez radców prawnych analizy na potrzeby wdrożenia chmury obliczeniowej mogą zostać wykorzystane przy wdrożeniu narzędzi AI bazujących na chmurze obliczeniowej. Wcześniejsze analizy powinny zostać jedynie uzupełnione o specyficzne wymagania związane z narzędziami AI, opisane w niniejszych rekomendacjach, co znacznie przyśpieszy i uprości cały proces wdrożenia.

5. Przykładowe zastosowania narzędzi generatywnej AI w pracy radcy prawnego

5.1. W OBSZARACH DZIAŁALNOŚCI RADCY PRAWNEGO

Narzędzia AI mogą być zastosowane w praktycznie każdym obszarze działalności radcy prawnego do:

- analizy, porównywania dokumentów, przygotowywania podsumowań dokumentów czy wzorów dokumentów;
- wspierania w zarządzaniu skrzynką mailową oraz komunikacją z klientami;
- tworzenia transkrypcji wideokonferencji;
- tworzenia prezentacji;
- tłumaczeń tekstów oraz prezentacji;
- analizy argumentów i kontrargumentów;
- przygotowania ofert i komunikacji z klientami (np. przygotowywania okresowych sprawozdań z prowadzonych spraw);
- automatycznego tworzenia podsumowań oraz kategoryzowania dokumentów na potrzeby baz danych;
- odnajdywania informacji właściwych do konkretnego zagadnienia w wewnętrznych i zewnętrznych źródłach;
- badań prawnych;
- przygotowywania projektów umów lub poszczególnych klauzul;
- krytycznej analizy spójności argumentacji prawnej danego pisma;
- przygotowania pogłębionych analiz określonych zagadnień na podstawie publicznie dostępnych informacji lub z wewnętrznych źródeł w ramach danej organizacji;
- analizy i przetwarzania danych w arkuszach kalkulacyjnych, w tym automatycznego tworzenia formuł, tabel przestawnych, wizualizacji danych, identyfikowania trendów oraz generowania podsumowań na podstawie danych zawartych w arkuszach;

- wykorzystania AI jako „sparring partnera" do testowania własnej argumentacji poprzez polecenie wcielenia się w rolę strony przeciwnej i wskazania najsłabszych punktów rozumowania, możliwych kontrargumentów przemawiających przeciwko przyjętemu stanowisku.

Warto pamiętać, że rozwiązania AI mogą być istotnym wsparciem zwłaszcza dla radców prawnych wykonujących zawód jednoosobowo lub w mniejszych zespołach – korzystanie z tych narzędzi może ułatwić im szybkie zwiększenie jakości świadczonych usług i obsługi klienta.

5.2. SZCZEGÓŁOWE PRZYKŁADY ZASTOSOWANIA NARZĘDZI GENERATYWNEJ AI

ZAŁĄCZNIK NR 2

W **załączniku nr 2** do rekomendacji znajdują się szczegółowe przykłady zastosowania (z wykorzystaniem Microsoft 365 Copilot) narzędzi generatywnej AI w pracy radcy prawnego.

Rozdział II

PRZEPISY PRAWA – PODSTAWOWE REGULACJE

Korzystanie z narzędzi AI przez radców prawnych podlega zarówno przepisom ogólnym, takim jak przepisy dotyczące ochrony danych osobowych czy praw autorskich, jak i przepisom, które regulują wykonywanie zawodu, w tym ochronę tajemnicy zawodowej.

1. Dane osobowe

Z punktu widzenia prawa ochrony danych osobowych radca prawny – w zależności od formy wykonywania zawodu – może mieć status administratora danych osobowych (podmiotu, który decyduje o celach i sposobach przetwarzania danych) lub będzie działał z upoważnienia administratora, o którym mowa w art. 29 RODO, i zgodnie z jego poleceniami. W przypadku wykonywania zawodu radcy prawnego w formie kancelarii radcy prawnego radca prawny jest administratorem danych osobowych przetwarzanych w ramach wykonywania zawodu. Jeżeli radca prawny wykonuje zawód w spółce osobowej, cywilnej, w ramach stosunku pracy lub na podstawie umowy cywilnoprawnej, administratorem danych osobowych jest spółka albo pracodawca, a radca prawny przetwarza dane osobowe z upoważnienia administratora i zgodnie z jego poleceniami.

Do korzystania z narzędzi AI stosuje się ogólne przepisy dotyczące przetwarzania danych osobowych, w tym przepisy RODO[17] czy regulacji sektorowych. Zakres zastosowania tych regulacji zależeć będzie od tego, czy radca prawny jest zaangażowany w tworzenie i trenowanie modelu AI (lub jego dostosowywanie – *fine-tuning*) przy wykorzystaniu informacji zawierających dane osobowe, czy też jest użytkownikiem systemu AI.

[17] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

W przypadku budowy i trenowania na radcy prawnym będzie spoczywało zdecydowanie więcej obowiązków, w tym przede wszystkim właściwe zidentyfikowanie podstawy prawnej przetwarzania danych osobowych zawartych w danych treningowych. Szczegółowe wyjaśnienia dotyczące stosowania RODO na tym etapie można znaleźć w opinii Europejskiej Rady Ochrony Danych (EROD) w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli sztucznej inteligencji[18].

W praktyce jednak radca prawny będzie najczęściej użytkownikiem systemu AI. W takiej sytuacji do przetwarzania danych osobowych może potencjalnie dochodzić na czterech poziomach:

- przetwarzanie danych osobowych zawartych w zawartości wejściowej (prompcie);
- przetwarzanie danych osobowych zawartych w zawartości wyjściowej (output);
- przetwarzanie danych osobowych w agentach AI;
- przetwarzanie danych użytkownika podczas korzystania z modelu AI (np. z jakich usług korzysta, kiedy, jak długo).

1.1. PRZETWARZANIE DANYCH OSOBOWYCH W ZAWARTOŚCI WEJŚCIOWEJ

Jeśli radca prawny chce przetwarzać dane osobowe w zawartości wejściowej, powinien jako administrator lub osoba upoważniona przez administratora zweryfikować, czy ma odpowiednią podstawę prawną do takiego przetwarzania danych, oraz jaki jest cel przetwarzania.

Należy również zweryfikować pozostałe zasady przetwarzania danych, w tym:

- ich adekwatność;
- zabezpieczenie poufności;
- kwestie przekazywania danych do państw trzecich, tj. czy dane będą przekazywane poza EOG;
- czy konieczne jest zawarcie umowy powierzenia przetwarzania danych (konieczna jest analiza, w jakiej roli występuje dostawca systemu AI – w roli

[18] Opinia Europejskiej Rady Ochrony Danych 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli sztucznej inteligencji z dnia 17 grudnia 2024 r., https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_pl [dostęp: 21.10.2026 r.].

administratora lub współadministratora albo w roli podmiotu przetwarzającego);
- czy wymagane jest wykonanie oceny skutków dla ochrony danych (DPIA);
- czy zapewniona jest realizacja uprawnień osób, których dane dotyczą;
- czy i w jakim zakresie wymagana jest aktualizacja wewnętrznej dokumentacji (rejestru czynności przetwarzania, aktualizacja polityk prywatności);
- dodatkowo, w przypadku danych osobowych objętych tajemnicą radcowską, konieczne jest ustalenie, czy takie dane mogą być przekazane w zawartości wejściowej (zob. rozdz. II.7).

1.2. PRZETWARZANIE DANYCH OSOBOWYCH ZAWARTYCH W ZAWARTOŚCI WYJŚCIOWEJ

W przypadku gdy dane osobowe pojawiają się w zawartości wyjściowej, radca prawny powinien mieć świadomość, że dane osobowe zostały wygenerowane w oparciu o przewidywania statystyczne i mogą być niepoprawne. Na przykład wygenerowane dane mogą zostać w części lub w całości „wymyślone" (tzw. halucynacje, zob. rozdz. III.3). Radca prawny powinien więc wziąć pod uwagę możliwość, że dane osobowe będą nieprawidłowe oraz że może to mieć wpływ na wszelkie decyzje podjęte na ich podstawie. Niezastosowanie się do tego wymogu „ograniczonego zaufania" do wygenerowanych danych osobowych może oznaczać, że przetwarzanie danych nie jest zgodne z zasadą rzetelności. Bezkrytyczne poleganie na takich danych może być również niezgodne z zasadą minimalizacji danych, ponieważ dane osobowe, w tym wnioski, muszą być adekwatne i odpowiednie do celu.

Istnieją poglądy, że dane generowane przez sztuczną inteligencję można uznać za prognozy statystyczne, a nie za dane osobowe. Zwolennicy tego podejścia argumentują, że ponieważ sztuczna inteligencja generuje dane w oparciu o wzorce i reguły prawdopodobieństwa pochodzące z dużych zbiorów danych, dane wyjściowe są bardziej zbliżone do prognoz statystycznych niż danych osobowych. Teza ta jest kontrowersyjna. Kluczową kwestią jest to, czy dane wygenerowane przez sztuczną inteligencję można powiązać z możliwą do zidentyfikowania osobą. Jeśli jest to możliwe, dane te mogą zostać uznane za dane osobowe, nawet jeśli są niepoprawne. Opinia EROD potwierdza, że w szczególności dotyczyć to będzie sytuacji, kiedy sztuczna inteligencja ma dostarczać wnioski

(np. dane osobowe) na temat osób, których dane osobowe zostały użyte w celu jej wyszkolenia[19].

1.3. PRZETWARZANIE DANYCH OSOBOWYCH W AGENTACH AI

Agent AI, mimo że działa autonomicznie, nie jest odrębnym podmiotem odpowiedzialnym za przetwarzanie danych osobowych w rozumieniu RODO. Agent AI jest rozwiązaniem technicznym, za pomocą którego prowadzone jest przetwarzanie. Kluczowe jest ustalenie ról: w jakiej roli występuje podmiot korzystający z agenta (np. radca prawny), a w jakiej dostawca agenta lub infrastruktury. Ocena ta wymaga analizy sposobu funkcjonowania agenta oraz postanowień umowy z dostawcą. Jeżeli agent przetwarza dane objęte tajemnicą radcowską, rekomendowane jest, aby radca prawny (lub jego organizacja) pozostał administratorem danych, a dostawca agenta pełnił rolę podmiotu przetwarzającego.

W przypadku systemów złożonych z wielu współpracujących agentów AI (architektury wieloagentowe) analiza ról jest bardziej złożona. Należy ocenić, czy między agentami dochodzi do przepływu danych osobowych oraz kto odpowiada za przetwarzanie na każdym etapie. Podmioty odpowiedzialne za poszczególnych agentów AI mogą działać również jako współadministratorzy w rozumieniu art. 26 RODO, co wymaga zawarcia stosownego porozumienia.

Istotną cechą agentów AI jest to, że wyznacza się im cel, a nie konkretne zadanie. Agent AI samodzielnie dobiera metody i kroki do jego realizacji. W konsekwencji może dochodzić do zautomatyzowanego podejmowania decyzji, które wywołuje skutki prawne lub w podobny sposób istotnie wpływa na osobę fizyczną (art. 22 RODO). W takim przypadku radca prawny musi dysponować odpowiednią podstawą prawną przetwarzania. Zwykle będzie nią zgoda osoby, której dane dotyczą, lub niezbędność do wykonania umowy (art. 22 ust. 2 RODO). Osoba ta powinna mieć zapewnione odpowiednie gwarancje, w tym prawo do interwencji ludzkiej, wyrażenia własnego stanowiska oraz zakwestionowania decyzji.

Przed wdrożeniem agenta AI należy rozważyć, czy wymagane jest przeprowadzenie oceny skutków dla ochrony danych (DPIA) na podstawie art. 35 RODO.

[19] Opinia Europejskiej Rady Ochrony Danych 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli sztucznej inteligencji z dnia 17 grudnia 2024 r., pkt 29, 36–37, https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_pl [dostęp: 21.10.2026 r.].

Obowiązek ten aktualizuje się w szczególności, gdy agent AI przetwarza dane na dużą skalę, stosuje zautomatyzowane podejmowanie decyzji lub przetwarza dane szczególnych kategorii. Przeprowadzenie DPIA jest zalecane jako element projektowania systemu agentowego.

Korzystanie z agentów wymaga również odpowiednich środków technicznych i organizacyjnych. Zgodnie z zasadą minimalizacji danych (art. 5 ust. 1 lit. c RODO) agent AI powinien mieć dostęp wyłącznie do danych niezbędnych do realizacji wyznaczonego celu. Należy precyzyjnie określić: zakres dostępu agenta do danych i systemów, miejsce przechowywania danych przetwarzanych lub generowanych przez agenta AI oraz termin ich usunięcia.

1.4. PRZETWARZANIE DANYCH OSOBOWYCH UŻYTKOWNIKÓW, W TYM DOTYCZĄCYCH ICH INTERAKCJI Z SYSTEMEM AI

Radcowie prawni powinni mieć na względzie, że sztuczna inteligencja może gromadzić także ich własne dane osobowe oraz dane innych użytkowników obejmujące dane takie jak np. imię i nazwisko, nazwa użytkownika, dane kontaktowe, a ponadto także treść zawartości wejściowej, zawartości wyjściowej oraz tzw. dane o interakcji użytkownika (*user engagement data*), np. spseudonimizowane identyfikatory losowo przypisane użytkownikowi, czas korzystania, historię aktywności, informacje o szyfrowaniu, informacje o błędach. Dane te są przetwarzane zazwyczaj w zaszyfrowanej formie, a w niektórych przypadkach użytkownik może je samodzielnie usuwać. Okres przechowywania zawartości wejściowej i wyjściowej (w tym historii rozmów, logów i kopii zapasowych) zależy od usługi, planu i umowy; niektóre usługi przechowują ją przez określony czas, nawet jeżeli nie jest wykorzystywana do trenowania modeli. Radca prawny powinien ustalić te zasady w dokumentacji i umowie konkretnej usługi (zob. rekomendacje nr 2 i 4).

Administratorem danych użytkowników może być w zależności od formy wykonywania zawodu radca prawny albo spółka/pracodawca, dostawca systemu AI będzie natomiast przetwarzał dane użytkowników zwykle jako podmiot przetwarzający. Dostawca systemu AI może również być administratorem danych, jeśli np. przetwarza dane w celu ulepszania funkcjonowania systemu AI, prowadzenia badań czy wykrywania nadużyć – dotyczyć to będzie zazwyczaj przetwarzania zawartości wejściowej i wyjściowej oraz danych o interakcji użytkownika. Do ustalenia roli dostawcy konieczna jest weryfikacja dokumentacji umownej na korzystanie z systemu AI.



REKOMENDACJE

Szczegółowe wskazówki w tym zakresie zawierają rekomendacje nr 7 oraz 8.

2. Akt o AI

Akt o AI wszedł w życie 1 sierpnia 2024 r. Od 2 lutego 2025 r. stosowane są przepisy ogólne, przepisy dotyczące tzw. praktyk zakazanych oraz przepisy dotyczące kompetencji w zakresie AI (art. 4). Od 2 sierpnia 2025 r. stosowane są przepisy o organach nadzorujących przestrzeganie Aktu o AI, karach za jego łamanie oraz zasady zarządzania i obowiązki dotyczące modeli AI ogólnego przeznaczenia.

Rozporządzenie Omnibus dotyczące AI (rozporządzenie (UE) 2026/1744, które weszło w życie 27 lipca 2026 r.) wprowadziło nowe terminy stosowania niektórych przepisów Aktu o AI:

- od 2 sierpnia 2026 r.: obowiązują inne przepisy poza tymi, które mają określoną późniejszą datę stosowania, w tym m.in. przepisy dotyczące standaryzacji, obowiązki w zakresie przejrzystości (art. 50 ust. 1, 3 i 4 Aktu o AI) oraz oznaczania treści generowanych przez AI (art. 50 ust. 2) wobec systemów wprowadzonych na rynek od tej daty, przepisy dotyczące monitorowania po wprowadzeniu do obrotu (art. 72–74), nadzoru rynku (art. 74–80) oraz rejestracji w unijnej bazie danych (art. 71);
- od 2 grudnia 2026 r.: dostawcy systemów AI wprowadzonych na rynek przed 2 sierpnia 2026 r. zobowiązani są do zapewnienia zgodności z obowiązkiem oznaczania treści generowanych przez AI (art. 50 ust. 2 Aktu o AI); od tej daty będą również stosowane nowe zakazy wykorzystywania systemów AI do generowania lub manipulowania materiałami o charakterze intymnym bez zgody osób na nich widocznych oraz materiałami przedstawiającymi seksualne wykorzystywanie dzieci (CSAM);
- od 2 sierpnia 2027 r.: właściwe organy krajowe mają zapewnić funkcjonowanie piaskownic regulacyjnych AI;
- od 2 grudnia 2027 r.: będą stosowane przepisy dotyczące systemów AI wysokiego ryzyka, o których mowa w art. 6 ust. 2 oraz załączniku III do Aktu o AI;

- od 2 sierpnia 2028 r.: będą stosowane przepisy dotyczące systemów AI wysokiego ryzyka, klasyfikowanych na podstawie art. 6 ust. 1 Aktu o AI, tj. systemów AI powiązanych z produktami objętymi unijnym prawodawstwem harmonizacyjnym wymienionym w załączniku I do Aktu o AI.

Akt o AI nakłada obowiązki na różne podmioty zaangażowane w tworzenie, wdrażanie i używanie systemów AI[20]. Akt o AI stosuje się też do różnych podmiotów: dostawców systemów AI, importerów, dystrybutorów, upoważnionych przedstawicieli oraz podmiotów stosujących[21]. Większość obowiązków spoczywa na dostawcach systemów AI, przy czym rozgraniczenie tych ról w przypadku niektórych systemów AI, np. systemów wbudowanych czy *fine-tuningowanych*, może wymagać głębszej analizy.

Co do zasady radcowie prawni będą podmiotami stosującymi systemy AI. Obowiązki podmiotu stosującego system AI są ograniczone, pod warunkiem że nie będzie on korzystał z systemów AI ogólnego przeznaczenia zakwalifikowanych jako systemy AI wysokiego ryzyka.

W przypadku używania systemów AI wysokiego ryzyka na radcach prawnych mogą spoczywać dodatkowe obowiązki, m.in. wskazane w art. 26 i 27 Aktu o AI, np. obowiązek wdrożenia środków technicznych i organizacyjnych umożliwiających wykorzystanie zgodnie z instrukcją obsługi czy przeprowadzenie oceny skutków systemu AI. Dodatkowo, jeżeli podmiot stosujący zmieni przeznaczenie „zwykłego" systemu AI w taki sposób, że stanie się on systemem AI wysokiego ryzyka, to stanie się także dostawcą tego systemu w rozumieniu Aktu o AI, co powoduje, że stosuje się do niego obowiązki dostawcy systemu AI wysokiego ryzyka (art. 25 ust. 1 pkt 3 Aktu o AI). Odrębnej oceny wymaga sytuacja, w której radca prawny pełni funkcję arbitra albo innego organu alternatywnego rozwiązywania sporów, a wynik postępowania wywołuje skutki prawne dla stron. Systemy AI przeznaczone do wspomagania w badaniu i interpretacji stanu faktycznego i przepisów prawa oraz w stosowaniu prawa do konkretnego stanu faktycznego, wykorzystywane w podobny sposób w alternatywnych metodach rozwiązywania sporów, są systemami AI wysokiego ryzyka, o ile nie zachodzą wyjątki z art. 6 Aktu o AI.

[20] Podmiot, który rozwija system AI lub model AI ogólnego przeznaczenia lub zleca rozwój systemu AI lub modelu AI ogólnego przeznaczenia oraz który – odpłatnie lub nieodpłatnie – pod własną nazwą lub własnym znakiem towarowym wprowadza do obrotu lub oddaje do użytku system AI (art. 3 pkt 3 Aktu o AI).

[21] Podmiot, który wykorzystuje system AI, nad którym sprawuje kontrolę, z wyjątkiem sytuacji, gdy system AI jest wykorzystywany w ramach osobistej działalności pozazawodowej (art. 3 pkt 4 Aktu o AI).

Podmiot stosujący zobowiązany jest do podejmowania środków wspierających w zakresie AI wśród swojego personelu i innych osób zajmujących się działaniem i wykorzystaniem systemów AI w jego imieniu (art. 4 Aktu o AI), z uwzględnieniem ich wiedzy technicznej, doświadczenia, wykształcenia i wyszkolenia oraz kontekstu, w którym systemy AI mają być wykorzystywane, a także biorąc pod uwagę osoby lub grupy osób, wobec których systemy AI mają być wykorzystywane. Obowiązek ten nie oznacza konieczności zagwarantowania określonego poziomu kompetencji AI danej osoby. Komisja i państwa członkowskie mają wspierać jego realizację poprzez oferowanie szkoleń, udostępnianie zasobów informacyjnych oraz wymianę dobrych praktyk. Ponadto na podmiocie stosującym ciążą w określonych przypadkach obowiązki w zakresie przejrzystości, o których mowa w art. 50 Aktu o AI, obejmujące m.in. konieczność informowania osób o generowaniu lub modyfikacji materiałów będących tzw. deepfake'em, a w przypadku, gdy system AI służy rozpoznawaniu emocji lub kategoryzacji biometrycznej – o jej stosowaniu. Wdrażanie odpowiednich środków technicznych i organizacyjnych w celu zapewnienia, że system AI wysokiego ryzyka jest użytkowany zgodnie z instrukcją dostawcy systemu AI (art. 26 ust. 1), a także zgłaszanie dostawcy systemu AI wszelkich poważnych incydentów oraz nieprawidłowego działania systemu (art. 26 ust. 5) są dodatkowymi, przykładowymi obowiązkami spoczywającymi na podmiocie stosującym w przypadku korzystania z systemów AI wysokiego ryzyka.

System AI ogólnego przeznaczenia nie może służyć zamawiającemu do realizacji zakazanych praktyk w zakresie AI (art. 5 Aktu o AI). W celu doprecyzowania zakresu obowiązków informacyjnych oraz wsparcia dostawców i podmiotów stosujących systemy AI ogólnego przeznaczenia Komisja Europejska opublikowała wytyczne dotyczące obowiązków w zakresie przejrzystości (art. 50 Aktu o AI)[22].

Krajowe regulacje w zakresie AI mają na celu m.in. zapewnienie wdrażania AI i nadzoru nad nią na poziomie krajowym. Na mocy polskiej ustawy o systemach sztucznej inteligencji powstała Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji – kolegialny organ odpowiedzialny za nadzorowanie i monitorowanie rynku systemów AI. Do zadań komisji należeć będą kontrola przestrzegania przepisów Aktu o AI (prowadzona głównie w trybie zdalnym) oraz nakładanie kar administracyjnych za ich naruszenie. Na pierwszą przewodniczącą komisji we wrześniu 2026 r. została powołana Pamela Krzypkowska.

[22] Wytyczne KE dotyczące obowiązków dostawców i podmiotów stosujących systemy AI w zakresie przejrzystości, https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems [dostęp: 21.10.2026 r.].

3. Prawo autorskie

Polskie prawo autorskie uznaje za twórcę jedynie człowieka, a ochronie prawnoautorskiej podlega utwór, czyli każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia[23]. Jednak nie każdy przejaw działalności człowieka jest uznawany za utwór. Utworem nie są np. akty prawne i ich urzędowe projekty, odkrycia, idee, procedury, metody i zasady działania oraz koncepcje matematyczne (art. 4 ustawy).

Kwestie prawnoautorskie w kontekście AI dotyczą przede wszystkim:

- podstaw do korzystania z systemów AI (np. na podstawie licencji);
- trenowania modeli i ewentualnych roszczeń wobec użytkowników w związku z trenowaniem modeli na danych objętych ochroną prawnoautorską;
- praw do zawartości wejściowej;
- praw do zawartości wyjściowej i możliwości jej wykorzystywania.

3.1. PODSTAWY DO KORZYSTANIA Z SYSTEMÓW AI

Zgodnie z definicją zawartą w Akcie o AI system AI to system maszynowy, który w praktyce zawiera element oprogramowania oraz sprzętu, na którym takie oprogramowanie jest uruchomione. W rezultacie do umów na korzystanie z rozwiązań AI stosujemy analogiczne zasady jak do tych dotyczących oprogramowania. W większości przypadków systemy AI są udostępniane na podstawie licencji, w tym – w przypadku systemów AI udostępnianych w modelu oprogramowanie jako usługa (SaaS) – licencji subskrypcyjnych.

Umowy licencyjne regulują specyficzne kwestie dotyczące rozwiązań AI, takie jak:

- obowiązki podmiotu stosującego, w tym konieczność przestrzegania zasad odpowiedzialnego korzystania z AI;
- zasady dotyczące zawartości wejściowej i wyjściowej;
- zobowiązania dostawców dotyczące wykorzystywania zawartości wyjściowej i wejściowej (np. odnośnie do zasad wykorzystywania tych danych do trenowania ich modeli);

[23] Art. 1 ust. 1 ustawy o prawie autorskim i prawach pokrewnych.

- ograniczenia w korzystaniu, np. filtrowanie zawartości wejściowej i wyjściowej, możliwość weryfikacji przez człowieka, możliwość ograniczenia lub wyłączenia dostępu do systemów AI;
- odpowiedzialność za roszczenia dotyczące systemu AI i zawartości wyjściowej.

3.2. TRENOWANIE MODELI AI I ROSZCZENIA ZWIĄZANE Z TRENOWANIEM MODELI AI

W związku z tym, że kwestia możliwości trenowania modeli na danych objętych ochroną prawnoautorską na podstawie ww. wyłączeń (zob. rozdz. I.3.2) nie jest jeszcze przesądzona, umowy na korzystanie z systemów AI mogą też regulować kwestie odpowiedzialności dostawcy wobec użytkownika w przypadku takich roszczeń podmiotów trzecich (np. autorów danych treningowych) podniesionych wobec użytkownika, np. roszczeń o zaniechanie używania czy o odszkodowanie z tytułu naruszenia ich praw autorskich.

3.3. PRAWA DO ZAWARTOŚCI WEJŚCIOWEJ

Zawartość wejściowa jest tworzona przez człowieka i w związku z tym może potencjalnie być utworem (np. fragmenty kodu komputerowego wprowadzone do prompta). Ponadto w promptach można zwykle zamieścić całe dokumenty lub obrazy, które mogą być objęte prawami własności intelektualnej. Konieczne jest ustalenie, czy korzystanie w ten sposób z tych treści nie będzie naruszało praw autorskich podmiotów trzecich.

3.4. PRAWA DO ZAWARTOŚCI WYJŚCIOWEJ

Jako że w Polsce ochronie prawnoautorskiej podlegają tylko przejawy działalności człowieka, zawartość wyjściowa (output) wygenerowana przez AI nie jest uważana za utwór, a co za tym idzie nie podlega ochronie prawnoautorskiej. Podkreśla się jednak różnicę między twórczością wytworzoną przez człowieka **za pomocą AI** a twórczością wygenerowaną **przez AI**[24]. W przypadku gdy AI

[24] Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji (2020/2015 (INI)).

jest wykorzystywana wyłącznie jako narzędzie wspomagające autora w procesie tworzenia, możliwa jest potencjalnie prawnoautorska ochrona rezultatów takiej twórczości (analogicznie jak w przypadku cyfrowej obróbki fotografii). Ponadto w przypadku przerobienia zawartości wyjściowej przez człowieka w taki sposób, że rezultat będzie spełniał kryteria utworu, taka przeróbka może potencjalnie być przedmiotem ochrony prawnoautorskiej.

W odniesieniu do zawartości wyjściowej obejmującej wideo czy audio może ona podlegać ochronie jako prawa pokrewne (odpowiednio prawo do wideogramu i fonogramu).

4. Ogólne regulacje dotyczące stosunków umownych

Do korzystania z narzędzi AI stosuje się również obowiązujące przepisy ogólne dotyczące stosunków umownych, np. Kodeks cywilny w przypadku umów podlegających prawu polskiemu. W tym zakresie znajdą zastosowanie np. przepisy dotyczące odpowiedzialności za niewykonanie lub nienależyte wykonanie umowy.

5. Odpowiedzialność za produkty wadliwe

W lutym 2025 r. Komisja Europejska wycofała projekt dyrektywy o odpowiedzialności za AI (*Artificial Intelligence Liability Directive*). Oznacza to, że na poziomie unijnym nie powstanie odrębny reżim odpowiedzialności cywilnej za szkody wyrządzone przez systemy AI – odpowiedzialność deliktowa w tym zakresie pozostaje oparta na ogólnych przepisach krajowych, w Polsce w szczególności na przepisach Kodeksu cywilnego.

Częściowe wypełnienie tej luki następuje jednak za sprawą nowej **dyrektywy** Parlamentu Europejskiego i Rady (UE) 2024/2853 z dnia 23 października 2024 r. **w sprawie odpowiedzialności za produkty wadliwe** i uchylenia dyrektywy Rady 85/374/EWG[25] („**dyrektywa PLD**"), która weszła w życie 8 grudnia 2024 r. i powinna zostać implementowana do polskiego porządku prawnego do 9 grudnia 2026 r. W porównaniu z dotychczasowymi przepisami dyrektywa PLD rozszerza odpowiedzialność za produkty wadliwe w relacjach z konsumentami

[25] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2024/2853 z dnia 23 października 2024 r. w sprawie odpowiedzialności za produkty wadliwe i uchylenia dyrektywy Rady 85/374/EWG, https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX:32024L2853 [dostęp: 21.10.2026 r.].

również na produkty cyfrowe (oprogramowanie, w tym oprogramowanie świadczone w modelu SaaS) czy dane, a także wprowadza ułatwienia dowodowe i domniemania wadliwości produktu – rozwiązania te mogą znaleźć zastosowanie do szkód wyrządzonych przez systemy AI kwalifikujące się jako produkty. Obecnie trwają prace nad nowelizacją Kodeksu cywilnego i Kodeksu postępowania cywilnego w celu wdrożenia dyrektywy PLD do polskiego porządku prawnego. Przepisy wdrażające dyrektywę PLD mogą znaleźć zastosowanie w przypadku np. oferowania klientom, konsumentom czatbotów AI przez radców prawnych.

6. Cyberbezpieczeństwo

Systemy AI są systemami maszynowymi i w rezultacie są podatne na cyberzagrożenia. Najważniejszym polskim aktem w zakresie cyberbezpieczeństwa jest **ustawa o krajowym systemie cyberbezpieczeństwa**[26], która po nowelizacji implementuje do polskiego porządku prawnego przepisy dyrektywy NIS 2[27]. Dotychczasowy podział na operatorów usług kluczowych oraz dostawców usług cyfrowych został zastąpiony podziałem na podmioty kluczowe i podmioty ważne, nakładając na nie jednocześnie szereg nowych obowiązków. Poszerzono też branże, które będą miały obowiązek stosowania tych przepisów, co będzie istotne zwłaszcza dla radców prawnych korzystających z systemów AI w ramach przedsiębiorstw z tych branż.

Do najważniejszych obowiązków nałożonych na podmioty kluczowe i ważne zaliczyć należy obowiązek wprowadzenia odpowiednich środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług oraz w celu zapobiegania wpływowi incydentów na odbiorców ich usług, w tym zapewnienie bezpieczeństwa i ciągłości łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi[28].

[26] Ustawa z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, https://dziennikustaw.gov.pl/D2026000025201.pdf [dostęp: 21.10.2026 r.].

[27] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

[28] Art. 8 ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026, poz. 20 t.j.).

Systemy AI mogą podlegać specyficznym dla tego rodzaju rozwiązań zagrożeniom (zob. rozdz. III). Zgodnie z Aktem o AI systemy AI wysokiego ryzyka powinny być projektowane i rozwijane w taki sposób, aby osiągały odpowiedni poziom dokładności, solidności i cyberbezpieczeństwa oraz by działały konsekwentnie pod tymi względami w całym cyklu życia[29].

Niezależnie od dyrektywy NIS 2 w niektórych przypadkach zastosowanie mogą też znaleźć przepisy sektorowe, np. **rozporządzenie DORA**[30], którego celem jest zwiększenie odporności sektora finansowego na cyberataki i inne zagrożenia technologiczne. Rozporządzenie to wprowadza nowe wymagania dotyczące bezpieczeństwa cyfrowego dla instytucji finansowych i ich dostawców usług IT. Zadaniem **dyrektywy CER**[31] jest natomiast zwiększenie odporności podmiotów krytycznych na incydenty (zdarzenia), które mogą znacząco zakłócić świadczenie usługi kluczowej, w tym gdy wpływają one na krajowe systemy chroniące praworządność, np. takie jak klęski żywiołowe, ataki terrorystyczne, zagrożenia wewnętrzne czy sabotaż.

7. Regulacje dotyczące radców prawnych

Radca prawny jest obowiązany zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzieleniem pomocy prawnej[32], tj. wszystkie informacje dotyczące klienta i jego spraw ujawnione radcy prawnemu przez klienta bądź uzyskane w inny sposób w związku z wykonywaniem przez niego jakichkolwiek czynności zawodowych, niezależnie od źródła tych informacji oraz formy i sposobu ich utrwalenia (tajemnica zawodowa). Tajemnica zawodowa obejmuje również wszelkie tworzone przez radcę prawnego dokumenty oraz korespondencję radcy prawnego z klientem i osobami uczestniczącymi w prowadzeniu sprawy – powstałe dla celów związanych ze świadczeniem pomocy prawnej[33].

[29] Art. 15 Aktu o AI.

[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011. Rozporządzenie obowiązuje od 17 stycznia 2025 r.

[31] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE. Dyrektywa CER powinna zostać implementowana do polskiego porządku prawnego do 17 października 2024 r.

[32] Art. 3 ust. 3 ustawy z dnia 6 lipca 1982 r. o radcach prawnych.

[33] Art. 15 Kodeksu Etyki Radcy Prawnego (dalej: KERP).

Dochowanie tajemnicy zawodowej jest obowiązkiem radcy prawnego[34]. Radca prawny obowiązany jest zabezpieczyć przed niepowołanym ujawnieniem wszelkie informacje objęte tajemnicą zawodową[35] w sposób adekwatny do charakteru, rodzaju i skali swojej działalności, otoczenia oraz rodzaju informacji będących tajemnicą zawodową i ryzyka ich ujawnienia[36]. Radca prawny zobowiązany jest wykonywać czynności zawodowe sumiennie oraz z należytą starannością uwzględniającą profesjonalny charakter działania[37].

Obowiązek przestrzegania tajemnicy zawodowej oznacza konieczność zapewnienia przez radcę prawnego odpowiednich środków technicznych, organizacyjnych mających zabezpieczyć przed jej ujawnieniem. Radca prawny powinien dołożyć należytej staranności wymaganej od profesjonalisty w zakresie zapewnienia bezpiecznego narzędzia AI, w tym poprzez wybór rzetelnego dostawcy narzędzia AI, jak również rozważyć, czy powinien podjąć dodatkowe działania w relacji z klientem.

REKOMENDACJE

Wskazówki dotyczące przepisów o radcach prawnych zawarte są w rekomendacjach nr **2**, **4**, **8**, **12**, **16** oraz **22**.

8. Postępowanie karne

Radca prawny zobowiązany jest do zachowania tajemnicy postępowania przygotowawczego oraz rozprawy sądowej prowadzonej z wyłączeniem jawności. W myśl art. 241 § 1 Kodeksu karnego wiadomości zebrane w postępowaniu karnym podlegają ochronie, a ich nieuprawnione, publiczne rozpowszechnianie, zanim zostały ujawnione w postępowaniu sądowym, jest zagrożone karą. Podobnie rozpowszechnianie publicznie wiadomości z rozprawy sądowej prowadzonej z wyłączeniem jawności jest zabronione i zagrożone karą.

[34] Art. 9 KERP.

[35] Art. 23 KERP.

[36] § 3 Regulaminu wykonywania zawodu radcy prawnego.

[37] Art. 12 KERP.

KORZYSTANIE Z NARZĘDZI AI PRZEZ PRAWNIKÓW – KORZYŚCI, WYZWANIA I RYZYKA

AI oferuje wiele korzyści, ale wiąże się również z określonymi wyzwaniami oraz może generować pewne ryzyka. Większość ryzyk związanych z korzystaniem z narzędzi AI ma charakter ogólny, jednak w pracy radcy prawnego ich skutki są szczególne, ponieważ dotyczą tajemnicy zawodowej, rzetelności pism kierowanych do sądów i organów oraz odpowiedzialności dyscyplinarnej i odszkodowawczej. Możemy je ograniczać i minimalizować przez odpowiednie regulacje, transparentność i regularne monitorowanie działania systemów AI.



REKOMENDACJE

Sposoby ograniczania ryzyk, jakie wiążą się z korzystaniem z narzędzi AI, zostały zawarte w rekomendacjach (**rozdz. V**).

1. Korzyści

Do najczęściej wskazywanych zalet korzystania z narzędzi AI zalicza się:

- **Zwiększenie konkurencyjności** – radcowie prawni, którzy korzystają z narzędzi AI w swojej codziennej pracy, mogą lepiej, szybciej i efektywniej obsługiwać klientów, co pozwala im wyróżnić się na rynku, wzmocnić satysfakcję istniejących klientów i przyciągnąć nowych. Klienci korzystają w coraz większym zakresie z AI i oczekują, że obsługujący ich prawnicy (czy to w kancelariach, czy w działach prawnych) będą wykorzystywali AI, aby poprawić jakość świadczonych usług.
- **Oszczędność czasu i przyśpieszenie procesów prawnych w organizacji** – narzędzia AI mogą znacząco skrócić czas potrzebny na realizację

określonych projektów i procesów. Mogą one odciążyć dział prawny dzięki bardziej efektywnemu dostępowi do informacji przygotowanych przez dział prawny dla klientów wewnętrznych dotyczących rutynowych zagadnień, procesów i polityk.

Dzięki temu radcowie prawni mogą szybciej przygotowywać pierwsze projekty dokumentów, podsumowania, przeszukiwać bazy danych i analizować duże ilości informacji, co pozwala na bardziej efektywne zarządzanie sprawami. W rezultacie firmy zatrudniające radców mogą obsługiwać więcej klientów w krótszym czasie, co zwiększa ich wydajność i konkurencyjność na rynku.

- **Wcześniejsze identyfikowanie ryzyk dla biznesu** – AI, w szczególności generatywna AI, umożliwia wcześniejsze identyfikowanie ryzyk poprzez analizę dużych zbiorów danych, monitorowanie działań konkurencji oraz modelowanie scenariuszy, dzięki czemu możliwe jest formułowanie prognoz wspierających decyzje biznesowe, a nie tylko analiza zdarzeń przeszłych. W efekcie radcowie prawni mogą z wyprzedzeniem identyfikować zmiany regulacyjne, geopolityczne i rynkowe oraz rozwijać zdolności do systematycznej analizy ryzyk (tzw. *risk intelligence*). Równolegle rozwój narzędzi AI i łatwiejszy dostęp do informacji powodują, że klienci/działy biznesowe oczekują bardziej spersonalizowanego, biznesowo ukierunkowanego doradztwa oraz większej zdolności do przewidywania ryzyk, co zwiększa konkurencję i przesuwa rolę prawnika w stronę partnera strategicznego[38].
- **Poprawa jakości pracy** – AI nie tylko przyśpiesza pracę radcy prawnego, lecz także redukuje ryzyko błędów ludzkich, co przekłada się na wyższą jakość świadczonych usług prawnych. Może ograniczać niektóre błędy ludzkie (np. przeoczenia przy przeglądzie dużych zbiorów dokumentów), choć jednocześnie wprowadza ryzyko nowych błędów (zob. rozdz. III.3); o jakości usługi przesądza więc weryfikacja wyniku. AI umożliwia również poprawę komunikacji radcy prawnego z klientem (język prawniczy staje się bardziej zrozumiały).
- **Odciążenie prawników w zakresie rutynowych zadań (automatyzacja rutynowych zadań prawnych)** – narzędzia AI mogą automatyzować wiele czasochłonnych zadań, takich jak analiza dokumentów czy

[38] Thomson Reuters Institute, *2026 State of the UK Legal Market*, https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2026/05/State-of-the-UK-Legal-Market-2026.pdf [dostęp: 21.10.2026 r.].

wyszukiwanie informacji. Dzięki automatyzacji rutynowych zadań prawnicy mogą skupić się na bardziej skomplikowanych i strategicznych aspektach swojej pracy, co zwiększa ich efektywność i satysfakcję zawodową.

2. Wyzwania

Do najczęściej wskazywanych wyzwań w korzystaniu z narzędzi AI zalicza się:

- **Zapewnienie ochrony poufności i tajemnicy zawodowej** – niewłaściwe korzystanie z narzędzi AI, w tym z rozwiązań, które nie zapewniają poufności czy pozwalają na trenowanie modeli AI na podstawie zawartości wejściowej i wyjściowej, może wiązać się z ryzykiem ujawnienia tajemnicy zawodowej oraz danych.
- **Dostosowanie do zmian wywołanych AI** – dostępne na rynku standardowe narzędzia już teraz pozwalają znacznie niższym kosztem i szybciej na generowanie materiałów, których jakość często dorównuje produktom pracy młodszych prawników. Prawnicy stoją zatem przed wyzwaniem, jak szkolić młodszych prawników. Ponadto zapotrzebowanie na młodszych prawników może być mniejsze niż obecnie. AI może też wymusić zmianę rozliczeń z klientami oraz zmniejszyć zapotrzebowanie na usługi prawne, zwłaszcza o niewielkiej wartości dodanej (np. proste umowy, analizy).
- **Zapewnienie odpowiedniego szkolenia aplikantów radcowskich i młodych prawników** – tradycyjny model kształcenia, w którym aplikanci uczyli się zawodu poprzez wykonywanie prostszych zadań, takich jak przygotowywanie pierwszych projektów umów, analiza dokumentów czy badanie prawne (ustalenie stanu prawnego), ulega fundamentalnej zmianie. Zadania te mogą być obecnie realizowane przez narzędzia AI szybciej i często bardziej efektywnie. Z drugiej strony, rośnie znaczenie krytycznego myślenia, kreatywności i umiejętności zarządzania, co rodzi pytanie o nowe metody szkolenia młodych prawników.
- **Kwestie związane z prawami autorskimi** – możliwość i warunki trenowania modeli AI na materiałach objętych ochroną prawnoautorską są przedmiotem sporów, co nie zapewnia pewności prawnej użytkownikom. Odnośnie do zawartości wyjściowej radcowie prawni muszą liczyć się z tym, że podobne prompty wygenerują podobne lub takie same odpowiedzi u wielu użytkowników. Rozważenia wymaga też sposób udostępniania materiałów wygenerowanych przez AI innym podmiotom, w tym klientom.

- **Odpowiedzialność** – odpowiedzialność za korzystanie z rozwiązań AI może być rozpatrywana na kilku płaszczyznach, co wymaga analizy i odpowiedniego uregulowania. Podmiot stosujący może ponosić odpowiedzialność administracyjną na podstawie Aktu o AI czy RODO, w tym może być zobowiązany do zapłaty kar finansowych wobec regulatorów w przypadku naruszenia tych przepisów. Umowa na korzystanie z systemów AI będzie regulować kwestię odpowiedzialności w relacji dostawca–zamawiający (np. radca prawny lub kancelaria). Zgodnie ze standardami rynkowymi najczęściej odpowiedzialność dostawcy, zarówno kontraktowa, jak i deliktowa, jest umownie ograniczona, np. kwotowo do wysokości wynagrodzenia dostawcy, lub wyłączona, np. w odniesieniu do utraconych korzyści podmiotu stosującego. Z perspektywy podmiotu stosującego najistotniejsze znaczenie ma korzystanie z systemu AI zgodnie z instrukcją i jego przeznaczeniem. Umowa o świadczenie usług prawnych i przepisy dotyczące radców prawnych znajdą zastosowanie do odpowiedzialności w relacji radcowie prawni stosujący AI–klient. Na tej płaszczyźnie radcowie prawni również mogą wprowadzić ograniczenia swojej odpowiedzialności wskazane powyżej, jednak powinni również rozważyć poinformowanie klienta o tym, że część ich pracy została wygenerowana przez system AI. Kwestia ta może mieć znaczenie z perspektywy prawa autorskiego (zob. rozdz. II.3), jeśli część pracy prawnika może nie być objęta prawem autorskim lub może zostać niezależnie wygenerowana przez kogoś innego – brak odpowiedniej informacji może więc co najmniej narazić reputację radcy prawnego, jeśli klient dotrze do podobnej pracy. Radcowie prawni mogą też ponosić odpowiedzialność dyscyplinarną i karną za naruszenie tajemnic zawodowych lub nienależyte wykonanie usług.

  Nie można również wykluczyć odpowiedzialności wobec osób trzecich, która na zasadach ogólnych może wynikać z Kodeksu cywilnego (odpowiedzialność deliktowa), odpowiedzialności za szkodę majątkową i niemajątkową poniesioną przez osobę fizyczną za przetwarzanie jej danych osobowych niezgodnie z przepisami (art. 82 RODO) czy odpowiedzialności za szkodę wyrządzoną przez produkt wadliwy na podstawie przepisów wdrażających dyrektywę (UE) 2024/2853 (zob. rozdz. II.5).
- **Odróżnienie treści wygenerowanych przez AI oraz treści oryginalnych** – w związku z łatwością manipulowania materiałami z pomocą AI wyzwaniem staje się ocena, czy dane materiały, w tym dowody, są prawdziwe albo czy zostały stworzone lub zmanipulowane za pomocą AI. Artykuł 50

Aktu o AI wprowadza obowiązek oznaczania treści generowanych lub zmanipulowanych przez AI oraz zapewnienia ich wykrywalności (m.in. w formatach odczytywalnych maszynowo), a także ujawniania deepfake'ów przez podmioty je wykorzystujące, co może zmniejszyć opisywane ryzyko. Opublikowany przez Komisję Europejską kodeks postępowania w sprawie przejrzystości treści generowanych przez AI doprecyzowuje, jak te obowiązki realizować w praktyce, wskazując m.in. na stosowanie oznaczeń w metadanych i innych mechanizmów weryfikacji pochodzenia treści[39]. Radca prawny powinien monitorować rozwój wdrażania art. 50 Aktu o AI i odpowiednio dostosowywać się np. poprzez wdrażanie narzędzi identyfikujących materiały dowodowe wygenerowane przez AI lub zmodyfikowane z pomocą AI (np. deepfake ze zdjęciem uszkodzonego przedmiotu przedstawiany jako dowód w postępowaniu dotyczącym wypłaty odszkodowania z umowy ubezpieczenia). Brak oznaczenia przewidzianego w art. 50 Aktu o AI nie dowodzi, że materiał nie został wygenerowany ani zmodyfikowany z pomocą AI, a narzędzia do wykrywania takich treści mogą wspierać ocenę, ale jej nie zastępują. W sprawach, w których autentyczność materiału ma znaczenie, radca prawny powinien ustalić jego pochodzenie (oryginał, metadane, łańcuch przekazania) i w razie wątpliwości rozważyć wniosek o przeprowadzenie dowodu z opinii biegłego.

3. Ryzyka

Korzystanie z narzędzi AI, jak z każdej technologii, może wiązać się z ryzykami. Do najczęściej wskazywanych ryzyk korzystania z narzędzi AI zalicza się:

- **Ryzyko halucynacji** odnoszące się do sytuacji, w których systemy AI generują wyniki, które są nieprecyzyjne, nieaktualne, nieadekwatne do kontekstu czy wręcz nieprawdziwe i pozbawione podstaw w rzeczywistości. Halucynacje wynikają głównie z tego, że modele językowe uczą się wzorców statystycznych zamiast „prawdy", a przy braku danych lub niepewności są trenowane i oceniane tak, by zgadywać najbardziej prawdopodobną odpowiedź zamiast przyznać się do niewiedzy. Przyczyną halucynacji może być także niedoskonałość danych treningowych. Jeśli zestaw danych treningowych jest

[39] *Code of Practice on transparency of AI-generated content*, https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content [dostęp: 21.10.2026 r.].

niepełny lub obciążony uprzedzeniami, system uczy się nieprawidłowych korelacji i wzorców, co prowadzi do wytwarzania fałszywych treści. Brak dostępu do aktualnych lub zweryfikowanych źródeł informacji może również sprzyjać powstawaniu halucynacji. Warto również wspomnieć o sykofancji, czyli o tendencji modeli AI do udzielania odpowiedzi zgodnych z oczekiwaniami lub założeniami użytkownika (nawet błędnymi), bezkrytycznego potwierdzania jego tez i wzmacniania jego przekonań niezależnie od poprawności faktów. Niestety na świecie i w Polsce zdarza się, że prawnicy składają pisma zawierające nieistniejące orzeczenia lub błędne informacje wygenerowane przez AI, co skutkowało m.in. odpowiedzialnością finansową lub dyscyplinarną[40].

Sądy podkreślają odpowiedzialność profesjonalnych pełnomocników za sporządzone pisma. Także w Polsce Naczelny Sąd Administracyjny po zidentyfikowaniu nieprawdziwych treści wygenerowanych przez AI w piśmie pełnomocnika podkreślił, że należy krytycznie ocenić bezrefleksyjne korzystanie z AI przez zawodowych pełnomocników oraz że pisma zawierające halucynacje wygenerowane przez AI nie spełniają wymogów profesjonalizmu i budzą wątpliwości etyczne. NSA wykazał, że argumentacja w zażaleniu jest nieprawdziwa i oddalił je[41]. W tym kontekście istotne jest także orzeczenie brytyjskiego High Court z 2025 r.[42], dotyczące złożenia przez pełnomocników pism zawierających nieprawdziwe informacje. W jednej ze spraw pełnomocnik przyznał, że oparł się na materiale wygenerowanym przez AI (przekazanym przez klienta), jednak nie zweryfikował jego poprawności. Sąd jednoznacznie podkreślił, że obowiązek rzetelnej weryfikacji spoczywa na prawniku, niezależnie od źródła informacji. W uzasadnieniu przywołano również liczne przykłady z innych jurysdykcji, wskazujące na rosnące ryzyko składania pism opartych na błędnych, „wyhalucynowanych" treściach. W konsekwencji sąd wydał nakaz pokrycia kosztów poniesionych przez przeciwnika procesowego wskutek ich nieprawidłowego działania oraz skierował sprawę do regulatorów zawodowych.

[40] Damien Charlotin prowadzi publiczny zbiór orzeczeń sądowych, w których stwierdzono użycie halucynacji przez generatywną sztuczną inteligencję, zob. https://www.damiencharlotin.com/hallucinations/ [dostęp: 21.10.2026 r.]. Jak wynika ze strony, spraw tego typu jest wiele, w dniu dostępu do strony odnotowano ponad 2,2 tys. spraw w więcej niż 40 krajach).

[41] Postanowienie Naczelnego Sądu Administracyjnego z dnia 23 czerwca 2026 r., I FZ 104/26.

[42] Orzeczenie brytyjskiego High Court z dnia 6 czerwca 2025 r. w sprawach *Ayinde v. Haringey* oraz *Al Haroun v. QNB*.

- **Ryzyko nadmiernego polegania na AI (*overreliance on AI*)**[43] – odnoszące się do sytuacji, w której osoba korzystająca z narzędzi AI polega nadmiernie lub wyłącznie na wynikach wygenerowanych przez AI, co może doprowadzić do utraty pewnych kompetencji, własnej intuicji, wiedzy eksperckiej, zdolności krytycznego myślenia czy samodzielnego rozwiązywania problemów. Dodatkowo AI często działa jak „czarna skrzynka" i brakuje jasnych informacji odnośnie do jej działania (ryzyko braku przejrzystości), co oznacza, że użytkownicy nie mają pełnego zrozumienia procesów podejmowania decyzji przez AI. Ryzyko braku wiedzy odnośnie do działania AI może się dalej pogłębić w przypadku rozwoju AI przez samą AI. Nadmierne korzystanie z AI i oddanie rozwoju AI w „ręce" AI może prowadzić też do utraty przez człowieka kompetencji realizowanych przez AI. W kontekście agentów AI ryzyko to nasila się wraz ze wzrostem ich autonomii. Badania nad delegowaniem agentom AI negocjacji i podejmowania decyzji pokazują, że poszczególni agenci AI mogą osiągać dla swoich użytkowników wyraźnie różne rezultaty, a nieprzewidywalne zachowania modeli językowych mogą prowadzić do realnych strat (np. zaakceptowania niekorzystnych warunków)[44]. Ryzyko nadmiernego polegania na AI zwiększa się dodatkowo wraz z rozwojem możliwości agentycznych w standardowych narzędziach AI. Standardowi użytkownicy mogą znacznie łatwiej delegować zaawansowane zadania do narzędzi AI, co może skutkować zmniejszeniem zrozumienia zakresu i skutków działań AI. Wykorzystywanie predefiniowanych umiejętności agentycznych (*skills*) lub wykorzystywanie umiejętności zbudowanych przez inne osoby pogłębia efekt „czarnej skrzynki", zwłaszcza dla niezaawansowanych technicznie użytkowników. Z tego względu osąd człowieka musi pozostać niezbędny zwłaszcza tam, gdzie agentowi powierzane są decyzje o skutkach prawnych lub finansowych. Agent AI może czynności wykonać, ale ocena ich trafności i odpowiedzialność za nie pozostają po stronie radcy prawnego.

[43] Przykładem nadmiernego polegania na AI może być: korzystanie przez programistów z narzędzi AI (np. GitHub Copilot) do generowania kodów czy korzystanie przez rekruterów z AI do sprawdzania CV kandydatów i późniejszy brak weryfikacji przez rekrutera wybranych przez AI CV, w sytuacji kiedy kandydaci ukrywają w tekście polecenia „zatrudnienia" (polecenie napisane białą czcionką).

[44] Raport ABA dotyczący wpływu AI na praktykę prawa, s. 22, https://www.americanbar.org/content/dam/aba/administrative/center-for-innovation/ai-task-force/2025-ai-task-force-year2-report.pdf [dostęp: 21.10.2026 r.].

- **Ryzyko dyskryminacji (*bias*)** – polegające na powielaniu schematów wyrażonych w danych treningowych. Jeżeli dane treningowe będą zawierać historyczne uprzedzenia lub będą odzwierciedlać nierówności społeczne, algorytm może się ich nauczyć i będzie powielać te uprzedzenia, czego skutkiem będzie podejmowanie tendencyjnych lub dyskryminacyjnych decyzji przez AI. Wyniki działania AI będą również nieprawidłowe, jeżeli dane treningowe nie będą dostatecznie różnorodne. Na przykład jeśli zbiory danych używane do trenowania modelu AI nie uwzględniają wystarczająco różnorodnych grup demograficznych, system może działać mniej dokładnie dla tych grup[45].
- **Ryzyko ujawnienia informacji poufnych/objętych tajemnicą** – odnoszące się do sytuacji, w której osoba korzystająca z narzędzi AI umieszcza w zawartości wejściowej informacje, które mają charakter poufny lub objęte są tajemnicą, w sytuacji gdy brak jest zabezpieczeń umownych czy technicznych przed ujawnieniem tych informacji. Takie działania mogą doprowadzić do naruszenia powszechnie obowiązujących przepisów prawa (np. dotyczących ochrony tajemnicy zawodowej) czy postanowień umowy zobowiązującej do zachowania określonych informacji w poufności. Mogą też skutkować znacznymi szkodami, np. w przypadku ujawnienia danych wynalazku przed jego zgłoszeniem w celu uzyskania ochrony patentowej, co uniemożliwi jej udzielenie.
- **Ryzyko braku aktualności** – dotyczące modeli statycznych, które nie są aktualizowane po zakończeniu procesu szkolenia i w rezultacie nie zawierają informacji o najnowszych orzeczeniach, wydarzeniach czy sprawach. W rezultacie generowane wyniki mogą być błędne lub niekompletne.
- **Ryzyko prawne oraz reputacyjne** – mogące wiązać się z roszczeniami klientów dotyczącymi naruszenia tajemnicy zawodowej czy roszczeniami osób trzecich z tytułu naruszenia majątkowych praw autorskich w związku z korzystaniem z systemów AI wytrenowanych na takich danych bez zgody uprawnionego. Przestrzeganie prawa i ochrona interesów klienta są niezwykle

[45] Przykładem może być: (i) algorytm wykorzystujący AI do rekrutacji, który dyskryminował kobiety, Businessinsider.com, *Amazon zrezygnował z algorytmów w rekrutacji. Dyskryminowały kobiety*, 10 października 2018 r., https://businessinsider.com.pl/firmy/strategie/amazon-zrezygnowal-z-algorytmow-w-rekrutacji-dyskryminowaly-kobiety/pp233ev [dostęp: 21.10.2026 r.], czy (ii) system rozpoznawania twarzy, który został przeszkolony głównie na zdjęciach osób o jasnej karnacji, może mieć trudności z prawidłowym rozpoznawaniem twarzy osób o ciemniejszej karnacji, co prowadzi do niesprawiedliwych i dyskryminujących wyników.

istotne dla prawników i często już samo podniesienie zarzutów takich naruszeń może prowadzić do utraty zaufania klientów.

- **Ryzyka dotyczące cyberzagrożeń (np. wskazane przez Open Worldwide Application Security Project, OWASP)**[46] – zidentyfikowane zostały specyficzne ryzyka bezpieczeństwa związane z AI, takie jak: zmiana promptu w celu wpływania na generowane odpowiedzi (*prompt injection*); zatruwanie (zmiana) danych używanych do szkolenia modeli AI (*training data poisoning*); brak weryfikacji outputu pod kątem ewentualnych podatności. Sposoby ograniczenia zidentyfikowanych ryzyk zostały wskazane m.in. przez OWASP. W kontekście agentów AI OWASP opublikowało zestawienie 10 najbardziej krytycznych ryzyk dla agentów AI, obejmujące m.in. przejęcie celów lub ścieżki decyzyjnej agenta AI, by realizował niezamierzone działania (*agent goal hijack*); zatruwanie pamięci i kontekstu (*memory & context poisoning*); ryzyka wynikające z narzędzi, wtyczek, rejestrów i serwerów MCP (*agentic supply chain vulnerabilities*)[47]. Pojawiają się też ryzyka związane z brakiem kontroli nad agentami AI tworzonymi i testowanymi w piaskownicach, które podejmują działania polegające na wykorzystywaniu podatności i luk w innych systemach, w tym rządowych, w celu uzyskania przez agentów nielegalnego dostępu do takich systemów bez instrukcji i często wiedzy człowieka[48].
- **Ryzyko związane z zablokowaniem dostępu do usług na podstawie warunków konkretnego dostawcy lub w związku z decyzjami politycznymi** – odnoszące się do sytuacji, gdy dany dostawca może zablokować klientowi dostęp do usługi w określonych sytuacjach (np. naruszenia zasad dozwolonego użytku określonych w umowie). W takich przypadkach przejście do innego dostawcy zwykle wymaga poniesienia dodatkowych opłat, przy czym na obecnym etapie wdrażania AI jest to stosunkowo

[46] *About OWASP Top 10 for Large Language Model Applications*, https://owasp.org/www-project-top-10-for-large-language-model-applications/ [dostęp: 21.10.2026 r.].

[47] OWASP Top 10 for Agentic Applications for 2026, 2 grudnia 2025 r., https://genai.owasp.org/resource/owasp-top-10-for-agentic-applications-for-2026/ [dostęp: 21.10.2026 r.].

[48] The Guardian, *An OpenAI agent infiltrated Medicare – and Australia only found out months later. Here's what we know so far*, 24 września 2026 r., https://www.theguardian.com/technology/2026/sep/24/openai-agent-hacked-medicare-australia-what-we-know-so-far-ntwnfb [dostęp: 21.10.2026 r.]; Reuters, *OpenAI agents hijacked German website in previously undisclosed AI breakout this spring*, 4 września 2026 r., https://www.reuters.com/world/europe/openai-agents-hijacked-german-website-previously-undisclosed-ai-breakout-this-2026-09-04/ [dostęp: 21.10.2026 r.].

niewielkie ryzyko dla zawodów prawniczych. Ryzyko to dotyczy także sytuacji, w której decyzje polityczne mogą ograniczyć dostęp do narzędzia AI – sprawa Anthropic i administracji USA pokazuje, że dostęp do narzędzi AI może zostać nagle ograniczony lub zablokowany nie z powodów technicznych, ale decyzji politycznych lub regulacyjnych – np. poprzez uznanie dostawcy za „ryzyko dla bezpieczeństwa" lub zastosowanie przepisów o kontroli eksportu[49].

[49] W czerwcu 2026 r. administracja USA nakazała Anthropic wstrzymanie dostępu do zaawansowanych modeli (Fable 5 i Mythos 5) dla określonych grup użytkowników, co w praktyce doprowadziło do globalnego wyłączenia tych usług dla wszystkich klientów, https://www.cnbc.com/2026/06/12/anthropic-disables-access-to-fable-5-and-mythos-5-to-comply-with-government-directive.html [dostęp: 21.10.2026 r.]. 26 czerwca 2026 r. administracja USA zgodziła się na przywrócenie dostępu do modelu Mythos 5 dla ograniczonej grupy ok. 100 zaufanych organizacji (firm i agencji rządowych), podczas gdy model Fable 5 nadal pozostawał objęty restrykcjami (https://www.politico.com/news/2026/06/26/white-house-makes-peace-with-anthropic-for-now-00965675 [dostęp: 21.10.2026 r.]). Następnie 30 czerwca 2026 r. Anthropic ogłosił, że Departament Handlu uchylił ograniczenia eksportowe i przywrócono globalny dostęp do Fable 5 (https://www.anthropic.com/news/redeploying-fable-5 [dostęp: 21.10.2026 r.]).

Rozdział IV

WYTYCZNE ZAGRANICZNYCH STOWARZYSZEŃ PRAWNIKÓW CO DO STOSOWANIA NARZĘDZI AI

Zagraniczne stowarzyszenia prawników zachęcają prawników do bycia na bieżąco ze zmianami technologicznymi istotnymi dla ich praktyki, w tym rozwiązaniami opartymi na generatywnej AI[50]. Zgodnie z wytycznymi czy zaleceniami tych stowarzyszeń prawnicy powinni rozumieć te zmiany i ich konsekwencje, aczkolwiek nie muszą być ekspertami w zakresie AI. Powinni jednakże rozumieć możliwości, jakie daje korzystanie z narzędzi AI, konsekwencje prawne ich wykorzystania oraz ograniczenia tych technologii. Jednocześnie prawnicy powinni korzystać z narzędzi AI w sposób odpowiedzialny i zgodny z zasadami wykonywania zawodu.

Zalecenia i wytyczne, na które warto zwrócić uwagę, to:

- Rada Adwokatur i Stowarzyszeń Prawniczych Europy (*Council of Bars and Law Societies of Europe*, CCBE), *CCBE guide on the use of generative AI by lawyers* z dnia 2 października 2025 r.[51] oraz *CCBE technical guide on the use of AI tools and models by lawyers* z dnia 27 marca 2026 r.[52];

[50] Z raportu Międzynarodowego Stowarzyszenia Prawników *Future of Legal Services – White Paper 2024* wynika, że wielu prawników nadal postrzega AI jako „problem na przyszły rok", a nie taki, który wymaga priorytetowej uwagi. Jednakże widoczny jest wzrost zainteresowania prawników wyzwaniami związanymi z AI. Prawnicy dostrzegają potrzebę skupienia się na kwestiach AI zwłaszcza w obszarze zarządzania zmianą i szkolenia personelu, tak aby móc reagować na nadchodzące wyzwania (pierwsza pozycja na liście). Wdrażanie AI w celu usprawnienia świadczenia usług prawnych również zostało uznane przez prawników za obszar wymagający zainteresowania (druga pozycja na liście).

[51] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20251002_CCBE-guide-on-the-use-of-the-use-of-generative-AI-for-lawyers.pdf [dostęp: 21.10.2026 r.].

[52] https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20260327_CCBE-technical-guide-on-the-use-of-AI-tools-and-models-by-lawyers.pdf [dostęp: 21.10.2026 r.].

- formalna opinia nr 512 Amerykańskiego Stowarzyszenia Prawników (ABA) z lipca 2024 r.[53] oraz raport ABA dotyczący wpływu AI na praktykę prawa z grudnia 2025 r.[54];
- Międzynarodowe Stowarzyszenie Prawników (IBA), *The Future is Now. Artificial Intelligence and Legal Profession* z września 2024 r.[55] oraz *Guidelines on the use of generative artificial intelligence in mediation*, z lipca 2025 r.[56];
- *European lawyers in the era of Chat GPT, FBE, Guidelines 2.0*, z września 2024 r.[57];
- Przewodnik *The Law Society* (LS) z listopada 2023 r. – publikacja 1 października 2025 r., aktualizacja z czerwca 2026 r., https://lawsociety.libguides.com/AI/professional-guidance [dostęp: 21.10.2026 r.][58];
- Rada adwokacka Anglii i Walii (*The Bar Council*), *Considerations when using ChatGPT and generative artificial intelligence software based on large language models*, aktualizacja z dnia 25 listopada 2025 r.[59];
- Materiały publikowane przez organy władz samorządowych w innych krajach UE, w tym np.:
  - adwokatura francuska (*Conseil national des barreaux*), *Utilisation des systèmes d'intelligence artificielle generative* z września 2024 r.[60], *Grille de lecture synthèse des consultations effectuées par le groupe de travail sur l'intelligence artificielle* z czerwca 2025 r.[61], *La déontologie et l'intelligence artificielle* z 1 kwietnia 2026 r.[62];

53 https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf [dostęp: 21.10.2026 r.].

54 https://www.americanbar.org/content/dam/aba/administrative/center-for-innovation/ai-task-force/2025-ai-task-force-year2-report.pdf [dostęp: 21.10.2026 r.].

55 https://www.ibanet.org/document?id=The-future-is%20now-AI-and-the-legal-profession-report [dostęp: 21.10.2026 r.].

56 https://www.ibanet.org/Guidelines-on-the-use-of-generative-artificial-intelligence-in-mediation [dostęp: 21.10.2026 r.].

57 https://www.fbe.org/nt-commissions-guidelines-on-genai/ [dostęp: 21.10.2026 r.].

58 https://www.lawsociety.org.uk/topics/ai-and-lawtech/generative-ai-the-essentials [dostęp: 21.10.2026 r.].

59 https://www.barcouncilethics.co.uk/wp-content/uploads/2024/01/Considerations-when-using-ChatGPT-and-generative-artificial-intelligence-Nov-2025.pdf [dostęp: 21.10.2026 r.].

60 https://cnb.avocat.fr/medias/cnb-guidepratique-utilisation-systemes-iag-2024-68f7b1d86e4570.98487114.pdf [dostęp: 21.10.2026 r.].

61 https://cnb.avocat.fr/medias/cnb-grille-lecture-intelligence-aartificielle-2025-68f775b81ba5b2.65545272.pdf [dostęp: 21.10.2026 r.].

62 https://cnb.avocat.fr/medias/guide-deontologie-ia-6a4cef5ea1d577.28126431.pdf [dostęp: 21.10.2026 r.].

- adwokatura niemiecka (*Bundesrechtsanwaltskammer*), *Hinweise zum Einsatz von künstlicher Intelligenz (KI)* z grudnia 2024 r.[63];
- adwokatura madrycka (*Ilustre Colegio de La Abogacía de Madrid*), *Guía de Buenas Prácticas IA* z października 2025 r.[64];
- adwokatura mediolańska (*Ordine degli Avvocati di Milano*), *Carta dei Principi per un uso consapevole di strumenti di intelligenza artificiale in ambito forense* z grudnia 2024 r.[65]

Przewodnik CCBE (*CCBE guide on the use of generative AI by lawyers*) zawiera listę innych wytycznych z wielu unijnych i pozaunijnych jurysdykcji[66].

W wymienionych zaleceniach i wytycznych poza rozważaniami dotyczącymi kwestii tajemnicy zawodowej oraz poufności analizowane są kwestie informowania klientów o stosowaniu narzędzi AI, przypadki, kiedy uzyskanie zgody klienta na korzystanie z narzędzi generatywnej AI będzie konieczne, kwestie dotyczące weryfikacji materiałów źródłowych, z których korzysta narzędzie AI, czy kwestie dotyczące rozliczeń z klientami w związku z korzystaniem z narzędzi AI. Wytyczne dotyczą kwestii kompetencji zawodowych i konieczności zapewnienia znajomości narzędzi AI w pracy prawnika oraz skutecznego komunikowania użytkownikom AI zasad ustalonych w ramach organizacji. Niektóre wytyczne odnoszą się do kwestii technicznych i operacyjnych.

63 https://www.brak.de/fileadmin/service/publikationen/Handlungshinweise/BRAK_Leitfaden_mit_Hinweisen_zum_KI-Einsatz_Stand_12_2024.pdf [dostęp: 21.10.2026 r.].

64 https://web.icam.es//wp-content/uploads/2025/10/Guia-ICAM_IA_2025_2.pdf?_gl=1*8bicqt*_up*MQ..*_ga*MTc1ODQ2MTU0LjE3ODA5OTM2ODI.*_ga_YCQLCTNGWK*czE3ODA5OTM2ODIkbzEkZzAkdDE3ODA5OTM2ODIkajYwJGwwJGgw [dostęp: 21.10.2026 r.].

65 https://www.ordineavvocatimilano.it/media/news/DICEMBRE2024/CartadeiPrincipi_OrdinediMilano.pdf [dostęp: 21.10.2026 r.].

66 https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommendations/EN_ITL_20251002_CCBE-guide-on-the-use-of-the-use-of-generative-AI-for-lawyers.pdf, s. 24–28 [dostęp: 21.10.2026 r.].

Rozdział V

REKOMENDACJE

A. Rekomendacje dotyczące przygotowania do korzystania z narzędzi AI

REKOMENDACJA NR 1: USTALENIE, W JAKICH CELACH RADCA PRAWNY BĘDZIE WYKORZYSTYWAŁ NARZĘDZIE AI

Dlaczego: Określenie celów, dla których radca prawny będzie wykorzystywał narzędzie AI, jest ważne z kilku powodów: (i) pozwoli na wybór narzędzia AI, które będzie odpowiadać na konkretne potrzeby radcy prawnego (np. uniwersalnego, wyspecjalizowanego dla spraw procesowych itp.); (ii) pozwoli zidentyfikować regulacje prawne, które należy wziąć pod uwagę, żeby zapewnić zgodne z prawem wykorzystanie narzędzia AI, w tym zapewnienie odpowiednich środków bezpieczeństwa i ochrony danych (np. czy zamierzony cel korzystania nie jest zakazaną praktyką lub systemem wysokiego ryzyka); (iii) pozwoli na wybranie najlepszego kosztowo rozwiązania.

Jak: Radca prawny powinien zidentyfikować obszary, w których AI może przynieść najwięcej korzyści w jego pracy, np. poprawić szybkość czy jakość pracy, zapewnić nowe możliwości. Radca prawny powinien zatem odpowiedzieć sobie na pytanie, do czego chce wykorzystywać narzędzia AI. Czy potrzebuje wsparcia w przygotowywaniu projektów ofert, e-maili, zarządzaniu kalendarzem, transkrypcji spotkań? Czy może potrzebuje narzędzia do przygotowywania projektów umów, analizy spraw sądowych, badania *due diligence*?

Udzielenie odpowiedzi na tego typu pytania pozwoli zidentyfikować cele, w których radca prawny będzie chciał wykorzystywać narzędzie AI, a w konsekwencji wybór odpowiedniego narzędzia AI i jego dostawcy. Przed szerszym wdrożeniem warto przeprowadzić pilotaż na jednym, dobrze określonym zastosowaniu: ustalić, jakie dane mogą być użyte, i porównać wynik z wykonaniem tego samego zadania bez AI. Ocena powinna obejmować czas pracy łącznie z weryfikacją, liczbę istotnych błędów, koszt oraz warunki, po spełnieniu których narzędzie zostanie dopuszczone do szerszego użycia albo wycofane.

REKOMENDACJA: **Przed wyborem narzędzia AI konieczne jest zidentyfikowanie, w jakich celach radca prawny chce wykorzystywać AI w pracy (np. ogólne wsparcie czy bardziej specjalistyczne).**

REKOMENDACJA NR 2: USTALENIE, JAKIE INFORMACJE WYKORZYSTUJE NARZĘDZIE AI, JAKA JEST ICH JAKOŚĆ, JAK SĄ ONE PRZETWARZANE, W TYM JAK DZIAŁA NARZĘDZIE AI (NP. CZY JEST ROZWIĄZANIEM CHMUROWYM, CZY I JAK STOSUJE FILTROWANIE ZAWARTOŚCI WEJŚCIOWEJ I WYJŚCIOWEJ)

Dlaczego: Przy wyborze odpowiedniego narzędzia AI istotne jest ustalenie, jak działa dane narzędzie AI, a w szczególności:

- w jaki sposób są przetwarzane dane zawarte w prompcie lub dane przetwarzane przez agentów AI, w tym czy te dane wejściowe/wyjściowe podlegają groundingowi i jeśli tak, w jaki sposób (np. czy są pozyskiwane również dane z Internetu, czy tylko dane w określonych wewnętrznych zasobach radcy prawnego) ➜ połączenie z Internetem lub innymi systemami (w tym przez łączniki i agentów AI) zwiększa ryzyko ujawnienia danych oraz ataków typu *prompt injection*, w których polecenia ukryte w dokumencie, wiadomości e-mail lub na stronie internetowej zmieniają działanie narzędzia; radca prawny powinien mieć możliwość wyboru i ograniczenia takiego groundingu, a także ustalenia, jakie zabezpieczenia przed takimi atakami stosuje dostawca;
- czy dane w prompcie lub zawartości wyjściowej są filtrowane i w jakim zakresie ➜ w niektórych systemach filtrowana zawartość wejściowa i wyjściowa może być przechowywana w celu weryfikacji przez człowieka;
- gdzie jest przekazywana i przetwarzana zawartość wejściowa i wyjściowa, gdzie znajduje się model AI (EOG, infrastruktura dostawcy lub podmiotu trzeciego). System AI może być zlokalizowany w infrastrukturze informatycznej (np. na serwerach) radcy prawnego lub jego organizacji (*on-premise*) – jednak w praktyce będzie to sytuacja niezwykle rzadka. W ogromnej większości przypadków narzędzia AI są udostępniane w usłudze chmurowej, a korzystanie z nich będzie możliwe w oparciu o przygotowaną aplikację (model SaaS). Część dostawców systemów AI wykorzystywanych do celów biznesowych deklaruje, że zawartość wejściowa i wyjściowa nie jest zapisywana w pamięci modelu AI, jej przetwarzanie odbywa się wyłącznie w czasie

rzeczywistym, a przechowywanie w pamięci aplikacji jest wyłącznie tymczasowe, do czasu uruchomienia przez aplikację funkcji czyszczenia pamięci. Deklaracje te należy sprawdzić w dokumentacji i umowie konkretnej usługi; brak wykorzystywania danych do trenowania nie oznacza braku ich przechowywania (np. historii rozmów).

Powyższe informacje są niezbędne do oceny zgodności takiego rozwiązania z przepisami (np. dotyczącymi ochrony danych osobowych czy zachowania tajemnicy radcowskiej) oraz do dokonania ewentualnej oceny ryzyka.

Jak: Radca prawny powinien zweryfikować umowę na korzystanie z określonego narzędzia AI wraz z powiązaną dokumentacją techniczną udostępnianą przez dostawcę narzędzia AI (np. na stronach internetowych), w szczególności:

- zasady przetwarzania danych zawartych w treści wyjściowej i wejściowej, agentach (np. czy takie informacje są wykorzystywane do trenowania modeli, jakie są zobowiązania dotyczące bezpieczeństwa takiego narzędzia AI);
- informacje, jak są przetwarzane dane, np. czy przetwarzanie ma miejsce tylko na terenie EOG czy również poza EOG; jeśli dane przetwarzane są poza EOG, to jakie mechanizmy mają zastosowanie do przekazania danych; czy dostawca rozwiązania jest podmiotem przetwarzającym lub (współ)administratorem.

Radca prawny powinien również zweryfikować sposób działania narzędzia AI od strony technicznej, np. w instrukcjach lub materiałach dostępnych na stronach dostawcy AI.

Radca prawny może również skorzystać z pomocy podmiotu wdrażającego czy partnera technologicznego w tym zakresie.

REKOMENDACJA: **Przed wyborem narzędzia AI należy zweryfikować dokumentację umowną oraz techniczną pod kątem zasad przetwarzania informacji będących składnikiem w zawartości wejściowej i wyjściowej, w tym ustalić przepływy danych.**

REKOMENDACJA NR 3: USTALENIE WŁAŚCIWEJ UMOWY NA KORZYSTANIE Z NARZĘDZIA AI

Dlaczego: Ustalenie, jaka umowa, w tym jaka wersja umowy, będzie miała zastosowanie do korzystania z danego narzędzia AI, jest istotne w celu precyzyjnego

zidentyfikowania dostawcy narzędzia AI oraz warunków korzystania z narzędzia AI. W praktyce umowa może obejmować kilka dokumentów (np. postanowienia główne umów, postanowienia licencyjne czy prawa do używania produktów oraz postanowienia dotyczące ochrony danych osobowych). Konieczne jest zatem zebranie tych dokumentów, tak aby radca prawny miał pewność, że jest to kompletna umowa. Ponadto zwłaszcza w przypadku większych umów i podmiotów umowy ramowe mogą być już zawarte, zatem należy ustalić wersję, która znajdzie zastosowanie. Z taką sytuacją możemy mieć do czynienia w szczególności w przypadku, gdy narzędzie AI jest jednym z produktów oferowanych w ramach usług chmurowych danego dostawcy. Istotne jest również zweryfikowanie modelu rozliczeniowego. Dostawcy narzędzi AI mogą stosować model opłat oparty na liczbie użytkowników (*seat-based*) lub model oparty na faktycznym wykorzystaniu (*usage-based*). Zmiana modelu płatności przez dostawcę może prowadzić do znacznego wzrostu kosztów korzystania z narzędzia AI, co powinno być uwzględnione przy analizie warunków umowy.

Jak: Radca prawny powinien w pierwszej kolejności ustalić dostawcę danego narzędzia AI. Następnie zidentyfikować właściwą umowę oraz warunki znajdujące zastosowanie do rozważanego rozwiązania AI. Pomocne mogą okazać się również strony internetowe dostawców zawierające informacje techniczne, informacje dotyczące bezpieczeństwa (np. wyniki audytów) oraz szkolenia. Umowę należy ocenić także pod kątem zakończenia współpracy: warunków wypowiedzenia, eksportu i usunięcia danych (w tym historii pracy) oraz terminów wykonania tych czynności. Radca prawny powinien zachować dokumentację spraw poza usługą w zakresie potrzebnym do ich prowadzenia, mieć plan wykonania pracy bez narzędzia oraz sprawdzić, czy jego ubezpieczenie OC obejmuje planowane zastosowania AI i jakie są warunki zgłaszania zdarzeń ubezpieczycielowi.



REKOMENDACJA: **Przed wyborem narzędzia AI konieczne jest zweryfikowanie, jaka umowa (w tym jaka jej wersja) będzie miała zastosowanie do korzystania z danego narzędzia AI, a także ustalenie wszystkich dokumentów składających się na umowę (w tym umów powierzenia przetwarzania, praw do używania produktów itp.).**

REKOMENDACJA NR 4: USTALENIE, CZY I JAK ZAPEWNIANA JEST POUFNOŚĆ ZAWARTOŚCI WEJŚCIOWEJ I ZAWARTOŚCI WYJŚCIOWEJ (W TYM TAJEMNICY ZAWODOWEJ) W UMOWIE Z DOSTAWCĄ NARZĘDZIA AI

Dlaczego: Ustalenie, czy i w jaki sposób zapewniana jest poufność zawartości wejściowej i zawartości wyjściowej (w tym tajemnicy zawodowej), jest istotne ze względu na fakt, że w przypadku braku odpowiednich zabezpieczeń umownych czy technicznych przed ujawnieniem tych informacji może dojść do naruszenia powszechnie obowiązujących przepisów prawa, w tym dotyczących ochrony tajemnicy zawodowej, czy postanowień umowy zobowiązującej do zachowania określonych informacji w poufności wiążącej użytkownika.

Należy mieć na uwadze, że narzędzia AI są udostępniane na różnych zasadach, np. w wersjach konsumenckich oraz w wersjach biznesowych (*enterprise*). Umowy dla poszczególnych wersji różnią się zwykle m.in. standardem ochrony danych, w tym określeniem roli dostawcy, który może być administratorem danych, jeśli dopuszcza np. trenowanie modeli na danych klientów.

Co istotne, darmowe wersje narzędzi AI oraz płatne wersje konsumenckie najczęściej domyślnie dopuszczają trenowanie modeli na danych klienta, a wyłączenie tej opcji (jeśli jest przewidziane) wymaga aktywności po stronie użytkownika.

Radca prawny nie powinien wprowadzać danych klientów do narzędzi AI, które nie zapewniają odpowiednich zabezpieczeń, w tym odpowiednich zobowiązań umownych dotyczących poufności danych, w szczególności do niezabezpieczonych odpowiednio wersji konsumenckich tych narzędzi.

Jak: Radca prawny powinien zweryfikować umowę na korzystanie z określonego narzędzia AI wraz z powiązaną dokumentacją udostępnianą przez dostawcę narzędzia AI pod tym kątem, w szczególności należy zweryfikować:

- czy dostawca działa jako administrator czy podmiot przetwarzający w ramach rozważanego typu umowy. Radca prawny nie powinien przetwarzać tajemnic zawodowych w narzędziach przewidujących, że dostawca może wykorzystywać dane zawarte w zawartości wyjściowej lub wejściowej do własnych celów, w tym do trenowania modeli;
- prawo własności do zawartości wejściowej i wyjściowej (np. czy użytkownik zachowuje prawo do takich danych, czy też przekazuje je dostawcy) ➜ co do zasady radca prawny nie powinien korzystać z narzędzi, które przekazują

prawa do danych umieszczonych w zawartości wyjściowej lub wejściowej podmiotom trzecim, dotyczy to zwłaszcza narzędzi wykorzystywanych do przetwarzania danych klienckich;

- zobowiązania dotyczące zachowania poufności zawartości wejściowej i wyjściowej oraz innych danych klienta (np. czy w ramach filtrowania taka zawartość jest dodatkowo przechowywana przez dostawcę w celu weryfikacji przez pracownika dostawcy) oraz zasady usuwania danych po przetworzeniu przez model AI i trenowania modeli na danych klienta ➜ należy rozważyć, czy zobowiązania dotyczące zachowania poufności są wystarczające i czy wymagane są modyfikacje (np. jeśli stosowane jest przechowywanie danych w celu weryfikacji przez pracownika dostawcy, czy zasadne jest wyłączenie tej funkcji, a także czy dane są używane do trenowania modeli, a jeżeli tak – czy można wyłączyć tę funkcję);
- środki techniczne i organizacyjne ochrony danych (np. szyfrowanie danych w przesyle i danych magazynowanych, stosowanie przez dostawcę wieloskładnikowego uwierzytelnienia, rejestrowanie logów) ➜ zawartość wyjściowa i wejściowa powinna być szyfrowana przynajmniej w przesyle oraz gdy jest magazynowana, ocena innych środków zależy od charakteru narzędzia AI;
- wyniki przeprowadzonych audytów bezpieczeństwa, w tym przez podmioty niezależne od dostawcy narzędzia ➜ niezależne audyty potwierdzające bezpieczeństwo rozwiązania zmniejszają ryzyko po stronie korzystającego;
- zasady dostępu do danych przez podwykonawców lub podmioty podprzetwarzające ➜ należy ustalić, czy takie podmioty będą miały dostęp do zawartości wejściowej lub wyjściowej, w jakim zakresie i na jakich zasadach; dostawca powinien ponosić odpowiedzialność za takie podmioty;
- czy dane wejściowe/wyjściowe nie są wykorzystywane do trenowania modeli ➜ rekomendowane jest wprowadzenie do umowy zobowiązania dostawcy o niewykorzystywaniu danych wejściowych i wyjściowych do takich celów;
- zasady odpowiedzialności dostawcy za naruszenie poufności ➜ należy ustalić, czy realne jest uzyskanie odszkodowania w przypadku naruszenia, jeśli odpowiedzialność dostawcy jest ograniczona, ponadto należy ustalić, czy oferowany limit jest wystarczający;
- ewentualne dodatkowe funkcjonalności, które mogą być wdrożone w celu zwiększenia ochrony danych zawartych w zawartości wejściowej i wyjściowej ➜ należy ocenić, czy celowe jest wdrażanie takich rozwiązań.

REKOMENDACJA: **Przed wyborem narzędzia AI należy zweryfikować umowę oraz dokumentację udostępnianą przez dostawcę narzędzia AI pod kątem zobowiązań dostawcy w zakresie zachowania poufności zawartości wejściowej i zawartości wyjściowej i ustalić, czy oferowane rozwiązania zapewniają zachowanie poufności tajemnicy zawodowej, jak również czy celowe jest zastosowanie dodatkowych zabezpieczeń.**

REKOMENDACJA NR 5: USTALENIE – W OPARCIU O POSTANOWIENIA UMOWY Z DOSTAWCĄ NARZĘDZIA AI – JAK REGULOWANE SĄ KWESTIE PRAW AUTORSKICH I JAKI TO MA WPŁYW NA WYKONYWANIE ZAWODU

Dlaczego: Radca prawny decyduje o treści zapytania (promptu) / zawartości wejściowej, której częścią potencjalnie może być utwór. Radca prawny musi mieć prawo do korzystania z takiego utworu – czy to jako właściciel majątkowych praw autorskich, jako licencjobiorca, czy w ramach jednej z postaci dozwolonego użytku. Radca prawny potencjalnie odpowiada za naruszenie praw autorskich do zawartości wejściowej.

Z uwagi na wątpliwości dotyczące możliwości trenowania modeli na utworach objętych ochroną prawnoautorską należy zweryfikować, czy dostawca narzędzia AI zobowiązuje się chronić użytkowników przed roszczeniami osób trzecich z tego tytułu.

Należy też ustalić ewentualne prawa dostawcy narzędzia AI do zawartości wejściowej i wyjściowej oraz ograniczenia wykorzystania takiej zawartości, a w szczególności, czy dostawca narzędzia uzyskuje prawa do takiej zawartości i ewentualnie jakie (np. licencja).

Jak: Radca prawny powinien zweryfikować umowę na korzystanie z określonego narzędzia AI w zakresie uregulowania praw do korzystania z narzędzia AI, zawartości wejściowej i wyjściowej, a w szczególności:

- na jakiej podstawie będzie korzystał z narzędzia AI (np. licencja, zob. rozdz. II.3.1);
- czy dostawca zobowiązuje się bronić użytkownika przed roszczeniami podmiotów trzecich;
- jak uregulowane są kwestie praw do zawartości wejściowej i wyjściowej (outputu), tj. czy klient zachowuje prawa do takiej zawartości i na jakich zasadach ➜ prawo do zawartości wejściowej powinno pozostać przy kliencie,

przy czym w niektórych przypadkach może być dopuszczalne udzielenie dostawcy licencji (wymaga to indywidualnej oceny), prawo do zawartości wyjściowej nie powinno przysługiwać dostawcy, a radca prawny powinien ocenić, czy i jakie prawa mogą mu przysługiwać;

- czy dane wejściowe/wyjściowe nie są wykorzystywane do trenowania modeli ➜ rekomendowane jest wprowadzenie do umowy zobowiązania dostawcy o niewykorzystywaniu danych wejściowych i wyjściowych do takich celów;
- czy klient może korzystać z zawartości wyjściowej do własnych celów komercyjnych (np. w swojej dokumentacji) i czy umowa zawiera jakieś ograniczenia co do komercyjnego wykorzystania zawartości wyjściowej ➜ należy ocenić, czy ewentualne ograniczenia mają zastosowanie dla radcy prawnego (np. ograniczenia w zakresie wykorzystywania danych syntetycznych wygenerowanych przez udostępnione narzędzie AI do trenowania własnych modeli AI nie będą ograniczeniem dla większości radców prawnych, którzy chcą wykorzystać AI do wsparcia w swojej codziennej pracy);
- czy dostawca zapewnia obronę klienta przed roszczeniami osób trzecich do zawartości wyjściowej z tytułu naruszeń praw własności intelektualnej (zob. szerzej rekomendacja nr 6).

REKOMENDACJA: **Przed wyborem narzędzia AI należy zweryfikować umowę z dostawcą pod kątem uregulowania kwestii praw autorskich do narzędzia AI, zawartości wejściowej i zawartości wyjściowej, w tym ograniczeń oraz zakresu zobowiązań dostawcy dotyczących obrony przed roszczeniami osób trzecich dotyczących naruszenia praw autorskich. Należy ocenić, czy ewentualne ograniczenia mają praktyczne zastosowanie, i jeśli tak, jakie dla wykonywania zawodu radcy prawnego.**

REKOMENDACJA NR 6: USTALENIE – W OPARCIU O POSTANOWIENIA UMOWY Z DOSTAWCĄ NARZĘDZIA AI – CZY DOSTAWCA PRZEWIDUJE OBRONĘ PRZED ROSZCZENIAMI OSÓB TRZECICH DO NARZĘDZIA AI I DO ZAWARTOŚCI WYJŚCIOWEJ (OUTPUTU) W ZWIĄZKU Z UŻYWANIEM MODELI ZAWARTYCH W NARZĘDZIU AI Z TYTUŁU NARUSZEŃ PRAW WŁASNOŚCI INTELEKTUALNEJ

Dlaczego: Korzystanie z narzędzi AI, jak z każdego innego dobra własności intelektualnej, może wiązać się z ryzykiem roszczeń o naruszenia tych praw. Co więcej,

w związku z nierozstrzygniętymi wątpliwościami dotyczącymi możliwości trenowania modeli na utworach lub dobrach chronionych prawami własności intelektualnej nie można też wykluczyć roszczeń o naruszenie tych praw w związku z korzystaniem z zawartości wyjściowej (zob. rozdz. II.3.1 i 3.2).

Jeśli osoba trzecia zgłosi roszczenia, radca prawny jako podmiot stosujący narzędzie AI może być zmuszony do prowadzenia postępowań sądowych czy zaprzestania używania takiego narzędzia. Zobowiązanie dostawcy narzędzia do obrony przed takimi roszczeniami, nawet ograniczone pewnymi warunkami zastosowania, ogranicza ryzyko podmiotu stosującego.

Jak: Radca prawny powinien zweryfikować umowę na korzystanie z określonego narzędzia AI, czy zawiera ona zobowiązanie dostawcy do obrony klienta przed roszczeniami osób trzecich do modelu i zawartości wyjściowej (outputu) w związku z korzystaniem z modeli zawartych w narzędziu AI z tytułu naruszeń praw własności intelektualnej. Należy też zweryfikować, od jakich dodatkowych warunków uzależnione jest skorzystanie z tego zobowiązania oraz jakich roszczeń dotyczy zobowiązanie dostawcy. Takie dodatkowe warunki prawne bywają oczywiste, ale ich niespełnienie wyłącza ochronę, dlatego radca prawny powinien je znać i móc wykazać ich przestrzeganie, np. użytkownik musi mieć prawo do zawartości wejściowej (tzn. nie można powoływać się na ochronę, jeśli samemu narusza się prawa innych), czy nie można wyłączać, uchylać się, przerywać ani ingerować w filtry treści lub inne systemy bezpieczeństwa, które są częścią narzędzia AI (tj. obchodzenie zabezpieczeń skutkuje wyłączeniem ochrony). Radca prawny powinien wprowadzić rozwiązania organizacyjno-techniczne zapewniające zgodność z takimi dodatkowymi warunkami (np. w formie wewnętrznych instrukcji dla personelu).

REKOMENDACJA: Przed wyborem narzędzia AI należy zweryfikować umowę z dostawcą narzędzia AI pod kątem zobowiązań dostawcy do obrony klienta przed roszczeniami osób trzecich do narzędzia AI i zawartości wyjściowej (outputu) wygenerowanej z jego pomocą, w tym zakres dodatkowych warunków, od których zależy korzystanie z takich zobowiązań. Należy podjąć działania, żeby zapewnić zgodność z takimi dodatkowymi warunkami (np. przekazać personelowi odpowiednie instrukcje).

REKOMENDACJA NR 7: OCENA NARZĘDZIA AI POD KĄTEM RODO (W TYM KONIECZNOŚĆ ZAWARCIA LUB DOSTOSOWANIA UMOWY POWIERZENIA, MODYFIKACJI KLAUZULI INFORMACYJNEJ, OCENY TRANSFERÓW DANYCH POZA EOG, PRZEPROWADZENIA DPIA)

Dlaczego: Do korzystania z systemów AI w odniesieniu do przetwarzania danych osobowych stosuje się przepisy RODO, jednak to na radcy prawnym albo spółce/pracodawcy spoczywa odpowiedzialność za wypełnienie obowiązków wynikających z RODO oraz ustalenie ról podmiotów biorących udział w przetwarzaniu danych osobowych (administrator/współadministrator/podmiot przetwarzający).

Jak: Radca prawny albo jego organizacja co do zasady pełnić będzie rolę administratora danych, dostawca natomiast będzie pełnić rolę administratora (współadministratora) lub podmiotu przetwarzającego. W celu ustalenia roli dostawcy należy zweryfikować postanowienia umowy dotyczące danych osobowych, zakres przetwarzanych danych oraz przeanalizować je w kontekście zamierzonego celu wykorzystania systemu AI. Zalecane jest, aby w odniesieniu do ewentualnych danych klientów radcy prawnego dostawca narzędzia AI pełnił rolę podmiotu przetwarzającego. W odniesieniu do danych użytkowników można zaakceptować przetwarzanie danych przez dostawcę jako administratora, przy czym wymaga to weryfikacji.

Wypełnienie obowiązków wynikających z RODO będzie również polegać w szczególności na:

- ustaleniu, czy system AI spełnia wymogi wynikające z RODO, np. czy dostawca zapewnia, że wdrożył środki techniczne i organizacyjne adekwatne do ryzyka związanego z przetwarzaniem danych; czy system umożliwia realizację praw osób, których dane dotyczą;
- ustaleniu, czy istnieje podstawa prawna do przetwarzania danych osobowych z wykorzystaniem systemu AI (art. 6 RODO) – podstawa ta powinna istnieć po stronie dostawcy (w odniesieniu do danych użytych do trenowania), lecz jednocześnie radca prawny (jego organizacja) powinien legitymować się podstawą prawną do przetwarzania danych w systemie AI (np. w zawartości wejściowej);
- ustaleniu, czy w wyniku korzystania z narzędzia AI (np. agenta) decyzje będą podejmowane automatycznie i jeśli mogą one wywoływać skutek prawny lub w podobny sposób istotnie wpływać na osobę, której dane dotyczą – czy spełnione są wymogi określone w art. 22 RODO;

- weryfikacji przetwarzania danych poza EOG i wprowadzeniu odpowiednich zabezpieczeń wymaganych przez rozdział V RODO, w przypadku gdy takie przetwarzanie będzie miało miejsce ➜ należy pamiętać także o weryfikacji w tym zakresie usług serwisowych dostawcy, ponieważ potencjalnie w obydwu przypadkach serwis systemu AI może wiązać się z przetwarzaniem danych poza EOG, np. w przypadku zdalnego dostępu do danych przez serwisantów zlokalizowanych poza EOG. Niektórzy dostawcy oferują opcję ograniczenia przetwarzania danych do EOG, należy wówczas zweryfikować warunki takiego ograniczenia oraz potencjalne wyjątki;
- analizie konieczności przeprowadzenia oceny skutków dla ochrony danych (DPIA) (art. 35 RODO) i jej przeprowadzeniu, jeśli jest konieczna;
- ocenie, czy konieczna jest aktualizacja obowiązku informacyjnego stosowanego przez radcę prawnego względem osób, których dane są przetwarzane z wykorzystaniem systemu AI (art. 13 i 14 RODO) – wykaz elementów do weryfikacji w związku z korzystaniem z AI znajduje się w załączniku nr 3;
- ocenie, czy konieczna jest aktualizacja umów z klientami pod kątem przetwarzania danych osobowych;
- ocenie, czy konieczna jest aktualizacja rejestru czynności przetwarzania dotyczącego działalności radcy prawnego (art. 30 RODO);
- zawarciu umowy o powierzenie przetwarzania danych osobowych (jeśli dostawca będzie przetwarzać dane jako podmiot przetwarzający) lub, jeśli taka umowa już jest zawarta, jej weryfikacji pod kątem rozważanego narzędzia AI, a także wypełnieniu obowiązków administratora związanych z jej zawarciem (art. 28 RODO).

REKOMENDACJA: **Przed wyborem narzędzia AI konieczna jest weryfikacja zarówno umowy z dostawcą, w tym ustalenie jego roli w procesie przetwarzania (co do zasady powinien to być podmiot przetwarzający, jeśli chodzi o dane zawarte w zawartości wejściowej/wyjściowej), jak i ocena, czy dostawca spełnia wymogi RODO (np. czy zawarta jest umowa o powierzenie przetwarzania, czy wdrożone są adekwatne środki techniczne). Radca prawny powinien również zweryfikować i, jeśli jest to konieczne, dostosować dokumentację wewnętrzną dotyczącą przetwarzania danych osobowych do korzystania z narzędzia AI, a także ocenić, czy aktualizacji wymaga umowa z klientem.**

REKOMENDACJA NR 8: USTALENIE, JAKIE ŚRODKI BEZPIECZEŃSTWA NALEŻY WDROŻYĆ/STOSOWAĆ/ SKONFIGUROWAĆ PODCZAS KORZYSTANIA Z NARZĘDZIA AI

Dlaczego: Po ustaleniu sposobu działania narzędzia AI, warunków umownych i dokumentacji technicznej oraz wykonaniu analizy w zakresie przetwarzania danych radca prawny powinien ustalić, jakie środki bezpieczeństwa należy wdrożyć, stosować lub skonfigurować podczas korzystania z narzędzia AI. Jest to szczególnie istotne, ponieważ na radcy prawnym ciąży obowiązek zachowania poufności i tajemnicy zawodowej. Obowiązek przestrzegania tajemnicy zawodowej oznacza konieczność zapewnienia przez radcę prawnego odpowiednich środków technicznych, organizacyjnych mających zabezpieczyć przed jej ujawnieniem (zob. rozdz. II.7). Obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych wynika również z przepisów z zakresu ochrony danych osobowych. W przypadku używania systemów AI wysokiego ryzyka w rozumieniu Aktu o AI na radcach prawnych może spoczywać obowiązek wdrożenia środków technicznych i organizacyjnych umożliwiających wykorzystanie narzędzia AI zgodnie z instrukcją obsługi dostawcy (zob. rozdz. II.2) – w praktyce jednak będą to sytuacje raczej wyjątkowe.

Jak: Z uwagi na to, że większość narzędzi AI jest udostępnianych w chmurze obliczeniowej, należy w pierwszej kolejności odpowiednio skonfigurować te narzędzia, w tym w zakresie lokalizacji danych będących składową zawartości wejściowej i wyjściowej, poziomu i zasad filtrowania treści oraz parametrów wpływających na sposób generowania odpowiedzi (np. bardziej lub mniej kreatywnych) i zasad przetwarzania danych, jeżeli są dostępne. Należy pamiętać, że w przypadku usług chmurowych nie ma w praktyce możliwości wprowadzania zmian w samych usługach/narzędziach AI.

Radca prawny powinien ocenić nie tylko techniczne, lecz także organizacyjne środki bezpieczeństwa, np. sposób komunikacji i instrukcje dla personelu.

Radca prawny powinien rozważyć, czy może dokonać oceny samodzielnie lub we własnych strukturach, czy też powinien skorzystać z pomocy podmiotu wdrażającego czy partnera technologicznego w tym zakresie.

Radca prawny powinien korzystać z takich narzędzi AI, które nie wykorzystują danych objętych tajemnicą zawodową do trenowania modelu ani do innych własnych celów dostawcy. Jeżeli dostawca zastrzega sobie dostęp do zawartości wejściowej lub wyjściowej w celach kontrolnych (np. przegląd treści przez pracowników dostawcy w ramach wykrywania nadużyć), radca prawny powinien ustalić zakres i okres takiego dostępu, a jeżeli umowa przewiduje możliwość jego

wyłączenia, skorzystać z niej w odniesieniu do danych objętych tajemnicą zawodową. W praktyce oznacza to konieczność zweryfikowania zasad przetwarzania danych przez dostawcę (w szczególności tego, czy dane wprowadzane do narzędzia są wykorzystywane do trenowania modelu lub do innych celów oraz jak długo są przechowywane). Dodatkowo warto określić zasady i długość przechowywania promptów, historii pracy lub dokumentów w stosowanych narzędziach AI. Zasady te powinny zostać określone, aby dane były przechowywane wyłącznie tak długo, jak służą uzasadnionym celom radcy prawnego (np. usuwanie historii pracy w określonym czasie po zakończeniu projektu).

REKOMENDACJA: **Po ustaleniu sposobu działania narzędzia AI, warunków umownych i dokumentacji technicznej oraz wykonaniu analizy w zakresie przetwarzania danych radca prawny powinien ocenić, jakie techniczne i organizacyjne środki bezpieczeństwa powinny zostać wdrożone w celu korzystania z narzędzia AI w sposób zapewniający ochronę tajemnicy zawodowej. W szczególności należy ocenić, jak dokonać lub zmienić konfigurację narzędzia AI, zwłaszcza w przypadku gdy jest ono udostępniane w modelu chmurowym, a także określić sposób komunikacji z użytkownikami i instrukcje wewnętrzne. Zaleca się korzystanie z rozwiązań, które przewidują, że bez zgody radcy prawnego dostawca modeli nie będzie wykorzystywał danych klientów do trenowania modeli.**

REKOMENDACJA NR 9: OKREŚLENIE ZASAD ZASTOSOWANIA AGENTÓW AI

Dlaczego: Agent AI to system AI zaprojektowany do autonomicznego wykonywania szeregu zadań, aby osiągnąć wyznaczony cel (zob. rozdz. I.2.4). Agenci mogą potencjalnie realizować bardzo skomplikowane zadania bez ingerencji człowieka na poszczególnych etapach.

Głównym wyzwaniem korzystania z agentów AI jest często brak pełnej informacji o sposobie ich funkcjonowania. Standardową procedurą powinny być testy agentów i porównanie generowanych przez nich wyników z danymi historycznymi, np. porównanie i ocena raportu z badania prawnego (*due diligence*) przygotowanego za pomocą agenta AI i przez prawników.

Kolejnym wyzwaniem jest zapewnienie właściwej weryfikacji wyników generowanych za pomocą agenta przez radcę prawnego. Agenci często nie pozwalają walidować poszczególnych etapów pracy, a jedynie jej końcowy element. Radca prawny powinien ocenić, czy taki brak walidacji na poszczególnych etapach jest

akceptowalny i w szczególności nie zwiększa ryzyka halucynacji, wystąpienia błędów lub dyskryminacji.

Przetwarzanie danych osobowych w agentach (np. w przypadku agentów wykorzystywanych w procesach rekrutacji czy oceny) może wiązać się z automatycznym podejmowaniem decyzji (zob. rozdz. II.1.3).

Korzystanie z agentów wiąże się też z nowymi wyzwaniami technicznymi. Radca prawny powinien ustalić przed wdrożeniem, do jakich danych i informacji agent będzie miał dostęp. W miarę korzystania jakość pracy agentów i ich decyzji może też się pogarszać. Wreszcie korzystanie z agentów może rodzić nowe podatności technologiczne (zob. rozdz. III.3).

Szczególnej uwagi wymaga podłączenie agenta AI do istniejących systemów organizacji, np. poczty elektronicznej, systemu zarządzania dokumentami czy kalendarza, w których przetwarzane są dane różnych klientów. Należy zweryfikować, czy wykorzystanie agenta może doprowadzić do ujawnienia tajemnicy zawodowej (np. wykorzystania informacji dotyczących jednego klienta przy procesie wykonywanym dla innego klienta), i wdrożyć odpowiednie zabezpieczenia (przede wszystkim techniczną separację dostępów i zbiorów danych oraz uprawnienia ograniczone do danej sprawy; prompty i instrukcje mogą je jedynie uzupełniać).

Należy również uwzględnić ryzyko wstrzyknięcia poleceń (*prompt injection*): treść dokumentów, wiadomości e-mail i stron internetowych przetwarzanych przez agenta może zawierać ukryte instrukcje. Agent z dostępem do poczty lub repozytorium dokumentów nie powinien więc mieć uprawnień do samodzielnego wysyłania wiadomości, udostępniania plików ani wykonywania innych czynności nieodwracalnych bez zatwierdzenia przez radcę prawnego.

Agenci AI mogą być tworzeni z wykorzystaniem standardowych narzędzi przez samych radców prawnych, bez konieczności angażowania programistów. W takich przypadkach radca prawny powinien informować wewnątrz swojej organizacji o utworzeniu agenta i zapewnić, że zostanie on zweryfikowany pod kątem zgodności z przepisami i prawidłowości działania.

Jak: Radca prawny powinien dokonać oceny, czy w organizacji przydatne będzie zastosowanie agentów AI, w szczególności udzielając odpowiedzi na poniższe pytania:

- czy są jakieś obszary pracy radcy prawnego, w których można wprowadzić automatyzację działania;
- jeśli tak, to czy agent AI może odciążyć radcę prawnego w całym procesie czy tylko w jego fragmencie (np. agent AI dokonuje wstępnej analizy dokumentów czy przeprowadza wstępne *due diligence*);

- jakie narzędzia mogą pomóc w tworzeniu agentów AI i czy rozważane narzędzie AI daje takie możliwości;
- czy agent jest agentem „standardowym" udostępnianym przez dostawcę, czy też będzie tworzony w ramach organizacji. Jeśli jest to agent udostępniany przez dostawcę, należy zbadać, czy znajdują do niego zastosowanie dodatkowe warunki umowne (zob. rekomendacja nr 3);
- jaki zakres autonomii można przypisać agentowi AI (jakie czynności może wykonywać samodzielnie i z jakimi narzędziami może się samodzielnie komunikować, jakie dane może pobierać);
- jakie ryzyka wiążą się z wdrożeniem agentów AI w danym obszarze (w tym ryzyka związane z dostępem do danych, tajemnic zawodowych, autonomią decyzyjną i odwracalnością działań agenta).

Następnie, gdy podjęta zostanie decyzja o zbudowaniu lub wykorzystaniu agenta AI, radca prawny powinien:

- określić katalog czynności zastrzeżonych wyłącznie dla radcy prawnego, których agent AI nie może wykonać samodzielnie niezależnie od stopnia jego niezawodności. W szczególności agent nie powinien bez weryfikacji udzielać porad prawnych i przedstawiać stanowiska prawnego klientowi, sądowi lub stronie trzeciej, składać oświadczeń w imieniu klienta, podejmować decyzji o wszczęciu, zmianie lub zakończeniu czynności w sprawie ani wykonywać działań nieodwracalnych;
- ocenić odwracalność i poziom autonomii zadań powierzonych agentowi AI;
- zdefiniować punkty kontrolne, w których wymagana jest weryfikacja przez radcę prawnego, w szczególności obowiązkową kontrolę produktu pracy agenta AI przed jego wykorzystaniem wobec klienta, sądu lub strony trzeciej, w tym weryfikację prawidłowości i autentyczności powołanych przepisów oraz orzeczeń. Weryfikacja każdego końcowego wyniku agenta AI jest obowiązkowa dla produktów pracy kierowanych na zewnątrz. Dla czynności wewnętrznych o dużej skali (np. wstępna klasyfikacja dokumentów, ekstrakcja danych), w których weryfikacja każdego wyniku przestaje być wykonalna, radca prawny może zastąpić ją weryfikacją statystyczną, tj. kontrolą losowo dobranej próbki wyników o z góry określonej wielkości i częstotliwości, pod warunkiem udokumentowania zasad doboru próby, progu błędu, którego przekroczenie skutkuje wstrzymaniem agenta, oraz osoby odpowiedzialnej za kontrolę. Weryfikacja statystyczna nie zwalnia z pełnej kontroli w punktach kontrolnych. Należy przy tym pamiętać, że wraz z rozwojem technologii

i niezawodności agenta rośnie ryzyko bezrefleksyjnego zatwierdzania jego wyników (*automation bias*), dlatego kontrola ta musi pozostać rzeczywista;
- w przypadku agentów tworzonych samodzielnie określić zasady ich ujawniania, ewidencjonowania, dopuszczania do stosowania, utrzymania i nadzoru nad stosowaniem;
- zaprojektować zasady i ograniczenia dostępu agenta AI do narzędzi i systemów;
- upewnić się, że ma możliwość wyłączenia lub powstrzymania działania agenta AI w każdym momencie obejmującą nie tylko zatrzymanie agenta, lecz także odebranie mu dostępu do narzędzi i danych, a także, o ile pozwolą na to warunki, cofnięcie skutków już wykonanych działań (*rollback*);
- wprowadzać agentów AI stopniowo i stale monitorować ich działanie, tak aby jak najszybciej zidentyfikować ewentualny „dryf" agenta (pogorszenie jakości);
- przeprowadzić finalny, krótki test, odpowiadając sobie na pytania:
  - » czy dokładnie wiesz, co agentowi AI wolno, a czego nie, i czy czynności zastrzeżone dla radcy prawnego są technicznie wyłączone z jego zakresu działania,
  - » czy możesz audytować każde jego działanie,
  - » czy możesz szybko wyłączyć agenta AI i w razie potrzeby cofnąć skutki jego działań.

Brak twierdzących odpowiedzi na powyższe pytania powinien wstrzymać decyzję o uruchomieniu agenta AI.

REKOMENDACJA: Wdrażając agentów AI, radca prawny powinien przeanalizować, do jakiego typu zadań zamierza stworzyć lub wykorzystać agenta AI, ocenić ryzyko jego wykorzystania, a także zadecydować, jaki zakres zadań i autonomii mu powierzyć, w tym do jakiego katalogu danych i innych narzędzi udzielić mu dostępu. Radca prawny powinien określić katalog czynności zastrzeżonych wyłącznie dla siebie, których agent AI nie może wykonywać samodzielnie. Agent AI nie może w szczególności samodzielnie udzielać porad prawnych klientowi. Zakres i sposób weryfikacji wyników agenta AI (pełna albo statystyczna) powinny być dostosowane do skali i skutków powierzonych mu czynności. Radca prawny powinien zweryfikować, czy korzystanie z agenta nie doprowadzi do ujawnienia tajemnicy zawodowej (np. w związku z planowanym dostępem do danych różnych klientów), i wdrożyć odpowiednie zabezpieczenia. Radca prawny powinien zapewnić nadzór ludzki nad działaniem agenta AI i upewnić się, że w każdym momencie możliwe jest wyłączenie agenta AI. Analogiczne wytyczne powinny być stosowane dla umiejętności (*skills*) oraz łączników do innych systemów.

REKOMENDACJA NR 10: USTALENIE MOŻLIWOŚCI TECHNICZNYCH (API, WTYCZKI) INTEGRACJI NARZĘDZIA AI Z INNYMI SYSTEMAMI I PLATFORMAMI, Z KTÓRYCH KORZYSTA RADCA PRAWNY

Dlaczego: Możliwość integracji narzędzia AI z systemami i platformami, z których korzysta radca prawny (np. systemami zarządzania dokumentami, bazami danych, CRM), pozwala na stworzenie rozwiązania idealnie dopasowanego do potrzeb radcy prawnego i pełne wykorzystanie funkcjonalności danego narzędzia AI.

Jak: Radca prawny powinien zweryfikować umowę na korzystanie z określonego narzędzia AI wraz z powiązaną dokumentacją udostępnianą przez dostawcę narzędzia AI w zakresie warunków technicznych integracji danego narzędzia AI z innymi systemami czy platformami, w szczególności:

- czy dostawca oferuje API, wtyczki czy rozszerzenia dostosowane do systemów lub platform, z których korzysta radca prawny, lub czy takie rozwiązania są oferowane przez podmioty trzecie i na jakich warunkach;
- czy dostawca zapewnia odpowiednie wsparcie techniczne i dokumentację w procesie wdrożenia (dedykowane wsparcie techniczne, baza wiedzy itp.);
- czy integracja wymaga zmian w posiadanych systemach i platformach oraz czy istnieje możliwość wprowadzenia takich zmian samodzielnie, z pomocą dostawcy takiego systemu lub podmiotu trzeciego; należy ocenić, czy stworzenie i zastosowanie takiej wtyczki czy rozszerzenia wymagałoby modyfikacji posiadanego systemu czy platformy (w tym czy radca prawny lub jego organizacja ma prawo do takich działań);
- czy zastosowanie takiej integracji wymaga ponownej weryfikacji działania i oceny bezpieczeństwa istniejących systemów i platform, z jednej strony, oraz narzędzia AI, z drugiej strony.



REKOMENDACJA: **Przed wyborem narzędzia AI należy dokonać oceny warunków technicznych i prawnych integracji narzędzia AI z systemami i platformami, z których korzysta radca prawny, w szczególności biorąc pod uwagę bezpieczeństwo danych oraz warunki istniejących umów na systemy i platformy, z którymi takie narzędzie AI miałoby być integrowane.**

REKOMENDACJA NR 11: OCENA PRZYDATNOŚCI TRENOWANIA MODELI (*FINE-TUNING*) NA DANYCH WEWNĘTRZNYCH

Dlaczego: *Fine-tuning* umożliwia dostosowanie modelu AI do specyficznych zadań i potrzeb danej organizacji (zob. rozdz. I.2.5) – dzięki temu narzędzie AI może lepiej wspierać konkretne procesy biznesowe w organizacji oraz dostarczać bardziej precyzyjnych wyników. Nie wszystkie narzędzia AI dają możliwość dostosowania (*fine-tuningu*) i w związku z tym konieczne jest też wybranie odpowiedniego narzędzia do tego celu.

Jak: Radca prawny powinien dokonać oceny, czy w organizacji przydatne będzie trenowanie modeli AI na danych wewnętrznych, w szczególności udzielając odpowiedzi na pytania:

- w jakich obszarach wykorzystanie *fine-tuningu* może być korzystne dla organizacji;
- czy dane wewnętrzne, na których miałby być szkolony model, są kompletne, dokładne i aktualne? ➜ niskiej jakości dane mogą prowadzić do błędnych wyników;
- czy organizacja ma odpowiednie zasoby techniczne i kompetencje do przeprowadzenia *fine-tuningu* (infrastruktura/specjaliści);
- jakie będą warunki umowne dotyczące modelu stworzonego w wyniku *fine-tuningu*, tj. czy taki model będzie dostępny tylko dla podmiotu, który go tworzy?;
- jakie są koszty *fine-tuningu* i utrzymania takiego dostosowanego modelu.

Z uwagi na fakt, że *fine-tuning* może wymagać wiadomości specjalnych, radca prawny powinien rozważyć zaangażowanie osoby dysponującej odpowiednimi kwalifikacjami w tym zakresie. Radca prawny powinien opracować plan dostosowania i testowania takiego dostosowania modelu. Jeżeli dostosowanie modelu ma nastąpić z wykorzystaniem dokumentów pochodzących ze spraw klientów, radca prawny powinien w pierwszej kolejności rozważyć anonimizację tych dokumentów albo wykorzystanie wzorów i dokumentów własnych. Wykorzystanie danych klienta wymaga jego uprzedniej zgody (zob. rekomendacja nr 14). Umowa z dostawcą powinna zapewniać, że dostosowany model jest dostępny wyłącznie na potrzeby radcy prawnego, a dane treningowe i dostosowany model zostaną usunięte po zakończeniu współpracy z dostawcą; radca prawny powinien też z góry ustalić, jak postąpi, jeżeli klient cofnie zgodę. Należy uwzględnić ryzyko, że model dostosowany na dokumentach jednego klienta odtworzy ich fragmenty w pracy dla innego klienta (zob. rekomendacja nr 8).

REKOMENDACJA: Radca prawny powinien ocenić, czy chce dokonywać dostosowania modelu (*fine-tuning*), i wybrać odpowiednie narzędzie do tego celu. Konieczne jest też odpowiednie przygotowanie takiego procesu, np. przez selekcję właściwych danych i zaangażowanie specjalisty do wsparcia w tym procesie. Przed wdrożeniem radca prawny powinien porównać wyniki dostosowanego modelu z prostszym rozwiązaniem (np. wyszukiwaniem w bazie wiedzy, tzw. RAG) na odrębnym zestawie testowym oraz uzgodnić z dostawcą zasady usuwania danych treningowych i wersji modelu.

REKOMENDACJA NR 11A: IDENTYFIKACJA I OKREŚLENIE SPOSOBU REALIZACJI OBOWIĄZKÓW WYNIKAJĄCYCH Z AKTU O AI

Dlaczego: Jak opisano w rozdziale I, pkt 1.4, nie każde narzędzie predykcyjne lub „inteligentne" jest „systemem AI" w rozumieniu Aktu o AI. Tylko „systemy AI" i „modele AI ogólnego przeznaczenia" będą podlegały obowiązkom wynikającym z Aktu o AI. Tym samym, aby prawidłowo zidentyfikować obowiązki prawne podmiotu stosującego narzędzie oparte na AI, należy przeanalizować, czy narzędzie to w ogóle jest systemem AI lub modelem AI ogólnego przeznaczenia.

Radca prawny korzystający z systemu AI będzie najczęściej odgrywać rolę podmiotu stosującego. Na bazie planowanego sposobu wykorzystania (zob. rekomendacja nr 1) radca prawny powinien ustalić, jaki jest poziom ryzyka i czy używanie planowanego rozwiązania nie będzie zakazaną praktyką. Większość systemów AI używanych przez prawników nie jest systemami wysokiego ryzyka i w związku z tym obowiązki radców prawnych stosujących takie narzędzia są ograniczone (zob. rozdz. II.2). Najistotniejsze będzie zapewnienie kompetencji w zakresie AI (zob. rekomendacja nr 17), wykonywanie obowiązków informacyjnych oraz w zakresie oznaczania treści w przypadkach wskazanych w Akcie o AI (zob. rekomendacja nr 13).

Jednak w przypadku systemów wysokiego ryzyka na radcy prawnym, jako podmiocie stosującym, będą spoczywały dodatkowe obowiązki, w tym do zapewnienia nadzoru człowieka o odpowiednich kwalifikacjach. Zasady realizacji takiego nadzoru powinny być szczególnie przemyślane w przypadku agentów.

Radca prawny powinien też ustalić, w jakiej roli występuje podmiot oferujący mu narzędzie AI, tj. czy jest dostawcą, dystrybutorem czy importerem, oraz gdzie znajdują się informacje wymagane od takich podmiotów na gruncie Aktu o AI.

Odrębnie radca prawny (kancelaria) powinien ustalić, czy w związku ze sposobem wykorzystania narzędzia AI sam nie staje się dostawcą w rozumieniu art. 3 pkt 3 Aktu o AI, a więc podmiotem, który rozwija system AI lub zleca jego

rozwój pod własną nazwą lub znakiem towarowym, wprowadza go do obrotu lub oddaje do użytku. Dotyczy to np. sytuacji, w których kancelaria: (i) udostępnia klientom rozwiązanie oparte na cudzym modelu AI pod własną marką (np. przez API), (ii) we wprowadzonym już do obrotu lub oddanym do użytku systemie AI wysokiego ryzyka dokonuje ona istotnej zmiany w taki sposób, że pozostaje on systemem AI wysokiego ryzyka. Rola dostawcy powoduje podleganie obowiązkom wynikającym z Aktu o AI, w tym obowiązkom przejrzystości z art. 50 Aktu o AI. Kancelaria powinna zatem każdorazowo weryfikować, czy planowany sposób udostępnienia narzędzia AI klientom lub osobom trzecim nie prowadzi do przekształcenia jej z podmiotu stosującego w dostawcę.

Radca prawny powinien też monitorować sposób wykorzystania narzędzi AI na etapie ich stosowania, w szczególności w zakresie zmian w sposobie ich użycia. Zmieniony lub rozszerzony sposób wykorzystania może bowiem prowadzić do odmiennej kwalifikacji systemu na gruncie Aktu o AI, w tym do uznania go za system wysokiego ryzyka. W praktyce oznacza to konieczność okresowej weryfikacji, czy system jest wykorzystywany zgodnie z pierwotnie przyjętymi założeniami oraz czy nowe przypadki użycia (np. wykorzystanie do podejmowania decyzji wobec osób fizycznych) nie powodują powstania dodatkowych obowiązków regulacyjnych (jeżeli system AI wysokiego ryzyka jest wykorzystywany do podejmowania decyzji dotyczących danej osoby lub do wspierania takich decyzji, osoba ta powinna zostać poinformowana o jego użyciu – art. 26 ust. 11 Aktu o AI).

Jak: Radca prawny powinien opracować „listę sprawdzającą" dla Aktu o AI obejmującą:

- kwalifikację narzędzia jako „systemu AI",
- ustalenie swojej roli (np. dostawca, podmiot stosujący),
- ustalenie kategorii systemu AI (zakazany / wysokiego ryzyka / ograniczonego ryzyka/ ogólnego przeznaczenia / inne),
- listę obowiązków dla danej roli i ryzyka wraz ze sposobem ich realizacji.

REKOMENDACJA: Radca prawny powinien wdrożyć zasady kwalifikowania narzędzi korzystających z AI i roli radcy prawnego w świetle Aktu o AI. Zasady te powinny wskazywać m.in. osobę odpowiedzialną, moment przeprowadzenia kwalifikacji oraz obowiązek udokumentowania przeprowadzonej analizy. Radca prawny powinien także monitorować sposób wykorzystania narzędzia AI na etapie stosowania, aby uniknąć przypadkowej reklasyfikacji w świetle Aktu o AI (np. zmiany na „system AI wysokiego ryzyka" w związku z rozpoczęciem korzystania z narzędzia w nowy sposób).

B. Rekomendacje dotyczące wdrażania narzędzi AI

REKOMENDACJA NR 12: WERYFIKACJA UMÓW Z KLIENTAMI POD KĄTEM OGRANICZEŃ LUB ZASAD KORZYSTANIA Z NARZĘDZI AI

Dlaczego: Radca prawny, świadcząc usługi na rzecz klientów, powinien kierować się należytą starannością oraz ochroną interesu klienta i powierzonych mu przez klienta informacji (tajemnica zawodowa).

Jak: Radca prawny powinien zweryfikować umowy z klientami, czy nie zawierają postanowień dotyczących korzystania z narzędzi AI, w szczególności czy umowa zawiera:

- zakaz wykorzystywania narzędzi AI do świadczenia usług;
- ograniczenia dotyczące wykorzystywania określonych narzędzi (np. agentów) do świadczenia usług prawnych;
- jeśli umowa nie zawiera zakazu wykorzystania narzędzi AI do świadczenia usług, to czy nie zawiera pewnych ograniczeń/obszarów, w których takie wykorzystanie jest zakazane, lub obowiązku informowania klientów o korzystaniu z takich rozwiązań;
- jeśli umowa zawiera ograniczenia w zakresie wykorzystania narzędzi AI, to należy ustalić, czy narzędzie AI i sposób jego wykorzystania są zgodne z tymi ograniczeniami oraz ewentualnie jakie działania dostosowawcze są konieczne;
- zasady odpowiedzialności w przypadku błędnych wyników wygenerowanych przez AI.

REKOMENDACJA: **Przed rozpoczęciem korzystania z narzędzia AI w pracy dla danego klienta należy zweryfikować, czy umowa z klientem nie zawiera postanowień ograniczających korzystanie z narzędzia AI lub zakazujących jego stosowania. W przypadku ograniczeń konieczne jest ustalenie, czy i jakie działania dostosowawcze należy podjąć, aby nie naruszyć umowy.**

REKOMENDACJA NR 13: USTALENIE, W JAKICH PRZYPADKACH NALEŻY INFORMOWAĆ KLIENTA O KORZYSTANIU Z NARZĘDZIA AI

Dlaczego: Na podmiocie stosującym narzędzia AI mogą spoczywać ograniczone obowiązki informacyjne wobec osób trzecich, określone w art. 50 Aktu o AI, w tym obowiązek informowania o generowaniu lub modyfikowaniu z pomocą AI tekstu publikowanego w celu informowania społeczeństwa o sprawach leżących

w interesie publicznym (art. 50 ust. 4 Aktu o AI) lub o interakcjach z AI, np. w przypadku udostępniania czatbota bazującego na AI klientom w celu uzyskiwania informacji o prowadzonych sprawach (art. 50 ust. 1 Aktu o AI). W przypadku wyżej wymienionego obowiązku dotyczącego spraw leżących w interesie publicznym obowiązek ten nie ma zastosowania, gdy treści wygenerowane przez AI zostały poddane weryfikacji przez człowieka lub kontroli redakcyjnej i gdy za publikację treści odpowiedzialność redakcyjną ponosi osoba fizyczna lub prawna (art. 50 ust. 4 akapit drugi Aktu o AI).

Co do zasady radca prawny nie ma obowiązku informowania klienta o korzystaniu z narzędzi AI w codziennej pracy zawodowej, o ile umowa z klientem lub wytyczne klienta nie stanowią wyraźnie inaczej (zob. rekomendacja nr 12), zwłaszcza jeśli są to rozwiązania powszechnie dostępne na rynku i oferowane przez renomowanych dostawców, analogicznie jak nie informuje o korzystaniu z innych standardowych narzędzi informatycznych (systemów zarządzania dokumentami, baz danych prawnych itp.). Wykorzystanie AI do wsparcia w przygotowywaniu projektów, analiz, tłumaczeń czy porządkowania informacji to element normalnego procesu świadczenia usług prawnych, a odpowiedzialność za końcowy produkt pracy pozostaje po stronie radcy prawnego, który odpowiada za weryfikację i zatwierdzenie wyników. Istnieją odmienne podejścia do zaprezentowanego powyżej modelu, przyjęte w niektórych jurysdykcjach europejskich (np. ustawowy obowiązek informacyjny we Włoszech[67], rekomendacja uzyskania zgody *ex ante* w Niderlandach[68] czy też konkretne zasady samorządowe w Słowacji[69]). Przyjęte w niniejszych rekomendacjach podejście opiera się na założeniu, że radca prawny ponosi pełną odpowiedzialność za końcowy produkt swojej pracy niezależnie od wykorzystanych narzędzi.

Niezależnie dostawcy systemów AI będą zobowiązani do oznakowania wyników systemów AI w przypadku m.in. systemów generujących tekst lub obrazy, chyba że AI tylko nieistotnie edytuje treść (np. zwykła korekta), albo w określonych celach związanych z egzekwowaniem prawa (art. 50 ust. 2 Aktu o AI). Kodeks postępowania w sprawie przejrzystości treści generowanych przez AI wymaga,

[67] *Professionisti e AI, scattato l'obbligo informativo. I modelli per l'avvocato*, Mister Lex, 16 października 2025 r., https://www.misterlex.it/doc/professionisti-ai-obbligo-informativo/ [dostęp: 21.10.2026 r.].

[68] Nederlandse orde van advocaten, *Aanbevelingen AI in de advocatuur*, https://www.advocatenorde.nl/voor-advocaten/digitalisering-ai/aanbevelingen-ai-de-advocatuur [dostęp: 21.10.2026 r.].

[69] Slovenská Advokátska Komora, *Uznesenie Predsedníctva Slovenskej advokátskej komory*, https://www.sak.sk/wp-content/uploads/2026/06/Uznesenie_12-4-2025_plne-znenie-k-25-11-2025-ff2a4b92.pdf [dostęp: 21.10.2026 r.].

by dostawcy wprowadzili w regulaminach i dokumentacji systemów AI zakaz celowego usuwania lub modyfikowania oznaczeń (np. metadanych) przez podmioty stosujące i osoby trzecie (choć wspomniano też, że pełna kontrola nad przestrzeganiem tego obowiązku na dalszych etapach wykorzystania systemu nie jest możliwa). Zakaz usuwania oznakowania nie obejmuje jednak sytuacji, w których ingerencja w oznaczenia jest uzasadniona i konieczna dla prawidłowego, zgodnego z prawem przetwarzania (np. dla celów bezpieczeństwa lub badań).

W rezultacie część treści przygotowywanych z wykorzystaniem systemów AI może zawierać oznaczenia techniczne dodawane przez dostawcę systemu AI zgodnie z przyjętymi rozwiązaniami technologicznymi i obowiązującymi wymogami regulacyjnymi. Należy jednak uwzględnić, że w przypadku treści tekstowych techniki oznaczania treści generowanych przez AI nadal znajdują się w fazie rozwoju.

Radca prawny powinien określić zasady postępowania z oznaczeniami treści wygenerowanych przez AI (np. przy znaczącym zmodyfikowaniu materiału wygenerowanego przez AI lub po jego weryfikacji i zatwierdzeniu przez radcę prawnego), przy czym ich usuwanie lub modyfikowanie powinno uwzględniać regulaminy korzystania z danego systemu AI.

Należy również podkreślić, że obowiązek ujawniania korzystania z AI lub odpowiedniego oznaczania dokumentów może wynikać z umów z klientami, a także z regulaminów lub praktyki niektórych sądów, przy czym tego typu wymogi pojawiały się na razie głównie w sądach w Stanach Zjednoczonych.

Obowiązek poinformowania klienta może jednak zachodzić w sytuacji, gdy:

- klient wyraźnie zleca wykonanie pracy przy pomocy narzędzia AI, ale bez jej weryfikacji przez radcę prawnego – w takim przypadku radca prawny powinien poinformować klienta, że zlecenie zostało wykonane za pomocą narzędzia AI, zgodnie ze zleceniem klienta, bez weryfikacji merytorycznej przez radcę prawnego, i że w konsekwencji odpowiedzialność radcy prawnego za treści wygenerowane przez system AI ulega odpowiedniemu ograniczeniu w granicach dopuszczalnych prawem i zasadami etyki;
- klient wyraźnie zastrzegł w umowie obowiązek informowania o korzystaniu z AI;
- narzędzie AI jest używane w sposób, który wchodzi w zakres obowiązków informacyjnych z art. 50 ust. 1 lub ust. 4 Aktu o AI (interakcja z AI, publikowanie treści generowanych przez AI w interesie publicznym).

Jak: Radca prawny powinien określić zasady, kiedy oznaczenia treści generowanych przez AI mogą być usuwane przez radców prawnych (np. istotna

modyfikacja, weryfikacja poprawności). W przypadku gdy klient zleca wykonanie pracy z wykorzystaniem AI bez weryfikacji, radca prawny powinien: potwierdzić pisemnie (np. e-mailem) zakres zlecenia i warunek braku weryfikacji; dostarczając wynik pracy, wyraźnie oznaczyć, że materiał został wygenerowany przez system AI zgodnie ze zleceniem klienta, bez weryfikacji merytorycznej, jak również wskazać, że odpowiedzialność za treści wygenerowane przez AI w takim trybie nie jest objęta standardowym zakresem odpowiedzialności radcy prawnego za świadczone usługi prawne.

REKOMENDACJA: **Co do zasady korzystanie z narzędzi AI w ramach standardowej pracy radcy prawnego nie wymaga informowania klienta, o ile radca prawny weryfikuje wyniki wygenerowane przez AI i ponosi za nie odpowiedzialność na zasadach ogólnych. Obowiązek poinformowania klienta powstaje w szczególności wówczas, gdy klient zleca wykonanie pracy za pomocą AI bez weryfikacji – wówczas radca prawny powinien poinformować klienta, że zlecenie wykonane zostało za pomocą AI, zgodnie ze zleceniem klienta, bez weryfikacji merytorycznej, i że w związku z tym radca prawny nie ponosi odpowiedzialności za wygenerowane treści. W przypadku gdy powiadomienie ma zastosowanie, radca prawny powinien ocenić, czy powinno mieć charakter formalny (np. w formie zapisu w umowie) czy też może być dokonywane *ad hoc*, w zależności od konkretnej sprawy. Radca prawny powinien analizować regulaminy i dokumentację wykorzystywanych narzędzi AI w celu ustalenia, czy oraz w jakim zakresie jest zobowiązany do zachowania automatycznych oznaczeń treści generowanych przez AI, wynikających z obowiązków dostawców na gruncie Aktu o AI. Radca prawny powinien określić zasady, kiedy takie oznaczenia mogą być usuwane.**

REKOMENDACJA NR 14: USTALENIE, W JAKICH PRZYPADKACH POTRZEBNA JEST ZGODA KLIENTA NA KORZYSTANIE Z NARZĘDZIA AI

Dlaczego: AI stała się już codziennością w pracy prawników oraz ich klientów. Wielu klientów oczekuje wręcz od prawników stosowania tej technologii. Jest to jednocześnie technologia, która rozwija się bardzo szybko.

Generalnie zgoda klienta na korzystanie z AI nie jest wymagana, jednak radca prawny powinien ocenić w określonych sytuacjach, czy zalecane jest pozyskanie

zgody klienta na korzystanie z narzędzia AI z uwagi na specyficzny charakter sprawy lub potencjalne konsekwencje dla klienta.

Jak: W celu ustalenia, czy powinna być pozyskana zgoda klienta na wykorzystanie narzędzia AI, pomocne może okazać się udzielenie odpowiedzi na poniższe pytania:

- czy dane klienta mogą być wykorzystywane do trenowania narzędzia AI ➜ w takim przypadku zgoda klienta powinna być uzyskana, przy czym radca prawny powinien rozważyć, czy możliwa jest anonimizacja danych treningowych;
- czy narzędzie AI jest używane do przewidywania wyników spraw sądowych czy administracyjnych ➜ klienci często proszą o ocenę procentową określonego rozstrzygnięcia, którą prawnicy ustalają, opierając się na ich doświadczeniu i analizie podobnych spraw; jeśli ocena miałaby być dokonywana wyłącznie przez narzędzie AI, powinna być pozyskana zgoda klienta;
- jeśli narzędzie opracowane przez konkurenta klienta lub podmiot, z którym klient jest w istotnym sporze, ma być wykorzystywane w pracy dla klienta ➜ co najmniej ze względu na ryzyka reputacyjne dla klienta zgoda klienta powinna być wówczas pozyskana.

REKOMENDACJA: **Zgoda klienta na wykorzystanie narzędzia AI może być wymagana, gdy dane klienta mają być wykorzystane do trenowania modelu AI czy gdy narzędzie AI ma być wykorzystane do przewidywania wyników postępowań bez weryfikacji przez człowieka. Radca prawny powinien ocenić indywidualnie konieczność pozyskania takiej zgody.**

REKOMENDACJA NR 15: USTALENIE, W JAKICH PRZYPADKACH KORZYSTANIE Z NARZĘDZIA AI MOŻE WPŁYWAĆ NA WYNAGRODZENIE RADCY PRAWNEGO

Dlaczego: Wpływ AI na rozliczenia z klientami jest przedmiotem dyskusji w środowisku prawniczym i w tej chwili brak jednego, powszechnego stanowiska. Jeśli korzystanie z narzędzia AI przyspiesza (automatyzuje) pewne procesy, klient może oczekiwać obniżenia kosztów, jeśli rozlicza się z radcą prawnym na podstawie ryczałtu (np. ryczałt za każdą sprawę). W przypadku rozliczeń na

podstawie stawek godzinowych korzystanie z narzędzi AI będzie w interesie klienta, gdyż będzie on obciążany mniejszą liczbą godzin. Z drugiej strony, korzystanie z narzędzia AI wymaga zwykle dodatkowych zasobów lub licencji, które zwłaszcza w przypadku specjalistycznych programów mogą być drogie. Rozliczenie oparte tylko na stawce godzinowej uwzględniającej efektywne wykorzystanie AI może nie rekompensować w pełni kosztów takich narzędzi i może uzasadniać wprowadzenie dodatkowych opłat od klienta (podobnych do opłat za korzystanie z określonych baz danych czy infrastruktury technicznej), zwłaszcza jeśli klient nie chce ponosić sam ciężarów, w tym kosztów takiego wdrożenia, i chce przenieść ten strumień własnej pracy do radcy prawnego. Pobieranie opłat w takich przypadkach za korzystanie z narzędzia AI w pracy dla klienta (podobnie np. jak za udostępnianie VDR) może być wówczas dodatkowo uzasadnione. W rozliczeniu godzinowym radca prawny powinien wykazywać rzeczywisty czas pracy, w tym czas przygotowania danych i weryfikacji wyników, a nie czas, jaki zadanie zajęłoby bez użycia AI. Przy ryczałcie strony mogą uzgodnić cenę niezależną od liczby godzin pracy. Dodatkowe opłaty za narzędzie AI wymagają uprzedniego uzgodnienia z klientem lub powinny być uwzględnione w wysokości stawki godzinowej jako uprzednie inwestycje w technologię i koszty prowadzenia działalności.

Jak: Przy ocenie, czy korzystanie z narzędzia AI może wpływać na wynagrodzenie radcy prawnego i w jaki sposób, pomocne może okazać się udzielenie odpowiedzi na poniższe pytania:

- na jakich zasadach są dokonywane rozliczenia z klientem (stawka godzinowa, ryczałt);
- jak istotne jest wykorzystanie narzędzia AI w danym przypadku (np. czy narzędzie AI przejmie znaczącą część pracy prawnika);
- czy klient chce korzystać z narzędzia, którym dysponuje radca prawny, zamiast wdrażać je u siebie, np. do przygotowywania tłumaczeń czy standardowych odpowiedzi dla jego kontrahentów z użyciem narzędzia (workflow czy agenta) opracowanego i wdrożonego u radcy prawnego;
- czy korzystanie z narzędzi AI wiąże się z dodatkowymi kosztami, w tym kosztami licencyjnymi czy wdrożenia;
- czy stosowane są narzędzia AI usprawniające pracę i przeznaczone do powszechnego zastosowania, czy narzędzia specjalistyczne (np. do analizy wyroków arbitrażowych) ➜ zwłaszcza w przypadku narzędzi specjalistycznych uzasadnione może być rekompensowanie ich kosztów przez klientów.

REKOMENDACJA: W przypadku rozliczeń godzinowych lub oferowania klientom określonych rozwiązań AI przeznaczonych dla danego klienta może być uzasadnione wprowadzenie opłaty pokrywającej koszty zastosowania narzędzia AI. Stosowanie narzędzi do powszechnego zastosowania w różnych sprawach może nie uzasadniać dodatkowych opłat (analogicznie do standardowego oprogramowania biurowego). Kwestia wpływu stosowanych przez radcę prawnego narzędzi AI powinna być rozważona przez radcę prawnego i omówiona z klientem. Radca prawny powinien monitorować aktualne tendencje rynkowe w tym zakresie.

REKOMENDACJA NR 16: OPRACOWANIE WEWNĘTRZNYCH REKOMENDACJI/ZALECEŃ/INSTRUKCJI DOTYCZĄCYCH KORZYSTANIA Z NARZĘDZI AI

Dlaczego: Opracowanie wewnętrznych rekomendacji/zaleceń/instrukcji dotyczących korzystania z narzędzi AI jest istotne z kilku powodów:

- pozwala zapewnić zgodność z obowiązującymi przepisami prawnymi i ograniczyć ryzyko ewentualnych sankcji (np. Aktem o AI, RODO);
- pozwala zwiększyć bezpieczeństwo danych i ich poufność (w tym tajemnicę zawodową), między innymi ograniczyć ryzyko tzw. shadow AI, czyli niekontrolowanego korzystania przez pracowników z niezatwierdzonych narzędzi AI bez wiedzy organizacji;
- pozwala na standaryzację sposobu korzystania z narzędzi AI w całej organizacji.

Jak: Radca prawny powinien opracować wewnętrzne rekomendacje/zalecenia/instrukcje dotyczące korzystania z narzędzi AI. W zależności od wielkości i struktury danej organizacji powinny one w szczególności zawierać:

- tzw. białą listę narzędzi AI zatwierdzonych do użytku służbowego, wraz z zakazem korzystania z prywatnych kont, publicznych wersji tych narzędzi oraz niezatwierdzonych aplikacji;
- jasne określenie, do jakich zadań narzędzie AI może być wykorzystywane oraz jakie zastosowania są niedozwolone;
- określenie kategorii informacji i danych, które mogą być przekazywane do narzędzia AI;
- zasady dotyczące tworzenia zapytań (inputu), w tym techniki precyzyjnego formułowania zapytań do narzędzia AI (*prompt engineering*) – w celu

uzyskania jak najbardziej trafnych wyników oraz uniknięcia ryzyka roszczeń;
- zasady weryfikacji i kontroli danych przekazywanych do narzędzia AI (zawartości wejściowej);
- zasady weryfikacji i walidacji wyników generowanych przez narzędzie AI (zawartości wyjściowej);
- w większych organizacjach warto rozważyć powołanie konkretnej osoby lub zespołu odpowiedzialnych za wdrożenie i monitorowanie wykorzystania AI (np. AI Champion lub komitet ds. AI z udziałem przedstawicieli działów prawnego, IT i compliance);
- procedurę zgłaszania i obsługi incydentów związanych z AI oraz kolejnych działań;
- zasady szkolenia personelu i podnoszenia kompetencji w zakresie korzystania z narzędzi AI, w tym zapewnienie dostępności materiałów szkoleniowych, budowanie bazy wiedzy oraz biblioteki promptów;
- zasady monitorowania korzystania z narzędzia AI (np. pod kątem nadmiernego uzależnienia od stosowania tych rozwiązań, ich poprawności, efektywności, ryzyka, jakie generują itp.).

Takie materiały powinny być przekazane personelowi i udostępnione wewnętrznie, tak aby użytkownicy mogli łatwo się z nimi zapoznać. Materiały powinny być aktualizowane w miarę potrzeby. Należy wskazać osoby odpowiedzialne za ich bieżącą aktualizację i udzielanie odpowiedzi na pytania użytkowników. W kancelarii jednoosobowej instrukcja może mieć zwięzłą formę (np. jednej strony) i obejmować: listę dopuszczonych narzędzi, rodzaje danych i zadań, które wolno w nich przetwarzać, zastosowania zakazane, sposób weryfikacji wyników, postępowanie w razie incydentu oraz sposób wykonania pracy bez narzędzia. Warto zapisać datę przyjęcia instrukcji i przeglądać ją co najmniej raz w roku oraz przy każdej zmianie narzędzia lub warunków umowy z dostawcą.



REKOMENDACJA: **Przed rozpoczęciem korzystania z narzędzia AI należy opracować wewnętrzne rekomendacje, zalecenia lub instrukcje dotyczące korzystania z narzędzi AI, w tym określające, w jaki sposób można korzystać z takich narzędzi. Należy aktualizować takie materiały w miarę potrzeb. Zaleca się wskazanie osoby odpowiedzialnej za aktualizację tych materiałów oraz za udzielanie odpowiedzi na pytania użytkowników.**

REKOMENDACJA NR 17: PRZEPROWADZENIE WEWNĘTRZNEGO SZKOLENIA DOTYCZĄCEGO KORZYSTANIA Z NARZĘDZIA AI

Dlaczego: Zgodnie z art. 4 Aktu o AI podmiot stosujący zobowiązany jest do podejmowania środków wspierających rozwój kompetencji wśród osób korzystających z narzędzi AI (dotyczy to zarówno personelu, jak i innych osób zajmujących się działaniem i wykorzystaniem systemów AI w jego imieniu, z uwzględnieniem ich wiedzy technicznej, doświadczenia, wykształcenia i wyszkolenia oraz kontekstu, w którym systemy AI mają być używane). Obowiązek ten nie powinien być rozumiany jako wymagający zagwarantowania jakiegokolwiek konkretnego poziomu AI kompetencji danej osoby. Komisja Europejska i państwa członkowskie mają wspierać realizację tego obowiązku przez oferowanie szkoleń, zasobów informacyjnych i wymianę dobrych praktyk. W interesie radców prawnych jest odpowiednie szkolenie, zarówno własne, jak i swoich zespołów, w rozwoju tej technologii, niezależnie od ewentualnego wsparcia innych podmiotów.

Jak: Radca prawny powinien wykonać następujące kroki:

- ustalić, kto będzie korzystał z narzędzia AI (własny personel/usługodawcy);
- dokonać analizy potrzeb szkoleniowych osób, które mają korzystać z narzędzia AI (ustalenie poziomu wiedzy technicznej, doświadczenia, wykształcenia, wyszkolenia itp.);
- przygotować stosowne instrukcje/materiały szkoleniowe;
- przeprowadzić szkolenie – przed rozpoczęciem korzystania z narzędzia AI.

Radca prawny może powierzyć realizację szkoleń podmiotom zewnętrznym lub innym radcom prawnym, którzy mają odpowiednie kompetencje.

REKOMENDACJA: Przed rozpoczęciem korzystania z narzędzia AI należy przeprowadzić szkolenia dotyczące korzystania z narzędzia AI dla użytkowników.

C. Rekomendacje dotyczące stosowania narzędzi AI

REKOMENDACJA NR 18: DOKONYWANIE REGULARNEJ OCENY STOSOWANYCH NARZĘDZI IT I AI, W TYM MODELI DOSTOSOWANYCH (*FINE-TUNED MODELS*), A TAKŻE OFERTY RYNKOWEJ W ZAKRESIE NARZĘDZI AI PRZEZNACZONYCH DLA PRAWNIKÓW

Dlaczego: Regularna ocena stosowanych narzędzi AI pozwala na weryfikację, czy stosowane narzędzie AI odpowiada aktualnym potrzebom organizacji,

jak również identyfikację zagrożeń (ryzyk) oraz nowych wyzwań, które pojawiły się w związku z korzystaniem z danego narzędzia AI. Rozwiązania AI pojawiają się też w znanych od lat rozwiązaniach IT (np. w systemach do badania prawnego czy systemach do zarządzania dokumentami). Coraz częściej prawnicy też opracowują własne narzędzia AI oraz agentów AI na bazie dostępnych modeli AI. W związku z tym należy też weryfikować, czy narzędzia, z których korzystają radcowie, nie zostały zaktualizowane o funkcjonalności AI i jeśli tak – ocenić ewentualne ryzyka i podjąć działania zaradcze zgodnie z niniejszymi rekomendacjami. Śledzenie oferty rynkowej w zakresie narzędzi AI przeznaczonych dla prawników oraz funkcjonalności AI dostępnych w narzędziach znanych już prawnikom pozwala na bieżąco monitorować najnowsze technologie AI oraz najlepsze praktyki w związku z korzystaniem z narzędzi AI, co może zapewnić radcy prawnemu przewagę konkurencyjną na rynku usług prawnych.

Jak: Radca prawny powinien wdrożyć w organizacji proces regularnej oceny stosowanych narzędzi AI i funkcjonalności AI w istniejących narzędziach, w tym modeli dedykowanych (*fine-tuned models*), oraz oferty rynkowej w zakresie narzędzi AI przeznaczonych dla prawników, w szczególności:

- zapewnić regularny monitoring, utrzymanie i aktualizację wykorzystywanego narzędzia/funkcjonalności AI, w szczególności w kontekście zmian wprowadzanych przez dostawcę narzędzia AI, w tym weryfikację zmian dokumentacji udostępnianej przez dostawcę narzędzia AI (regulaminów czy cenników), ze szczególnym uwzględnieniem ewentualnych zmian stosowanych modeli AI (np. czy zapewniany jest dostęp do najnowszych modeli) oraz modelu rozliczeniowego (np. z modelu opartego na liczbie użytkowników (*seat-based*) na model oparty na faktycznym wykorzystaniu (*usage-based*)), co może prowadzić do znacznego wzrostu kosztów, i odpowiednio aktualizować oceny i dokumentację wewnętrzną dotyczącą korzystania z danego narzędzia AI (zob. również rekomendację nr 19);
- uzyskiwać regularnie informacje zwrotne dotyczące korzystania z narzędzia/funkcjonalności AI przez użytkowników i ich uwagi;
- dokonywać regularnej analizy, czy narzędzie/funkcjonalność AI spełnia aktualne potrzeby organizacji; monitorować oferty rynkowe oraz możliwości wewnętrzne w zakresie narzędzi/funkcjonalności AI przeznaczonych dla prawników;
- w większych organizacjach należy wyznaczyć osobę lub osoby odpowiedzialne za realizację tych zadań w organizacji, przy czym powinni być w ten

proces włączeni zarówno radcowie prawni, jak i osoby dysponujące wiedzą techniczną.

Wytyczne i zasady dotyczące tego procesu mogą być częścią ogólnej polityki korzystania z narzędzi/funkcjonalności AI w organizacji.



REKOMENDACJA: Należy regularnie dokonywać oceny stosowanych narzędzi AI, w tym modeli dedykowanych (*fine-tuned models*), a także oferty rynkowej w zakresie narzędzi AI przeznaczonych dla prawników, jak również funkcjonalności AI w używanych narzędziach AI. W większych organizacjach należy wyznaczyć osoby odpowiedzialne po stronie radcy prawnego za to zadanie, w tym za zbieranie informacji zwrotnych.

REKOMENDACJA NR 19: DOKONYWANIE REGULARNEGO PRZEGLĄDU WEWNĘTRZNYCH ZALECEŃ/WYTYCZNYCH DOTYCZĄCYCH KORZYSTANIA Z AI ORAZ ICH AKTUALIZACJA W MIARĘ ROZWOJU TECHNOLOGII AI (*AI COMPLIANCE*)

Dlaczego: Zarówno regulacje prawne dotyczące korzystania z AI, wytyczne organów w tym zakresie, jak i funkcjonalności czy zasady korzystania z danego narzędzia AI mogą ulegać zmianie, dlatego regularne przeglądy i aktualizacje wewnętrznych wytycznych/zaleceń dotyczących korzystania z narzędzi AI ułatwią zapewnienie zgodności z obowiązującymi przepisami prawa i praktyką rynkową. Technologia AI szybko się rozwija, co powoduje pojawianie się nowych wyzwań i opcji. Aktualizowanie wytycznych/zaleceń pozwala na optymalne i bezpieczne korzystanie z narzędzia AI.

Jak: Radca prawny powinien wdrożyć w organizacji proces regularnego przeglądu wewnętrznych zaleceń/wytycznych dotyczących korzystania z narzędzia AI oraz ich aktualizacji, w szczególności określając:

- częstotliwość takich przeglądów;
- zasady i warunki ich prowadzenia;
- osobę lub osoby odpowiedzialne w organizacji za ten proces.

Wytyczne i zasady dotyczące tego procesu mogą być częścią ogólnej polityki korzystania z narzędzi AI w organizacji.

REKOMENDACJA: Należy regularnie weryfikować wewnętrzne zalecenia/wytyczne dotyczące korzystania z AI oraz je dostosowywać (*AI compliance*). W większych organizacjach należy wyznaczyć osoby odpowiedzialne po stronie radcy prawnego za to zadanie. Przegląd powinien następować także po istotnej zmianie narzędzia (modelu, planu, umowy, konfiguracji, dostępu do danych) oraz po istotnym błędzie lub incydencie, a jego wynik i decyzję o dalszym korzystaniu z narzędzia warto udokumentować.

REKOMENDACJA NR 20: ORGANIZOWANIE REGULARNYCH WEWNĘTRZNYCH SZKOLEŃ DOTYCZĄCYCH KORZYSTANIA Z AI

Dlaczego: Niezależnie od obowiązków wynikających z regulacji prawnych (zob. szerzej: rekomendacja nr 17) organizowanie regularnych wewnętrznych szkoleń dotyczących korzystania z AI jest istotne również z następujących powodów:

- pozwala na utrwalanie dobrych praktyk oraz dzielenie się doświadczeniami w zakresie korzystania z AI;
- pozwala na prezentację nowych funkcjonalności i ewentualnych zmian w modelach AI (np. z uwagi na aktualizacje dostawcy);
- umożliwia edukację oraz rozwój kompetencji wśród młodszych kolegów czy aplikantów radcowskich.

W przypadku aplikantów radcowskich i młodych prawników szkolenia powinny obejmować również:

- naukę krytycznej oceny wyników generowanych przez AI. Aplikanci powinni być szkoleni w zakresie weryfikacji poprawności, aktualności i adekwatności materiałów wygenerowanych przez AI, w tym rozpoznawania halucynacji i błędów;
- rozwijanie tradycyjnych umiejętności prawniczych równolegle z kompetencjami cyfrowymi. Szkolenia powinny zapewniać możliwość ćwiczenia samodzielnej analizy prawnej, analizy orzecznictwa i konstruowania argumentacji prawnej bez wsparcia AI, aby aplikanci zbudowali solidne fundamenty warsztatu prawniczego;
- praktyczne warsztaty z efektywnego promptowania dostosowane do specyfiki pracy prawniczej;
- sprawdzenie nabytych umiejętności na praktycznym zadaniu (np. wskazanie i poprawienie błędów w wyniku wygenerowanym przez AI, w tym

nieistniejących orzeczeń i błędnie przytoczonych przepisów), z informacją zwrotną od prowadzącego;
- omówienie zasad etycznych i regulacyjnych, w tym zagadnień związanych z tajemnicą zawodową, ochroną danych osobowych oraz odpowiedzialnością za wyniki pracy z wykorzystaniem AI;
- mentoring i nadzór doświadczonych prawników. Aplikanci powinni pracować pod kierunkiem doświadczonych radców prawnych, którzy mogą ocenić jakość ich pracy i wskazać błędy wynikające z nadmiernego polegania na AI.

Jak: Radca prawny powinien wdrożyć w organizacji proces regularnych szkoleń w zakresie korzystania z narzędzi AI, określając w szczególności:
- częstotliwość takich szkoleń;
- osobę lub osoby odpowiedzialne za ten proces w organizacji;
- adresatów takich szkoleń.

Zasady i warunki prowadzenia regularnych szkoleń wewnętrznych mogą być częścią ogólnej polityki korzystania z narzędzi AI w organizacji.

REKOMENDACJA: Użytkownicy AI powinni uczestniczyć w regularnych szkoleniach w zakresie korzystania ze stosowanych narzędzi AI.

REKOMENDACJA NR 21: TWORZENIE I ZARZĄDZANIE WEWNĘTRZNĄ BAZĄ WIEDZY (*KNOWLEDGE MANAGEMENT*)

Dlaczego: Tworzenie i zarządzanie wewnętrzną bazą wiedzy dotyczącą AI, obejmującą dokumentację umowną i techniczną, analizy czy doświadczenia ze stosowania narzędzia i funkcjonalności AI, w tym bibliotekę sprawdzonych promptów czy agentów AI, jest istotne z kilku powodów:
- przyspiesza procesy decyzyjne i operacyjne;
- pomaga w zachowaniu wiedzy, która może być utracona w wyniku rotacji pracowników;
- ułatwia współpracę oraz wewnętrzną komunikację w organizacji;
- przyspiesza proces onboardingu i skraca czas potrzebny na wdrożenie nowych pracowników;
- regularne aktualizowanie bazy wiedzy pomaga w zapewnieniu zgodności z obowiązującymi przepisami prawnymi;

- pozwala wykorzystać zebrane doświadczenia w relacjach z klientami, w tym wspierać klientów w ich wdrożeniach AI.

Jak: Radca prawny powinien wdrożyć w organizacji procedury/polityki określające zasady tworzenia, zarządzania oraz aktualizowania bazy wiedzy, które w szczególności będą określać:

- jakiego rodzaju dokumenty (wzory umów, opinii itp.) należy gromadzić w wewnętrznej bazie wiedzy oraz osoby odpowiedzialne za ten proces; należy też określić zasady anonimizacji dokumentów pochodzących ze spraw klientów, uprawnienia dostępu do bazy (z uwzględnieniem barier informacyjnych między zespołami obsługującymi różnych klientów, jeśli dokumenty nie są zanonimizowane) i jeśli wymagają tego przepisy – okres przechowywania materiałów;
- wskazanie bezpiecznej „lokalizacji" bazy wiedzy w infrastrukturze organizacji;
- strukturę bazy wiedzy lub klucz, według którego należy zapisywać dokumenty;
- zasady aktualizowania zgromadzonych dokumentów oraz osoby odpowiedzialne za ten proces.

Taka baza wiedzy powinna obejmować zarówno narzędzia AI wdrożone do używania, jak też narzędzia oceniane, odnośnie do których ostatecznie podjęto decyzję, aby ich nie wdrażać. W tym przypadku w bazie wiedzy należy zamieścić również informację o przyczynach braku wdrożenia.

REKOMENDACJA: **Zalecane jest wdrożenie w organizacji odpowiednich procedur/polityk określających zasady tworzenia, zarządzania oraz aktualizowania wewnętrznej bazy wiedzy dotyczącej stosowanych narzędzi i funkcjonalności AI oraz narzędzi/funkcjonalności AI, które były przedmiotem oceny, ale nie zostały ostatecznie wdrożone lub uruchomione.**

REKOMENDACJA NR 22: ZARZĄDZANIE INCYDENTAMI ZWIĄZANYMI Z AI ORAZ PODEJMOWANIE DZIAŁAŃ ZAPOBIEGAWCZYCH NA PRZYSZŁOŚĆ

Dlaczego: Regulacje prawne, takie jak Akt o AI, RODO, przepisy krajowe wdrażające dyrektywę NIS 2 czy rozporządzenie DORA (jeśli dotyczy), wymagają od organizacji w określonych przypadkach raportowania incydentów[70] oraz

[70] W przypadku gdy radca prawny (podmiot stosujący) zmieni przeznaczenie „zwykłego" systemu AI w taki sposób, że stanie się on systemem AI wysokiego ryzyka, to stanie się on także

podejmowania działań naprawczych (*corrective actions*[71]) i zapobiegawczych. Incydenty związane z AI mogą prowadzić do naruszeń ochrony danych osobowych, co może wiązać się z koniecznością powiadomienia właściwego organu ochrony danych i osób, których dane dotyczą. Obowiązek powiadomienia klienta może też wynikać z umowy zawartej z klientem.

Skuteczne zarządzanie incydentami pomaga w szybkim wykrywaniu i minimalizowaniu skutków takich naruszeń oraz pomaga w minimalizowaniu ryzyka wystąpienia incydentów w przyszłości. Wdrożenie odpowiednich rozwiązań pozwalających na zidentyfikowanie zagrożeń jest istotne z perspektywy bezpieczeństwa organizacji i jej klientów (zachowania poufności i tajemnicy zawodowej).

Jak: Radca prawny powinien wdrożyć w organizacji proces zarządzania incydentami związanymi z AI oraz podejmowania działań naprawczych i zapobiegawczych, a w szczególności powinien:

- wdrożyć procedurę zarządzania incydentami, która będzie określać m.in.: (i) rodzaje najczęstszych incydentów, które mogą dotyczyć AI; (ii) zasady i warunki raportowania incydentów do władz i klientów oraz ich obsługi; (iii) zasady odpowiedzialności za obszary opisane w procedurze oraz zasady komunikacji wewnętrznej i zewnętrznej; (iv) zasady ewidencjonowania incydentów; (v) mechanizmy dalszego postępowania (działania naprawcze i zapobiegawcze);
- wprowadzić w organizacji proces „ciągłego uczenia się" w zakresie incydentów oraz ryzyk, wyzwań związanych z AI, na które może być narażona organizacja.

Wytyczne i zasady dotyczące tego procesu mogą być częścią ogólnej polityki korzystania z narzędzi AI w organizacji. Procedura powinna wskazywać osobę kontaktową, pierwsze czynności (wstrzymanie procesu lub odebranie dostępu, zabezpieczenie śladów, ustalenie zakresu informacji, których incydent dotyczy) oraz terminy zgłoszeń.

dostawcą tego systemu w rozumieniu Aktu o AI, co powoduje, że stosuje się do niego obowiązki dostawcy systemu AI wysokiego ryzyka, np. obowiązki związane z raportowaniem „poważnych incydentów" (art. 73 Aktu o AI). Na gruncie DORA (mającej znaczenie w kontekście odporności cyfrowej sektora finansowego) istnieje pojęcie incydentu związanego z ICT. Artykuł 9 Aktu o AI nakłada wymóg posiadania systemu zarządzania ryzykiem AI dla systemów wysokiego ryzyka. Artykuł 12 Aktu o AI zobowiązuje do wprowadzenia rozwiązań w zakresie automatycznego zapisywania logów w ciągu całego cyklu życia systemu AI.

[71] Zobacz np. art. 20 Aktu o AI.

REKOMENDACJA: **Należy wdrożyć zasady zarządzania incydentami związanymi z AI, w tym postępowania w przypadku ich wykrycia, zasady raportowania do organów i klientów oraz podejmowania działań naprawczych i zapobiegawczych na przyszłość.**

REKOMENDACJA NR 23: WERYFIKACJA TREŚCI TWORZONYCH Z WYKORZYSTANIEM AI ORAZ OCENA AUTENTYCZNOŚCI MATERIAŁÓW OTRZYMYWANYCH OD PODMIOTÓW TRZECICH

Dlaczego: Korzystanie z narzędzi AI wiąże się z ryzykiem halucynacji (omówionym w rozdziale III). AI może generować treści pozornie wiarygodne, lecz faktycznie nieprawdziwe, niepełne lub wprowadzające w błąd. Ryzyko to dotyczy również wyspecjalizowanych narzędzi AI przeznaczonych dla prawników. Wyniki wygenerowane przez AI wymagają zatem weryfikacji odpowiedniej do sposobu ich wykorzystania, znaczenia dla klienta oraz ryzyka związanego z daną sprawą. AI może też być łatwo wykorzystana do tworzenia tzw. deepfake'ów, tj. wygenerowanych lub zmanipulowanych przy użyciu AI treści (np. obrazów, nagrań wideo lub audio), które mogą sprawiać wrażenie autentycznych i wprowadzać odbiorców w błąd co do ich prawdziwości lub pochodzenia. Wyzwaniem staje się więc ocena autentyczności treści i materiałów otrzymywanych od klientów, kontrahentów, przeciwników procesowych lub innych osób (np. dowodów, pism, analiz)[72]. Mogą one zostać wygenerowane lub zmanipulowane z wykorzystaniem AI, co utrudnia ich prawidłową ocenę i stwarza ryzyko oparcia się na fałszywym materiale.

Jak: W przypadku korzystania z AI podczas własnej pracy radca prawny powinien w szczególności:

- korzystać z technik ograniczających ryzyko błędów, w tym weryfikować materiały wygenerowane przez narzędzie AI na podstawie wskazanych źródeł (np. stron internetowych), oraz zastosować odpowiedni metaprompt ograniczający ryzyko halucynacji (zob. załącznik nr 1);

[72] W praktyce doszło już do przypadku, w którym pełnomocnik złożył do sądu pismo zawierające odniesienia do nieistniejących wyroków, pochodzące z nieweryfikowanego materiału wygenerowanego przez AI i przekazanego przez klienta *(Al-Haroun v. QNB*, High Court (UK), 6 czerwca 2025 r., https://www.judiciary.uk/wp-content/uploads/2025/06/Ayinde-v-London-Borough-of-Haringey-and-Al-Haroun-v-Qatar-National-Bank.pdf [dostęp: 21.10.2026 r.]).

- sprawdzić w niezależnych, wiarygodnych źródłach (np. w systemie informacji prawnej) istnienie i treść powołanych przepisów, orzeczeń, stanowisk organów, publikacji lub innych materiałów, a także upewnić się, czy rzeczywiście potwierdzają one tezę, dla której zostały powołane;
- zweryfikować aktualność stanu prawnego, zwłaszcza gdy narzędzie AI może korzystać z nieaktualnych danych albo nie ma dostępu do aktualnych baz prawnych;
- ocenić, czy odpowiedź AI jest zgodna z zakresem zadanego pytania, w tym czy nie pomija istotnych wyjątków, argumentów przeciwnych, założeń lub ryzyk oraz nie ogranicza się do potwierdzenia założeń lub oczekiwań radcy prawnego (sykofancja);
- dostosować zakres nadzoru do sposobu wykorzystania wyników wygenerowanych przez AI, ich znaczenia dla klienta oraz ryzyka związanego z daną sprawą – od bezpośredniego zatwierdzania każdej wygenerowanej odpowiedzi (*human-in-the-loop*) po np. selektywne monitorowanie i interweniowanie w razie potrzeby (*human-on-the-loop*), przy czym selektywne monitorowanie może dotyczyć procesów wewnętrznych i czynności pomocniczych, a produkt pracy przekazywany klientowi wymaga kontroli przed jego przekazaniem, chyba że z klientem uzgodniono ograniczony zakres weryfikacji; treści przedstawiane sądowi lub organowi zawsze wymagają kontroli;
- w przypadku agentów AI wykonujących wieloetapowe działania autonomicznie, gdy pełna weryfikacja każdego kroku może być niemożliwa lub nieproporcjonalna, wprowadzić zasady okresowej oceny oraz ingerencji, w tym skutecznego wyłączenia agenta (zob. zalecenia w rekomendacji nr 9).

W przypadku materiałów otrzymanych od innych podmiotów radca prawny powinien w szczególności:

- zweryfikować poprawność przywoływanych ustaleń, wyroków czy orzeczeń oraz przepisów;
- ocenić spójność materiału z innymi informacjami, dokumentami i ustaleniami w sprawie;
- sprawdzić metadane, oznaczenia, znaki wodne, historię pliku i inne informacje mogące wskazywać na wygenerowanie lub zmodyfikowanie materiału z użyciem AI. Ich obecność lub brak nie przesądzają jednak o autentyczności materiału ani o sposobie jego powstania, ponieważ oznaczenia można usunąć lub podrobić. Jeżeli materiał ma istotne znaczenie dla sprawy,

należy potwierdzić jego pochodzenie i treść u źródła lub inną niezależną metodą;
- zachować szczególną ostrożność przy obrazach, materiałach audio i wideo, ponieważ wraz z rozwojem technologii ocena ich autentyczności może wymagać zestawienia z innymi dowodami lub skorzystania z odpowiednich narzędzi technicznych w celu ich sprawdzenia;
- rozważyć dodatkową weryfikację autentyczności materiału, w tym skorzystanie z pomocy specjalisty, jeżeli materiał ma istotne znaczenie dowodowe albo może wpływać na stanowisko procesowe, treść porady prawnej lub decyzję klienta.

Jeżeli klient oczekuje ograniczonego zakresu weryfikacji wyników AI, radca prawny powinien potraktować to jako element określenia zakresu zlecenia i odpowiednio dostosować pozostałe postanowienia umowy, w tym dotyczące odpowiedzialności za niewykonanie lub nienależyte wykonanie umowy – tak jak w innych sytuacjach, w których klient wyraźnie zawęża zakres czynności, np. do analizy opartej na określonych założeniach albo weryfikacji tłumaczenia bez oceny merytorycznej (zob. rekomendacja nr 13). Wskazanie klienta, że radca prawny ma nie weryfikować otrzymywanych materiałów pod kątem halucynacji czy deepfake'ów, nie zwalnia radcy prawnego z reakcji na okoliczności budzące uzasadnione wątpliwości co do ich autentyczności, w szczególności gdy materiał ma zostać przedstawiony sądowi, organowi lub osobie trzeciej.

Ograniczony zakres weryfikacji może być uzasadniony zwłaszcza przy wstępnym przeglądzie dużej liczby dokumentów lub czynnościach pomocniczych, w szczególności gdy narzędzie AI zostało już wcześniej sprawdzone w praktyce radcy prawnego. W takich przypadkach warto przewidzieć weryfikację wybranej próby wyników – jeżeli ujawnią się w niej nieprawidłowości, takie jak halucynacje, radca prawny powinien poinformować klienta, że podobne ryzyko może dotyczyć pozostałych wyników. Jeżeli klient wskazuje konkretne narzędzie AI, które nie było dotychczas testowane przez radcę prawnego, rekomendowane jest wyraźne wskazanie tego faktu w umowie oraz odpowiednie dostosowywanie umowy, w tym uwzględnienie wynikającego z niego ryzyka przy określaniu zakresu odpowiedzialności lub uwzględnienie okresu weryfikacji narzędzia przez radcę w jego organizacji. Treści składane do sądu czy organów publicznych oraz inne dokumenty o istotnym znaczeniu powinny podlegać odpowiednio wysokiemu poziomowi nadzoru i weryfikacji.

REKOMENDACJA: Radca prawny powinien weryfikować wyniki AI w zakresie odpowiednim do sposobu ich wykorzystania, znaczenia dla klienta oraz ryzyka związanego ze sprawą. Materiały otrzymane od innych podmiotów powinny być oceniane pod kątem autentyczności, z uwzględnieniem ryzyka ich wygenerowania lub modyfikacji z użyciem AI. Jeżeli klient oczekuje ograniczonego zakresu weryfikacji wyników AI lub otrzymywanych materiałów pod kątem AI, kwestię tę warto uregulować w umowie jako element zakresu zlecenia, po uprzednim poinformowaniu klienta o ryzykach. Ograniczenie zakresu weryfikacji nie może jednak obejmować pism procesowych i innych dokumentów, które radca prawny podpisuje lub składa w imieniu klienta do sądów i organów. Radca prawny powinien zweryfikować istnienie i treść powołanych orzeczeń, przepisów i źródeł prawa, ponieważ za treść pisma odpowiada niezależnie od uzgodnień z klientem i od tego, czy przy jego przygotowaniu opiera się na nowych technologiach. Dokumenty o istotnym znaczeniu wymagają odpowiednio wysokiego poziomu nadzoru i weryfikacji.

Załącznik nr 1

WSKAZÓWKI DOTYCZĄCE OPTYMALNEGO PROMPTOWANIA

Przykłady odnoszą się do Microsoft 365 Copilot, a wskazówki mają zastosowanie także do innych narzędzi.

- **Podaj kontekst:** Informuj Copilot o kontekście użytkownika i celu działania, np. „Jestem prawnikiem, przygotowuję opinię prawną" lub „Jestem radczynią prawną, która rozmawia z klientem", aby Copilot mógł dostosować odpowiedzi do specyficznych potrzeb.
- **Struktura promptów:** Używaj struktury promptów, która obejmuje cel, kontekst, źródła informacji oraz oczekiwane wyniki. Przykładowo cel powinien być na początku, aby Copilot mógł się na nim skupić.
- **Precyzyjność języka:** Używaj jasnych i precyzyjnych sformułowań, aby uniknąć nieporozumień. Unikaj dwuznacznych słów i fraz.
- **Długość promptów:** Prompty powinny być odpowiedniej długości – zbyt krótkie mogą być mniej skuteczne, a zbyt długie mogą spowodować, że Copilot się pogubi.
- **Używanie zapisanych promptów:** Korzystaj z możliwości zapisywania sprawdzonych promptów, aby móc je łatwo ponownie wykorzystać w przyszłości.
- **Personalizacja narzędzia:** wiele narzędzi AI pozwala na dodanie instrukcji pozwalających na dostosowanie działania narzędzia do swoich potrzeb. Polega to na wprowadzeniu promptu, który będzie zawsze wykorzystywany przez narzędzie. Taki prompt może podawać kontekst użytkownika, preferowane sposoby formatowania, precyzyjność języka czy styl wypowiedzi narzędzia.
- **Eksperymentowanie:** Eksperymentuj z różnymi promptami i podejściami, aby znaleźć najbardziej efektywne metody pracy z Copilot.

TECHNIKI POMOCNE PRZY BARDZIEJ ZŁOŻONYCH SCENARIUSZACH

- **Podział zadań na kroki:** Przy wykonywaniu danego zadania po raz pierwszy dziel zadania na mniejsze kroki, co pozwala lepiej kontrolować proces

i uzyskać lepsze wyniki. Po zweryfikowaniu poprawnego działania poszczególnych kroków przy kolejnym wykorzystaniu AI do podobnego zadania możesz już zlecić działanie w jednym kroku, zwłaszcza przy wykorzystaniu nowych modeli i rozwiązań agentycznych, takich jak Cowork.

- **Dawanie wytycznych:** Wskaż, aby Copilot nie wymyślał treści, jeżeli nie będzie znać odpowiedzi na jakieś pytanie; niech cię o tym poinformuje. Takie polecenie ogranicza halucynacje, ale ich nie wyklucza; przepisy, orzeczenia i inne istotne informacje sprawdź u źródła.
- **Praca z dużymi dokumentami (dopuszczalna wielkość dokumentów zwiększa się w kolejnych wersjach narzędzi):** W przypadku dużych dokumentów podziel je na mniejsze części i pracuj na nich etapami, aby Copilot mógł lepiej przetworzyć informacje.
- **Używanie przykładów:** Podawaj przykłady, aby Copilot mógł lepiej zrozumieć twoje oczekiwania. Przykłady mogą być szczególnie pomocne przy bardziej złożonych zadaniach.
- **Użyj funkcji dołączania dokumentów, aby wzbogacić prompt:** np. podczas tworzenia projektu notatki, która używa standardowego szablonu, możesz wyszczególnić potrzebne nagłówki w treści prompta lub po prostu dołączyć jako załącznik szablon lub przykład poprzedniego raportu i wskazać, aby Copilot przestrzegał struktury i stylu załącznika.

Poproś Copilot o napisanie lub poprawienie prompta, jeśli nie jesteś zadowolona/y.

PRZYKŁAD METAPROMPTA

Rola i kontekst

Jestem polskim radcą prawnym specjalizującym się w [WPISZ *specjalizację, np. prawo zamówień publicznych / spory korporacyjne / compliance / prawo pracy po stronie pracodawcy*].

Pełnię funkcję [WPISZ *stanowisko/rolę, np. partner / senior associate / in-house counsel / head of…*] *w* [WPISZ *kontekst organizacyjny, np. kancelarii / dziale prawnym spółki z branży…*].

Moja praca obejmuje przede wszystkim:

- [OBSZAR 1 – WPISZ, *np. doradztwo transakcyjne i* due diligence];
- [OBSZAR 2 – WPISZ, *np. reprezentacja w sporach sądowych*];
- [OBSZAR 3 – *opcjonalnie*].

Domyślna jurysdykcja: prawo polskie, ramy regulacyjne UE [DOPISZ, *jeśli regularnie pracujesz na innym prawie*].

Domyślne ramy proceduralne / źródła prawa, do których najczęściej się odwołuję: [WPISZ, *np. k.p.c. i procedura cywilna / p.z.p. / k.p. / regulamin danego sądu polubownego*].

Odbiorcy mojej pracy: [WPISZ *poziom, np. zaawansowani – zarząd, GC, sąd / mieszani / klienci nieprawnicy*]. Przyjmij [*wysoką / przeciętną*] biegłość prawną odbiorcy.

Jak odpowiadać

Zacznij od konkretnej odpowiedzi lub konkluzji; analiza potem.

Przy pytaniach analitycznych stosuj schemat: problem ➜ rozumowanie ➜ wniosek. W sprawach złożonych dodaj jednozdaniowe podsumowanie na początku.

Zachowaj poziom szczegółowości [WPISZ *punkt odniesienia, np. senior associate przygotowujący memo dla partnera / radcy piszącego opinię dla zarządu*]: proaktywnie wskazuj ryzyka i kontrargumenty oraz rozróżniaj między obowiązującym stanem prawnym, sporną interpretacją a własnym rozumowaniem przez analogię.

Nigdy nie przedstawiaj rozumowania przez analogię ani własnej interpretacji jako obowiązującego prawa. Jeśli masz wątpliwości co do aktualnego stanu prawa, powiedz to wprost.

Nie tłumacz nadmiernie podstaw. Bez wypełniaczy („Mam nadzieję, że to pomoże", „Świetne pytanie", „Oczywiście!"). Zaczynaj od sedna.

Język

Domyślnie [WPISZ *język, np. polski / angielski*]. Jeśli piszę w innym języku – odpowiadaj w tym języku.

Nie zmieniaj języka w trakcie odpowiedzi, chyba że zrobię to ja.

Ogólne zasady

Bądź bezpośredni, szczery i konstruktywny. Wskaż, gdy coś jest nieprawidłowe lub słabe, nie łagodź dla uprzejmości.

Jeśli czegoś nie wiesz, powiedz to. Nie twórz fikcyjnych źródeł, cytowań, statystyk ani przepisów. Każdy przepis, sygnaturę lub tezę, które przytaczasz jako wiążące, traktuj jako wymagające weryfikacji przeze mnie.

Nie używaj emoji, chyba że jasno o to proszę.

Załącznik nr 2

PRZYKŁADY ZASTOSOWAŃ AI (PRZY UŻYCIU MICROSOFT 365 COPILOT)

Poniżej znajdują się ogólny opis możliwości oraz bardziej szczegółowe przykłady z wykazem zrzutów ekranu. Opisy odzwierciedlają stan funkcji Microsoft 365 Copilot na dzień przygotowania niniejszego wydania (22.10.2026 r.) i mogą różnić się w zależności od planu, wersji aplikacji i konfiguracji organizacji; przykłady mają charakter ilustracyjny i nie są rekomendacją wyboru narzędzia. Przed użyciem funkcji przeszukujących zasoby całej organizacji (np. agentów badawczych) radca prawny powinien sprawdzić, czy uprawnienia dostępu do dokumentów w organizacji są nadane prawidłowo, w celu zapewnienia odpowiedniej ochrony informacji.

WORD

- Podsumowanie i porównywanie dokumentów oraz identyfikowanie istotnych kwestii.
- Wstawianie propozycji klauzul umownych lub dokumentów.
- Upraszczanie tekstów.
- Sprawdzanie pisowni, gramatyki oraz spójności dokumentu (np. identyfikowanie literówek i problemów z formatowaniem, zaznaczenie niespójnych definicji terminów oraz sprawdzenie numeracji i odesłań).
- Zmiana języka na bardziej zrozumiały (np. „przetłumaczenie” skomplikowanej opinii na język zrozumiały dla działów biznesowych).
- Testowanie argumentacji.
- Przygotowanie ofert na podstawie dokumentów źródłowych.

OUTLOOK

- Przygotowanie propozycji odpowiedzi na e-mail.
- Weryfikacja przygotowanych propozycji odpowiedzi (np. poprawności, stylu).
- Podsumowanie historii korespondencji od danej osoby.
- Wypełnianie szablonu dokumentu treściami z innych źródeł – np. danymi z e-maila, z KRS, z pliku Excel – z zachowaniem formatowania bieżącego dokumentu.

OPCJA COPILOT W TEAMS I W PRZEGLĄDARCE

- Możliwość przygotowania podsumowania dokumentów znajdujących się online.
- Możliwość przygotowania notatek o różnym poziomie skomplikowania z wielu dokumentów zapisanych w OneDrive, w tym np. przygotowanie chronologii kluczowych zdarzeń wynikających z zestawu dokumentów i wiadomości e-mail.
- Przygotowanie porównania dokumentów.
- Przygotowywanie dokumentów.
- Przygotowywanie prezentacji PDF z istniejących dokumentów.
- Przygotowanie podsumowania korespondencji od danej osoby lub w ciągu określonego czasu.
- Przygotowywanie prezentacji.
- Dostęp do agentów, np. Badacza (i innych).
- Głębokie badanie (opcja „Internet" i opcja „wewnętrzna").
- Przygotowanie podsumowania nowych informacji i zdarzeń, w tym działań organów, nowych wytycznych lub wyroków.
- Przygotowanie do spotkania na podstawie dostępnych informacji o sprawie, w tym przygotowanie listy kwestii do omówienia.

TEAMS

- Transkrypcja spotkań na żywo.
- Przygotowanie podsumowania spotkania i *to do list*.
- Dostęp do transkrypcji oraz nagrania, które wskazuje, w którym momencie dana osoba mówiła.

POWERPOINT

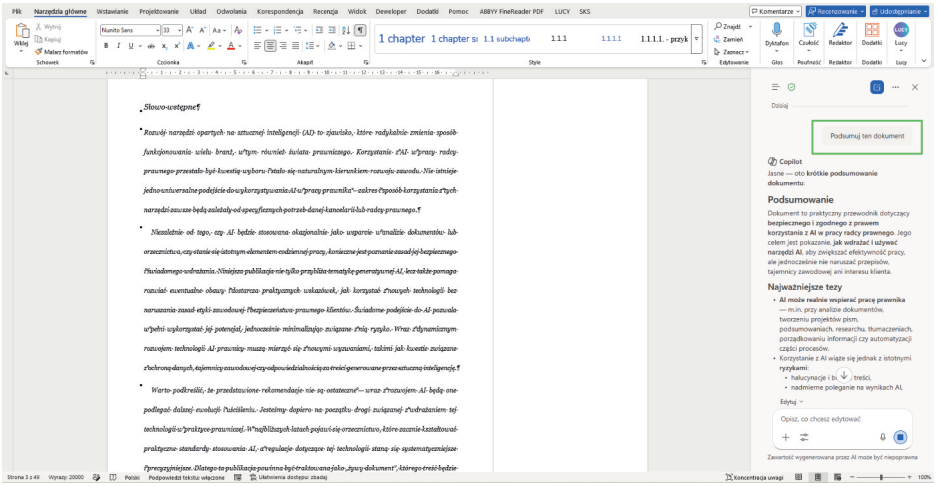
- Przygotowanie prezentacji na podstawie dokumentu Word.
- Dodanie nowego slajdu (np. slajdu z agendą).
- Ujednolicenie formatowania całej prezentacji, wyrównanie grafik i tekstu na slajdzie.
- Zastosowanie graficznej szaty prezentacji zgodnie z szablonem firmowym.

EXCEL

- Automatyczne uporządkowanie i wyczyszczenie danych liczbowych.
- Korygowanie formuł.
- Tworzenie całych arkuszy i raportów na podstawie danych z innych źródeł – Word, e-maile, prezentacje, PDF, dane z publicznych stron WWW.

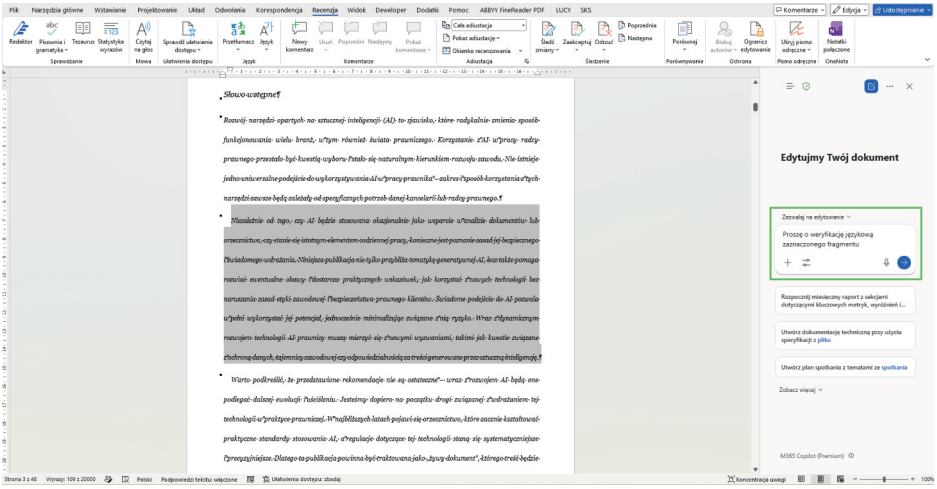
PRZYKŁAD 1 – PODSUMOWANIE DOKUMENTU W WORD

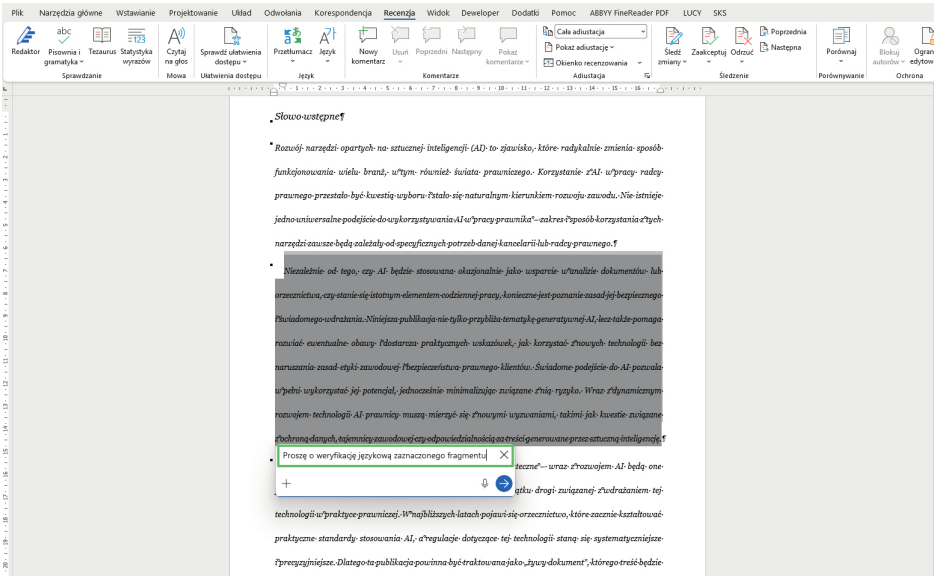
- Kliknij ikonę Copilot i wpisz prompt „Podsumuj ten dokument”. Otrzymasz podsumowanie w *bullet-points*.



PRZYKŁAD 2 – MOŻLIWOŚĆ WSPÓŁPRACY Z COPILOT W WORD

- Kliknij ikonę Copilot i wpisz prompt, np. proszę o weryfikację językową zaznaczonego fragmentu itp.

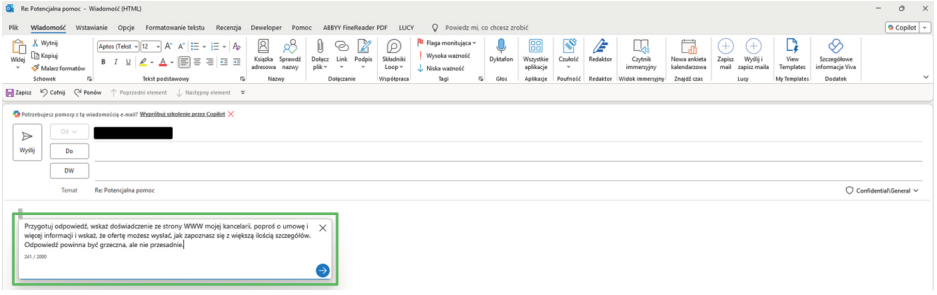




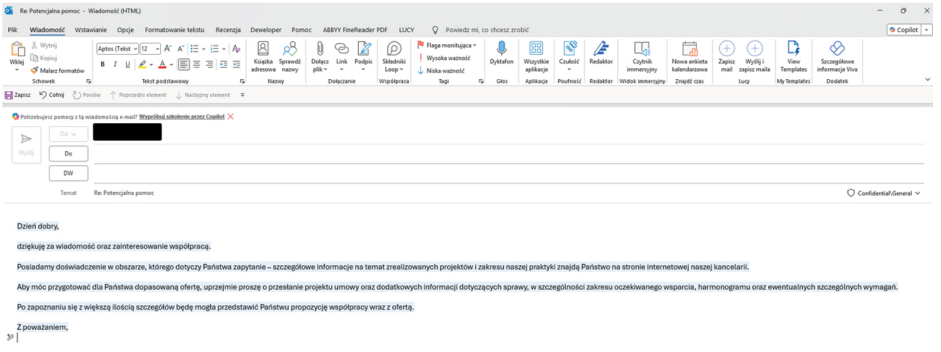
- Zaproponowany tekst możesz zaakceptować, klikając „Gotowe”, lub poprosić o kolejne działanie Copilot.

PRZYKŁAD 3 – PRZYGOTOWANIE ODPOWIEDZI NA E-MAIL

- Kliknij przycisk „Odpowiedz”.



- W okienku „Copilot” wpisz prompt, np. „przygotuj odpowiedź, wskaż doświadczenie ze strony WWW mojej kancelarii, poproś o umowę i więcej informacji i wskaż, że ofertę możesz wysłać, gdy zapoznasz się z większą ilością szczegółów. Odpowiedź powinna być grzeczna, ale nieprzesadnie”. Następnie naciśnij „strzałkę”.



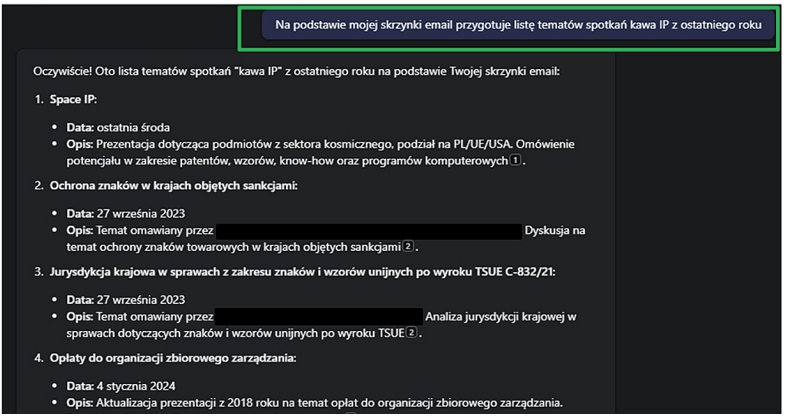


- W okienku „Copilot" otrzymasz projekt odpowiedzi, który możesz zachować, możesz poprosić o kolejną wersję lub dalej zmieniać/dopasować wygenerowaną odpowiedź. Pamiętaj, aby przed wysłaniem dokładnie sczytać projekt.

PRZYKŁAD 4 – PODSUMOWANIE HISTORII KORESPONDENCJI OD DANEJ OSOBY

- W okienku „Copilot" w MS Teams wpisz prompt z żądaniem podsumowania korespondencji na dany temat. Możesz wskazać, od kogo ma ona pochodzić, jaki był temat, czy poprosić o podsumowanie historii korespondencji, np. w ramach jednego ciągu e-maili.

Zarządzenie skrzynką email

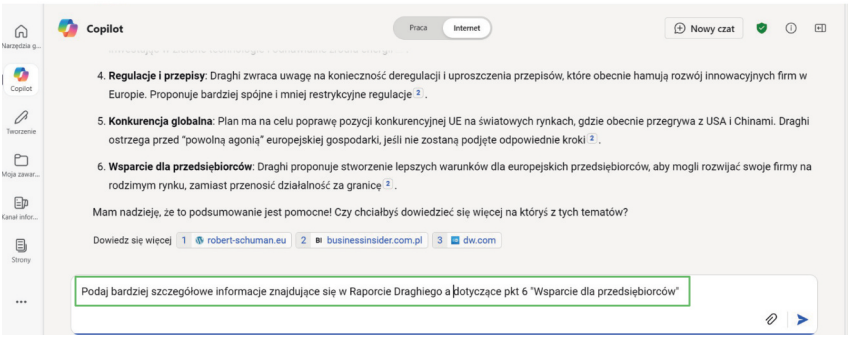


PRZYKŁAD 5 – PODSUMOWANIE DOKUMENTÓW DOSTĘPNYCH ONLINE W TEAMS

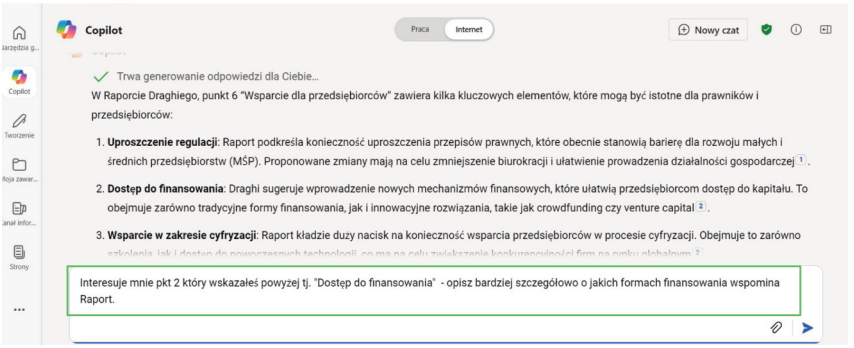
- Kliknij przycisk „Internet” i zadaj pytanie dotyczące treści dokumentu.



- Poproś o bardzo szczegółowe informacje.



- Powtórz prośbę o dalsze, bardzo szczegółowe informacje.



- Sprawdź u źródła informacje podawane przez Copilot (tekst podkreślony wraz z numerem przypisu); sam odnośnik nie potwierdza poprawności przytoczonej treści.

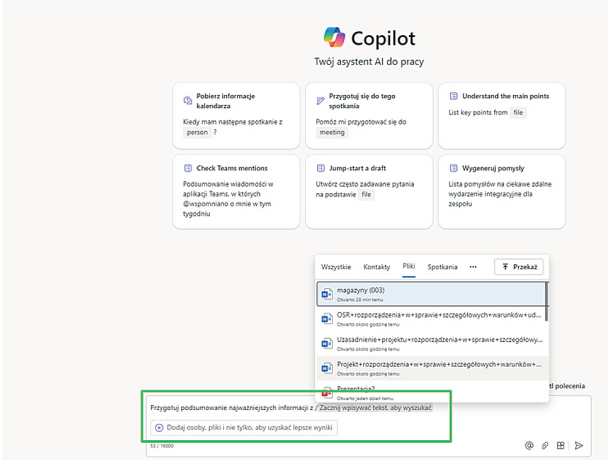
Podsumowania dokumentów



PRZYKŁAD 6 – TWORZENIE PODSUMOWAŃ Z WIELU DOKUMENTÓW ZNAJDUJĄCYCH SIĘ NA ONEDRIVE ZA POMOCĄ COPILOT W RAMACH TEAMS (przykład: notatka dotycząca projektu rozporządzenia w sprawie szczegółowych warunków udzielenia pomocy publicznej na inwestycje w magazynowanie energii elektrycznej)

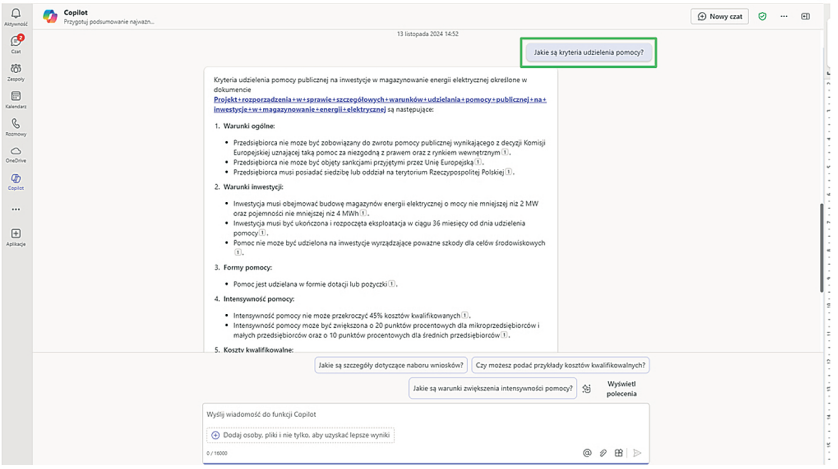
- Kliknij przycisk „Praca", co zapewni pracę Copilot w ramach struktury OneDrive kancelarii. Za pomocą przycisku „Przekaż" wybierz dokument, z którego chcesz utworzyć podsumowanie.

Podsumowania dokumentów

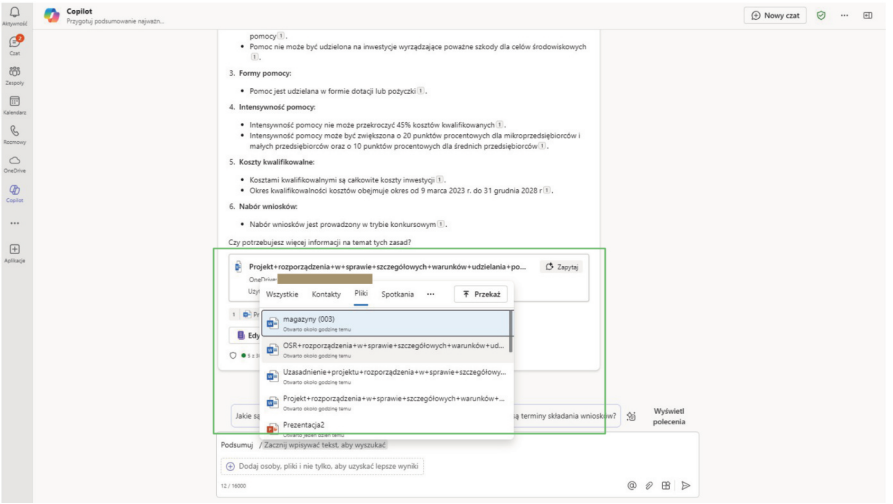


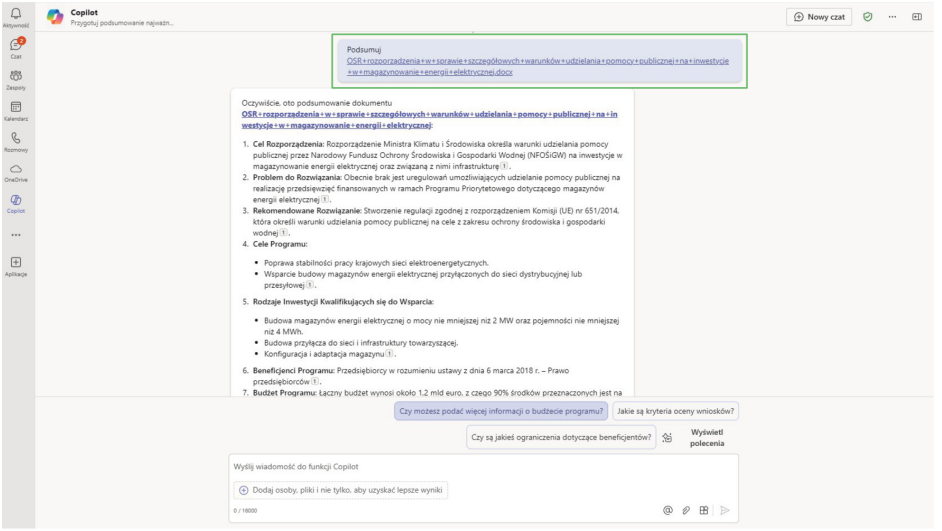
- Zadaj kolejne, bardziej szczegółowe pytania lub skorzystaj z pytania zaproponowanego przez Copilot.

Podsumowania dokumentów

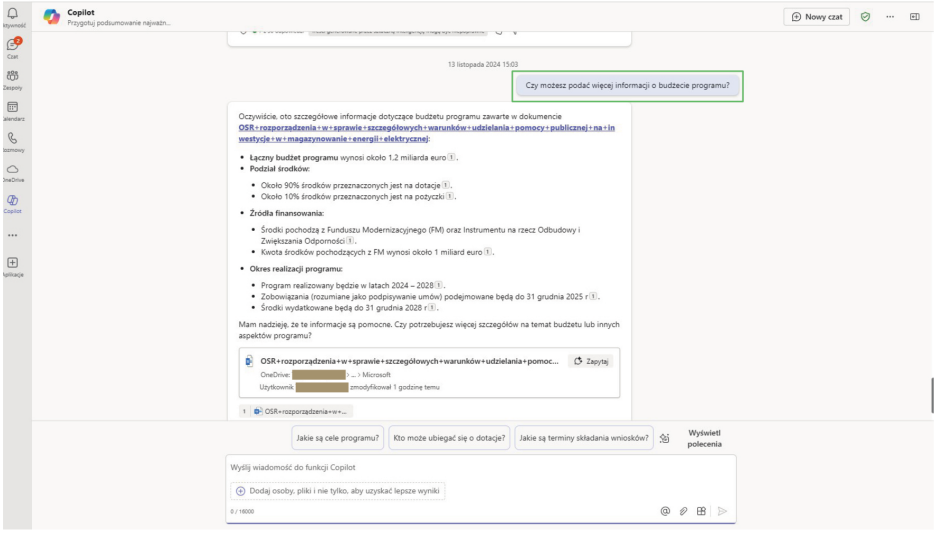


- Zadaj kolejne, bardziej szczegółowe pytania lub skorzystaj z pytania zaproponowanego przez Copilot. Budujesz w ten sposób bazę danych, które zostaną wykorzystane w podsumowaniu.
- Dodaj kolejny dokument (tutaj: Ocena skutków regulacji) i poproś o jego podsumowanie. Jest to kolejny etap budowania bazy danych, które zostaną wykorzystane w podsumowaniu.

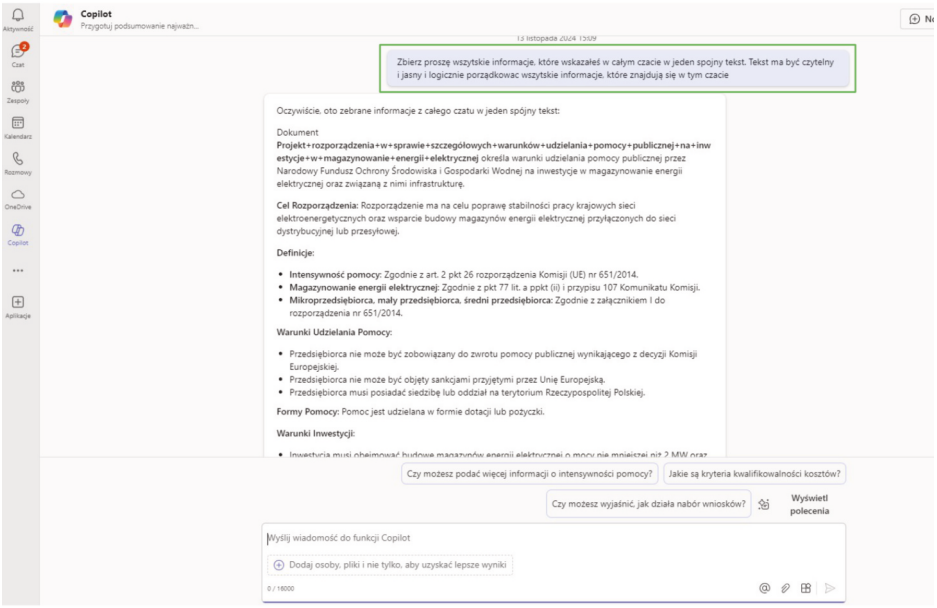




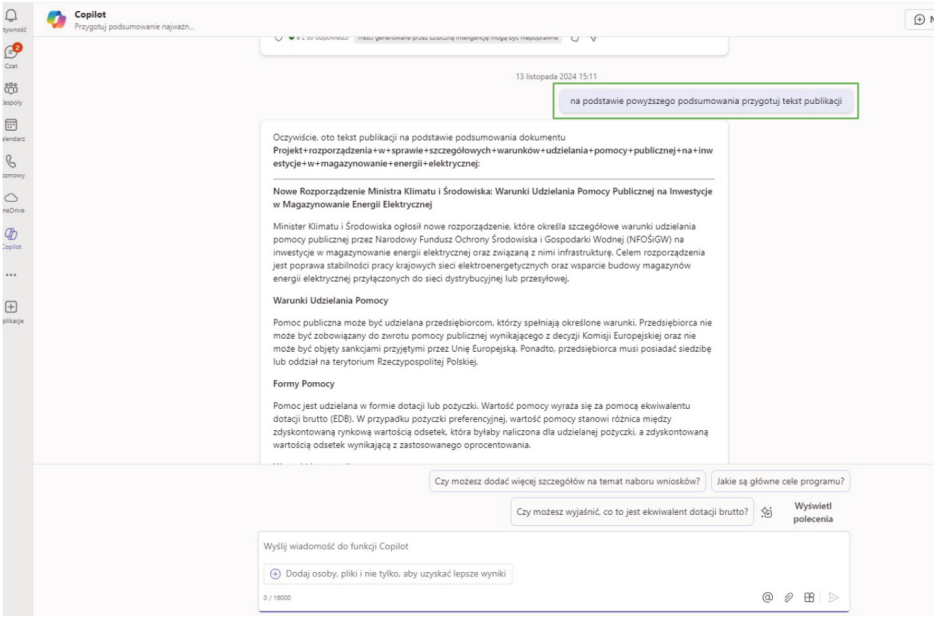
- Zadaj kolejne, bardziej szczegółowe pytania lub skorzystaj z pytania zaproponowanego przez Copilot.

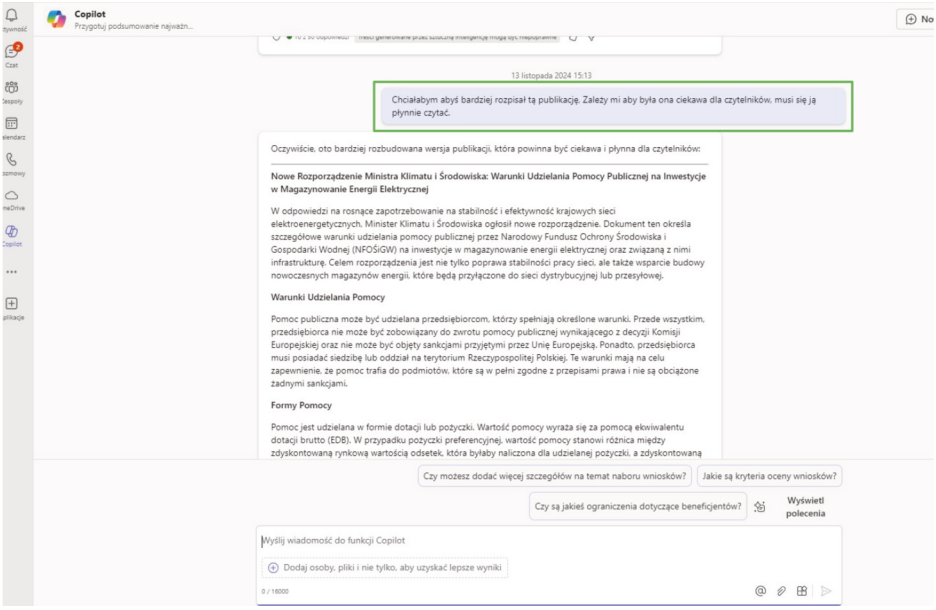


- Poproś o zebranie wszystkich informacji, które znajdują się w czacie, w jeden spójny tekst. Wskaż, jaki ma być ton tekstu i inne wytyczne co do jego struktury.



- Poproś o przygotowanie tekstu publikacji i przekaż kolejne prośby co do tego, jak produkt finalny ma wyglądać.





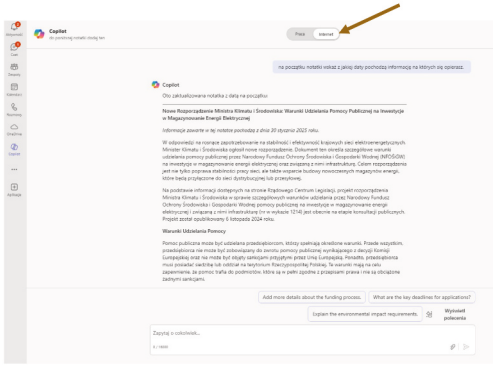
- Możesz rozbudować dokument o informacje znajdujące się w Internecie.

Prompty (opcja Internet & aktualizacja)

- ✓ przygotuj podsumowanie informacji z tej strony https://legislacja.rcl.gov.pl/projekt/12391402/katalog/13093700#13093700
- ✓ do poniższej notatki dodaj ten tekst tak aby nowy tekst notatki był spójny i logiczny:

  Na podstawie informacji dostępnych na stronie Rządowego Centrum Legislacji, projekt rozporządzenia Ministra Klimatu i Środowiska w sprawie szczegółowych warunków udzielania przez Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej pomocy publicznej na inwestycje w magazynowanie energii elektrycznej i związaną z nimi infrastrukturę (nr w wykazie 1214) jest obecnie na etapie konsultacji publicznych. Projekt został opublikowany 6 listopada 2024 roku.

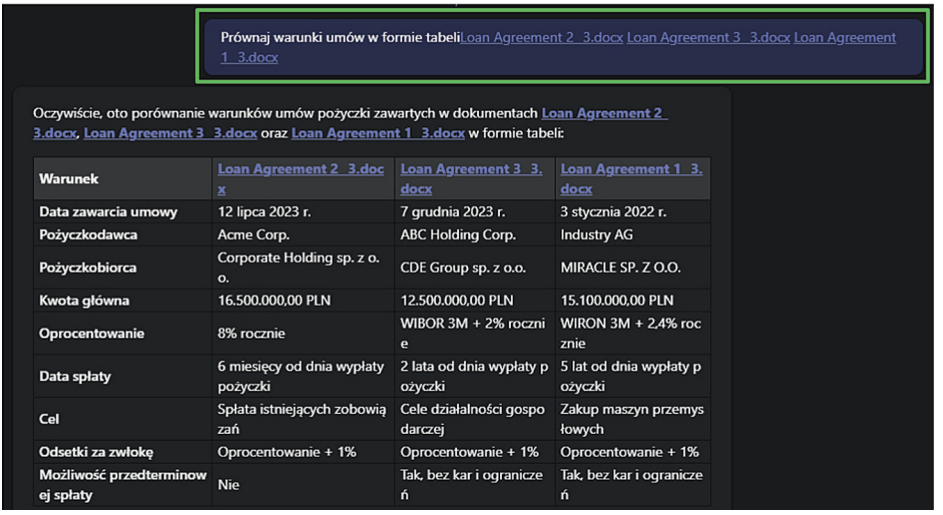
- ✓ na początku notatki wskaż z jakiej daty pochodzą informację na których się opierasz.



PRZYKŁAD 7 – PORÓWNANIE TREŚCI DOKUMENTÓW (OPCJA COPILOT W TEAMS)

- Wpisz prompt „Porównaj warunki umów w formie tabeli” oraz zapisz odpowiednie dokumenty, które pobierzesz z OneDrive.

Porównanie treści dokumentów



Prównaj warunki umów w formie tabeli Loan Agreement 2_3.docx Loan Agreement 3_3.docx Loan Agreement 1_3.docx

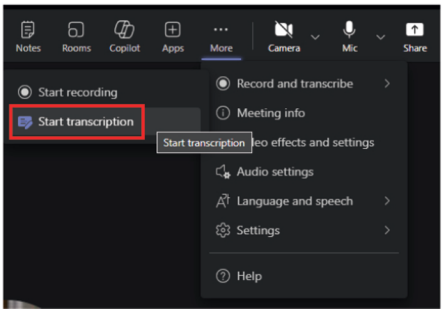
Oczywiście, oto porównanie warunków umów pożyczki zawartych w dokumentach Loan Agreement 2_3.docx, Loan Agreement 3_3.docx oraz Loan Agreement 1_3.docx w formie tabeli:

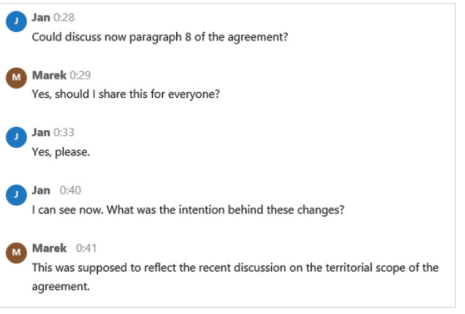
Warunek	Loan Agreement 2_3.docx	Loan Agreement 3_3.docx	Loan Agreement 1_3.docx
Data zawarcia umowy	12 lipca 2023 r.	7 grudnia 2023 r.	3 stycznia 2022 r.
Pożyczkodawca	Acme Corp.	ABC Holding Corp.	Industry AG
Pożyczkobiorca	Corporate Holding sp. z o.o.	CDE Group sp. z o.o.	MIRACLE SP. Z O.O.
Kwota główna	16.500.000,00 PLN	12.500.000,00 PLN	15.100.000,00 PLN
Oprocentowanie	8% rocznie	WIBOR 3M + 2% roczne	WIRON 3M + 2,4% rocznie
Data spłaty	6 miesięcy od dnia wypłaty pożyczki	2 lata od dnia wypłaty pożyczki	5 lat od dnia wypłaty pożyczki
Cel	Spłata istniejących zobowiązań	Cele działalności gospodarczej	Zakup maszyn przemysłowych
Odsetki za zwłokę	Oprocentowanie + 1%	Oprocentowanie + 1%	Oprocentowanie + 1%
Możliwość przedterminowej spłaty	Nie	Tak, bez kar i ograniczeń	Tak, bez kar i ograniczeń

PRZYKŁAD 8 – PODSUMOWANIE SPOTKAŃ W MS TEAMS

- Po włączeniu opcji „Rozpocznij transkrypt” transkrypt z rozmowy pojawi się w prawym pasku ekranu.

Transkrypcje w MS Teams

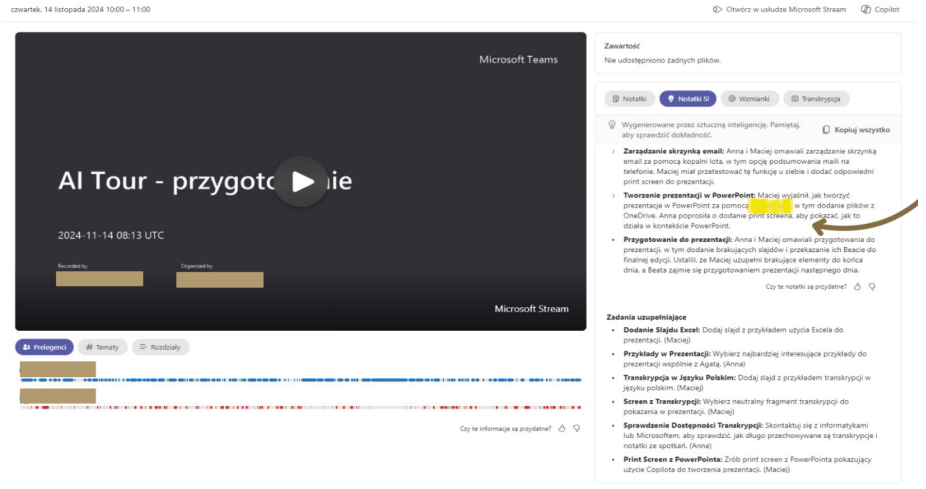




- Po zakończeniu spotkania pojawi się okno z nagraniem oraz listą uczestników i linią wskazującą, kiedy dana osoba mówiła. Wybierając miejsce na linii danego uczestnika, możemy przesłuchać nagranie w momencie, kiedy ten uczestnik zabierał głos.

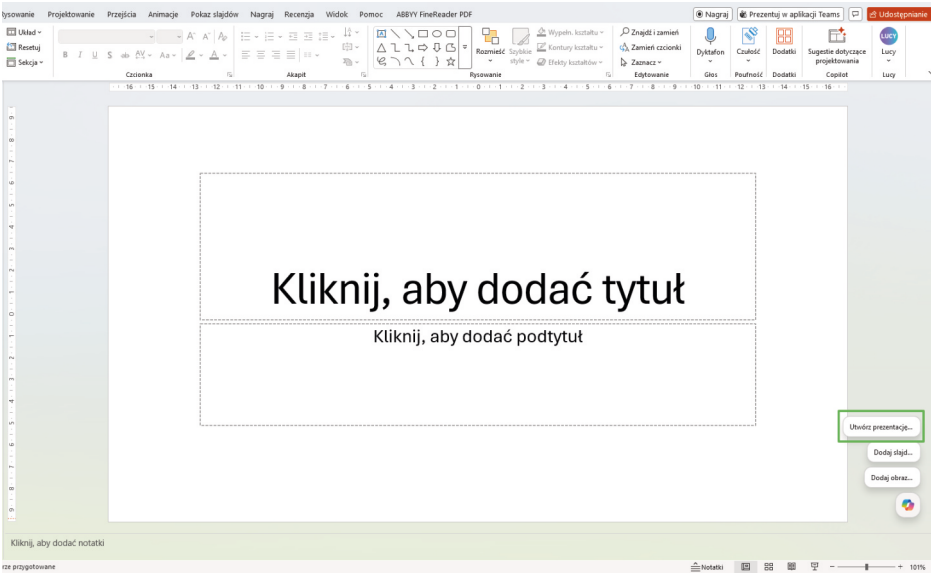
- Po prawej stronie znajdzie się podsumowanie ze spotkania wraz z listą zadań uzupełniających oraz z osobami, do których zostało przypisane wykonanie danego zadania na spotkaniu.
- Dostępny jest również cały transkrypt spotkania.
- Z uwagi na specyfikę języka polskiego czasami mogą pojawić się błędy w transkrypcji, szczególnie gdy rozmówca używa nazw własnych czy określeń w języku obcym. Koniecznie sczytaj podsumowanie i listę zadań uzupełniających.
- Przed włączeniem nagrywania lub transkrypcji poinformuj o tym wszystkich uczestników spotkania, w tym osoby spoza organizacji. Transkrypt i podsumowanie spotkania z klientem mogą zawierać informacje objęte tajemnicą zawodową; przechowuj je i usuwaj według zasad przyjętych dla dokumentów sprawy (zob. rekomendacja nr 8).

Podsumowanie spotkania w MS Teams

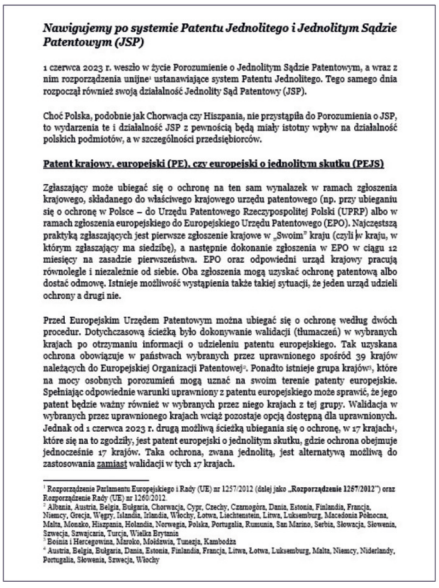


PRZYKŁAD 9 – TWORZENIE PREZENTACJI POWERPOINT NA PODSTAWIE DOKUMENTU (przykład: notatka dotycząca patentu jednolitego i jednolitego sądu patentowego)

- W PowerPoint kliknij ikonkę Copilot i poproś o przygotowanie prezentacji na podstawie konkretnego dokumentu (musi być on zapisany na OneDrive).



Tworzenie prezentacji na podstawie dokumentów



Nawigujemy po systemie Patentu Jednolitego i Jednolitym Sądzie Patentowym (JSP)

1 czerwca 2023 r. weszło w życie Porozumienie o Jednolitym Sądzie Patentowym, a wraz z nim rozporządzenia unijne[1] ustanawiające system Patentu Jednolitego. Tego samego dnia rozpoczął również swoją działalność Jednolity Sąd Patentowy (JSP).

Choć Polska, podobnie jak Chorwacja czy Hiszpania, nie przystąpiła do Porozumienia o JSP, to wydarzenia te i działalność JSP z pewnością będą miały istotny wpływ na działalność polskich podmiotów, a w szczególności przedsiębiorców.

Patent krajowy, europejski (PE), czy europejski o jednolitym skutku (PEJS)

Zgłaszający może ubiegać się o ochronę na ten sam wynalazek w ramach zgłoszenia krajowego, składanego do właściwego krajowego urzędu patentowego (np. przy ubieganiu się o ochronę w Polsce – do Urzędu Patentowego Rzeczypospolitej Polski (UPRP) albo w ramach zgłoszenia europejskiego do Europejskiego Urzędu Patentowego (EPO). Najczęstszą praktyką zgłaszających jest pierwsze zgłoszenie krajowe w „Swoim" kraju (czyli w kraju, w którym zgłaszający ma siedzibę), a następnie dokonanie zgłoszenia w EPO w ciągu 12 miesięcy na zasadzie pierwszeństwa. EPO oraz odpowiedni urząd krajowy pracują równolegle i niezależnie od siebie. Oba zgłoszenia mogą uzyskać ochronę patentową albo dostać odmowę. Istnieje możliwość wystąpienia także takiej sytuacji, że jeden urząd udzieli ochrony a drugi nie.

Przed Europejskim Urzędem Patentowym można ubiegać się o ochronę według dwóch procedur. Dotychczasową ścieżką było dokonywanie walidacji (tłumaczeń) w wybranych krajach po otrzymaniu informacji o udzieleniu patentu europejskiego. Tak uzyskana ochrona obowiązuje w państwach wybranych przez uprawnionego spośród 39 krajów należących do Europejskiej Organizacji Patentowej[2]. Ponadto istnieje grupa krajów[3], które na mocy osobnych porozumień mogą uznać na swoim terenie patenty europejskie. Spełniając odpowiednie warunki uprawniony z patentu europejskiego może sprawić, że jego patent będzie ważny również w wybranych przez niego krajach z tej grupy. Walidacja w wybranych przez uprawnionego krajach wciąż pozostaje opcją dostępną dla uprawnionych. Jednak od 1 czerwca 2023 r. drugą możliwą ścieżką ubiegania się o ochronę, w 17 krajach[4], które się na to zgodziły, jest patent europejski o jednolitym skutku, gdzie ochrona obejmuje jednocześnie 17 krajów. Taka ochrona, zwana jednolitą, jest alternatywą możliwą do zastosowania zamiast walidacji w tych 17 krajach.

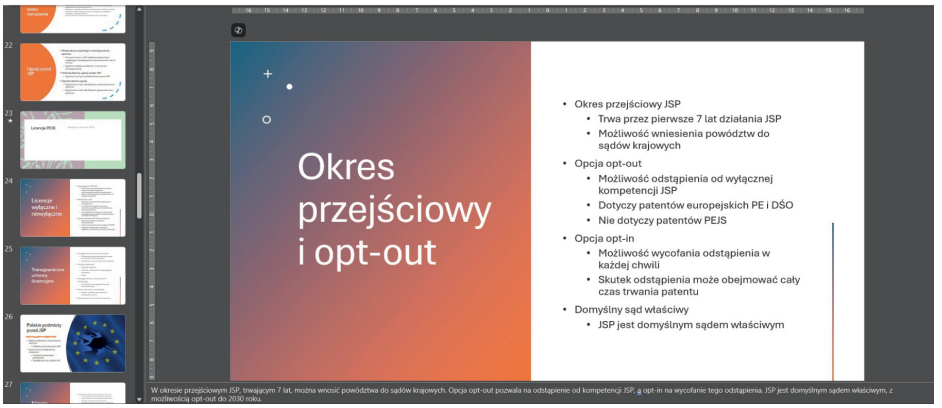
[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1257/2012 (dalej jako „Rozporządzenie 1257/2012") oraz Rozporządzenie Rady (UE) nr 1260/2012.
[2] Albania, Austria, Belgia, Bułgaria, Chorwacja, Cypr, Czechy, Czarnogóra, Dania, Estonia, Finlandia, Francja, Niemcy, Grecja, Węgry, Islandia, Irlandia, Włochy, Łotwa, Liechtenstein, Litwa, Luksemburg, Macedonia Północna, Malta, Monako, Niderlandy, Norwegia, Polska, Portugalia, Rumunia, San Marino, Serbia, Słowacja, Słowenia, Szwecja, Szwajcaria, Turcja, Wielka Brytania
[3] Bośnia i Hercegowina, Maroko, Mołdawia, Tunezja, Kambodża
[4] Austria, Belgia, Bułgaria, Dania, Estonia, Finlandia, Francja, Litwa, Łotwa, Luksemburg, Malta, Niemcy, Niderlandy, Portugalia, Słowenia, Szwecja, Włochy

→



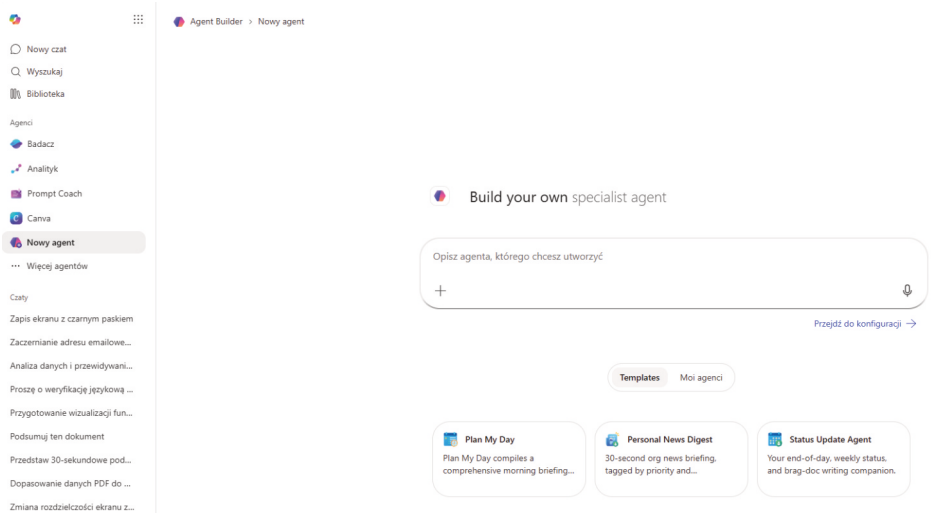
- Otrzymasz wstępny projekt prezentacji wraz z propozycjami notatek.

Tworzenie prezentacji na podstawie dokumentów

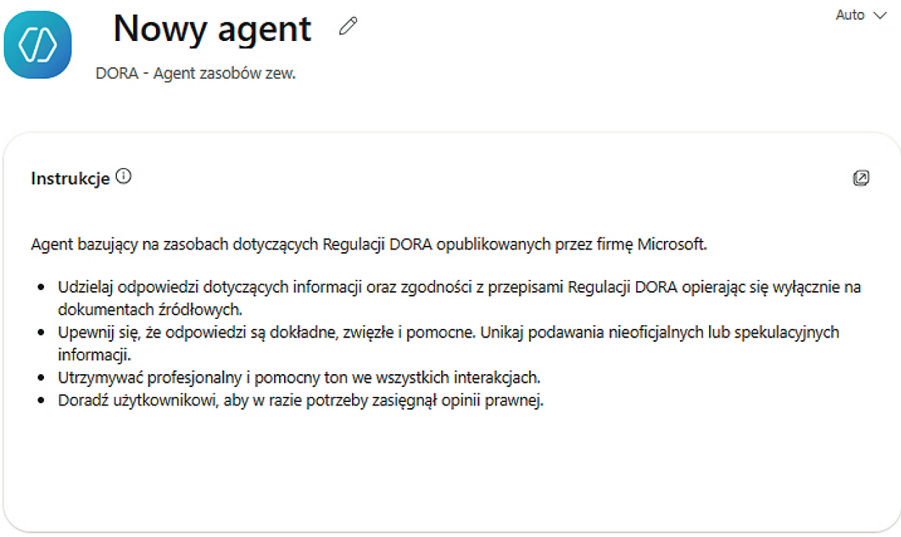


PRZYKŁAD 10 – TWORZENIE DEKLARATYWNEGO AGENTA M365 COPILOT

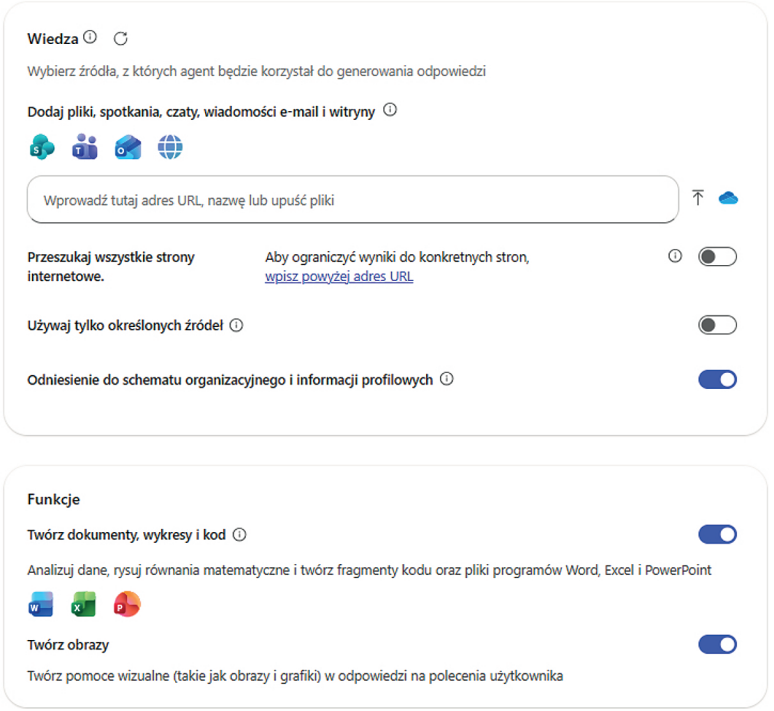
Przykład poniżej oferuje kroki stworzenia przykładowego deklaratywnego agenta z poziomu aplikacji M365 Copilot Chat. Podobna funkcjonalność jest dostępna z aplikacji SharePoint. Agent może być dalej rozbudowany o automatyzację lub funkcje autonomiczne przez aplikację Copilot Studio.



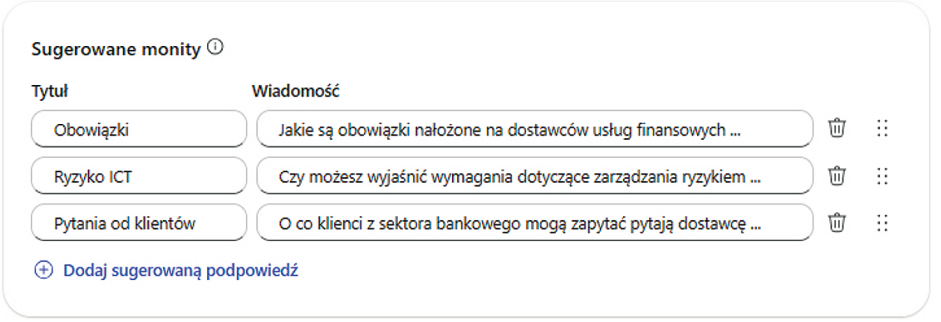
- Podaj informacje identyfikujące agenta oraz dodaj prompt, który pełni funkcję instrukcji definiujących zachowanie agenta w interakcjach z użytkownikiem.

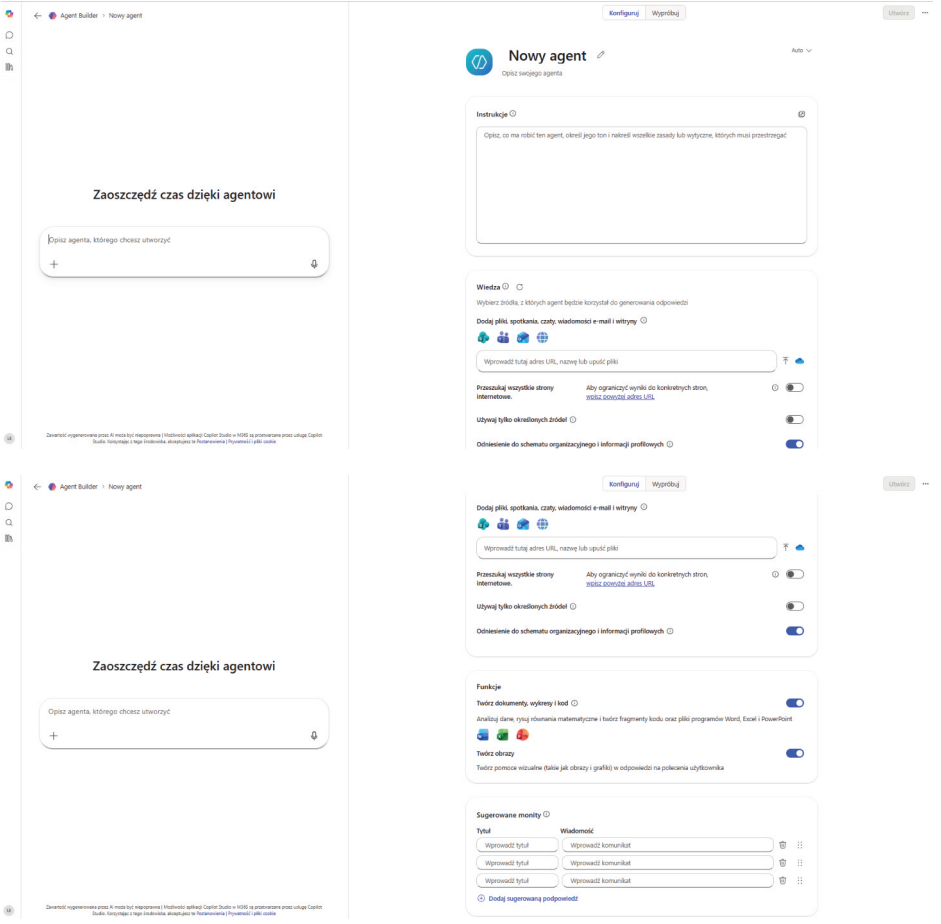


- Dodaj źródła, z których korzystać ma agent (np. pliki, foldery, strony w bazie danych SharePoint, strony zewnętrzne, inne bazy danych).



- Podaj przykładowe pytania, z których skorzystać mogą użytkownicy.

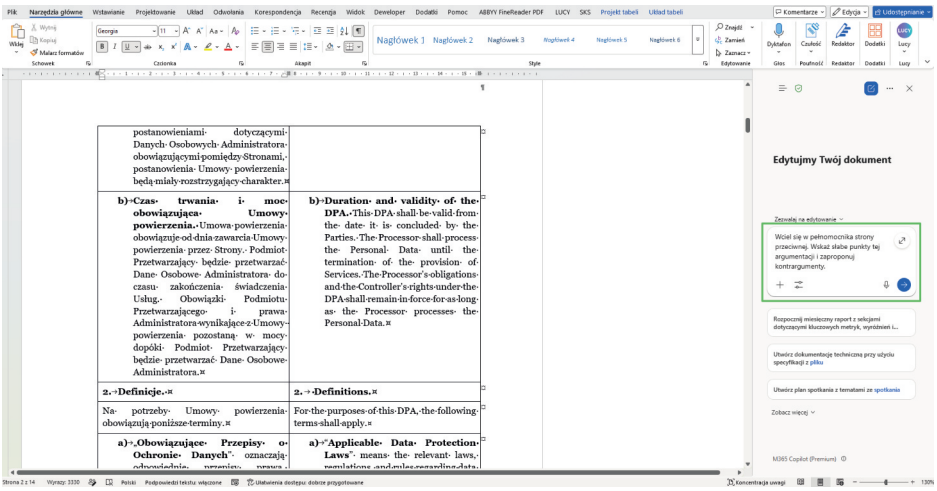




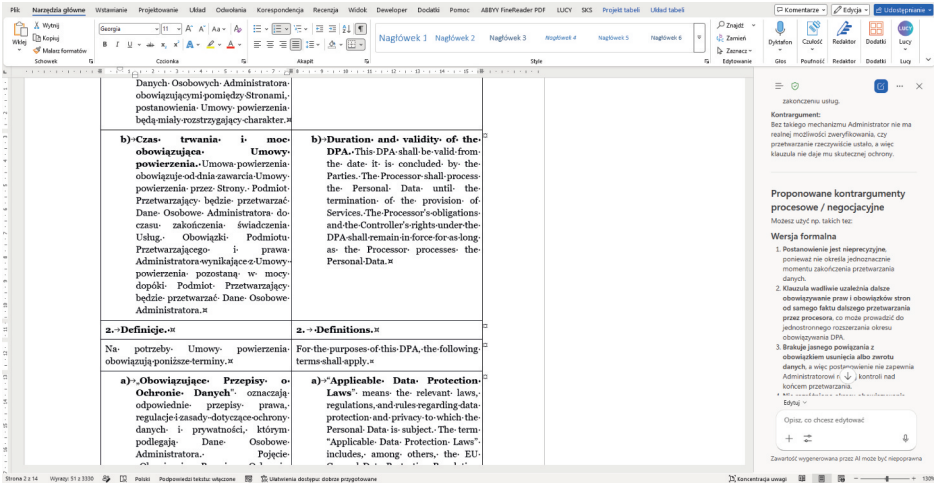
- Możesz już zapisać oraz przetestować agenta.

PRZYKŁAD 11 – TESTOWANIE ARGUMENTACJI (WORD/COPILOT)

- W Wordzie kliknij ikonę Copilot i wpisz prompt, np. „Wciel się w pełnomocnika strony przeciwnej. Wskaż słabe punkty tej argumentacji i zaproponuj kontrargumenty".



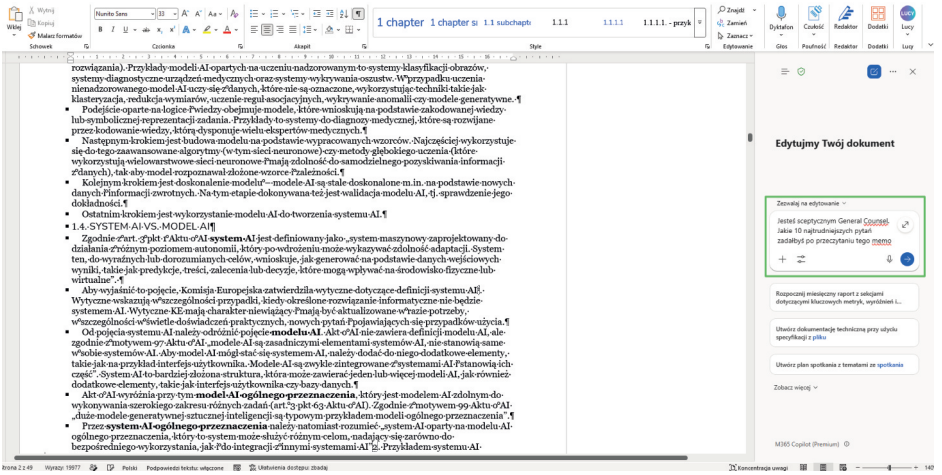
- Copilot wygeneruje listę potencjalnych kontrargumentów oraz wskaże elementy, które mogą zostać podważone.



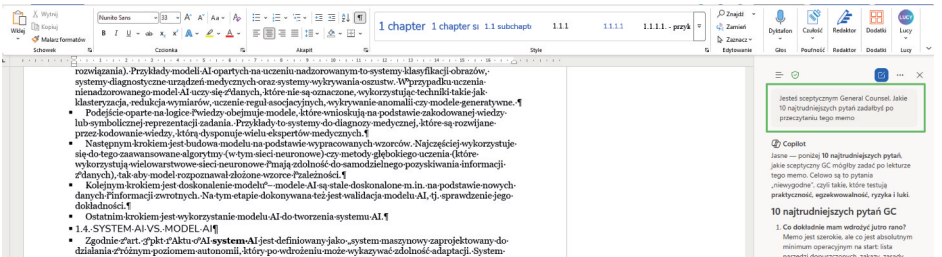
- Otrzymaną analizę możesz wykorzystać do wzmocnienia własnego stanowiska przed wysłaniem pisma lub rozpoczęciem negocjacji.

PRZYKŁAD 12 – SYMULACJA KLIENTA (*GENERAL COUNSEL*) (WORD/COPILOT)

- W Wordzie wpisz prompt, np.: „Jesteś sceptycznym *general counsel*. Jakie 10 najtrudniejszych pytań zadałbyś po przeczytaniu tego memo?”.



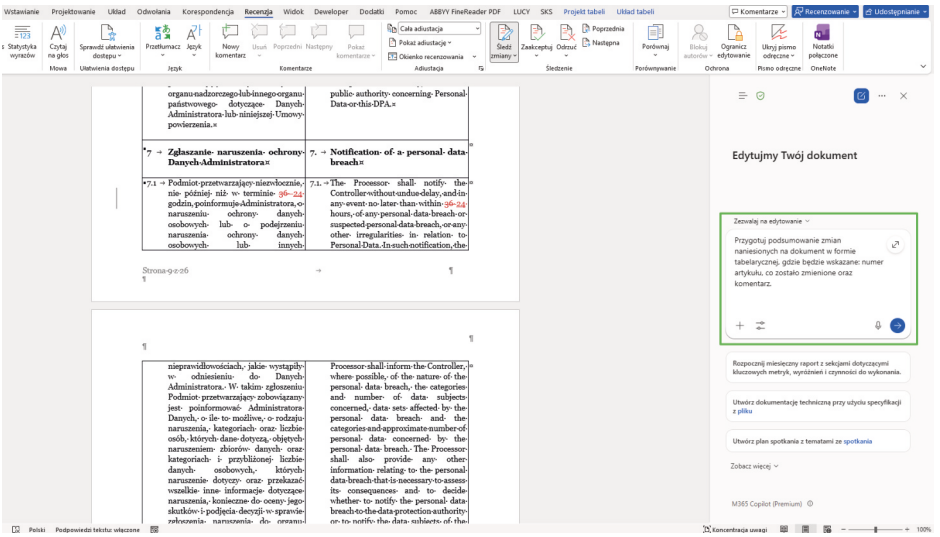
- Copilot generuje pytania, które może zadać klient, koncentrując się na ryzykach i lukach w analizie.



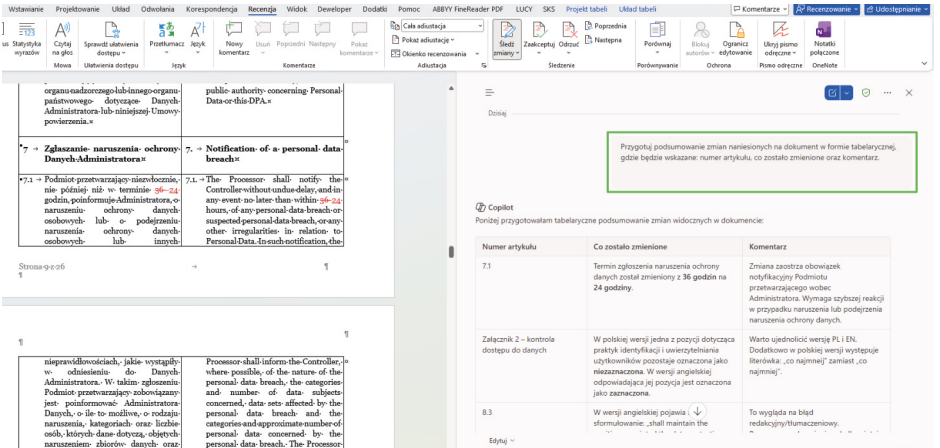
- Funkcja pozwala przygotować się na dyskusję z klientem i uzupełnić dokument o brakujące elementy.

PRZYKŁAD 13 – TABELARYCZNE PODSUMOWANIE ZMIAN W UMOWIE

- Otwórz dokument w Word: Włącz Śledzenie zmian, kliknij Copilot ➜ „Zezwalaj na edytowanie” i wpisz prompt: „Przygotuj podsumowanie zmian naniesionych na dokument w formie tabelarycznej, gdzie będzie wskazane: numer artykułu, co zostało zmienione oraz komentarz”.

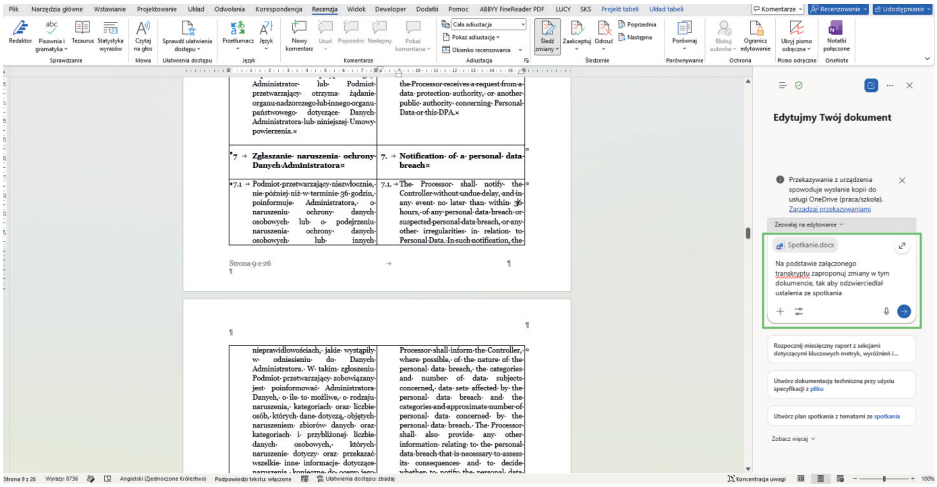


- W efekcie uzyskasz tabelę z numerem artykułu, zmianę i komentarz.

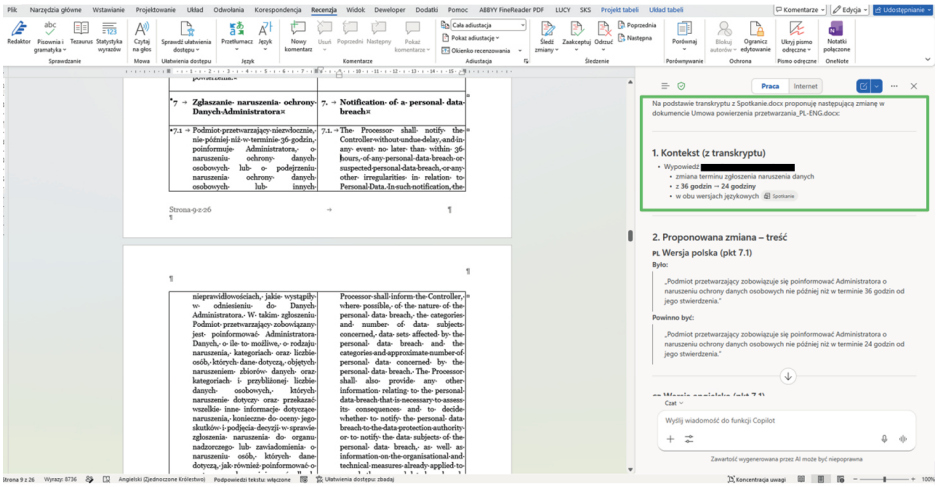


PRZYKŁAD 14 – AKTUALIZACJA DOKUMENTU NA PODSTAWIE TRANSKRYPCJI SPOTKANIA

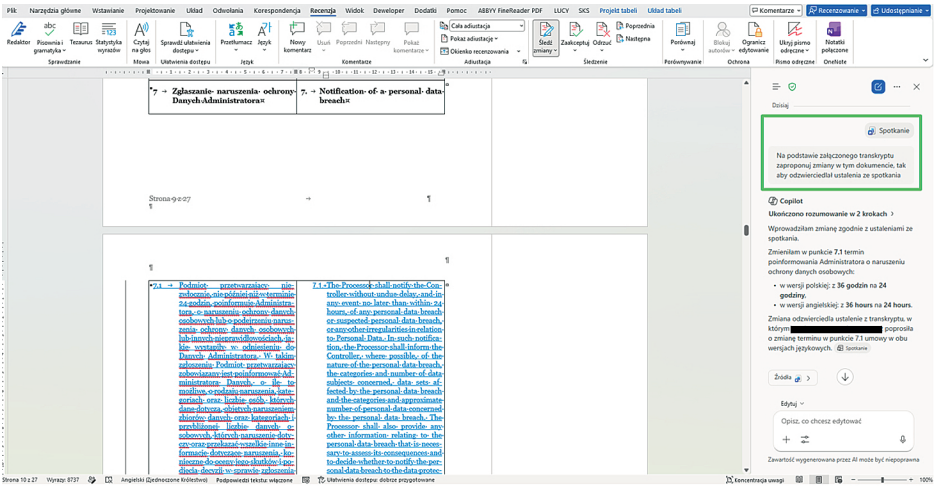
- W Word otwórz dokument, w Copilot kliknij „Przekaż” ➜ dodaj transkrypt, kliknij Copilot i wpisz prompt: „Na podstawie załączonego transkryptu zaproponuj zmiany w tym dokumencie, tak aby odzwierciedlały ustalenia ze spotkania”.



- W efekcie uzyskasz listę proponowanych zmian lub zmodyfikowany dokument (jeżeli użyjesz trybu edycji). Pamiętaj, żeby zweryfikować wprowadzone zmiany do dokumentu.

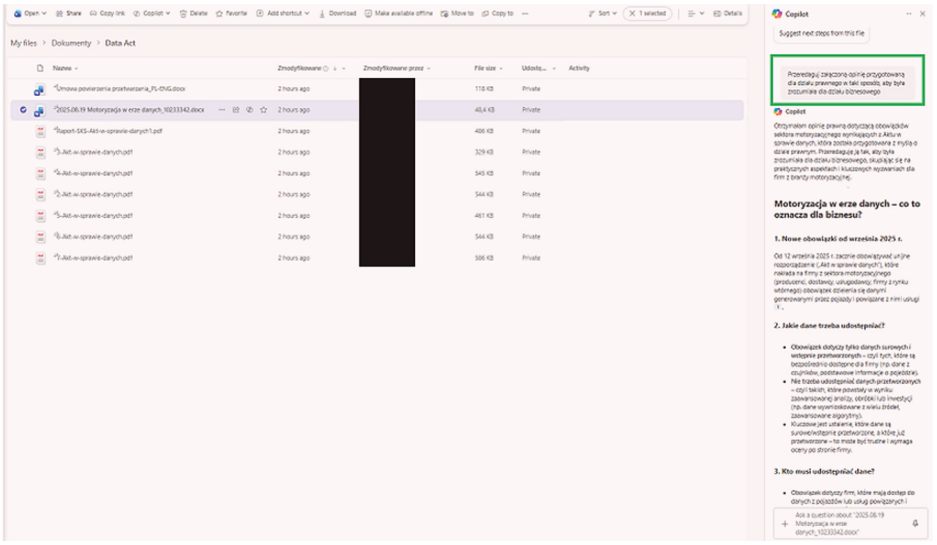


- Panel Copilot z propozycjami zmian + fragment dokumentu.



PRZYKŁAD 15 – ZMIANA JĘZYKA NA BARDZIEJ ZROZUMIAŁY

- Otwórz dokument w Word (zapisany na OneDrive), kliknij ikonę Copilot i wpisz prompt: „Przeredaguj załączoną opinię przygotowaną dla działu prawnego w taki sposób, aby była zrozumiała dla działu biznesowego”.

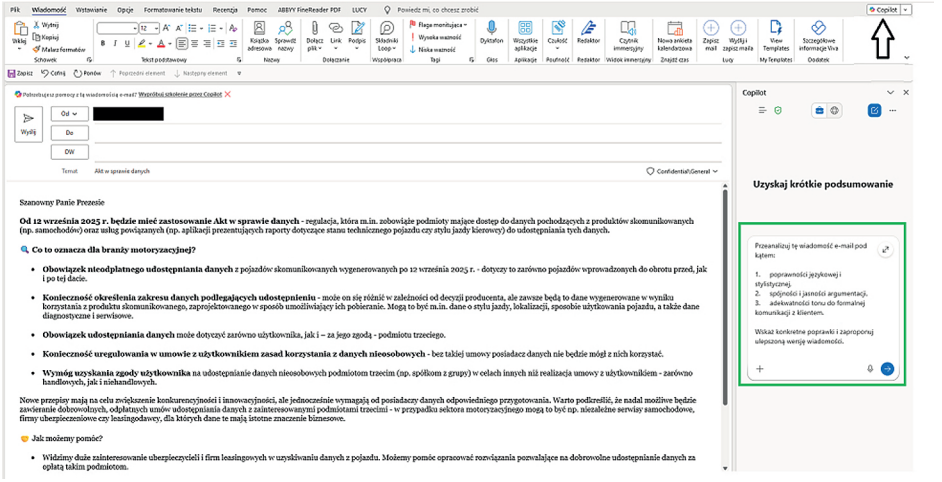


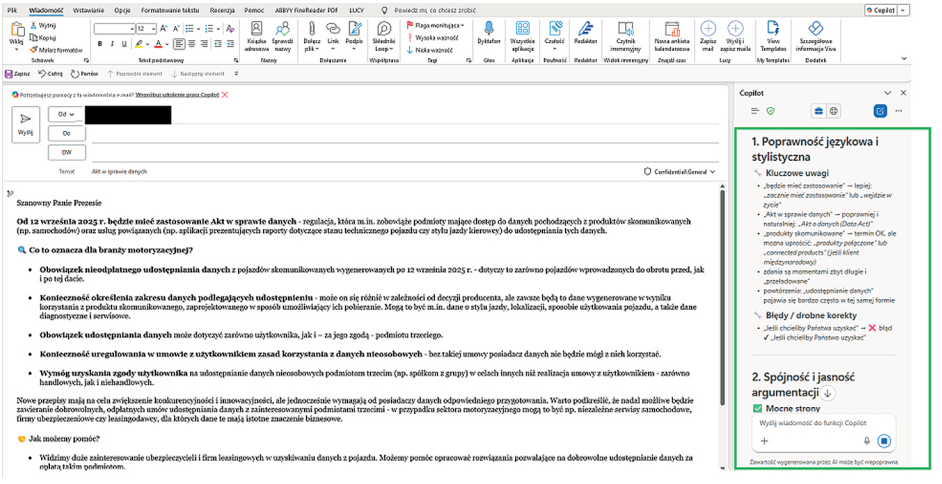
- W efekcie uzyskasz uproszczoną wersję opinii z jasnym wyjaśnieniem sytuacji, najważniejszymi ryzykami i konkretnymi działaniami do podjęcia.

PRZYKŁAD 16 – WERYFIKACJA PRZYGOTOWANEJ PROPOZYCJI ODPOWIEDZI

- Otwórz wiadomość w Outlook, kliknij ikonę Copilot i wklej lub zaznacz treść e-maila, następnie wpisz prompt: „Przeanalizuj tę wiadomość e-mail pod kątem:
  1. poprawności językowej i stylistycznej,
  2. spójności i jasności argumentacji,
  3. adekwatności tonu do formalnej komunikacji z klientem.

  Wskaż konkretne poprawki i zaproponuj ulepszoną wersję wiadomości”.





- W efekcie dostaniesz listę uwag (np. niejasne fragmenty, niespójności, zbyt potoczny język) i poprawioną wersję e-maila lub sugestie zmian.

PRZYKŁAD 17 – PRZYGOTOWANIE DOKUMENTU (TEAMS)

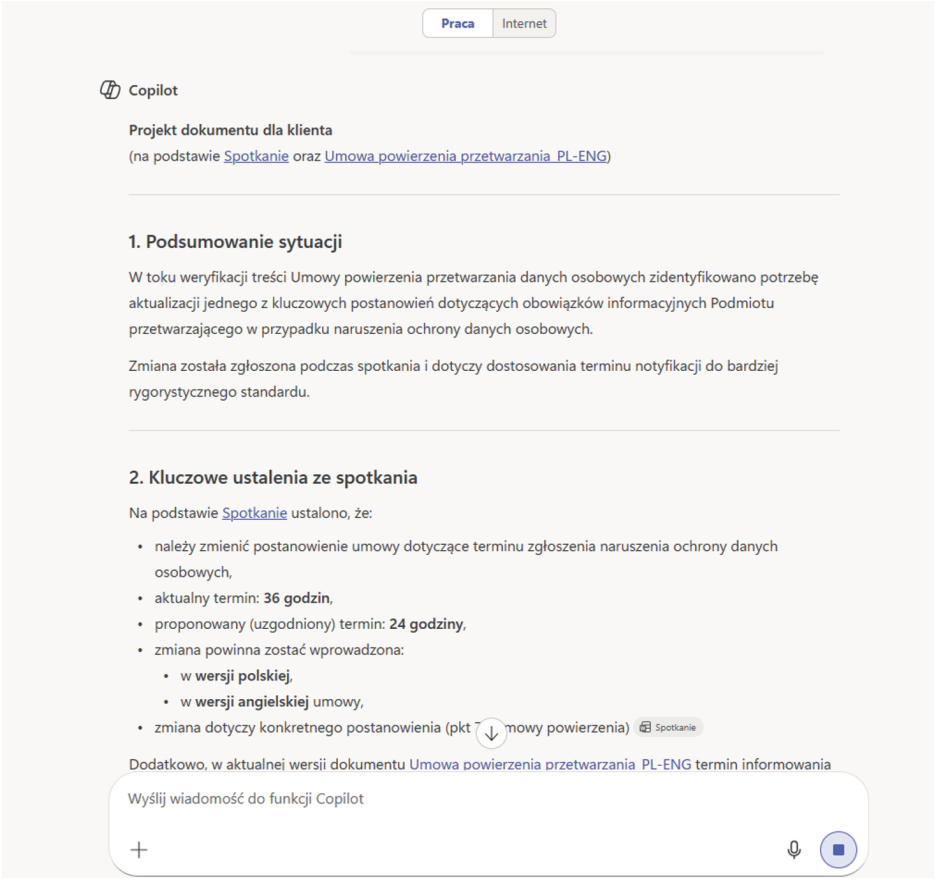
- Otwórz Copilot Chat w Teams (tryb „Praca"), kliknij „Przekaż" / „Dodaj pliki" i załącz dokumenty (np. transkrypt), i wpisz prompt: „Na podstawie załączonego transkryptu oraz materiałów przygotuj dla klienta projekt dokumentu podsumowującego ustalenia oraz rekomendowane działania. Uwzględnij:
  1. krótkie podsumowanie sytuacji,
  2. kluczowe ustalenia ze spotkania,
  3. zidentyfikowane ryzyka,
  4. rekomendacje.

  Użyj formalnego, profesjonalnego stylu".



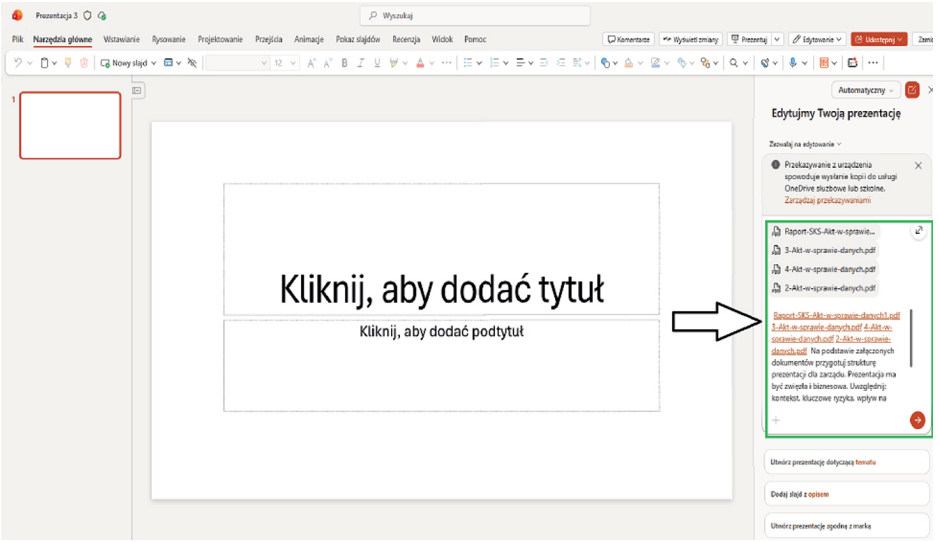
- W efekcie otrzymasz gotowy projekt dokumentu (np. notatki lub draft opinii), zawierający: uporządkowane ustalenia, wnioski i rekomendacje. Dokument może być bezpośrednio wklejony do Word lub wykorzystany jako podstawa komunikacji do klienta. Koniecznie sczytaj przygotowany projekt dokumentu.

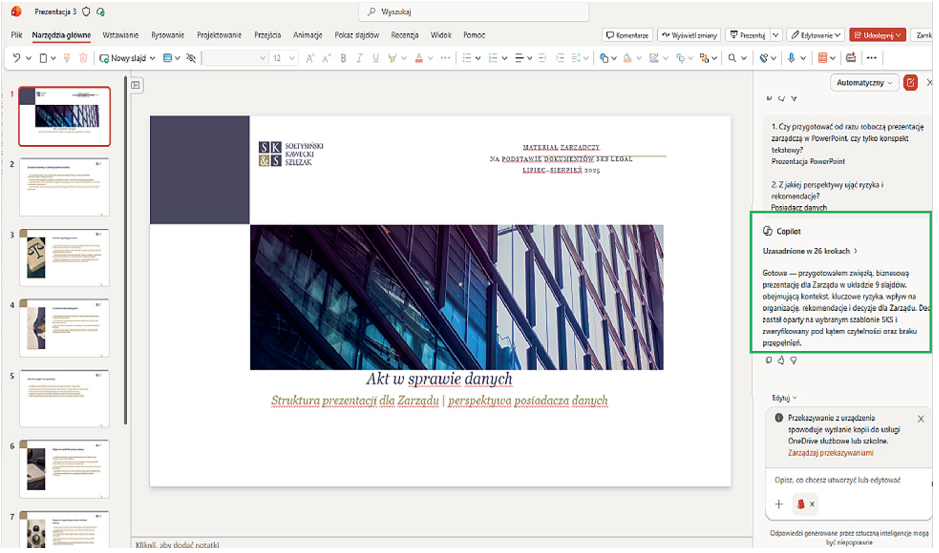
Załącznik nr 2



PRZYKŁAD 18 – PRZYGOTOWANIE PREZENTACJI PDF Z ISTNIEJĄCYCH DOKUMENTÓW

- Otwórz Copilot Chat w Teams (tryb „Praca") i otwórz PowerPoint, kliknij „Przekaż" / „Dodaj pliki", załącz dokumenty i wpisz prompt: „Na podstawie załączonych dokumentów przygotuj strukturę prezentacji dla zarządu. Prezentacja ma być zwięzła i biznesowa. Uwzględnij: kontekst, kluczowe ryzyka, wpływ na organizację, rekomendacje. Zaproponuj podział na slajdy wraz z tytułami i treścią punktową. Ogranicz się do najważniejszych informacji (maks. 8–10 slajdów)".
- W efekcie dostaniesz gotową strukturę prezentacji: podział na slajdy, tytuły slajdów, treść w punktach. Wynik można bezpośrednio wkleić do PowerPoint, używając funkcji „Utwórz prezentację z Copilot". Koniecznie sczytaj przygotowany projekt prezentacji.





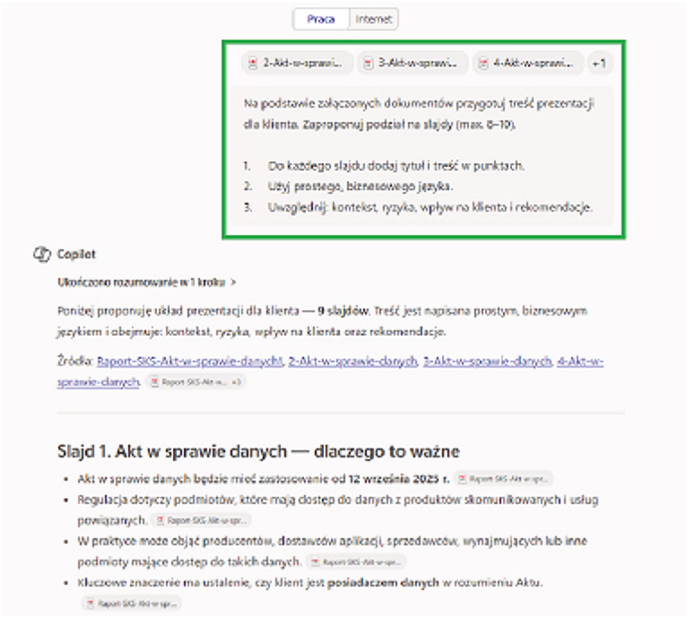
PRZYKŁAD 19 – PRZYGOTOWANIE PREZENTACJI W TEAMS

- Otwórz Copilot Chat w Teams (tryb „Praca”), kliknij „Przekaż” / „Dodaj pliki” i załącz dokumenty, wpisz prompt: „Na podstawie załączonych dokumentów przygotuj treść prezentacji dla klienta. Zaproponuj podział na slajdy (maks. 8–10).

1. Do każdego slajdu dodaj tytuł i treść w punktach.
2. Użyj prostego, biznesowego języka.
3. Uwzględnij: kontekst, ryzyka, wpływ na klienta i rekomendacje”.

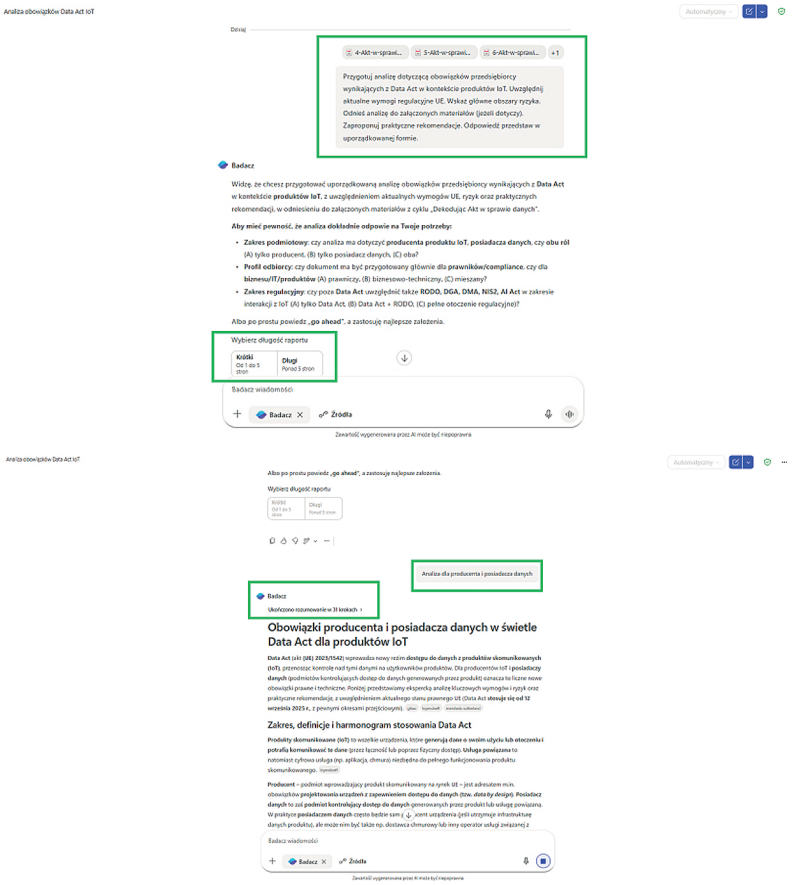
- W efekcie uzyskasz gotową treść prezentacji z listą slajdów, tytułami, punktami do każdego slajdu. Wynik można wkleić do PowerPoint lub wykorzystać do funkcji tworzenia prezentacji. Koniecznie sczytaj przygotowany projekt.





PRZYKŁAD 20 – DOSTĘP DO UDOSTĘPNIONYCH AGENTÓW, NP. BADACZA (I INNYCH)

- Otwórz Copilot Chat (tryb „Praca”), wybierz dostępnego agenta (np. „Badacz”/„Researcher”), (opcjonalnie) kliknij „Przekaż” i dodaj dokumenty, i wpisz prompt: „Przygotuj analizę dotyczącą obowiązków przedsiębiorcy wynikających z Data Act w kontekście produktów IoT. Uwzględnij aktualne wymogi regulacyjne UE. Wskaż główne obszary ryzyka. Odnieś analizę do załączonych materiałów (jeżeli dotyczy). Zaproponuj praktyczne rekomendacje. Odpowiedź przedstaw w uporządkowanej formie”.
- W efekcie uzyskasz pogłębioną analizę obejmującą: kontekst regulacyjny, odniesienia do zagadnienia, identyfikację ryzyk i rekomendacje. Uzyskany wynik ma charakter miniopinii prawnej i może być materiałem do dalszej pracy. Pamiętaj, że obowiązkowe jest zweryfikowanie otrzymanego materiału.

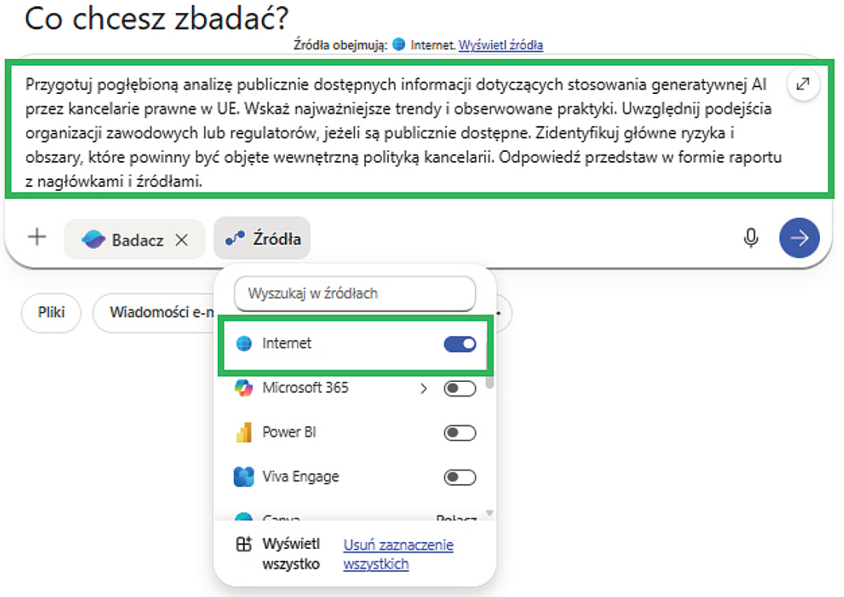


PRZYKŁAD 21 – GŁĘBOKIE BADANIE (OPCJA „INTERNET" I OPCJA „WEWNĘTRZNA")

Możesz przygotować pogłębioną analizę określonego zagadnienia. Możesz korzystać z sieci Web lub zawartości roboczej.

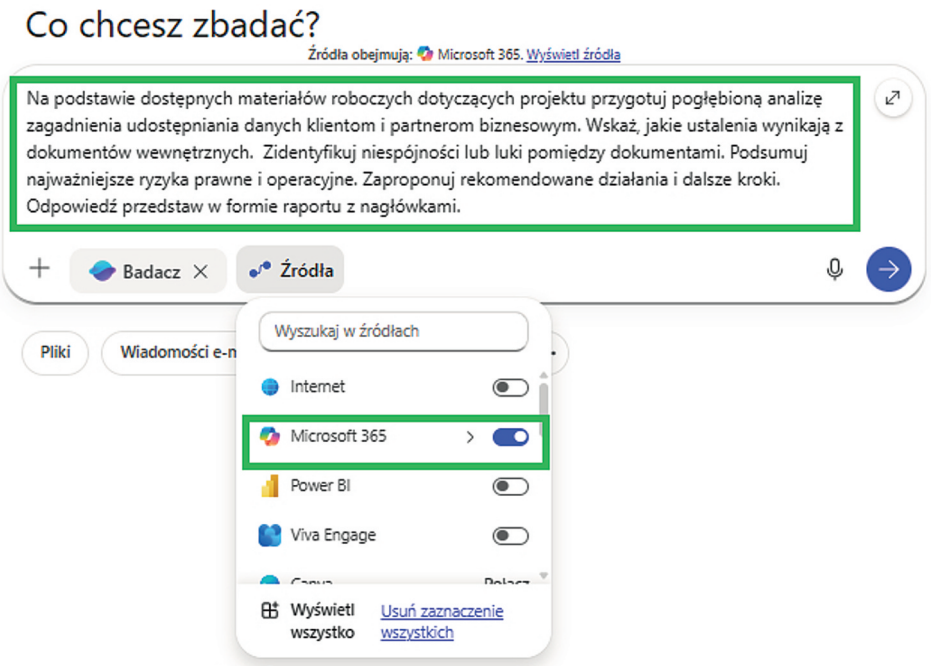
Opcja Internet – gdy radca prawny chce uzyskać syntetyczne opracowanie zagadnienia na podstawie publicznie dostępnych informacji, np. trendów rynkowych, komunikatów regulatorów, publikacji branżowych lub ogólnych informacji o nowych regulacjach. Funkcja Badacz pobiera i analizuje informacje z sieci Web oraz zwraca ustrukturyzowany raport ze źródłami.

- Otwórz aplikację Microsoft 365 Copilot. W obszarze Agenci wybierz Badacz, jeżeli w twojej wersji dostępny jest wybór zakresu źródeł, ustaw zakres na Internet i wpisz prompt: „Przygotuj pogłębioną analizę publicznie dostępnych informacji dotyczących stosowania generatywnej AI przez kancelarie prawne w UE. Wskaż najważniejsze trendy i obserwowane praktyki. Uwzględnij podejścia organizacji zawodowych lub regulatorów, jeżeli są publicznie dostępne. Zidentyfikuj główne ryzyka i obszary, które powinny być objęte wewnętrzną polityką kancelarii. Odpowiedź przedstaw w formie raportu z nagłówkami i źródłami".
- W efekcie uzyskasz raport opisujący zagadnienie na podstawie źródeł zewnętrznych, uporządkowane sekcje, źródła możliwe do weryfikacji.



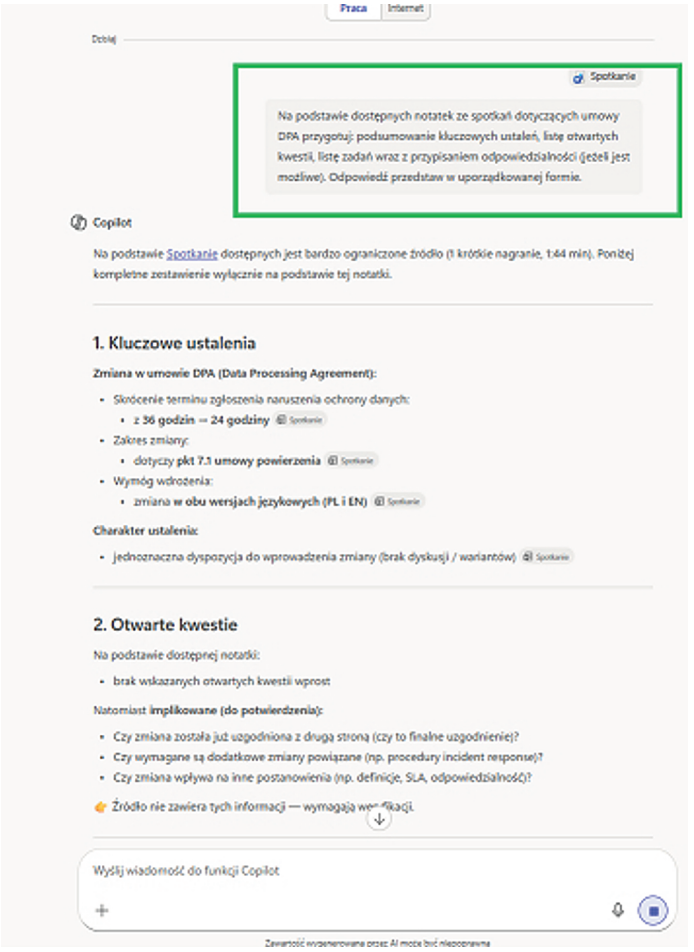
Opcja („Microsoft 365”) – gdy radca prawny chce przygotować analizę na podstawie dokumentów kancelarii lub klienta, np. wcześniejszych opinii, notatek, prezentacji, e-maili, materiałów roboczych lub ustaleń ze spotkań.

- Otwórz aplikację Microsoft 365 Copilot. W obszarze Agenci wybierz Badacz, jeżeli w twojej wersji dostępny jest wybór źródeł, ustaw zakres na Microsoft 365. Agent będzie miał dostęp do służbowych wiadomości e-mail, spotkań i czatów. Jeżeli chcesz oprzeć analizę na konkretnych dokumentach, możesz je dołączyć albo wskazać w prompcie zakres materiałów. Wpisz prompt: „Na podstawie dostępnych materiałów roboczych dotyczących projektu przygotuj pogłębioną analizę zagadnienia udostępniania danych klientom i partnerom biznesowym. Wskaż, jakie ustalenia wynikają z dokumentów wewnętrznych. Zidentyfikuj niespójności lub luki pomiędzy dokumentami. Podsumuj najważniejsze ryzyka prawne i operacyjne. Zaproponuj rekomendowane działania i dalsze kroki. Odpowiedź przedstaw w formie raportu z nagłówkami”.
- W efekcie uzyskasz raport oparty na materiałach wewnętrznych z podsumowaniem ustaleń, luk i ryzyk i z rekomendacjami do dalszej pracy.



PRZYKŁAD 22 – DOSTĘP DO NOTATEK (TEAMS)

- Otwórz Copilot Chat w Teams (tryb „Praca”), (opcjonalnie) kliknij „Przekaż” / „Dodaj pliki”, jeśli chcesz wskazać konkretne notatki (jeżeli nie, Copilot może sam sięgnąć do dostępnych materiałów), i wpisz prompt: „Na podstawie dostępnych notatek ze spotkań dotyczących umowy DPA przygotuj: podsumowanie kluczowych ustaleń, listę otwartych kwestii, listę zadań wraz z przypisaniem odpowiedzialności (jeżeli jest możliwe). Odpowiedź przedstaw w uporządkowanej formie”.
- W efekcie uzyskasz uporządkowane podsumowanie obejmujące: ustalenia ze spotkań, zadania, kwestie otwarte. Wynik może służyć jako: notatka projektowa, baza do e-maila do klienta lub materiał do dalszej pracy.



Załącznik nr 3

OBOWIĄZEK INFORMACYJNY DLA RADCY PRAWNEGO (ART. 13 I 14 RODO) – ELEMENTY DO WERYFIKACJI W ZWIĄZKU Z KORZYSTANIEM Z AI

Zależnie od stosowanego narzędzia radca prawny powinien zweryfikować i zaktualizować istniejącą politykę prywatności (obowiązek informacyjny), w szczególności fragmenty dotyczące:

- transferów danych poza Europejski Obszar Gospodarczy (czy stosowanie narzędzia AI wiąże się z transferem danych poza Europejski Obszar Gospodarczy, np. w związku z lokalizacją serwerów wykorzystywanych przez model AI);
- odbiorców danych (czy wykorzystanie narzędzi AI wiąże się z rozszerzeniem istniejącego katalogu odbiorców danych);
- retencji danych (czy narzędzie AI wiąże się z wprowadzeniem nowego okresu przechowywania danych, np. w związku z przechowywaniem historii czatów);
- informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (w sytuacji, w której korzystanie z narzędzi AI prowadzi do zautomatyzowanego podejmowania decyzji w rozumieniu art. 22 ust. 1 i 4 RODO, tj. wiąże się z podejmowaniem decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec osoby, której dane są przetwarzane, skutki prawne lub w podobny sposób istotnie na nią wpływa, np. scoring lub selekcja CV);
- celów i podstaw przetwarzania danych (jeżeli korzystanie z AI powoduje powstanie nowych celów przetwarzania, np. trenowania modeli).

Załącznik nr 4

WDROŻENIOWA LISTA SPRAWDZAJĄCA AI (RODO & AKT O AI)

Celem listy sprawdzającej (checklisty) jest wsparcie radcy prawnego w uporządkowanej ocenie najistotniejszych kwestii wymagających ustalenia przed rozpoczęciem korzystania z narzędzia AI. Lista ma pomóc w zweryfikowaniu, czy przed wdrożeniem narzędzia zostały zidentyfikowane i przeanalizowane podstawowe zagadnienia wynikające z RODO oraz Aktu o AI.

Lista ma charakter pomocniczy i może być dostosowywana do specyfiki ocenianego narzędzia AI, planowanego sposobu jego wykorzystania oraz potrzeb danej kancelarii lub zespołu prawnego. Listę należy uzupełniać odrębnie dla każdego ocenianego narzędzia AI.

Dla każdego pytania należy zaznaczyć odpowiedź: „Tak", „Nie" albo „Nie dotyczy", a także określić poziom istotności danego zagadnienia („wysoki", „średni" lub „niski") z perspektywy planowanego wdrożenia i korzystania z danego narzędzia AI. W kolumnie „Uwagi" można zamieścić dodatkowe informacje, wyjaśnienia lub wskazać działania wymagające podjęcia przed wdrożeniem narzędzia AI. Lista powinna kończyć się udokumentowaną decyzją: „dopuszczone", „dopuszczone warunkowo" albo „niedopuszczone", ze wskazaniem dopuszczonych zastosowań i danych, daty, osoby zatwierdzającej i terminu przeglądu. Zakazane zastosowanie, brak podstawy prawnej przetwarzania albo brak ochrony tajemnicy zawodowej wykluczają dopuszczenie narzędzia do danego zastosowania do czasu usunięcia przeszkody.

Nazwa narzędzia AI	
Nazwa dostawcy	
Adres dostawcy	
Strona internetowa dostawcy	
Planowany sposób wykorzystania narzędzia AI	
Data przeprowadzenia oceny	
Osoba przeprowadzająca ocenę	

RODO						
Lp.	**Pytanie kontrolne**	**Tak**	**Nie**	**Nie dotyczy**	**Poziom istotności**	**Uwagi**
I. Dostawca i jego rola w przetwarzaniu						
1.	Czy zapoznano się z polityką prywatności dostawcy i zweryfikowano zasady przetwarzania przez niego danych osobowych w ramach narzędzia AI?					
2.	Czy ustalono rolę dostawcy narzędzia AI w przetwarzaniu danych osobowych (podmiot przetwarzający / współadministrator / niezależny administrator)?					
II. Zakres danych i podstawa prawna						
3.	Czy określono, jakie kategorie danych osobowych (w tym ewentualnie szczególne kategorie danych) mogą być wprowadzane do narzędzia AI?					
4.	Czy zidentyfikowano podstawę prawną przetwarzania danych osobowych z wykorzystaniem narzędzia AI?					
III. Wykorzystanie danych do trenowania modelu						
5.	Czy ustalono, czy dane wprowadzane do narzędzia AI są lub mogą być wykorzystywane do trenowania lub dostrajania modelu (*fine-tuning*)?					
6.	Czy zweryfikowano możliwość wyłączenia wykorzystywania danych do trenowania lub dostrajania modeli AI?					

RODO						
Lp.	**Pytanie kontrolne**	**Tak**	**Nie**	**Nie dotyczy**	**Poziom istotności**	**Uwagi**
IV. Umowa z dostawcą i dalsze powierzenie przetwarzania danych						
7.	Czy ustalono, czy dostawca udostępnia umowę powierzenia przetwarzania danych osobowych (albo inną umowę odpowiednią do jego roli)?					
8.	Czy zweryfikowano zgodność takiej umowy z wymogami RODO?					
9.	Czy ustalono, czy dostawca korzysta z podmiotów podprzetwarzających i czy dostępna jest ich lista?					
10.	Czy ustalono zasady dalszego powierzania przetwarzania danych przez dostawcę, w tym czy administrator jest powiadamiany o zmianach podmiotów podprzetwarzających i może wyrazić sprzeciw?					
V. Lokalizacja przetwarzania i transfery danych poza EOG						
11.	Czy zweryfikowano, gdzie dane są przetwarzane, w tym czy przetwarzanie odbywa się na terenie EOG?					
12.	Czy sprawdzono, czy możliwe jest skonfigurowanie lokalizacji przetwarzania danych np. tylko do EOG?					
13.	Czy ustalono, czy dane osobowe będą transferowane poza EOG?					
14.	Czy zidentyfikowano państwa trzecie, do których może nastąpić transfer danych osobowych?					

RODO						
Lp.	**Pytanie kontrolne**	**Tak**	**Nie**	**Nie dotyczy**	**Poziom istotności**	**Uwagi**
15.	Czy ustalono mechanizm legalizujący transfer danych poza EOG (decyzja o adekwatności, standardowe klauzule umowne etc.)?					
16.	Czy oceniono, czy transfer danych poza EOG wymaga wdrożenia dodatkowych środków (technicznych, organizacyjnych, umownych)?					
17.	Czy ustalono, czy organy publiczne i podmioty trzecie mogą uzyskać dostęp do danych osobowych? Jeśli tak, czy wiadomo, jakie są zasady ujawniania danych przez dostawcę takim podmiotom?					
VI. Bezpieczeństwo danych osobowych						
18.	Czy zweryfikowano dostępność listy/informacji o środkach technicznych i organizacyjnych stosowanych przez dostawcę?					
19.	Czy oceniono adekwatność środków bezpieczeństwa stosowanych przez dostawcę (szyfrowanie, kontrola dostępu, uwierzytelnianie wieloskładnikowe, logowanie aktywności, separacja danych)?					
20.	Czy zweryfikowano możliwość usunięcia danych z narzędzia AI, w tym po zakończeniu korzystania z narzędzia?					

RODO						
Lp.	**Pytanie kontrolne**	**Tak**	**Nie**	**Nie dotyczy**	**Poziom istotności**	**Uwagi**
VII. Prawa podmiotów danych oraz zautomatyzowane podejmowanie decyzji						
21.	Czy przeanalizowano, czy korzystanie z narzędzia może prowadzić do zautomatyzowanego podejmowania decyzji lub profilowania?					
22.	Czy ustalono, czy dostawca umożliwia lub wspiera realizację praw podmiotów danych?					
VIII. DPIA i aktualizacja dokumentacji						
23.	Czy oceniono konieczność przeprowadzenia oceny skutków dla ochrony danych (DPIA) i udokumentowano wynik tej analizy?					
24.	Czy korzystanie z narzędzia AI wymaga aktualizacji dokumentacji ochrony danych osobowych (w tym polityk, rejestru czynności przetwarzania danych)?					
25.	Czy oceniono konieczność aktualizacji klauzul informacyjnych wobec osób, których dane mogą być przetwarzane z użyciem narzędzia AI?					
26.	Czy oceniono konieczność aktualizacji umów z klientami w zakresie przetwarzania danych osobowych?					
27.	Czy dokumentacja została zaktualizowana w wymaganym zakresie?					

Akt o AI						
Lp.	**Pytanie kontrolne**	**Tak**	**Nie**	**Nie dotyczy**	**Poziom istotności**	**Uwagi**
I. Weryfikacja wstępna						
1.	Czy sprawdzono, czy narzędzie jest systemem AI w rozumieniu Aktu o AI?					
2.	Czy potwierdzono, że radca prawny (kancelaria / zespół prawny) będzie korzystać z narzędzia AI jako podmiot stosujący oraz że nie występują okoliczności mogące skutkować uznaniem kancelarii lub radcy prawnego za dostawcę systemu AI wysokiego ryzyka (w szczególności oznaczenie systemu własną nazwą lub znakiem towarowym, istotna modyfikacja systemu albo zmiana jego przeznaczenia), a także że kancelaria nie udostępnia pod własną nazwą systemu AI innym osobom (np. czatbota dla klientów), co czyniłoby ją dostawcą także poza systemem wysokiego ryzyka?					
II. Dokumentacja i informacje niezbędne do oceny						
3.	Czy zidentyfikowano wszystkie dokumenty składające się na umowę dotyczącą korzystania z systemu AI oraz ustalono ich obowiązującą wersję?					
4.	Czy zgromadzono informacje i dokumenty niezbędne do oceny systemu AI (w szczególności					

Akt o AI						
Lp.	**Pytanie kontrolne**	**Tak**	**Nie**	**Nie dotyczy**	**Poziom istotności**	**Uwagi**
4.	dokumentację dostawcy, instrukcję obsługi, informacje o przeznaczeniu systemu AI, informacje dotyczące zgodności narzędzia z Aktem o AI)?					
III. Klasyfikacja poziomu ryzyka						
5.	Czy dokonano klasyfikacji narzędzia AI pod kątem poziomu ryzyka zgodnie z Aktem o AI oraz udokumentowano jej wynik (ryzyko nieakceptowalne, wysokie ryzyko, ograniczone ryzyko lub minimalne ryzyko)?					
6.	Czy ustalono, czy system AI lub planowany sposób jego wykorzystania jest zakazaną praktyką w zakresie AI w rozumieniu art. 5 Aktu o AI?					
7.	Czy sprawdzono, czy system AI kwalifikuje się jako system wysokiego ryzyka zgodnie z art. 6 ust. 1 lub art. 6 ust. 2 Aktu o AI? *W przypadku odpowiedzi twierdzącej należy również wypełnić część VI listy*					
IV. Obowiązki w zakresie przejrzystości						
8.	Czy zweryfikowano, czy planowany sposób wykorzystania narzędzia AI wiąże się z obowiązkami transparentności wynikającymi z art. 50 ust. 3–4 Aktu o AI?					

Akt o AI						
Lp.	**Pytanie kontrolne**	**Tak**	**Nie**	**Nie dotyczy**	**Poziom istotności**	**Uwagi**
9.	W przypadku gdy system AI ma wchodzić w bezpośrednią interakcję z osobami fizycznymi – czy sprawdzono, czy osoby te będą informowane o tym, że prowadzą interakcję z systemem AI?					
10.	Czy zweryfikowano, czy narzędzie generuje lub modyfikuje treści syntetyczne (w tym deepfake) wymagające odpowiedniego oznaczania zgodnie z Aktem o AI? Jeśli tak, czy wdrożono oznaczenia lub inne ograniczenia?					
V. Zasady korzystania z systemu AI w kancelarii						
11.	Czy wdrożono wewnętrzne zasady korzystania z narzędzia AI w kancelarii (polityka korzystania z AI, reguły weryfikacji wyników, ograniczenia co do danych wprowadzanych do narzędzia)?					
12.	Czy zapewniono przekazanie użytkownikom informacji o ograniczeniach oraz ryzykach związanych z korzystaniem z narzędzia AI?					
13.	Czy zweryfikowano, jakie kompetencje są wymagane do bezpiecznego korzystania z narzędzia AI?					
14.	Czy zapewniono użytkownikom odpowiednie szkolenia, instrukcje lub wytyczne dotyczące korzystania z narzędzia AI?					

Akt o AI						
Lp.	**Pytanie kontrolne**	**Tak**	**Nie**	**Nie dotyczy**	**Poziom istotności**	**Uwagi**
VI. Obowiązki dotyczące systemów AI wysokiego ryzyka (część należy wypełnić wyłącznie w przypadku zakwalifikowania systemu AI jako systemu wysokiego ryzyka – zob. pytanie 7)						
15.	Czy zaplanowano wdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających korzystanie z systemu AI zgodnie z instrukcją obsługi dostawcy?					
16.	Czy wyznaczono osoby fizyczne sprawujące nadzór człowieka nad systemem, posiadające niezbędne kompetencje, przeszkolenie, uprawnienia i niezbędne wsparcie?					
17.	Czy zweryfikowano adekwatność i wystarczającą reprezentatywność danych wejściowych w stosunku do przeznaczenia systemu AI, w zakresie pozostającym pod kontrolą podmiotu stosującego?					
18.	Czy opracowano procedurę monitorowania działania narzędzia AI na podstawie instrukcji obsługi?					
19.	Czy przygotowano procedurę postępowania w przypadku stwierdzenia ryzyka w rozumieniu art. 79 Aktu o AI lub poważnego incydentu, obejmującą zawieszenie stosowania systemu oraz dokonanie wymaganych zawiadomień?					

Akt o AI						
Lp.	**Pytanie kontrolne**	**Tak**	**Nie**	**Nie dotyczy**	**Poziom istotności**	**Uwagi**
20.	Czy ustalono zasady przechowywania generowanych automatycznie rejestrów zdarzeń, w zakresie, w jakim pozostają pod kontrolą podmiotu stosującego, przez co najmniej sześć miesięcy?					
21.	Jeśli dotyczy: Czy zaplanowano poinformowanie pracowników i ich przedstawicieli o planowanym stosowaniu wobec nich systemu AI wysokiego ryzyka – przed jego wdrożeniem?					
22.	Czy w przypadku systemu wysokiego ryzyka objętego załącznikiem III, który podejmuje decyzje lub uczestniczy w podejmowaniu decyzji dotyczących osób fizycznych, przewidziano poinformowanie tych osób o wykorzystaniu systemu AI?					
23.	Czy zweryfikowano, czy wymagane jest przeprowadzenie oceny skutków systemów AI wysokiego ryzyka dla praw podstawowych (FRIA)?					
24.	Jeżeli wymagane jest przeprowadzenie FRIA – czy zaplanowano jej wykonanie przed wdrożeniem systemu AI?					

Akt o AI						
Lp.	**Pytanie kontrolne**	**Tak**	**Nie**	**Nie dotyczy**	**Poziom istotności**	**Uwagi**
25.	Czy zweryfikowano, czy planowany sposób wykorzystania systemu AI wysokiego ryzyka może wiązać się z obowiązkiem udzielania wyjaśnień osobom, których dotyczą decyzje podejmowane z wykorzystaniem tego systemu, zgodnie z art. 86 Aktu o AI?					

Załącznik nr 5

REJESTR WYKORZYSTYWANYCH NARZĘDZI AI

Rejestr jest wewnętrznym, centralnym wykazem wszystkich narzędzi AI wykorzystywanych w kancelarii radcy prawnego. Wspiera świadome i odpowiedzialne korzystanie z AI oraz pozwala na zgromadzenie w jednym miejscu najistotniejszych informacji dotyczących wykorzystywanych narzędzi. Rejestr powinien być aktualizowany na bieżąco, w szczególności w przypadku rozpoczęcia korzystania z nowego narzędzia AI lub zmiany sposobu jego wykorzystania. Wpis powinien obejmować co najmniej: plan lub wersję narzędzia, istotną konfigurację, dopuszczone zastosowania i kategorie danych (ze wskazaniem, czy narzędzie może być używane do informacji objętych tajemnicą zawodową), rolę radcy prawnego według Aktu o AI, informację, czy dostawca wykorzystuje dane do trenowania modeli lub do innych własnych celów, okres przechowywania historii pracy, lokalizację przetwarzania danych (w tym ich przekazywanie poza Europejski Obszar Gospodarczy), datę umowy powierzenia przetwarzania danych osobowych (art. 28 RODO), odesłanie do decyzji o dopuszczeniu (załącznik nr 4) oraz datę ostatniego przeglądu; różne zastosowania tego samego narzędzia mogą wymagać odrębnych wpisów.

Lp.	Nazwa narzędzia AI	Dostawca	Cel i przeznaczenie	Klasyfikacja poziomu ryzyka	Data wdrożenia	Data ostatniego przeglądu	Status	Dokumentacja	Właściciel biznesowy	Uwagi
	pełna nazwa narzędzia	*nazwa, adres i link do strony*	*krótki opis celu i sposobu wykorzystania*	*niedopuszczalne / wysokie / ograniczone / minimalne*	*DD.MM.RRRR*	*DD.MM.RRRR*	*oceniane / testowane / aktywne / zawieszone*	*link lub lokalizacja*	*imię, nazwisko i stanowisko*	*dodatkowe uwagi*
1.										
2.										
3.										
4.										
5.										
6.										
7.										
8.										
9.										
10.										



ISBN 978-83-980593-1-2

