

AI W PRACY RADCY PRAWNEGO



KRAJOWA IZBA
RADCÓW PRAWNYCH

WARSZAWA, 2025

AI W PRACY RADCY PRAWNEGO

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

Wydanie 1
Warszawa 2025



KRAJOWA IZBA
RADCÓW PRAWNYCH



Microsoft



SOŁTYSIŃSKI
KAWECKI
SZŁĘZAK

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

© Copyright by Microsoft sp. z o.o., 2025

ISBN 978-83-972004-4-9

Korekta: Aleksandra Sachanowicz-Wrzal

Skład i łamanie: Aleksandra Snitsaruk

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

Słowo wstępne

Rozwój narzędzi opartych na sztucznej inteligencji (AI) to zjawisko, które radykalnie zmienia sposób funkcjonowania wielu branż, w tym również świata prawniczego. Korzystanie z AI w pracy radcy prawnego przestało być kwestią wyboru i stało się naturalnym kierunkiem rozwoju zawodu. Nie istnieje jedno uniwersalne podejście do wykorzystywania AI w pracy prawnika – zakres i sposób korzystania z tych narzędzi zawsze będą zależały od specyficznych potrzeb danej kancelarii lub radcy prawnego.



Niezależnie od tego, czy AI będzie stosowana okazjonalnie jako wsparcie w analizie dokumentów lub orzecznictwa, czy stanie się istotnym elementem codziennej pracy, konieczne jest poznanie zasad jej bezpiecznego i świadomego wdrażania. Niniejsza publikacja nie tylko przybliża tematykę generatywnej AI, lecz także pomaga rozwiać ewentualne obawy i dostarcza praktycznych wskazówek, jak korzystać z nowych technologii bez naruszania zasad etyki zawodowej i bezpieczeństwa prawnego klientów. Świadome podejście do AI pozwala w pełni wykorzystać jej potencjał, jednocześnie minimalizując związane z nią ryzyko. Wraz z dynamicznym rozwojem technologii AI prawnicy muszą mierzyć się z nowymi wyzwaniami, takimi jak kwestie związane z ochroną danych, tajemnicy zawodowej czy odpowiedzialnością za treści generowane przez sztuczną inteligencję.

Warto podkreślić, że przedstawione rekomendacje nie są ostateczne – wraz z rozwojem AI będą one podlegały dalszej ewolucji i uściśleniu. Jesteśmy dopiero na początku drogi związanej z wdrażaniem tej technologii w praktyce prawniczej. W najbliższych latach pojawi się orzecznictwo, które zacznie kształtować praktyczne standardy stosowania AI, a regulacje dotyczące tej technologii staną się systematyczniejsze i precyzyjniejsze. Dlatego ta publikacja powinna być traktowana jako „żywy dokument”, którego treść będzie aktualizowana i dostosowywana do zmieniającego się otoczenia prawnego i technologicznego.

Mamy nadzieję, że przedstawione rekomendacje okażą się wartościowe w codziennej pracy radców prawnych. Ich zasadniczym celem jest bowiem praktyczna przydatność – dostarczenie konkretnych wskazówek, które pomogą bezpiecznie i efektywnie korzystać z narzędzi AI w codziennych zajęciach radców prawnych.

Włodzimierz Chróścik
Prezes Krajowej Rady Radców Prawnych

REKOMENDACJE PRZYGOTOWANE WE WSPÓŁPRACY Z:



KRAJOWA IZBA
RADCÓW PRAWNYCH

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

Microsoft sp. z o.o.

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



SOŁTYSIŃSKI
KAWECKI
SZLĘZAK

Sołtysiński Kawecki & Szlęzak Kancelaria Radców Prawnych
i Adwokatów Spółka Komandytowa

- Agata Szeliga – radca prawny, partner
- Sylwia Macura-Targosz – radca prawny, starszy prawnik
- Katarzyna Paziewska-Młodawska – radca prawny, starszy prawnik
- Anna Tujakowska – adwokat, senior counsel

W listopadzie 2022 r. po raz pierwszy publicznie udostępniono narzędzie generatywnej sztucznej inteligencji – ChatGPT. Sztuczna inteligencja stała się dostępna dla każdego, w tym dla prawników. Wkrótce pojawiły się pierwsze doniesienia o korzystaniu z tego narzędzia bez weryfikacji, w szczególności przez wskazywanie nieistniejących orzeczeń sądowych. Wywołało to dyskusję, czy prawnicy mogą korzystać z rozwiązań AI. Nie jest to jednak nowa dyskusja – podobne pytanie pojawia się wraz z każdą nową technologią. Jak pokazuje chociażby przykład chmury obliczeniowej (*cloud computing*), prawnicy mogą zgodnie z prawem i zasadami etyki korzystać z nowych technologii. Konieczne są jednak odpowiednie przygotowanie i kompetencje.

Spośród nowych technologii to właśnie AI wskazuje się jako tę, która może mieć najistotniejszy wpływ na zawody prawnicze. Już obecnie standardowe narzędzia pozwalają na generowanie w kilka minut materiałów dotyczących przygotowywanych przez aplikantów lub młodszych prawników. Nie ma już raczej wątpliwości, że AI spowoduje istotne zmiany w sposobie wykonywania zawodu, od kształcenia przez sposób i zakres doradztwa po rozliczenia z klientami. Celem tych rekomendacji jest właśnie ułatwienie radcom prawnym i prawnikom przygotowania się do stosowania AI w odpowiedzialny i zgodny z przepisami sposób.

Niniejsze rekomendacje składają się z dwóch części. Pierwsza zawiera podstawowe pojęcia i ogólne informacje o regulacjach dotyczących korzystania ze sztucznej inteligencji. Druga zawiera rekomendacje podzielone na trzy grupy:

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

..... SPIS TREŚCI

Rozdział I	7
SZTUCZNA INTELIGENCJA – PODSTAWOWE ZAGADNIENIA	
1. Czym jest AI?	7
2. Przykładowe dostępne narzędzia AI	12
3. Podstawowe pojęcia – generowanie i używanie (trenowanie) danych	14
4. AI a chmura obliczeniowa	16
5. Przykładowe zastosowania narzędzi generatywnej AI w pracy radcy prawnego	17
Rozdział II	18
PRZEPISY PRAWA – PODSTAWOWE REGULACJE	
1. Dane osobowe	18
2. Akt o AI	22
3. Prawo autorskie	23
4. Ogólne regulacje dotyczące stosunków umownych	25
5. Odpowiedzialność za produkty wadliwe	25
6. Cyberbezpieczeństwo	26
7. Regulacje dotyczące radców prawnych	27
8. Postępowanie karne	28
Rozdział III	29
KORZYSTANIE Z NARZĘDZI AI PRZEZ PRAWNIKÓW – KORZYŚCI, WYZWANIA I RYZYKA	
1. Korzyści	29
2. Wyzwania	30
3. Ryzyka	32
Rozdział IV	35
WYTYCZNE ZAGRANICZNYCH STOWARZYSZEŃ PRAWNIKÓW CO DO STOSOWANIA NARZĘDZI AI	
Rozdział V	37
REKOMENDACJE	
Załączniki	63
1. Wskazówki dotyczące optymalnego promptowania	63
2. Przykłady zastosowań AI (przy użyciu Microsoft 365 Copilot)	65

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 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. Wraz z pojawieniem się tzw. agentów możemy samodzielnie tworzyć rozwiązania bardziej dostosowane do potrzeb konkretnych prawników.

Rozwój i błyskawiczne upowszechnienie AI przyspieszyły prace nad określeniem prawnych zasad z jej korzystania. W dniu 13 czerwca 2024 r. zostało przyjęte Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. 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), określane w tych rekomendacjach również jako Akt o AI. Rozporządzeniu będą również towarzyszyły regulacje krajowe, które mają zapewnić odpowiednie wdrożenie i nadzór w państwach członkowskich UE (ustawa o systemach sztucznej inteligencji), oraz wytyczne, wyjaśnienia i kodeksy dobrych praktyk.

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. Kluczowym 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. Kluczowym elementem generatywnej AI są duże modele językowe (LLM; *large language models*), sieci neuronowe czy 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.

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 i doskonalenie modelu AI,
- tworzenie systemu AI.

Pierwszym krokiem jest zbieranie dużych zbiorów danych, które mogą pochodzić z różnych źródeł, w tym z Internetu lub zasobów określonych podmiotów (np. z książek, archiwów prasowych). 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 wnioskuje 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 wnioskuje 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 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 zaprojektowany do działania z różnym poziomem autonomii, który po wdrożeniu może wykazywać zdolność adaptacji. System ten, do wyraźnych lub dorozumianych celów, wnioskuje, jak generować na podstawie 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 AI¹. Wytyczne wskazują w szczególności przypadki, kiedy 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 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 modele generatywnej sztucznej inteligencji 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”². Przykładem systemu AI ogólnego przeznaczenia jest np. ChatGPT.

¹ Wytyczne KE, <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application> [dostęp: 9.04.2025 r.].

² Art. 3 pkt 66 Aktu o AI.

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 wytyczne dotyczące zakazanych praktyk w zakresie sztucznej inteligencji³. 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*), wysokiego poziomu solidności, bezpieczeństwa i dokładności (*accuracy, robustness and cybersecurity*).

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.

³ Wytyczne KE dostępne są tutaj: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act> [dostęp: 9.04.2025 r.].

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 ostrożności⁴.

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, zarządzaniu sprawami, badaniach prawnych i automatyzacji procesów biurowych. Przykładem takiego narzędzia jest aplikacja Harvey.

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

Możliwe jest też tworzenie przy pomocy tej aplikacji lub M365 Copilot tzw. agentów do wykonywania określonych zadań. W zależności od potrzeb agencji

⁴ Więcej informacji na temat podziału systemów AI znajdziesz np. tutaj: <https://digital-strategy.ec.europa.eu/pl/policies/regulatory-framework-ai> [dostęp: 9.04.2025 r.].

M365 Copilot pozwalają na dokładne zdefiniowanie materiałów źródłowych, skonfigurowanie agenta przy pomocy promptu, dodanie akcji oraz funkcji autonomicznych.

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 spotkań⁵.

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. 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. *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.

⁵ 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: 9.04.2025 r.]; przygotowywanie biuletynu dotyczącego regulacji: https://www.linkedin.com/posts/activity-7289592679540174848-o-75?utm_source=share&utm_medium=member_desktop&rcm=ACoAAAg7tOMBN9bZ4-CaP-cH3AcYwKF57_IBX5Q [dostęp: 9.04.2025 r.]; ułatwianie dostępu do informacji udostępnionych przez dział prawny: <https://www.microsoft.com/insidettrack/blog/boosting-efficiency-with-sharepoint-agents-how-our-microsoft-legal-team-is-helping-clients-find-answers-faster/> [dostęp: 9.04.2025 r.].

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

3.1. GENEROWANIE DANYCH

Najbardziej kluczowe pojęcia w tym zakresie:

- **prompt** – polecenie kierowane przez użytkownika, aby zainicjować tworzenie zawartości wyjściowej w dużych modelach językowych i generatywnej AI.
- **metaprompt** – to 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** – to 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)** – to 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)** – to wynik 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 są bardzo często wykorzystywane do trenowania modeli, co wynika np. z odnośników do źródeł danych, które zawarte są w wygenerowanej zawartości wyjściowej.

Możliwość trenowania modeli, zwłaszcza na danych objętych ochroną prawnoutorską, 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 eksploatacji 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 producenci modeli AI ogólnego przeznaczenia zobowiązani są, m.in. podczas procesu trenowania modeli AI, do przestrzegania europejskich standardów prawa autorskiego, a zatem również klauzuli opt-out.

- **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.

3.3. WSKAZÓWKI DOTYCZĄCE PROMPTOWANIA



ZAŁĄCZNIK NR 1

W **Załączniku nr 1** rekomendacji znajdują się praktyczne wskazówki dotyczące prawidłowego promptowania.

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)⁶.

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) usługa może być w pełni dostępna dla użytkownika w maksimum kilka godzin po zamówieniu.

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.

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

⁶ Art. 2 pkt 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/2854 z dnia 13 grudnia 2023 r. (Akt w sprawie danych).

o specyficzne wymagania związane z narzędziami AI, opisane w niniejszych rekomendacjach, co znacznie przyspieszy 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.

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.

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 RODO⁷ 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.

W przypadku budowy i trenowania na radcy prawnym będzie spoczywało zdecydowanie więcej obowiązków, w tym przede wszystkim właściwe zidentyfikowanie

⁷ 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.

podstawy prawnej przetwarzania danych osobowych zawartych w danych trenin-
gowych. 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 inteligencji⁸.

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

- przetwarzanie danych osobowych zawartych w zawartości wejściowej (prompt);
- przetwarzanie danych osobowych zawartych w zawartości wyjściowej (out-put);
- 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 zwer-
yfikować, czy ma odpowiednią podstawę prawną do takiego przetwarzania da-
nych 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 prze-
kazywane poza EOG;
- czy konieczne jest zawarcie umowy powierzenia przetwarzania danych (ko-
nieczna jest analiza, w jakiej roli występuje dostawca systemu AI – w roli
administratora lub współadministratora albo w roli podmiotu przetwarzają-
cego);
- czy wymagane jest wykonanie oceny skutków dla ochrony danych (DPIA);

⁸ Opinia Europejskiej Rady Ochrony Danych 28/2024 w sprawie niektórych aspektów ochrony da-
nych 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/opi-nion-board-art-64/opinion-282024-certain-data-protection-aspects_pl [dostęp: 9.04.2025 r.].

- 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 „wymyślane” (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 celu⁹.

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 dotyczy to będzie sytuacji, kiedy sztuczna inteligencja ma dostarczać wnioski (np. dane osobowe) na temat osób, których dane osobowe zostały użyte w celu jej wyszkolenia¹⁰.

⁹ Publikacja Information Commissioner's Office, *How to use AI and personal data appropriately and lawfully*, s. 9, <https://ico.org.uk/media2/migrated/4022261/how-to-use-ai-and-personal-data.pdf> [dostęp: 9.04.2025 r.].

¹⁰ Opinia Europejskiej Rady Ochrony Danych 28/2024 w sprawie niektórych aspektów ochrony danych związanych z przetwarzaniem danych osobowych w kontekście modeli sztucznej

1.3. 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. Ponadto zawartość wejściowa i wyjściowa są z reguły wykorzystywane wyłącznie w celu świadczenia usługi i nie są przechowywane (choć mogą być przechowywane tymczasowo w pamięci aplikacji do czasu uruchomienia przez aplikację funkcji czyszczenia pamięci).

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 zaangażowaniu 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**.

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: 9.04.2025 r.].

2. Akt o AI

Akt o AI wszedł w życie 1 sierpnia 2024 r. Większość przepisów będzie stosowana od 2 sierpnia 2026 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. zaczną być stosowane przepisy o organach nadzorujących przestrzeganie Aktu o AI, karach za jego łamanie oraz zasady zarządzania i obowiązki dotyczące modeli AI ogólnego przeznaczenia. Od 2 sierpnia 2026 r. Akt o AI w większości znajdzie zastosowanie – zaczną obowiązywać przepisy dotyczące systemów wysokiego ryzyka, m.in. w rekrutacji, finansach czy zarządzaniu infrastrukturą krytyczną. Przepisy dotyczące systemów AI wysokiego ryzyka, o których mowa w art. 6 ust. 1 Aktu o AI, będą stosowane od 2 sierpnia 2027 r.

Akt o AI nakłada obowiązki na różne podmioty zaangażowane w tworzenie, wdrażanie i używanie systemów AI. Akt o AI stosuje się też do różnych podmiotów: dostawców systemów AI¹¹, importerów, dystrybutorów, upoważnionych przedstawicieli oraz podmiotów stosujących¹². 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 zmienia 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

¹¹ 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).

¹² 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).

powoduje, że stosuje się do niego obowiązki dostawcy systemu AI wysokiego ryzyka (art. 25 ust. 1 pkt 3 Aktu o AI).

Na podmiocie stosującym ciężar przede wszystkim obowiązki w zakresie budowania kompetencji dotyczących AI (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. Dodatkowo na podmiocie stosującym ciężar w określonych przypadkach obowiązki w zakresie przejrzystości, o których mowa w art. 50 Aktu o AI, obejmujące m.in. konieczność informowania osób o wchodzeniu w interakcje z systemami AI czy o generowaniu lub modyfikacji (tzw. *deepfake*), a w przypadku gdy system AI służy do generowania materiałów graficznych, dźwiękowych, filmowych i tekstowych – obowiązek projektowania systemu AI w taki sposób, żeby automatycznie oznaczał generowany materiał jako sztucznie wygenerowany lub zmanipulowany. System AI ogólnego przeznaczenia nie może służyć zamawiającemu do realizacji zakazanych praktyk w zakresie AI (art. 5 Aktu o AI).

Krajowe regulacje w zakresie AI mają na celu m.in. zapewnienie wdrażania AI i nadzoru nad nią na poziomie krajowym.

3. Prawo autorskie

Polskie prawo autorskie uznaje za twórcę jedynie człowieka, a ochronie prawnoutorskiej podlega utwór, czyli każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia¹³. 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 prawnoutorskie 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 prawnoutorską;
- praw do zawartości wejściowej;
- praw do zawartości wyjściowej i możliwości jej wykorzystywania.

¹³ Art. 1 ust. 1 ustawy o prawie autorskim i prawach pokrewnych.

3.1. PODSTAWY DO KORZYSTANIA Z SYSTEMÓW AI

Zgodnie z definicją zawartą w Akcie o AI system AI to system maszynowy, który 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);
- 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. 1.3.2](#)) 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 stanowić utwór (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**¹⁴. W przypadku gdy AI 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 znajdują zastosowanie np. przepisy dotyczące odpowiedzialności za niewykonanie lub nienależyte wykonanie umowy.

5. Odpowiedzialność za produkty wadliwe

Nowa **dyrektywa** Parlamentu Europejskiego i Rady (UE) 2024/2853 z dnia 23 października 2024 r. w **sprawie odpowiedzialności za produkty wadliwe**

¹⁴ Rezolucja Parlamentu Europejskiego z dnia 20 października 2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji (2020/2015 (INI)).

i uchylenia dyrektywy Rady 85/374/EWG, która weszła w życie 8 grudnia 2024 r. i powinna zostać implementowana do polskiego porządku prawnego do 9 grudnia 2026 r., rozszerza w porównaniu z dotychczasowymi przepisami odpowiedzialność za produkty wadliwe w relacjach z konsumentami również na produkty cyfrowe (oprogramowanie, w tym oprogramowanie świadczone w modelu SaaS) czy dane. Przepisy wdrażające dyrektywę mogą znaleźć zastosowanie w przypadku np. oferowania klientom konsumentom chatbotów 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 obecnie nowelizowana **ustawa o krajowym systemie cyberbezpieczeństwa**¹⁵, której zadaniem jest implementacja do polskiego porządku prawnego przepisów dyrektywy NIS 2¹⁶. Zgodnie z dyrektywą NIS 2 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 ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usług¹⁷.

¹⁵ Projekt ustawy, <https://legislacja.rcl.gov.pl/projekt/123845404/katalog/13055217#13055217> [dostęp: 9.04.2025 r.].

¹⁶ 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). Dyrektywa powinna być implementowana do polskiego porządku prawnego do 17 października 2024 r.

¹⁷ Art. 8 projektu ustawy o krajowym systemie cyberbezpieczeństwa.

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 życia¹⁸.

Niezależnie od dyrektywy NIS 2 w niektórych przypadkach zastosowanie mogą też znaleźć przepisy sektorowe, np. **rozporządzenie DORA**¹⁹, 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**²⁰ 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 łańcuchy żywnościowe, 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 prawnej²¹, 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 prawnej²².

¹⁸ Art. 15 Aktu o AI.

¹⁹ 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.

²⁰ 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.

²¹ Art. 3 ust. 3 ustawy z dnia 6 lipca 1982 r. o radcach prawnych.

²² Art. 15 Kodeksu Etyki Radcy Prawnego (dalej: KERP).

Dochowanie tajemnicy zawodowej jest obowiązkiem radcy prawnego²³. Radca prawny obowiązany jest zabezpieczyć przed niepożądanym ujawnieniem wszelkie informacje objęte tajemnicą zawodową²⁴ w sposób adekwatny do charakteru, rodzaju i skali swojej działalności, otoczenia oraz rodzaju informacji będących tajemnicą zawodową i ryzyka ich ujawnienia²⁵. Radca prawny zobowiązany jest wykonywać czynności zawodowe sumiennie oraz z należyłą starannością uwzględniającą profesjonalny charakter działania²⁶.

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.

²³ Art. 9 KERP.

²⁴ Art. 23 KERP.

²⁵ § 3 Regulaminu wykonywania zawodu radcy prawnego.

²⁶ 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. Ryzyka związane z korzystaniem z narzędzi AI nie są specyficznymi ryzykami dla branży prawniczej, lecz mają charakter ogólny. 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 szybciej i efektywniej obsługiwać klientów, co pozwala im wyróżnić się na rynku i przyciągnąć nowych klientów. Wykorzystanie nowoczesnych technologii może przyciągnąć również klientów poszukujących innowacyjnych i nowoczesnych rozwiązań prawnych.
- **Oszczędność czasu i przyspieszenie procesów prawnych w organizacji** – narzędzia AI mogą znacząco skrócić czas potrzebny na realizację określonych projektów i procesów. Narzędzia AI mogą w znaczący sposób 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.

- **Poprawę jakości pracy** – AI nie tylko przyspiesza pracę radcy prawnego, lecz także redukuje ryzyko błędów ludzkich, co przekłada się na wyższą jakość świadczonych usług prawnych. 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 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).
- **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. Odnosnie 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 kluczowe znaczenie ma korzystanie z systemu AI zgodnie z instrukcją i jego przeznaczeniem. Umowa o świadczenie usług prawnych i przepisy dotyczące radców prawnych znajdują 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, np. może to dotyczyć ilustracji do opinii prawnej czy fragmentu lub elementu prezentacji. Kwestia ta ma znaczenie z perspektywy prawa autorskiego (zob. rozdz. II.3), ponieważ taka część pracy 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.

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

wobec klientów wynikającej z dyrektywy w sprawie odpowiedzialności za produkty wadliwe (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. Niezależnie od stosowania AI w praktyce prawniczej konieczne będzie wdrażanie rozwiązań pozwalających na identyfikację materiałów wygenerowanych przez AI lub zmodyfikowanych z pomocą AI w ramach procedury oceny dowodów w celu uniknięcia powołania się na dowód nieprawdziwy, ale wygenerowany przez AI (np. *deepfake* ze zdjęciem uszkodzonego przedmiotu przedstawiany jako dowód w postępowaniu dotyczącym wypłaty odszkodowania z umowy ubezpieczenia). Jest to obecnie utrudnione np. z uwagi na brak jednolitych standardów dotyczących oznaczania treści zmodyfikowanych za pomocą AI.

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**²⁷ 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. Jedną z przyczyn halucynacji są niedoskonałości danych treningowych. Jeśli zestaw danych treningowych jest niepełny lub obciążony uprzedzeniami, system uczy się nieprawidłowych korelacji i wzorców, co prowadzi do wytwarzania fałszywych treści. Kolejną przyczyną halucynacji może być tzw. przeuczenie modelu, czyli sytuacja, gdy algorytm zbyt precyzyjnie dopasowuje się do zestawu danych treningowych. W rezultacie model traci zdolność do uogólniania i poprawnego rozpoznawania nowych, nieznanych wcześniej wzorców.

²⁷ Przykładem halucynacji AI może być sprawa amerykańskich prawników, którzy do przygotowania pisma procesowego wykorzystali ChatGPT. Jak się okazało, AI zawarła w piśmie fikcyjne cytaty z orzeczeń sądowych i nieistniejące precedensy prawne. Prawnicy twierdzili, że nie zdawali sobie sprawy ze zdolności ChatGPT do generowania fałszywych informacji. Sąd ukarał prawników grzywną w wysokości 5 tys. dol., https://storage.courtlistener.com/recap/gov.uscourts.nysd.575368/gov.uscourts.nysd.575368.54.o_3.pdf [dostęp: 9.04.2025 r.].

- **Ryzyko nadmiernego polegania na AI (*overreliance on AI*)**²⁸ – 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 jako „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. Nadmierne korzystanie z AI może prowadzić też do utraty przez człowieka kompetencji realizowanych przez AI.
- **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 grup²⁹.
- **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

²⁸ Przykładem nadmiernego polegania na AI może być: (i) 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).

²⁹ Przykładem może być: (i) algorytm wykorzystujący AI do rekrutacji, który dyskryminował kobiety, <https://businessinsider.com.pl/firmy/strategie/amazon-zrezygnowal-z-algorytmow-w-rekrutacji-dyskryminowaly-kobiety/pp233ev>, 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.

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 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)**³⁰ – zidentyfikowane zostały specyficzne ryzyka bezpieczeństwa związane z AI, takie jak: zmiana promptu w celu wpływania na generowane odpowiedzi (*prompt injection*); zatrucie (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.
- **Ryzyko związane z zablokowaniem dostępu do usług na podstawie warunków konkretnego dostawcy** – 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 niewielkie ryzyko dla zawodów prawniczych.

³⁰ <https://owasp.org/www-project-top-10-for-large-language-model-applications/>.

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 AI³¹. 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:

- formalna opinia nr 512 Amerykańskiego Stowarzyszenia Prawników (ABA) z dnia 29 lipca 2024 r.³²;
- Międzynarodowe Stowarzyszenie Prawników (IBA), *The Future is Now. Artificial Intelligence and Legal Profession*, wrzesień 2024 r.³³;
- *European lawyers in the era of Chat GPT, FBE, Guidelines 2.0*, wrzesień 2024 r.³⁴;

³¹ 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).

³² https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf [dostęp: 9.04.2025 r.].

³³ <https://www.ibanet.org/document?id=The-future-is%20now-AI-and-the-legal-profession-report> [dostęp: 9.04.2025 r.].

³⁴ <https://www.fbe.org/nt-commission-guidelines-on-generative-ai/> [dostęp: 9.04.2025 r.].

- Przewodnik The Law Society (LS) z listopada 2023 r. – aktualizacja: sierpień 2024 r.³⁵

W wyżej 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.

³⁵ <https://www.lawsociety.org.uk/topics/ai-and-lawtech/generative-ai-the-essentials> [dostęp: 9.04.2025 r.].

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 kluczowe 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?

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.



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, 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) → samo połączenie z Internetem czy innymi systemami nie musi zwiększać ryzyka, idealnie radca prawny powinien mieć możliwość wyboru i ograniczenia takiego groundingu;
- 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.

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 zawartości wyjściowej i wejściowej (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.

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.



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.

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:

- 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 zawartych 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) → 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);

- środki techniczne i organizacyjne ochrony danych (np. szyfrowanie danych w przesyłce i danych magazynowanych, stosowanie przez dostawcę wieloskładnikowego uwierzytelnienia, rejestrowanie logów) → zawartość wejściowa i wyjściowa powinna być szyfrowana przynajmniej w przesyłce 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 będzie 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 ROSZCZENIAM 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. [pkt 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 są często dosyć oczywiste i nie rodzą ryzyka dla radców prawnych, np. użytkownik musi mieć prawo do zawartości wyjściowej (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 wartości wejściowej);
- 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);
- 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 (od mniej do bardziej kreatywnych). 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.



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.

REKOMENDACJA NR 9: OCENA PRZYDATNOŚCI ZASTOSOWANIA AGENTÓW AI W AUTOMATYZACJI PROCESÓW W ORGANIZACJI

Dlaczego: Agent AI to program komputerowy lub system oparty na sztucznej inteligencji, który jest zaprojektowany do wykonywania określonych zadań w sposób autonomiczny. Dzięki zaawansowanym algorytmom uczenia maszynowego agent AI może analizować dane, podejmować decyzje i uczyć się na podstawie doświadczeń. W praktyce agenci AI znajdują zastosowanie w wielu

dziedzinach, od obsługi klienta po zaawansowane systemy zarządzania procesami biznesowymi (wirtualni asystenci, chatboty, systemy rekomendacyjne czy autonomiczne roboty).

Agenci AI mogą zatem być wsparciem w automatyzacji rutynowych (czasochłonnych) zadań, co w konsekwencji pozwala zwiększyć efektywność pracy oraz poprawę jakości świadczonych usług. Mogą być wykorzystywani np. do monitorowania zmian w procesie legislacyjnym, przygotowywania scenariuszy spotkań na bazie wskazanych dokumentów itp.

Agenci AI mogą być tworzeni z wykorzystaniem standardowych narzędzi przez samych radców prawnych, bez konieczności angażowania programistów.

Jak: Radca prawny powinien zidentyfikować i 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.

W przypadku tworzenia agentów AI konieczne jest opisanie procesu tworzenia oraz ocena skutków pracy agenta AI. Dokumentacja agenta AI powinna być na bieżąco aktualizowana.



REKOMENDACJA: Przed wyborem narzędzia AI należy ustalić, czy daje ono możliwości tworzenia własnych agentów AI i na jakich zasadach.

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. 1.2.4](#)) – 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 zidentyfikować/dokonać oceny, czy w organizacji przydatne będzie trenowanie modeli AI na danych wewnętrznych, w szczególności udzielając odpowiedzi na poniższe 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 posiada 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.



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.

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 należyłą 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;
- 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).

Niezależnie od obowiązków wskazanych wprost w Akcie o AI radca prawny powinien ocenić, czy obowiązek wykonywania usług prawnych z należytą starannością również nie wymaga powiadomienia klienta o stosowaniu narzędzi AI oraz czy takie powiadomienie powinno nastąpić w sposób sformalizowany (np. w formie zapisu w umowie lub oficjalnego powiadomienia), czy też może być dokonane w toku bieżącego świadczenia usług (np. przed rozpoczęciem nagrania i transkrypcji spotkania w celu przygotowania jego podsumowania i listy

zadań za pomocą narzędzia AI). Podobnie jak w Akcie o AI ocena może bazować na ocenie ryzyka zastosowania takiego rozwiązania dla klienta.

Jak: Ocena, czy konieczne jest poinformowanie klienta o korzystaniu z narzędzi AI, i w przypadku odpowiedzi pozytywnej – o trybie powiadomienia, powinna w szczególności brać pod uwagę następujące okoliczności:

- czy radca prawnych zamierza korzystać z rozwiązań standardowych, służących usprawnieniu codziennej pracy i zwiększeniu jej efektywności, które nie są przeznaczone wyłącznie dla prawników, czy też ze specjalistycznych rozwiązań dla prawników → korzystanie ze standardowych rozwiązań zgodnie z ich przeznaczeniem, podobnie jak w przypadku innych standardowych rozwiązań informatycznych, nie powinno generować obowiązku informowania klientów (analogicznie jak klienci nie są informowani np. o standardowych systemach zarządzania dokumentami stosowanych przez kancelarie czy radców prawnych), ocena specjalistycznych rozwiązań powinna być dokonywana indywidualnie, biorąc pod uwagę ryzyko zastosowania takich narzędzi dla klienta;
- czy jest to rozwiązanie powszechnie dostępne na rynku i oferowane przez renomowanych dostawców, czy też jest to rozwiązanie w fazie testów lub przygotowywane dla radcy prawnego lub jego organizacji czy przez danego radcę prawnego lub jego organizację, bez weryfikacji przez niezależny podmiot → w przypadku rozwiązań powszechnie dostępnych oferowanych przez renomowanych dostawców ich używanie zgodnie z przeznaczeniem nie wymaga co do zasady informowania klientów, chyba że jest to rozwiązanie, które generuje wyższe niż przeciętne ryzyko dla klienta; w przypadku rozwiązań w fazie testów lub rozwiązań wewnętrznych należy ocenić ryzyko i rozważyć powiadomienie klienta;
- jakiego obszaru świadczonych usług/doradztwa będzie dotyczyć korzystanie z narzędzia AI, tj. czy narzędzie AI będzie używane do standardowych działań, czy też do specyficznych zadań powierzonych przez klienta, które mają lub mogą mieć wpływ na jego działalność (np. wykorzystanie AI do rekomendowania zawarcia ugody w istotnej sprawie i warunków takiej ugody lub przygotowania podsumowania wideokonferencji, podczas której omawiane mają być strategiczne kwestie dotyczące planowanej transakcji lub innego przedsięwzięcia, których ujawnienie może mieć znaczący wpływ na klienta) → jeśli chodzi o kwestie istotne dla działalności klienta, to rekomendowane jest co najmniej jego powiadomienie (zob. również [rekomendację nr 14](#)),

przy czym nie zawsze jest wymagane uregulowanie tej kwestii w umowie, np. w przypadku wideokonferencji dotyczącej strategicznych kwestii informacja może być przekazana ustnie i nagrana lub wcześniej przekazana mailem, co pozwala klientowi na wyrażenie sprzeciwu;

- charakter usług świadczonych przez radcę prawnego, np. doradztwo strategiczne, czy zaangażowanie konkretnego radcy prawnego ze względu na jego szczególne kwalifikacje, które miałyby przejąć nawet częściowo stosowane narzędzie AI → w takim przypadku rekomendowane jest powiadomienie o korzystaniu ze specjalistycznych narzędzi AI, które przejmowałyby częściowo funkcje powierzone takim prawnikom.

Jeśli radca prawny podejmie decyzję o konieczności powiadomienia klienta o korzystaniu z narzędzia AI, powinien wskazać, z jakiego narzędzia AI będzie korzystał oraz w jakim celu i zakresie. Radca prawny powinien na prośbę klienta udostępnić informacje o podjętych środkach zabezpieczenia i wynikach analizy narzędzia AI.



REKOMENDACJA: Radcowie prawni powinni dokonać przeglądu realizowanych usług oraz oceniać przy przyjmowaniu nowych zleceń, czy z uwagi na sensytywną naturę zlecenia lub rodzaj stosowanego narzędzia AI i jego planowane wykorzystanie konieczne jest powiadomienie klienta. Ocena powinna brać pod uwagę ryzyko dla klienta. Stosowanie standardowych narzędzi AI zgodnie z przeznaczeniem w rutynowych sprawach nie wymaga co do zasady powiadomienia klienta. W przypadku spraw istotnych, które w przypadku ujawnienia mogłyby niekorzystnie wpłynąć na klienta, radca prawny powinien powiadomić o korzystaniu i zakresie wykorzystania narzędzia. Radca prawny powinien ocenić, czy powiadomienie ma być formalne (np. w umowie) czy też może być dokonywane *ad hoc*, w zależności od konkretnej sprawy.

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

Dlaczego: AI jest technologią od stosunkowo niedawna dostępną publicznie. Charakteryzuje się też specyficznymi ryzykami, takimi jak halucynacje. Przepisy dotyczące AI, w tym Akt o AI, dopiero zaczynają być stosowane i rozwiązywania w nich przewidziane, w tym dotyczące kodeksów postępowania czy

oceny ryzyka, zapewne pozwolą zwiększyć komfort prawny korzystania z tych narzędzi.

Z powyższych względów radca prawny powinien ocenić, w jakich przypadkach, oprócz poinformowania klienta o wykorzystaniu narzędzi AI, zalecane jest pozyskanie zgody klienta na korzystanie z narzędzia AI.

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 klient angażuje konkretnego prawnika i oczekuje jego osobistego zaangażowania w daną sprawę → wykorzystanie narzędzi AI, które przejęłyby istotną część zadań takiego prawnika, powinno być uzgodnione z klientem, gdyż zwykle klient zgadza się ponieść wyższe honoraria, aby zapewnić sobie osobiste zaangażowanie określonej osoby;
- 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 w szczególności w przypadku, gdy klient wymagał osobistego zaangażowania konkretnego prawnika, a narzędzie AI ma przejąć istotną część tych funkcji; 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 KLIENTA

Dlaczego: 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 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).

Jak: Przy ocenie, czy korzystanie z narzędzia AI może wpływać na wynagrodzenie klienta 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 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 stosowanie AI może uzasadniać wprowadzenie opłaty pokrywającej koszty zastosowania narzędzia AI, zwłaszcza jeśli są to specjalistyczne narzędzia nabywane przez radcę prawnego na potrzeby tej konkretnej sprawy. 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.

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 kluczowe z kilku powodów:

- pozwala zapewnić zgodność z obowiązującymi przepisami prawnymi (np. Aktem o AI, RODO);
- pozwala zwiększyć bezpieczeństwo danych i ich poufność (w tym tajemnicę zawodową);
- 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, które powinny w szczególności zawierać:

- jasne określenie, do jakich zadań można wykorzystywać narzędzie AI, a do jakich jest to zabronione;
- określenie, jakiego rodzaju informacje czy dane 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 dotyczące kontroli zawartości wejściowej (inputu);
- zasady weryfikacji i walidacji zawartości wyjściowej (outputu) generowanej przez AI;
- zasady szkolenia personelu i podnoszenia kwalifikacji/dostępności materiałów szkoleniowych dla personelu;
- 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.



REKOMENDACJA: Przed rozpoczęciem korzystania z narzędzia AI należy opracować wewnętrzne rekomendacje/zalecenia/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 zapewniania osobom korzystającym z narzędzi AI kompetencji dotyczących AI z uwzględnieniem ich wiedzy technicznej, doświadczenia, wykształcenia i wykształcenia oraz kontekstu, w którym systemy AI mają być przez nich wykorzystywane. Przeszkolenie osób, które mają korzystać z narzędzia AI, spowoduje efektywniejsze wykorzystanie narzędzi AI, zmniejszenie błędów oraz zwiększenie bezpieczeństwa danych. Przeszkolony personel będzie świadomy swoich obowiązków, istniejących zagrożeń i wyzwań związanych z korzystaniem z narzędzi AI, a w konsekwencji bardziej skłonny do korzystania z narzędzia AI (budowanie zaufania do AI).

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, wykształcenia itp.);
- przygotować stosowne instrukcje/materiały szkoleniowe w tym zakresie;
- 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 AI, W TYM MODELI DEDYKOWANYCH (*FINE-TUNED MODELS*), ORAZ 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. Śledzenie oferty rynkowej w zakresie narzędzi AI przeznaczonych dla prawników, która na polskim rynku dopiero się pojawia, 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, 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 AI w szczególności w kontekście zmian wprowadzanych przez dostawcę narzędzia AI, w tym weryfikację zmian dokumentacji udostępnianej przez dostawcę narzędzia AI (regulaminów czy cenników), 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 AI przez użytkowników i ich uwagi;
- dokonywać regularnej analizy, czy narzędzie AI spełnia aktualne potrzeby organizacji; monitorować oferty rynkowe w zakresie narzędzi 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 AI w organizacji.



REKOMENDACJA: Należy regularnie dokonywać oceny stosowanych narzędzi AI, w tym modeli dedykowanych (*fine-tuned models*), oraz oferty rynkowej w zakresie narzędzi AI przeznaczonych dla prawników. 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/WYTTCZNYCH DOTYCZĄCYCH KORZYSTANIA Z NARZĘDZIA 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 narzędzia AI oraz je dostosowywać (*AI compliance*). W większych organizacjach należy wyznaczyć osoby odpowiedzialne po stronie radcy prawnego za to zadanie.

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

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

- pozwala na utrwalanie dobrych praktyk oraz dzielenie się doświadczeniami w zakresie korzystania z narzędzia 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.

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 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.

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;
- wskazanie bezpiecznej „lokalizacji” bazy wiedzy w infrastrukturze organizacji;
- strukturę bazy wiedzy/klucz, według jakiego 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, odośnie 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 AI oraz narzędzi AI, które były przedmiotem oceny, ale nie zostały ostatecznie wdrożone.

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 dyrektywy NIS 2 czy DORA (jeśli dotyczy), wymagają od organizacji w określonych przypadkach raportowania incydentów³⁶ oraz podejmowania

³⁶ 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 także 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

działań naprawczych (*corrective actions*³⁷) 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 kluczowe 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.



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.

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.

³⁷ Zobacz np. art. 20 Aktu o AI.

WSKAZÓWKI DOTYCZĄCE OPTIMALNEGO PROMPTOWANIA



- **Podaj kontekst:** Informuj Copilot o kontekście użytkownika, np. „Jestem prawnikiem” 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 promptów, aby móc je łatwo ponownie wykorzystać w przyszłości.
- **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:** Dziel zadania na mniejsze kroki, co pozwala lepiej kontrolować proces i uzyskać lepsze wyniki.
- **Dawanie wytycznych:** Wskaż, aby Copilot nie wymyślał treści, jeżeli nie będzie znał odpowiedzi na jakieś pytanie; niech cię o tym poinformuje.
- **Praca z dużymi dokumentami:** 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:

Załącznik nr 1

- » 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.

PRZYKŁADY ZASTOSOWAŃ AI (PRZY UŻYCIU MICROSOFT 365 COPILOT)



Poniżej znajdują się ogólny opis możliwości oraz bardziej szczegółowe przykłady z wykazem printscreenów.

WORD

- Podsumowanie dokumentów.
- Wstawianie propozycji klauzul umownych.
- Upraszczenie tekstów.
- Sprawdzanie pisowni.

OFFICE

- Przygotowanie propozycji odpowiedzi na e-mail.
- Podsumowanie historii korespondencji od danej osoby.

OPCJA COPILOT W TEAMS

- Możliwość przygotowania podsumowania dokumentów znajdujących się online.
- Możliwość przygotowania syntetycznej notatki z wielu dokumentów zapisanych w Onedrive.
- Przygotowanie porównania dokumentów.
- Przygotowanie podsumowania korespondencji od danej osoby lub w ciągu określonego czasu.

TEAMS

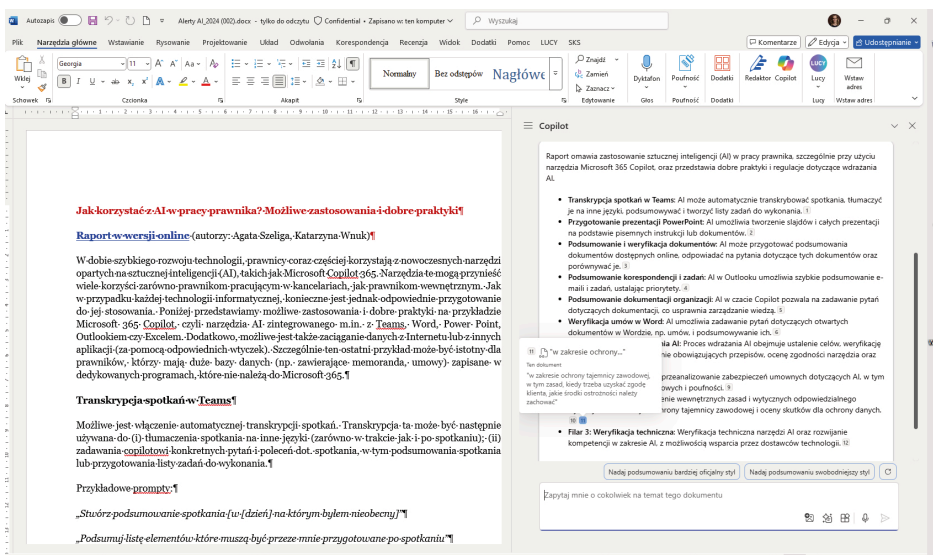
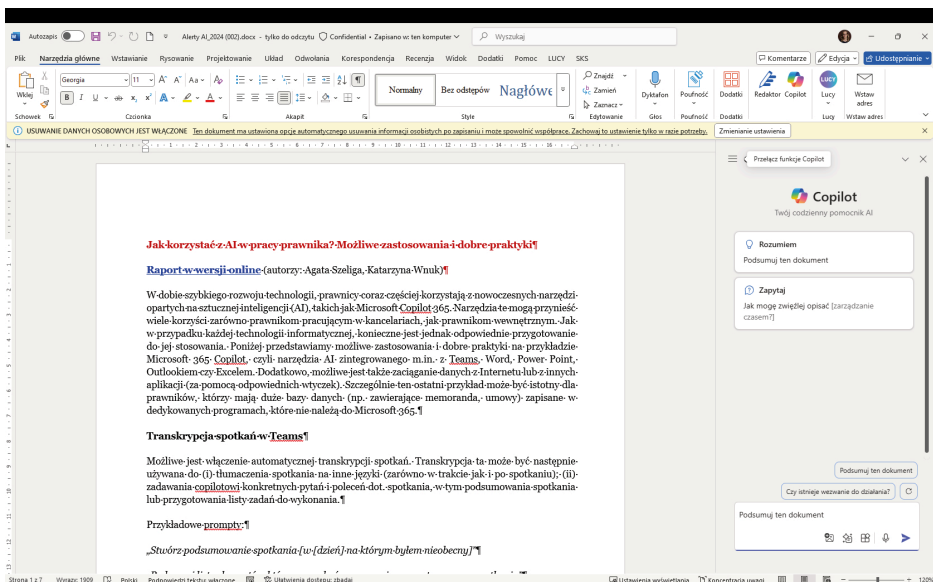
- Transkrypcja spotkań na żywo.
- Przygotowanie podsumowania spotkania i *to do list*.
- Dostęp do transkrypcji oraz nagrania, które wskazuje, w którym momencie dana osoba mówiła.

POWERPOINT

- Przygotowanie prezentacji na podstawie dokumentu Word.

PRZYKŁAD 1 – PODSUMOWANIE DOKUMENTU W WORD

- Kliknij ikonę Copilot i wpisz prompt „Podsumuj ten dokument”. Otrzymasz podsumowanie w *bullet-points*. Każdej informacji towarzyszy odnośnik, który wskazuje fragment tekstu, z którego pochodzi informacja.

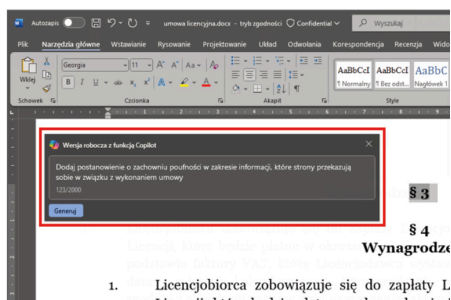
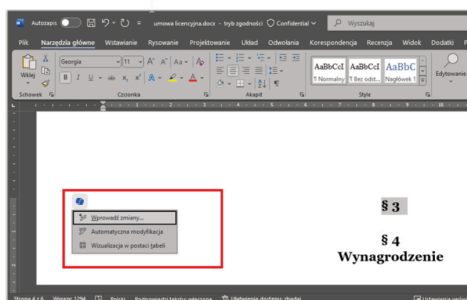


PRZYKŁAD 2 – MOŻLIWOŚĆ WSPÓŁPRACY Z COPILOT W WORD

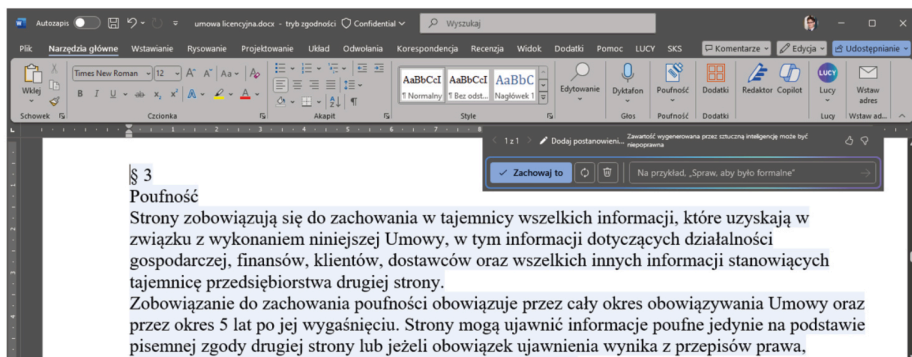
- Kliknij ikonę Copilot i wpisz prompt, np. poproś o zaproponowanie postanowienia, weryfikację językową zaznaczonego fragmentu itp.
- Zaproponowany tekst możesz zaakceptować, klikając „Zachowaj to”, lub poprosić o ponowne wygenerowanie innej propozycji.

Funkcjonalności M365 Copilot

Nie tylko chat – szereg funkcjonalności dostosowanych do poszczególnych programów Microsoft 365, w tym możliwość bezpośredniej edycji tekstu



Funkcjonalności M365 Copilot

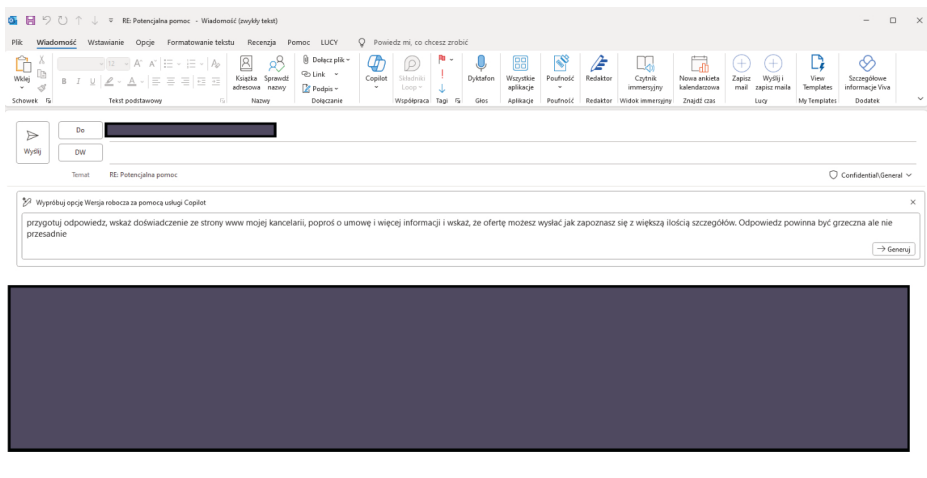


PRZYKŁAD 3 – PRZYGOTOWANIE ODPOWIEDZI NA E-MAIL

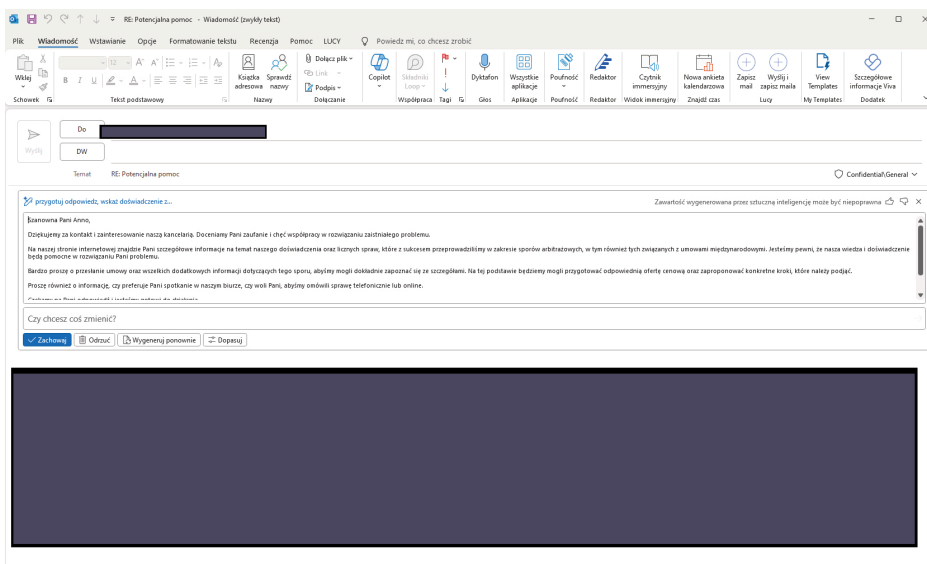
- Kliknij przycisk „Odpowiedz”, a następnie w ikonke Copilot „Wersja robocza z funkcją Copilot”.
- W okienku „Copilot” wpisz prompt, np. „przygotuj odpowiedź, wskaż doświadczenie ze strony WWW mojej kancelarii, poproś o umowę i więcej

Załącznik nr 2

informacji i wskaż, że ofertę możesz wysłać, gdy zapoznasz się z większą ilością szczegółów. Odpowiedź powinna być grzeczna, ale nieprzesadnie”. Następnie naciśnij ikonę „Generuj”.



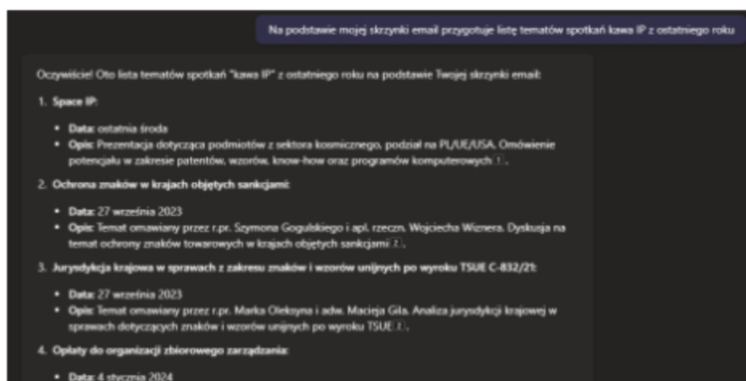
- W okienku „Copilot” otrzymasz projekt odpowiedzi, który możesz zachować, możesz poprosić o kolejną wersję lub dalej zmieniać/dopasować wygenerowaną odpowiedź. Pamiętaj, aby przed wysłaniem dokładnie przeczytać projekt.



PRZYKŁAD 4 – PODSUMOWANIE HISTORII KORESPONDENCJI OD DANEJ OSOBY

- W okienku „Copilot” 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.

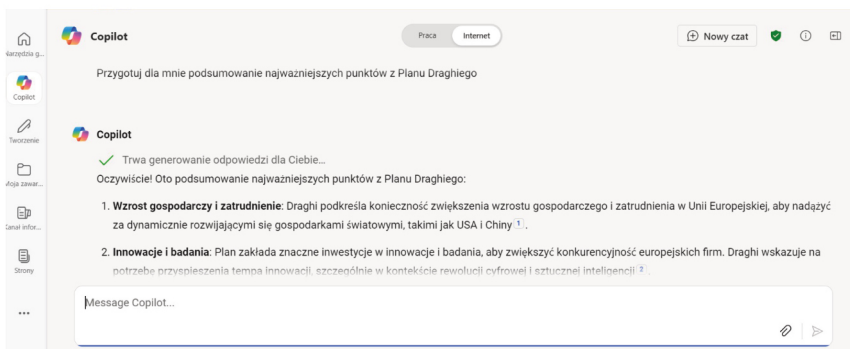
Zarządzanie skrzynką e-mail



PRZYKŁAD 5 – PODSUMOWANIE DOKUMENTÓW DOSTĘPNYCH ONLINE W TEAMS

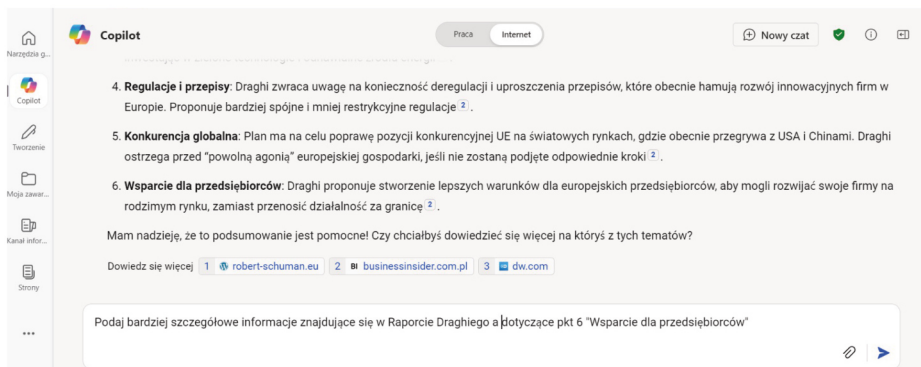
- Kliknij przycisk „Internet” i zadaj pytanie dotyczące treści dokumentu.

Podsumowania dokumentów



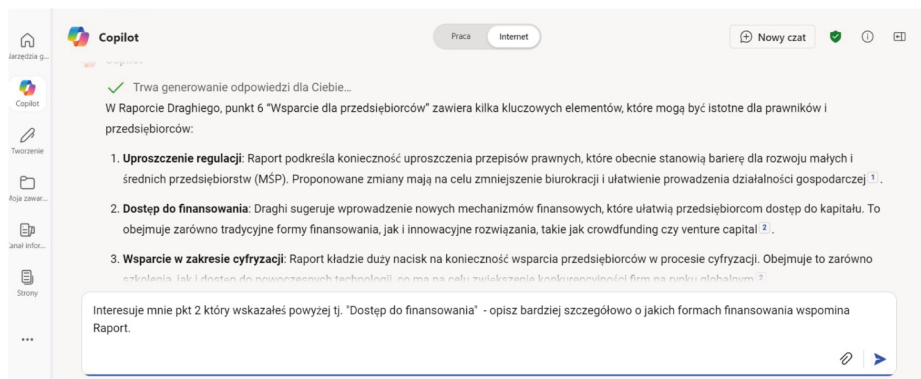
- Poproś o bardzo szczegółowe informacje.

Podsumowania dokumentów



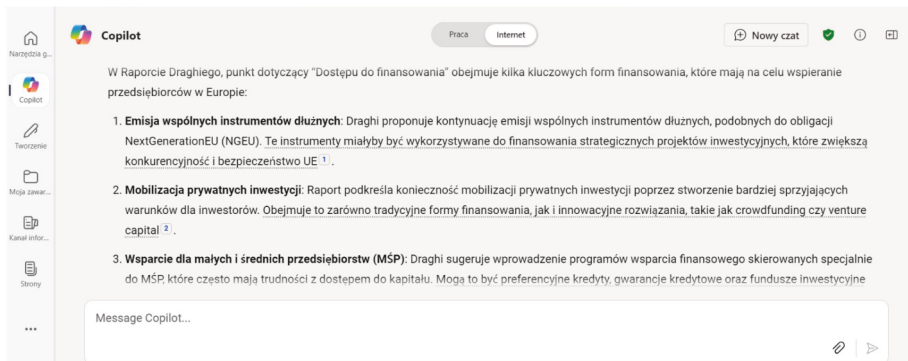
- Powtórz prośbę o dalsze, bardzo szczegółowe informacje.

Podsumowania dokumentów



- W razie potrzeby sprawdź źródło informacji podawanych przez Copilot (tekst podkreślony wraz z numerem przypisu).

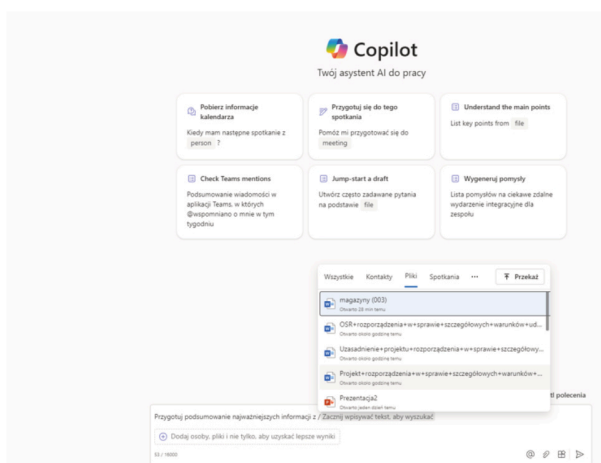
Podsumowania dokumentów



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 „Przełącz” wybierz dokument, z którego chcesz utworzyć podsumowanie.

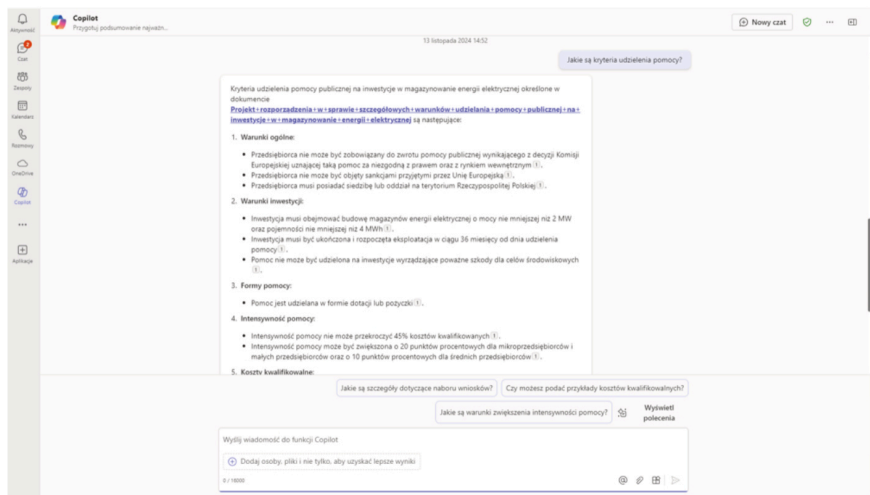
Podsumowania dokumentów



Załącznik nr 2

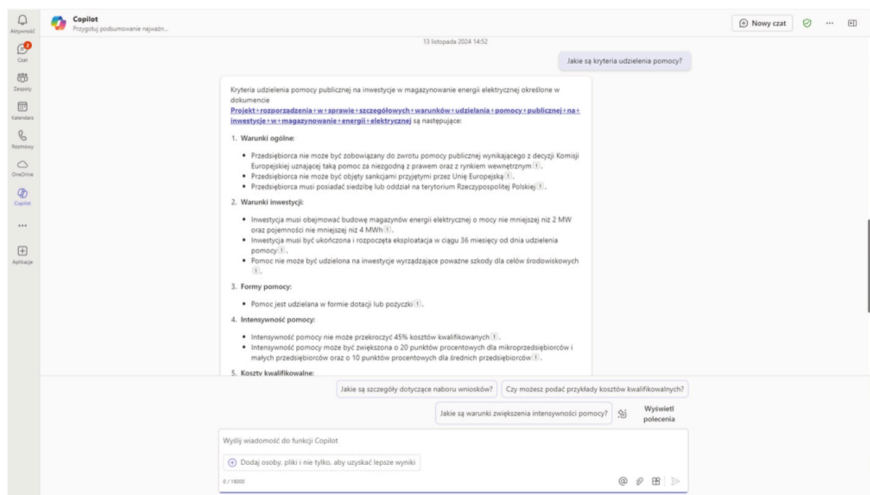
- Zadaj kolejne, bardziej szczegółowe pytania lub skorzystaj z pytania zaproponowanego przez Copilot.

Podsumowania dokumentów



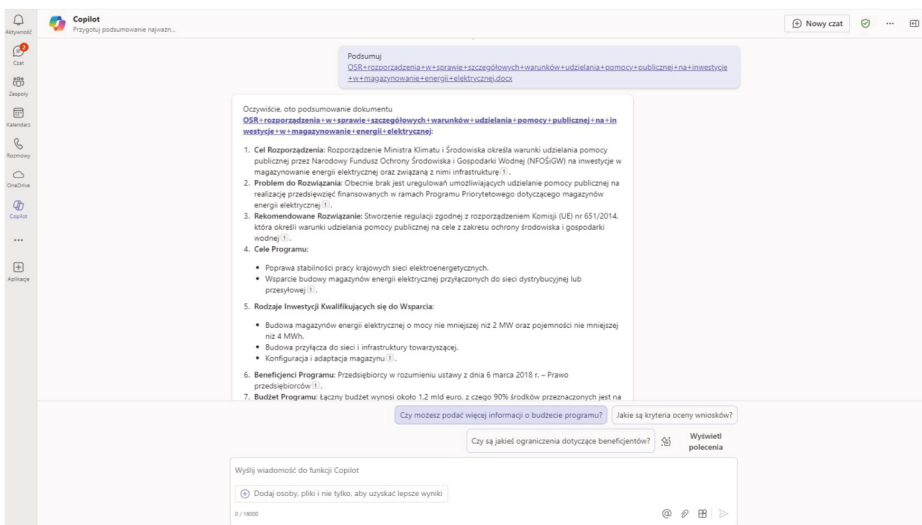
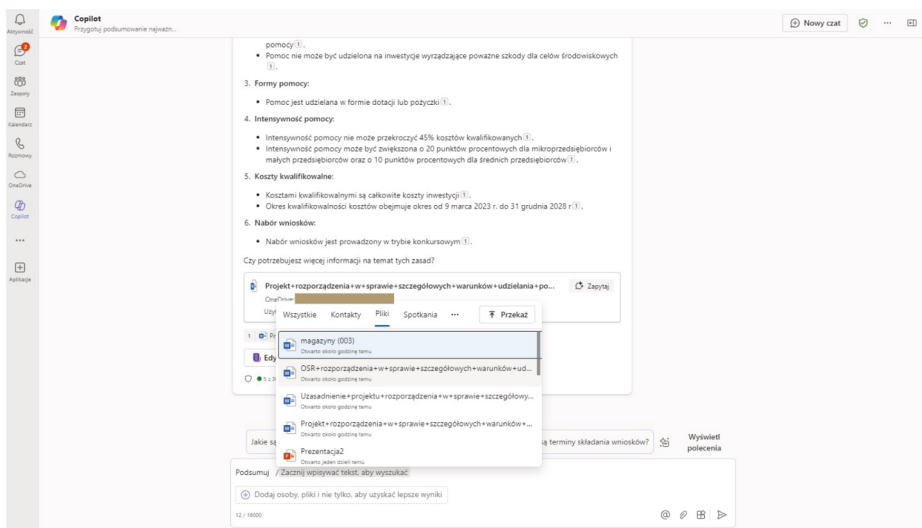
- Zadaj kolejne, bardziej szczegółowe pytania lub skorzystaj z pytania zaproponowanego przez Copilot. Budujesz w ten sposób bazę danych, które zostaną wykorzystane w podsumowaniu.

Podsumowania dokumentów



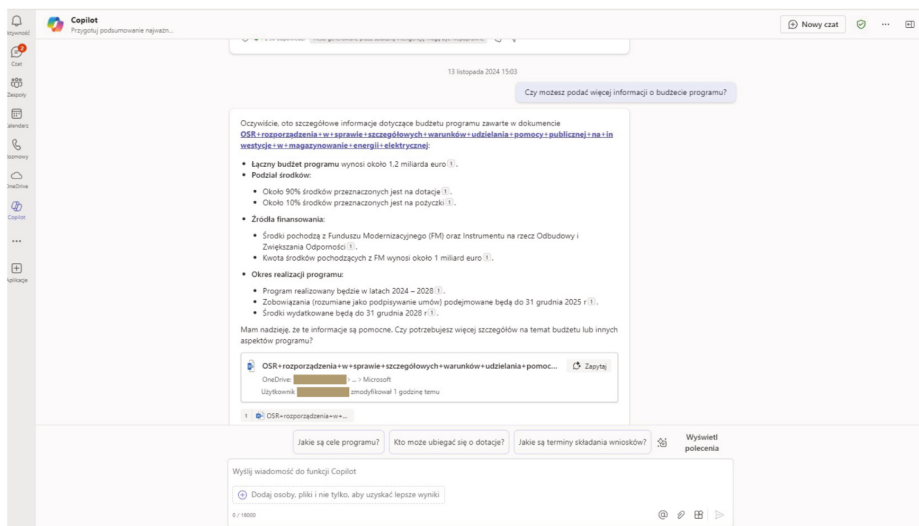
Załącznik nr 2

- Dodaj kolejny dokument (tutaj: Ocena skutków regulacji) i poproś o jego podsumowanie. Jest to kolejny etap budowania bazy danych, które zostaną wykorzystane w podsumowaniu.

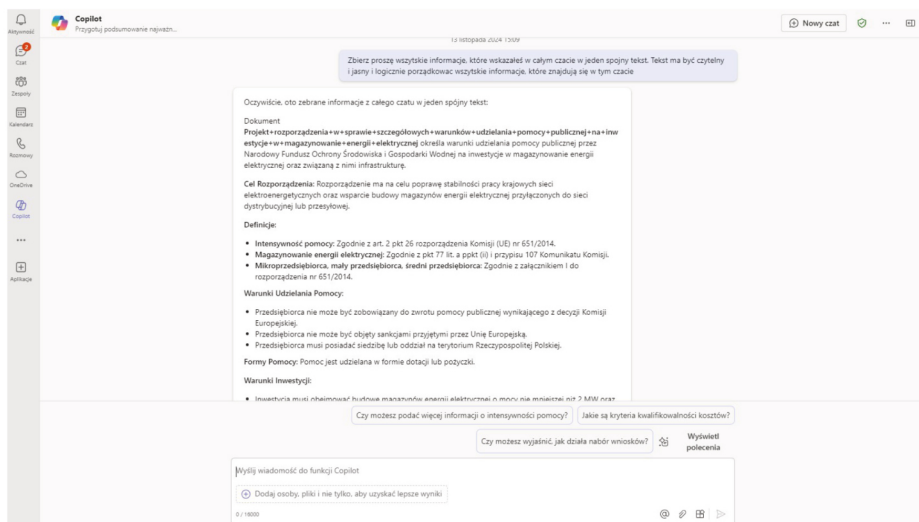


Załącznik nr 2

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

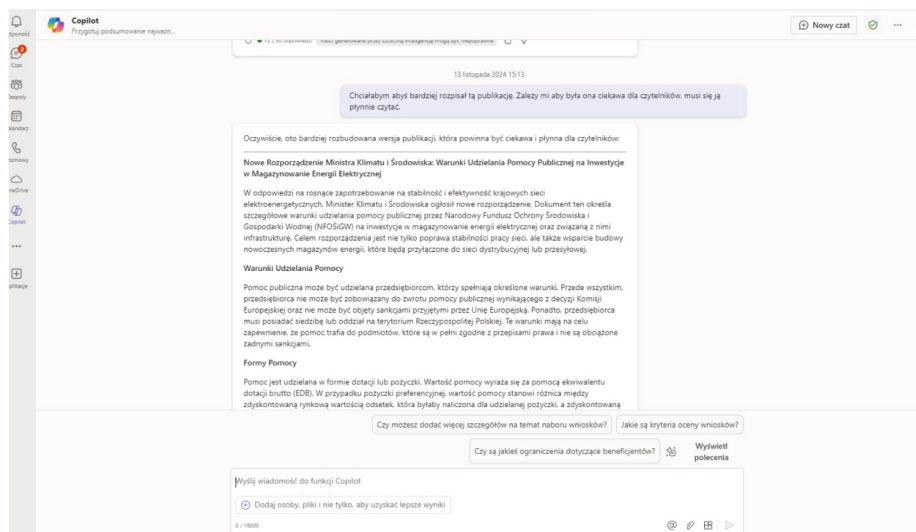
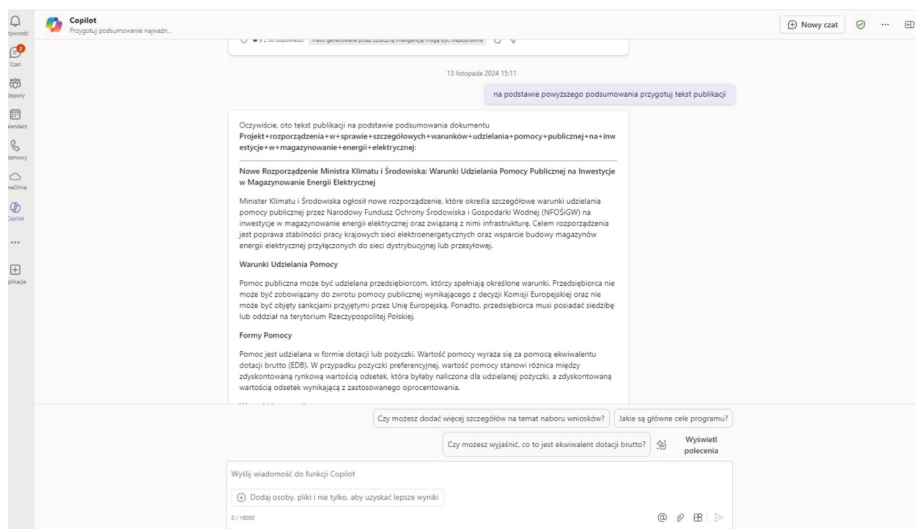


- Poproś o zebranie wszystkich informacji, które znajdują się w czacie, w jeden, spójny tekst. Wskaż, jaki ma być ton tekstu i inne wytyczne co do jego struktury.



Załącznik nr 2

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



Załącznik nr 2

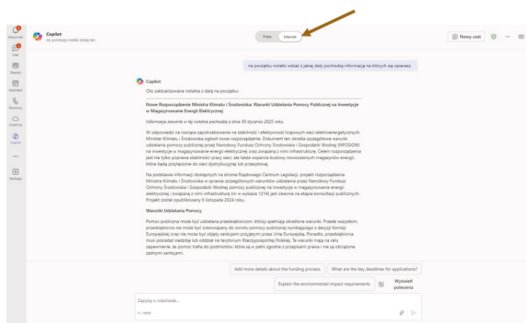
- Możesz rozbudować dokument o informacje znajdujące się w Internecie.

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 informacje 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

Przeanalizuj warunki umów w formie tabeli. Loan Agreement 2, 3.docx; Loan Agreement 3, 3.docx; Loan Agreement 1, 3.docx

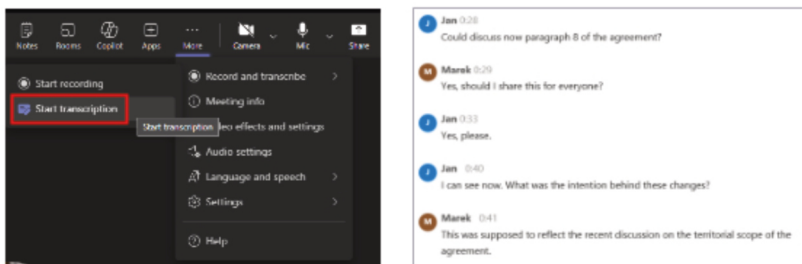
Oczywiście, oto porównanie warunków umów pożyczki zawartych w dokumentach Loan Agreement 2, 3.docx, Loan Agreement 3, 3.docx oraz Loan Agreement 1, 3.docx w formie tabeli:

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 AC
Pożyczkobiorca	Corporate Holding sp. z o.o.	CIVIL Group sp. z o.o.	MIRACLE SP. Z O.O.
Kwota główna	16,500,000.00 PLN	17,500,000.00 PLN	15,100,000.00 PLN
Oprocentowanie	8% rocznie	WIBOR 3M + 2% rocznie	WIBOR 3M + 2.4% rocznie
Data spłaty	6 miesięcy od dnia wypłaty pożyczki	2 lata od dnia wypłaty p. ocyzki	5 lat od dnia wypłaty p. ocyzki
Cel	Splata istniejących zobowiązań	Cele działalności gospodarczej	Zakup maszyn przemysłowych
Odstępki 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

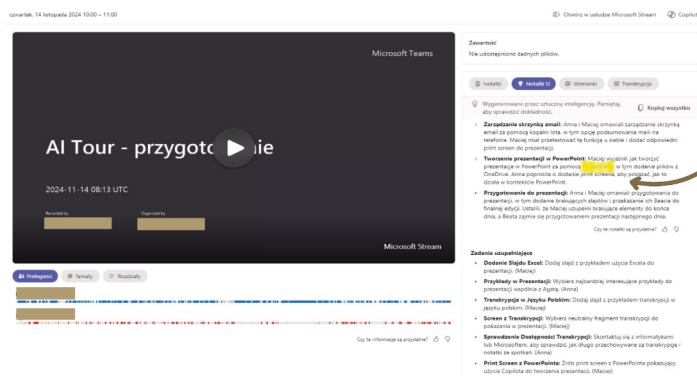
- Po włączeniu opcji „Rozpocznij transkrypt” transkrypt z rozmowy pojawi się w prawym pasku ekranu.

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 uczestnik ten 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 określiń w języku obcym. Koniecznie czytaj podsumowanie i listę zadań uzupełniających.

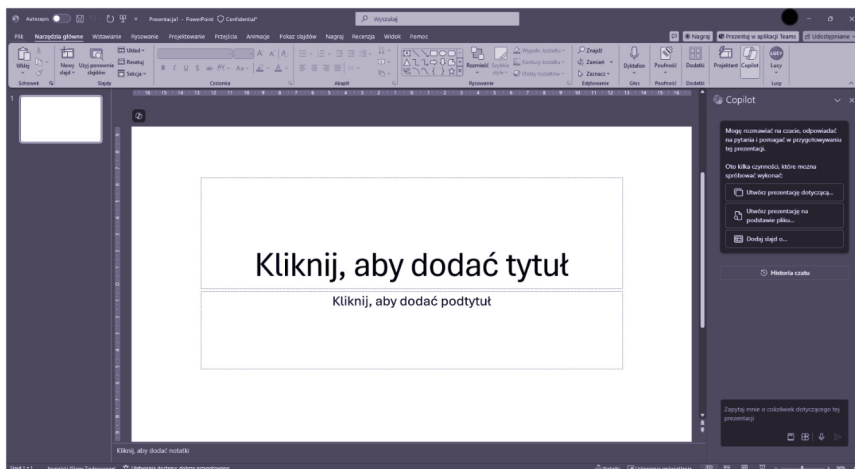
Podsumowanie spotkania w MS Teams



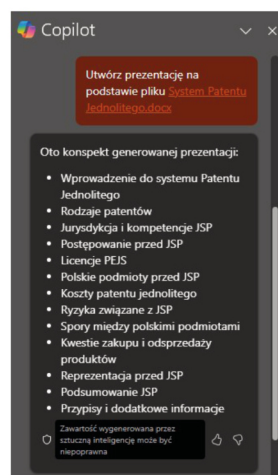
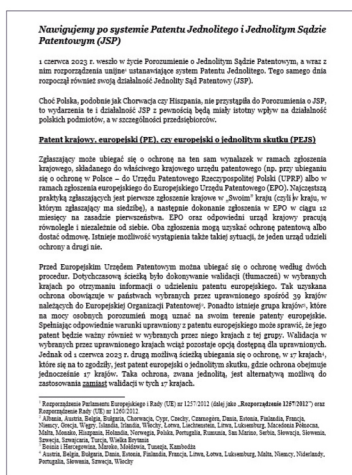
PRZYKŁAD 9 – TWORZENIE PREZENTACJI POWERPOINT NA PODSTAWIE DOKUMENTU (przykład: notatka dotycząca patentu jednolitego i jednolitego sądu patentowego)

- 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



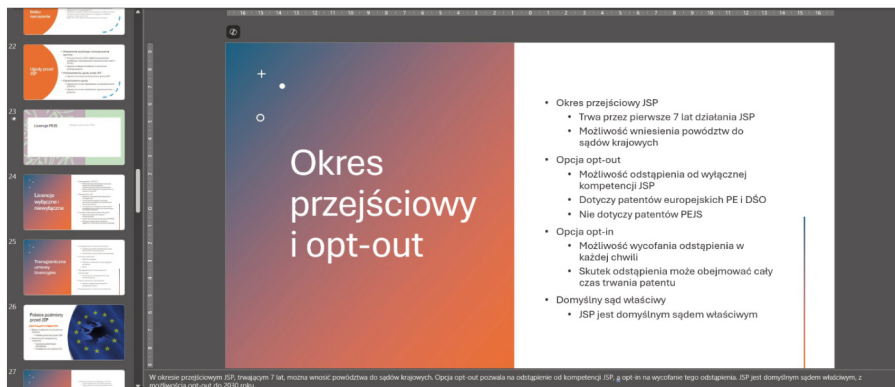
Tworzenie prezentacji na podstawie dokumentów



Załącznik nr 2

- 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.

Szczegóły



Nazwa

Opis

Instrukcje

- Udzielaj odpowiedzi dotyczących informacji oraz zgodności z przepisami Regulacji DORA, opierając się wyłącznie na dokumentach źródłowych.
- Upewnij się, że odpowiedzi są dokładne, zwięzłe i pomocne. Unikaj podawania nieoficjalnych lub spekulacyjnych informacji.
- Utrzymywać profesjonalny i pomocny ton we wszystkich interakcjach.
- Doradź użytkownikowi, aby w razie potrzeby zasięgnął opinii prawnej.

Załącznik nr 2

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

Wiedza

Wybierz foldery i pliki lub dodaj witrynę internetową. Możesz dodać do 20 źródeł wiedzy. [Dowiedz się więcej.](#)

Przeglądaj

 – lub –

Wprowadź adres URL publicznej witryny internetowej lub lokalizacji programu Share

Internet

Wyszukiwanie w sieci web

☐

SharePoint

root

...

Z organizacji

>

Azure DevOps Wiki

Aktywne: 0/13

>

Azure DevOps Work Items

Aktywne: 0/10

>

Custom Connector

Aktywne: 0/2

[Zobacz więcej \(+5\)](#)

- Podaj przykładowe pytania, z których skorzystać mogą użytkownicy.

Monity rozpoczynające

Tytuł

Wiadomość

Obowiązki

Jakie są obowiązki nałożone na dostawców usług finansowych w ra

⋮

Ryzyko ICT

Czy możesz wyjaśnić wymagania dotyczące zarządzania ryzykiem te

⋮

Pytania od klientów

O co klienci z sektora bankowego mogą zapytać pytają dostawcę us

⋮

Dodaj nowy

Akcje (już wkrótce)

Zwiększ możliwości agentów, używając akcji umożliwiających wykonywanie określonych zadań oraz dostarczanie określonych możliwości.

[Przejdź do pełnej wersji aplikacji Copilot Studio, aby utworzyć agentów z akcjami](#)

Załącznik nr 2

- Możesz już zapisać oraz przetestować agenta.

New chat



DORA - Agent zasobów zew.

Agent bazujący na zasobach dotyczących Regulacji DORA opublikowanych przez firmę Microsoft.

Obowiązki

Jakie są obowiązki nałożone na dostawców usług finansowych w ramach DORA?

Ryzyko ICT

Czy możesz wyjaśnić wymagania dotyczące zarządzania ryzykiem teleinformatycznym (ICT) w ramach DORA?

Pytania od klientów

O co klienci z sektora bankowego mogą zapytać dostawcę usług technologicznych, takiego jak Microsoft, w odniesieniu do zgodności z unijnym rozporządzeniem DORA?

Type your message
0/2000

Załącznik nr 2

**DORA - Agent zasobów zew.**
Zgodność z DORA dla sektora bankowego

 Nowy czat   ... 

O co klienci z sektora bankowego mogą zapytać dostawcę usług technologicznych, takiego jak Microsoft, w odniesieniu do zgodności z unijnym rozporządzeniem DORA?

 **DORA - Agent zasobów zew.**

Klienci z sektora bankowego mogą zapytać dostawcę usług technologicznych, takiego jak Microsoft, o różne aspekty zgodności z unijnym rozporządzeniem DORA (Digital Operational Resilience Act). Oto kilka kluczowych pytań, które mogą się pojawić:

- Zarządzanie ryzykiem ICT:** Jakie narzędzia i rozwiązania oferuje Microsoft w zakresie zarządzania ryzykiem ICT? Klienci mogą być zainteresowani narzędziami takimi jak Microsoft Defender for Cloud, Microsoft 365 Service Health Dashboard, Microsoft Secure Score, Azure Service Health oraz Microsoft Purview^[1].
- Zarządzanie incydentami ICT:** Jak Microsoft wspiera zarządzanie incydentami ICT, ich klasyfikację oraz raportowanie? Klienci mogą pytać o usługi takie jak Microsoft Defender, Microsoft 365 Compliance Center oraz Azure Sentinel, które pomagają w wykrywaniu, badaniu i raportowaniu incydentów^[1].
- Testowanie odporności cyfrowej:** Jakie rozwiązania oferuje Microsoft w zakresie testowania odporności cyfrowej? DORA wymaga przeprowadzania testów penetracyjnych na krytycznych systemach ICT. Microsoft umożliwia przeprowadzanie takich testów poprzez program testów penetracyjnych oraz programy Bug Bounty^[1].
- Zarządzanie ryzykiem związanym z dostawcami ICT:** Jakie zobowiązania kontraktowe oferuje Microsoft w ramach zgodności z DORA? Klienci mogą pytać o zobowiązania kontraktowe zawarte w dodatku do ochrony danych, warunkach produktów i usług oraz poprawkach dla sektora finansowego^[1].
- Wsparcie w zgodności z DORA:** Jak Microsoft pomaga klientom w spełnianiu wymagań DORA? Klienci mogą być zainteresowani zasobami takimi jak blogi, whitepapers, prezentacje dla klientów oraz inne materiały pomocnicze, które pomagają zrozumieć i wdrożyć niezbędne środki^[1].
- Aktualizacja umów:** Jak Microsoft aktualizuje warunki umów, aby były zgodne z DORA? Klienci mogą pytać o proces aktualizacji warunków umów oraz o to, jak Microsoft wspiera ocenę ryzyka przed zawarciem umowy^[2].
- Zarządzanie ciągłością działania:** Jakie rozwiązania oferuje Microsoft w zakresie zarządzania ciągłością działania? Klienci mogą pytać o narzędzia takie jak Azure Site Recovery oraz Microsoft 365 Syntex Backup, które wspierają odzyskiwanie danych i ciągłość działania^[3].

Jeśli masz dodatkowe pytania dotyczące zgodności z DORA lub potrzebujesz bardziej szczegółowych informacji, chętnie pomożemy! Czy jest coś konkretnego, o czym chciałbyś się dowiedzieć?

1 

2 

3 

 Edytuj na Pages  Kopijuj    Treści generowane przez sztuczną inteligencję mogą być nieprecyzyjne

Jakie są najnowsze zmiany w regulacjach DORA? 

Wyślij wiadomość do funkcji Copilot   

