



JDD

NEWSLETTER | październik 2025

AI w pracy działu prawnego

CZ. 4

Jak ocenić, czy korzystanie z narzędzia AI dla prawników będzie zgodne z prawem i etyką?

Korzystanie z narzędzi AI budzi wśród części prawników duży niepokój związany z bezpieczeństwem. Wynika to prawdopodobnie z połączenia dwóch okoliczności.



Korzystanie z większości narzędzi AI, które mogłyby być przydatne dla prawników wiąże się z wysyłaniem danych na serwery dostawców tych narzędzi. Ponadto, do rozwoju dużych modeli językowych, na których opierają się te narzędzia, potrzebne są ogromne ilości danych, które mogą być pozyskiwane od użytkowników.

Są to zasadne obawy, ale dostawcy narzędzi wiedzą o tym i adresują w swoich ofertach te zagadnienia.

Dostrzegła je również Krajowa Izba Radców Prawnych, która w kwietniu 2025 opublikowała dokument "AI w pracy radcy prawnego - Rekomendacje dotyczące korzystania przez radców prawnych z narzędzi opartych na sztucznej inteligencji" ("**Rekomendacje KIRP**"). Dokument ten zawiera całą grupę rekomendacji dotyczących analizy, która powinna poprzedzać wdrożenie narzędzia.

Przystępując do wyboru narzędzia AI, a przed rozpoczęciem testów merytorycznych, przeprowadziliśmy w JDP wstępną ocenę prawną testowanych narzędzi AI w zgodzie z Rekomendacjami KIRP. Poniżej opisujemy najważniejsze elementy naszej oceny.

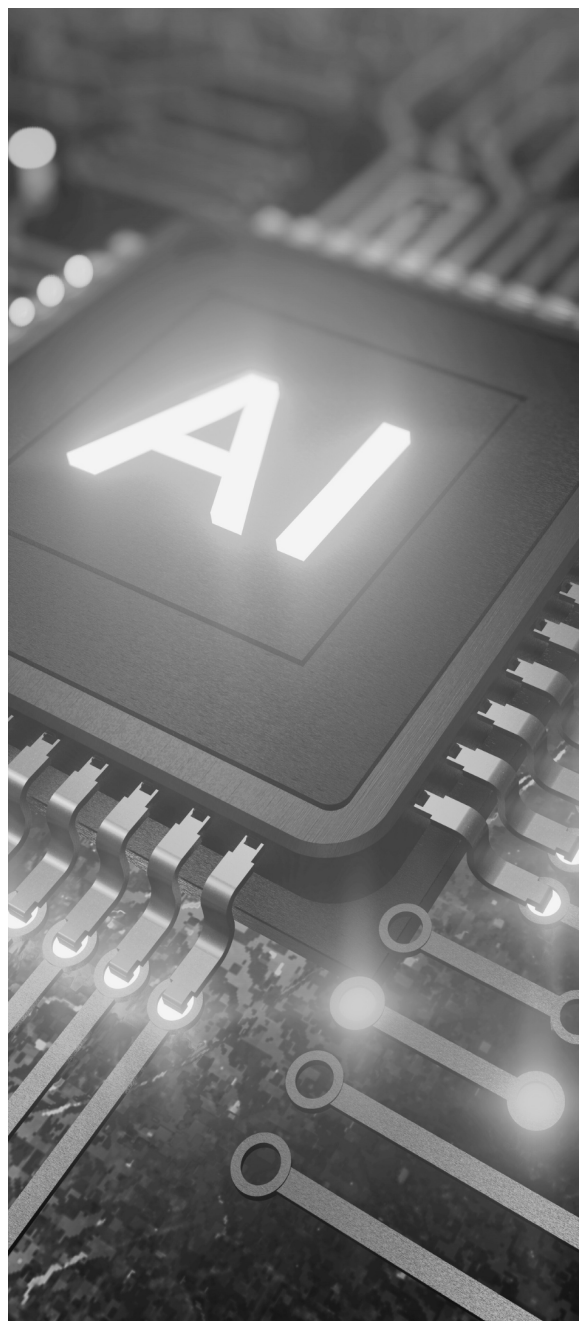
Elementy oceny

Poszczególne elementy są wyodrębnione dla uporządkowania i ułatwienia procesu oceny, ale są one ściśle powiązane ze sobą i przenikają się, np. oceniając zgodność z RODO, musimy wziąć pod uwagę ocenę środków bezpieczeństwa, oceniając poufność, bierzemy pod uwagę umowę i środki bezpieczeństwa.

O tym, gdzie szukać informacji, które należy zweryfikować, pisaliśmy w pierwszym odcinku tej serii, dostępnym po kliknięciu w przycisk poniżej.

Wdrożenie AI w dziale prawnym - pierwsze kroki

> [Kliknij tutaj](#) <



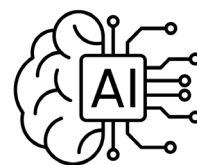
Kwestie umowne

Po pierwsze, ocenialiśmy standardowe kwestie umowne takie jak:

1. Jakie są obowiązki umowne obu stron?
2. Jak uregulowana jest odpowiedzialność za działanie narzędzia?
 - ➔ Czy są limity odpowiedzialności? Jakie?
 - ➔ Czy jest SLA i na jakim poziomie?
 - ➔ Czy dostawca odpowiada za szkody wyrządzone działaniem narzędzia?
 - ➔ Czy zwalnia z odpowiedzialności za naruszenie cudzych praw poprzez korzystanie z narzędzia?
3. Czy umowa przewiduje zakaz konkurencji?
4. Jaki jest okres umowy? W jaki sposób można wypowiedzieć umowę?
5. Jak uregulowane są płatności?

Po drugie, ocenialiśmy kwestie charakterystyczne dla systemów AI:

1. Czy zachowujemy prawa do zawartości wejściowej?
2. Czy możemy dowolnie korzystać z wygenerowanych treści?
3. Czy dostawca zwolni nas z odpowiedzialności za naruszenie praw osób trzecich poprzez korzystanie z wygenerowanych treści?
4. Czy wykluczone jest wykorzystanie naszych danych wejściowych do nauki modeli językowych wykorzystywanych przez narzędzie?



Po trzecie, ocenialiśmy również kwestie poufności i ochrony danych osobowych, o których poniżej.

Zgodność przetwarzania danych z prawem

Wiele zadań prawników wiąże się z przetwarzaniem danych osobowych, dlatego ocena narzędzi AI pod względem ochrony danych osobowych jest niezbędna.



W pierwszej kolejności należy zrozumieć, jak przetwarzane są dane, ponieważ w zależności od przyjętej architektury rozwiązania w przetwarzanie zaangażowanych może być kilka podmiotów przetwarzających.

Najważniejsze kwestie, które analizowaliśmy to:

1. Bezpieczeństwo przetwarzania - o tym więcej poniżej.
2. Czy dochodzi do transferów poza EOG? Do jakich państw i na jakiej podstawie?
3. Czy umowa o powierzeniu przetwarzania danych zawiera wymagane elementy i jakie są podmioty przetwarzające?
4. Czy odpowiedzialność za naruszenie danych osobowych nie jest ograniczona?

Ze względu na

- ➔ innowacyjność rozwiązań opartych o AI,
 - ➔ ograniczone możliwości wykonywania praw osób, których dane dotyczą oraz
 - ➔ przetwarzanie szczególnych kategorii danych osobowych,
- konieczne jest, w naszej ocenie, przeprowadzenie oceny skutków dla ochrony danych (DPIA).

Środki bezpieczeństwa

Ten element był dla nas kluczowy w ocenie dostawcy. Badaliśmy przy tym następujące kwestie:

1. Czy stosowane przez dostawcę szyfrowanie jest adekwatne do potrzeb procesu?
2. Czy dostawca posiada uznane certyfikaty bezpieczeństwa jak SOC Type 2 lub ISO 27001?
3. Jakie są zasady zarządzania dostępem do danych?
4. Czy dane przechowywane są poza EOG?
5. Czy dostawca podejmuje dodatkowe środki bezpieczeństwa, np.:
 - a. testy penetracyjne?
 - b. plan ciągłości działania?
 - c. firewallle?
 - d. uwierzytelnianie wieloskładnikowe?
6. Jakie są prawo i sądy właściwe dla sporów wynikających z umowy?



Poufność

Mając zweryfikowane środki bezpieczeństwa, konieczne było sprawdzenie czy umowa z dostawcą zawiera odpowiednie postanowienia dotyczące poufności.

Kluczowe są zobowiązania dostawcy do:

1. zachowania informacji w tajemnicy w formie dokumentowej;
2. posługiwania się osobami zobowiązanymi do tajemnicy w formie dokumentowej;
3. niewykorzystywania informacji objętej tajemnicą zawodową dla własnych celów;
4. stosowania środków bezpieczeństwa, o których była mowa powyżej;
5. usunięcia danych po zakończeniu umowy.

Sprawdzaliśmy również ewentualne ograniczenia odpowiedzialności w zakresie poufności.

Narzędzia wspomagające pracę prawników a AI Act

Podchodząc do analizy narzędzia, musieliśmy również odpowiedzieć na pytanie, co w tym kontekście wynika dla nas z AI Act.

Dokonaliśmy więc klasyfikacji testowanych systemów wg AI Act i uznaliśmy, że korzystając z systemów AI wspierających pracę prawników:

- ✗ nie stosujemy zakazanych praktyk w zakresie AI;
- ✗ nie korzystamy z systemów wysokiego ryzyka;
- ✗ nie stajemy się dostawcą modeli ogólnego przeznaczenia;
- ✗ nie dotyczą nas obowiązki z art. 50.

Jedynym obowiązkiem, jaki wynika dla nas z AI Act, jest **obowiązek zapewnienia odpowiedniego poziomu wiedzy o AI w organizacji, tzw. AI literacy**, o którym pisaliśmy w **poprzednim newsletterze**:

Jak przygotować organizację na spełnienie obowiązku AI literacy z art. 4 AI Act?

[> Kliknij tutaj <](#)

Podsumowanie

Analizując prawne kwestie wdrożenia narzędzia AI wspomagającego pracę prawników, należy pamiętać o:

1. odpowiednich zabezpieczeniach umownych, w szczególności zabezpieczeniu kwestii odpowiedzialności i praw do treści wejściowych i wyjściowych;
2. zgodności przetwarzania danych z prawem;
3. weryfikacji środków bezpieczeństwa, jakie oferują dostawcy;
4. kwestiach poufności informacji.

Obowiązki regulacyjne, jakie spoczywają na wdrażającym takie narzędzia polegają na przeprowadzaniu oceny skutków dla ochrony danych (DPIA) i zapewnieniu stosownego poziomu wiedzy o korzystaniu z AI w organizacji.

O wymaganej i rekomendowanej dokumentacji będziemy pisać w kolejnych odcinkach newslettera.



Kontakt



Michał Pietrzyk

radca prawny, Senior Associate,
Digital Transformation and Automation Lead
IP/IT

michal.pietrzyk@jdp-law.pl

Wszelkie informacje zawarte w niniejszym newsletterze są dostępne nieodpłatnie. Publikacja nie ma charakteru reklamowego i służy wyłącznie celom informacyjnym. Żadnej z informacji zawartych w niniejszym materiale nie należy traktować jako porady prawnej ani oferty handlowej, w tym w rozumieniu art. 66 § 1 Kodeksu cywilnego. JDP DRAPAŁA & PARTNERS Sp. k. niniejszym wyłącza swoją odpowiedzialność tytułem jakichkolwiek roszczeń, strat, żądań lub szkód wynikających lub związanych z korzystaniem z informacji, treści lub materiałów zawartych w newsletterze.

JDP Drapała &
Partners

JDP DRAPAŁA & PARTNERS Sp. k.
ul. Bonifraterska 17, 00-203 Warszawa
+48 22 246 00 30
office@jdp-law.pl

Sąd Rejonowy dla m.st. Warszawy,
XII Wydział Gospodarczy
Krajowego Rejestru Sądowego
KRS: 0001145849
REGON: 140887753
NIP: 7010056483