

Jak wdrożyć AI w firmie zgodnie z prawem?

Czy myślisz o wdrożeniu ChatGPT lub Copilota w swojej firmie, ale obawiasz się prawnych pułapek? Dobrze trafiłeś – w tym materiale w przystępny sposób wyjaśnimy, jak korzystać ze sztucznej inteligencji w biznesie zgodnie z polskim prawem i regulacjami UE. Zastanawiasz się, czy możesz wysłać dane klientów do ChatGPT? Wyjaśnimy to krok po kroku – od definicji AI w przepisach, przez politykę używania AI w firmie i RODO, po relacje AI z prawem pracy. Dzięki temu dowiesz się, jak innowacyjnie korzystać z AI, nie łamiąc przy tym prawa.

1. Definicja sztucznej inteligencji w prawie

Na początek ustalmy, **co to właściwie jest AI według prawa**. W 2024 r. Unia Europejska przyjęła tzw. **AI Act** – pierwsze kompleksowe przepisy o sztucznej inteligencji (Rozporządzenie UE 2024/1689) ¹ ². Zgodnie z AI Act „**system AI**” to system informatyczny, który:

- **działa z pewną autonomią** – potrafi samodzielnie podejmować decyzje bez stałego nadzoru człowieka,
- **uczy się i adaptuje** po wdrożeniu – samodoskonali się na podstawie zebranych danych i doświadczeń,
- **generuje określone wyniki** (rekomendacje, decyzje, prognozy, treści) na podstawie danych wejściowych i zamierzonych celów,
- **może oddziaływać na otoczenie** fizyczne (np. robot w fabryce) lub cyfrowe (np. aplikacja online) ³.

Innymi słowy, **prawo UE definiuje AI przez pryzmat „systemu AI”** zdolnego do samouczenia się i działania bez ciągłego sterowania przez człowieka. To odróżnia AI od zwykłego oprogramowania o stałych regułach – **system AI potrafi się zmieniać i podejmować różne decyzje w zależności od danych** ⁴. W Polsce brakowało dotąd ustawowej definicji AI, ale **AI Act będzie bezpośrednio stosowany także u nas**, ujednolicając rozumienie AI we wszystkich krajach UE.

Przykład: W praktyce **ChatGPT** czy **Copilot** spełniają tę definicję – to modele uczące się na ogromnych zbiorach danych, potrafiące generować odpowiedzi i rekomendacje na nasze polecenia. Przedsiębiorca używający takich narzędzi powinien więc znać reguły, które UE i polskie prawo przewidują dla **systemów AI**.

2. Polityka korzystania z AI w firmie

Skoro wiemy już, czym jest AI, kolejne pytanie brzmi: **czy Twoi pracownicy mogą swobodnie używać AI w pracy?** Okazuje się, że już **ponad połowa pracowników w Polsce korzysta z narzędzi AI na własną rękę** – często **bez wiedzy pracodawcy** ⁵! Takie zjawisko określa się jako **“shadow AI”** – używanie sztucznej inteligencji w firmie poza oficjalną kontrolą i zgodą działów IT czy przełożonych ⁶. Choć AI zwiększa produktywność, brak nadzoru może sprowadzić na firmę poważne ryzyka (wyciek danych, naruszenie przepisów, błędne decyzje).

Rozwiązanie? Wdrożenie wewnętrznej polityki korzystania z AI. Taka **polityka AI** to dokument, który jasno określa **zasady używania sztucznej inteligencji przez pracowników** – co wolno, czego nie wolno

i jak dbać o bezpieczeństwo. Powinna być napisana przystępnym językiem (to poradnik dla pracowników, nie tylko dla prawników) i budować kulturę odpowiedzialnego użycia AI ⁷. Oto kluczowe elementy, jakie powinna zawierać:

-  **Dozwolone narzędzia AI:** Wskaż konkretnie, z jakich narzędzi AI wolno korzystać, a z jakich nie. Dotyczy to zarówno **wewnętrznych rozwiązań, zewnętrznych narzędzi na licencjach firmowych**, jak i **publicznie dostępnych usług** (np. ChatGPT w wersji publicznej) ⁸. Np. można dopuścić korzystanie z ChatGPT **Enterprise** (z wykupioną licencją i umową o ochronę danych), ale **zabronić używania darmowej wersji** na prywatnych kontach. To ważne dla bezpieczeństwa informacji ⁹.
- **Kto i w jakim zakresie może używać AI:** Określ, **których pracowników lub zespołów** obejmują zasady i czy również podwykonawcy mogą korzystać z AI ¹⁰. Można np. ustalić, że narzędzia generatywnej AI są dostępne dla działu R&D i marketerów, ale np. już nie dla działu prawnego bez specjalnej zgody.
- **Do jakich zadań używać AI:** Podaj **przykłady dozwolonych zastosowań** AI w firmie – np. **research i burza mózgów**, tworzenie **wstępnych szkiców dokumentów**, pomoc w kodowaniu czy obsłudze klienta ¹¹. Ważne, by jasno zaznaczyć granicę: AI ma **wspierać** pracę, a nie całkowicie zastępować pracownika przy kluczowych obowiązkach. Taki opis chroni przed zjawiskiem **shadow AI** – jeśli ludzie wiedzą, jak **oficjalnie** mogą korzystać z AI, rzadziej sięgną po nią potajemnie ¹².
-  **Zakazane działania:** Niezbędne jest wypunktowanie, czego **absolutnie nie wolno robić** z użyciem AI. Takie czerwone linie chronią zarówno firmę, jak i wyznaczają konsekwencje dla pracownika, który je przekroczy ¹³ ¹⁴. Przykładowe **zakazy** to m.in.:
 - **Wprowadzanie wrażliwych danych firmy lub danych osobowych** do niezatwierdzonych narzędzi AI (np. kopiowanie poufnych informacji do prywatnego konta ChatGPT) ¹⁵. Tego typu dane to tajemnice przedsiębiorstwa, dane finansowe, dane klientów – nie mogą „wypłynąć” na zewnątrz.
 - **Omijanie zabezpieczeń** – np. używanie AI do łamania haseł, obchodzenia firmowych polityk bezpieczeństwa czy wyłączania zabezpieczeń systemowych ¹⁶.
 - **Generowanie treści niezgodnych z prawem lub naruszających prawa innych** – np. treści obraźliwych, dyskryminujących albo naruszających czyjeś prawa autorskie ¹⁷.
- **Ukrywanie użycia AI** – przedstawianie materiałów wygenerowanych przez AI jako w pełni własne, **bez ujawnienia, że korzystano z narzędzia AI** ¹⁷. Taka niejawność może wprowadzać w błąd przełożonych lub klientów co do sposobu powstania treści.
-  **Zarządzanie danymi i bezpieczeństwo:** Polityka AI musi powiązać się z zasadami ochrony danych w firmie. Jeśli wprowadzamy do AI **dane osobowe** lub inne wrażliwe informacje, trzeba postępować zgodnie z RODO i wewnętrzną polityką bezpieczeństwa informacji ¹⁸. Np. pracownik **musi wiedzieć, jakie dane wolno mu wprowadzać**, a jakich nie (żadnych danych pozwalających zidentyfikować klienta bez zgody!). Firma powinna też zapewnić, że używane narzędzia AI spełniają wymogi bezpieczeństwa – np. czy dostawca AI szyfruje przesyłane dane. Pamiętaj: to przedsiębiorca jako administrator danych ponosi odpowiedzialność za to, co dzieje się z danymi osobowymi **nawet gdy korzysta z AI** ¹⁹.
-  **Powiązanie z innymi regulacjami:** Warto zaznaczyć, że polityka AI **nie działa w próżni** – powinna być spójna z innymi procedurami w firmie (np. polityką ochrony danych osobowych, polityką bezpieczeństwa IT, zasadami ochrony własności intelektualnej) ²⁰. Pomocne może być

dodanie krótkiego **słowniczka** w polityce AI, aby wyjaśnić podstawowe pojęcia (np. „system AI”, „dane osobowe”) i nawiązać do definicji z tych innych dokumentów ²¹ .

- **♀ Egzekwowanie i konsekwencje:** Polityka powinna wskazać, **kto nadzoruje przestrzeganie zasad** (np. dedykowany zespół ds. AI, dział IT lub Inspektor Ochrony Danych) oraz jakie **konsekwencje grożą za ich łamanie**. Pracownik musi mieć świadomość, że złamanie zakazów (np. ujawnienie danych wrażliwych przez AI) to podstawa do wyciągnięcia konsekwencji służbowych. Wyraźnie określone konsekwencje wzmacniają powagę zasad ¹³ ¹⁴ .
- **Aktualizacja zasad:** Technologia AI rozwija się błyskawicznie, więc dobra polityka przewiduje, **kiedy będzie aktualizowana**. Należy określić, że pojawienie się **nowych narzędzi, zmian w przepisach lub nowych zagrożeń** oznacza przegląd i dostosowanie polityki ²² . Dzięki temu dokument pozostanie żywy i użyteczny – nie będzie tylko „półkownikiem”.

Na koniec, **sucha polityka to za mało** – kluczowe jest przeszkolenie pracowników, by naprawdę **rozumieli zasady i umieli je stosować** ²³ . Badania pokazują, że aż **90% polskich pracowników nie zna regulacji dotyczących AI** ²⁴ , a większość wybiera łatwo dostępne narzędzia, które nie wymagają szkolenia ²⁵ ²⁶ . Dlatego firma powinna zorganizować **szkolenia** z korzystania z AI: omówić dobre praktyki, pokazać przykłady ryzyk i nauczyć obsługi zatwierdzonych narzędzi ²⁷ . To podniesie świadomość i zmniejszy pokusę sięgania po „dzikie” rozwiązania z pominięciem zasad.

Dlaczego warto mieć taką politykę? Dobrze wdrożona **wewnętrzna polityka AI** pomaga: **zidentyfikować i ograniczyć ryzyka** (prawne, finansowe, operacyjne) związane z AI ²⁸ , **zapewnić zgodność z przepisami** (RODO, przyszły AI Act) ²⁸ , **dać pracownikom jasne wytyczne** i poczucie pewności co do używania nowych narzędzi ²⁹ , a także **buduje zaufanie** u klientów i partnerów, pokazując że firma poważnie traktuje kwestie etycznego wykorzystania AI ³⁰ . To fundament odpowiedzialnej i strategicznej digitalizacji firmy.

3. Zgodność z RODO – dane osobowe a AI

Przejdźmy teraz do kluczowej kwestii: **ochrona danych osobowych (RODO)** podczas używania AI. **Zastanawiasz się, czy możesz wysłać dane klientów do ChatGPT?** Odpowiedź brzmi: **to zależy, ale wymaga spełnienia konkretnych warunków prawnych**. Wyjaśnijmy to krok po kroku.

Kiedy AI „przetwarza dane osobowe”? – Zawsze gdy wprowadzasz do narzędzia AI informacje pozwalające zidentyfikować osobę (np. imię i nazwisko, adres email, numer PESEL, dane klientów czy pracowników). Nawet opis sprawy klienta może zawierać dane osobowe. Jeśli więc używasz AI do zadań związanych z konkretnymi osobami, **wchodzisz w reżim RODO**. Co to oznacza dla firmy?

Po pierwsze: potrzeba umowy powierzenia przetwarzania (DPA). Zgodnie z art. 28 RODO, gdy przekazujesz dane osobowe **zewnętrznemu dostawcy** (np. firmie oferującej usługę AI) do przetwarzania, musisz zawrzeć z nim tzw. **umowę powierzenia danych**. Formalnie to ten dostawca staje się **podmiotem przetwarzającym (procesorem)**, a Twoja firma pozostaje administratorem danych. **Przykład:** Jeśli korzystasz z API OpenAI (ChatGPT) i wysyłasz tam dane klientów, OpenAI staje się procesorem, a Ty odpowiadasz za legalność przekazania danych ³¹ . **Każde przekazanie danych do OpenAI czy innej AI powinno być uregulowane umową powierzenia** – inaczej łamiesz RODO ³² . Taka umowa (DPA) precyzuje m.in. cel i zakres przetwarzania danych przez dostawcę AI, wymogi bezpieczeństwa, warunki poufności oraz zobowiązania dostawcy wobec Twojej firmy ³³ ³⁴ . Upewnij się więc, że **Twój dostawca AI oferuje podpisanie DPA** – wielu poważnych dostawców (jak Microsoft czy Google) ma standardowe dodatki dot. ochrony danych, a OpenAI dla użytkowników biznesowych

również deklaruje zgodność z RODO i możliwość zawarcia takiej umowy ³⁵. Jeśli jakiś popularny chatbot *nie* daje możliwości podpisania umowy powierzenia – **nie wolno używać go do danych osobowych!**

Po drugie: podstawa prawna i minimalizacja danych. RODO wymaga, by każde przetwarzanie danych osobowych miało **podstawę prawną** (np. zgodę osoby, wykonanie umowy, uzasadniony interes) i by przetwarzać tylko **niezbędne minimum danych**. Przed wysłaniem danych do AI zastanów się, **czy to konieczne**. Może da się **zanonimizować dane**? Np. zamiast pełnych danych klienta użyj pseudonimu lub ID. **Anonimizacja** to świetny sposób na zmniejszenie ryzyka – jeśli usuniesz z danych informacje identyfikujące, RODO nie będzie mieć zastosowania ³⁶ ³⁷. W praktyce: **nie wysyłaj do AI danych wrażliwych ani zbędnych**. Rozważ także uzyskanie **zgody osób**, jeśli chcesz wykorzystywać ich dane w procesach AI – szczególnie, gdy mówimy o klientach i nowych, nieoczywistych celach przetwarzania ³⁸.

³⁹.

Po trzecie: transfer danych poza EOG. Wielu dostawców AI (np. OpenAI) ma siedziby lub serwery poza Europą, najczęściej w USA. **RODO nie zabrania przekazywania danych do USA czy innych krajów, ale stawia warunki**. Trzeba zapewnić, że dane trafią do kraju gwarantującego „odpowiedni poziom ochrony” ⁴⁰. Jak to zrobić? Są dwa główne sposoby: - **Standardowe klauzule umowne (Standard Contractual Clauses, SCC)** – to wzorcowe umowy zatwierdzone przez Komisję Europejską, które Ty i dostawca z USA podpisujecie, zobowiązując się do ochrony danych zgodnie ze standardami UE. Wiele firm (w tym OpenAI) udostępnia klientom takie **SCC** do podpisu ⁴¹. - **Data Privacy Framework (Tarcza Danych UE-USA)** – to nowe porozumienie UE-USA z 2023 r., przywracające możliwość przekazywania danych do certyfikowanych firm w Stanach. Sprawdź, czy Twój dostawca AI jest na liście podmiotów, które przystąpiły do tego programu. Jeśli tak, transfer może odbywać się legalnie w ramach tej „klauzuli generalnej”.

Jeżeli nie masz ani SCC, ani nie obowiązuje żaden **mechanizm ochronny**, przekazywanie danych do np. OpenAI może być **niezgodne z prawem** ⁴². **Przykład:** Korzystasz z darmowego ChatGPT (serwery w USA) i wysyłasz dane klientów bez żadnej umowy – to transfer poza EOG bez podstawy prawnej. W razie kontroli UODO będzie problem. Rozwiązanie: korzystać z usługi *Enterprise*, gdzie OpenAI oferuje umowę powierzenia i zobowiązuje się do standardów bezpieczeństwa (a najlepiej, by przechowywała dane na serwerach UE, jeśli to możliwe).

Po czwarte: transparentność wobec osób, których dane dotyczą. RODO nakłada obowiązek informowania ludzi o tym **kto, jak i w jakim celu przetwarza ich dane** (art. 13 i 14 RODO). Jeśli w Twojej firmie zaczynasz używać AI, które będzie przetwarzać dane osobowe klientów lub pracowników, **musisz to odzwierciedlić w dokumentach takich jak polityka prywatności, regulamin usług czy klauzule informacyjne** ⁴³. W praktyce oznacza to dodanie w polityce prywatności informacji, że np. *“W celu [np. obsługi klienta / analizy danych] firma może wykorzystywać narzędzia oparte na sztucznej inteligencji dostarczane przez [nazwa dostawcy]. W związku z tym pewne dane (np. treść zapytań klientów) mogą być przekazywane temu dostawcy w celu wygenerowania odpowiedzi. Dostawca ten gwarantuje zgodność z RODO (umowa powierzenia) i odpowiedni poziom ochrony danych.”* Taka klauzula zapewnia przejrzystość. **Jeśli AI podejmuje zautomatyzowane decyzje dotyczące osoby (profilowanie)** – np. algorytm decyduje o przyznaniu kredytu lub selekcji CV – to **koniecznie poinformuj o tym osobę** oraz o jej prawie do sprzeciwu lub interwencji człowieka (wymóg z art. 22 RODO). Transparentność buduje zaufanie i chroni przed zarzutem ukrywania istotnych informacji.

Podsumowując ten segment: Można używać AI przy danych osobowych, ale **trzeba spełnić rygory RODO** – mieć umowę z dostawcą, podstawę prawną, chronić dane przed wypłynięciem za granicę bez zabezpieczeń i **informować ludzi o wykorzystaniu AI** w procesach przetwarzania danych. Ignorowanie tych kwestii grozi poważnymi konsekwencjami – **kary za naruszenie RODO sięgają 20 mln euro lub**

4% globalnego obrotu ⁴⁴, nie licząc utraty reputacji czy odszkodowań dla poszkodowanych ⁴⁵. Dlatego warto dmuchać na zimne i zawczasu uregulować wszystkie aspekty zgodności z RODO przy wdrażaniu sztucznej inteligencji.

4. Dostawcy AI jako podprocesorzy – co z OpenAI, Microsoftem i innymi?

W kontekście ochrony danych warto jeszcze podkreślić rolę **dostawców AI** – takich jak OpenAI (ChatGPT), Microsoft (Copilot), Google (Bard) czy inne firmy oferujące AI w chmurze. Dla Twojej firmy to oni są właśnie **podmiotami przetwarzającymi dane**, a z perspektywy RODO często **pod-procesorami** w łańcuchu dostaw (zwłaszcza jeśli korzystasz z AI za pośrednictwem innego usługodawcy). Co to oznacza praktycznie?

Traktuj dostawcę AI tak samo, jak każdego innego procesora danych. Musisz mieć z nim **umowę powierzenia** (jak opisaliśmy wyżej) i upewnić się, że spełnia wymogi RODO – ma odpowiednie zabezpieczenia, przestrzega praw osób, umożliwia audyty itp. ³². **Przykład:** Korzystając z **ChatGPT API** bezpośrednio od OpenAI, zawrzyj umowę powierzenia z OpenAI i włącz w niej **Standardowe Klauzule Umowne** na transfer do USA. Gdy natomiast używasz **Microsoft 365 Copilot**, sprawdź warunki Microsoftu – czy Copilot jest objęty standardową **umową przetwarzania danych Microsoft i EU Data Boundary**. Microsoft zapowiada lokalizację danych AI w Europie, ale uwaga: niektóre funkcje (np. wyszukiwanie internetowe w Copilocie Chat) **mogą wykraczać poza dotychczasowe ustalenia** ⁴⁶ ⁴⁷. Z publicznych analiz wynika, że nie zawsze wiadomo, jakie dane Copilot zbiera i gdzie je przesyła, co rodzi pewne ryzyka ⁴⁸. **Dlatego obowiązkiem firmy jest dociekać i dokumentować**, jakie dane trafiają do dostawców AI i na jakich zasadach.

Włącz swoich kluczowych **dostawców AI do rejestru podmiotów przetwarzających** i listy podwykonawców. Np. jeśli korzystasz z usługi SaaS, która **pod maską używa OpenAI**, to dostawca SaaS powinien Ci ujawnić, że OpenAI jest jego sub-procesorem – dopilnuj tego w umowie. Transparentność w łańcuchu przetwarzania jest wymagana przez RODO. **Twoi klienci lub pracownicy mają prawo wiedzieć**, komu ostatecznie powierzane są ich dane ⁴³.

Kontroluj też warunki licencyjne dostawców AI. Upewnij się, że używając ich narzędzi nie przekazujesz im więcej praw niż zamierzasz. Przykładowo, dawniej darmowy regulamin OpenAI pozwalał im wykorzystywać Twoje konwersacje do trenowania modeli, chyba że je wyłączyłeś. W zastosowaniu firmowym warto korzystać z płatnych planów biznesowych, gdzie dostawcy deklarują **niewykorzystywanie danych klientów do treningu** i zapewniają większą prywatność.

Podsumowując: OpenAI, Microsoft i inni dostawcy AI to Twoi partnerzy, ale i podwykonawcy w przetwarzaniu danych. **Włącz ich w swoją “układankę” zgodności z prawem** – umowy, audyty, zabezpieczenia. Traktuj ich jak przedłużenie własnego procesu. Jeśli oni popełnią błąd (np. wyciek danych z chmury AI), **Tvoja firma też za to odpowie przed klientami i regulatorami**, dopóki to Ty jesteś administratorem danych. Wybieraj zatem dostawców **godnych zaufania, renomowanych, z certyfikatami bezpieczeństwa**, a unikaj kuszących, ale niezwyfikowanych rozwiązań AI od nieznanymi firm.

5. Odpowiedzialność pracodawcy – jak zabezpieczyć firmę przy korzystaniu z AI?

Wprowadzając AI do firmy, **pracodawca (przedsiębiorca) musi pamiętać, że to on ponosi główną odpowiedzialność za zgodność z prawem**. Nawet jeśli błąd popełnił pracownik albo AI „sama” zrobiła coś niepożądanego, to wobec klientów, sądu czy urzędu odpowiada firma. Pracodawca jest administratorem danych na gruncie RODO (więc to jemu grożą ewentualne kary), a także to on może zostać pozwany np. za naruszenie prywatności czy tajemnicy przez działanie AI w firmie. **Jak się przed tym chronić?**

Kluczowe jest **wdrożenie środków zaradczych** – organizacyjnych i technicznych – o których już częściowo mówiliśmy. Zbierzmy je w formie checklisty:

-  **Edukacja i świadomość:** Przede wszystkim, **zwiększ świadomość pracowników**. Przeprowadź szkolenia o zagrożeniach związanych z niekontrolowanym użyciem AI (shadow AI) i przypomnij zasady ochrony danych osobowych ⁴⁹. Każdy powinien wiedzieć, jakie ryzyka niesie wrzucenie firmowych danych do otwartego chatbota czy wygenerowanie treści bez weryfikacji. Pracownicy poinformowani o konsekwencjach będą ostrożniejsi.
- **Polityki i procedury:** **Wprowadź jasno określoną politykę korzystania z AI** (o której mówiliśmy w sekcji 2) i inne wewnętrzne procedury kontrolne ⁵⁰. Zjawisko shadow AI bierze się często stąd, że firma nie ma żadnych wytycznych – wówczas pracownicy działają na własną rękę. Dobrze napisana polityka AI i np. procedura zgłaszania nowych narzędzi do akceptacji sprawią, że użytkowanie AI będzie się odbywać w **uregulowany sposób, zgodny z RODO** ⁵⁰.
-  **Audyty i nadzór:** Nie poprzestawaj na spisaniu zasad – **regularnie sprawdzaj, jak AI jest używana w firmie**. Można robić okresowe **audyty techniczne i prawne**: które działy korzystają z jakich narzędzi, czy przestrzegają polityki, czy nie pojawiły się „dzikie” aplikacje AI w obiegu ⁵¹. Audyt pozwoli wychwycić nieprawidłowości zanim przerodzą się w poważny incydent. Dobrą praktyką jest też monitorowanie ruchu sieciowego pod kątem korzystania z zewnętrznych usług AI – dział IT może zidentyfikować, czy np. ktoś masowo nie wysyła danych do podejrzanych usług.
- **Zabezpieczenia danych:** **Wdroż odpowiednie środki techniczne i organizacyjne** chroniące dane osobowe oraz poufne informacje w kontekście AI ⁵². Co to znaczy? Zapewnij szyfrowanie komunikacji z dostawcami AI, stosuj anonimizację lub pseudonimizację danych przed przekazaniem do AI (np. zamiana nazwisk na ID) ³⁶ ⁵³, ogranicz dostęp tylko dla upoważnionych osób, korzystaj z wbudowanych opcji prywatności u dostawców (np. wyłącz logowanie wrażliwych treści). Również **kontroluj uprawnienia** – nie każdy pracownik musi mieć dostęp do każdego narzędzia AI, ogranicz dostęp do tych, którzy rzeczywiście ich potrzebują. Te kroki zmniejszają ryzyko incydentu.
-  **Konsultacje prawne i compliance:** Trzymaj rękę na pulsie zmian prawnych. AI Act UE wejdzie w pełni w życie za kilkanaście miesięcy – warto już teraz przeanalizować, czy narzędzia z których korzystasz nie będą podlegać tam dodatkowym obowiązkom (np. systemy AI wysokiego ryzyka). W razie wątpliwości, **skonsultuj się z prawnikiem specjalizującym się w nowych technologiach**. W dużych firmach rolę doradczą odegra Inspektor Ochrony Danych (IOD), który powinien być zaangażowany przy ocenie ryzyka związanego z AI. Np. jeśli planujesz wdrożyć AI do oceny kandydatów do pracy, być może trzeba będzie przeprowadzić **DPIA (ocenę skutków dla ochrony danych)**. Lepiej zawczasu dopełnić takich obowiązków.

Mając powyższe działania wdrożone, pracodawca znacznie zmniejsza szansę naruszenia prawa. Pamiętajmy, że **jeśli jednak dojdzie do incydentu** (np. wyciek danych przez AI), to firma ponosi odpowiedzialność przed organami. UODO może nałożyć wspomnianą karę finansową, a poszkodowany klient – pozwać o odszkodowanie ^{44 54}. Dlatego to **w interesie pracodawcy jest działać prewencyjnie**. Zabezpieczenie się nie tylko chroni przed sankcjami, ale też **chroni wizerunek firmy** – pokazuje partnerom i klientom, że poważnie traktujemy kwestie prawne i bezpieczeństwo w innowacjach.

6. AI a prawo pracy – czy sztuczna inteligencja zastąpi pracownika?

Na koniec zajmijmy się **relacją AI – pracownik** i kwestiami prawa pracy. Coraz więcej mówi się o tym, że AI odbierze ludziom pracę. Czy **pracodawca może zwolnić kogoś i zastąpić go sztuczną inteligencją?** Albo odwrotnie – czy **pracownik może wyręczyć się AI** przy swoich obowiązkach bez naruszenia umowy o pracę? Spójrzmy na to przez pryzmat polskiego Kodeksu pracy.

AI zamiast człowieka – co na to prawo?

Z formalnego punktu widzenia, **tylko człowiek może być pracownikiem** zatrudnionym na umowę o pracę. Definicja pracownika (art. 2 K.p.) mówi jasno: „*Pracownikiem jest osoba zatrudniona na podstawie umowy o pracę...*” – a więc **AI nie może być stroną stosunku pracy** ⁵⁵. Nie da się zawrzeć umowy o pracę z chatbotem ani wystawić robotowi świadectwa pracy. **Nie oznacza to jednak, że AI nie może wyeliminować pewnych stanowisk**. Pracodawca ma prawo tak organizować pracę, by była efektywna – jeśli wprowadzenie systemu AI sprawi, że obowiązki dotychczas wykonywane przez człowieka mogą być automatyzowane, to **może dojść do redukcji etatu z przyczyn organizacyjnych**. To podobna sytuacja jak automatyzacja linii produkcyjnej czy wdrożenie nowego oprogramowania zastępującego manualną pracę – prawo pracy **dopuszcza wypowiedzenie umowy z powodu likwidacji stanowiska** (art. 30 §1¹ K.p.), oczywiście z zachowaniem odpowiednich procedur (okres wypowiedzenia, konsultacje ze związkami jeśli działają, odprawy przy zwolnieniach grupowych itp.). **Innymi słowy, pracodawca może zwolnić pracownika, jeśli jego pracę przejmie AI, ale musi zrobić to zgodnie z kodeksem pracy** – uczciwie uzasadnić przyczynę i dopełnić formalności.

Dobra wiadomość jest taka, że na razie **AI częściej wspomaga niż zastępuje całkowicie**. Co prawda, niemal połowa pracowników obawia się, że zostanie w tyle, jeśli nie będą korzystać z AI, a 31% boi się utraty pracy z powodu AI ⁵⁶. Jednak większość firm postrzega AI jako narzędzie podnoszące **wydajność pracy ludzi, a nie prosty zamiennik pracownika**. Przykładowo, bank może wdrożyć chatbota AI do obsługi prostych pytań klientów – ale wciąż potrzebuje konsultantów do trudniejszych spraw. Niemniej **trend automatyzacji** jest faktem, więc pracownicy powinni się dokształcać i nabywać kompetencje komplementarne do AI, aby wspólnie z nią (a nie w konkurencji) tworzyć wartość. Z kolei pracodawca planujący redukcję dzięki AI powinien rozważyć, czy nie przeszkolić obecnych pracowników do nowych ról (reskilling) – to często bardziej opłacalne niż zwolnienia i rekrutacja od zera.

Osobisty charakter świadczenia pracy a korzystanie z AI

Przyjrzyjmy się teraz drugiej stronie medalu: **pracownik korzysta z AI przy wykonywaniu swoich obowiązków**. Czy to nie narusza zasad stosunku pracy, zwłaszcza tzw. *osobistego charakteru świadczenia pracy*? Kodeks pracy (art. 22 §1) stanowi, że pracownik zobowiązuje się do wykonywania pracy **osobiście**, a pracodawca do zapłaty wynagrodzenia ⁵⁷. Oznacza to, że pracownik **nie może przekazać swojej pracy komuś innemu** – nie może wysłać zastępcy zamiast siebie. Na pierwszy rzut oka mogłoby się wydawać, że jeśli pracownik „każe” pewne zadania wykonać AI, to **nie wykonuje pracy osobiście**.

Jednak analizy prawne wskazują coś innego: **korzystanie z AI to użycie narzędzia, a nie zastępczego wykonawcy** ⁵⁸ ⁵⁹ .

Orzecznictwo Sądu Najwyższego dopuszcza **incydentalną pomoc osób trzecich** przy pracy – np. kolega pomoże pracownikowi w wyjątkowej sytuacji – byle ta pomoc miała charakter **wspierający, a nie zastępczy** ⁶⁰ ⁶¹ . **AI można porównać do takiego narzędzia pomocniczego**. Jak zauważyła jedna z ekspertek, to człowiek **inicjuje proces** (daje zadanie AI), a AI wykonuje pewną część pracy, lecz **ostateczna kontrola i odpowiedzialność spoczywa na człowieku** ⁶² ⁶³ . Pracownik uruchamia system, nadzoruje wyniki i decyduje, co z nimi zrobić – **AI pełni rolę instrumentu, przedłużenia jego ręki czy umysłu**.

Dlatego **korzystanie z narzędzi AI nie pozbawia pracy cechy osobistego świadczenia** ⁵⁹ . To podobnie jak użycie kalkulatora, komputera czy programu biurowego – nadal pracę wykonuje pracownik, tylko wspomagany technologią. Ważne jest, aby **pracownik zachował kontrolę**: samodzielnie uruchamia narzędzie, **weryfikuje wyniki AI, poprawia błędy i bierze odpowiedzialność** za efekt końcowy ⁶⁴ . Jeśli te warunki są spełnione, nie można zarzucić mu, że „podzlecił” pracę AI.

Przykład: Marta, analityczka finansowa, używa AI do wygenerowania wstępnego raportu z danymi rynkowymi. **System AI** przetwarza dane i podsuwa jej rekomendacje inwestycyjne, ale to **Marta samodzielnie ocenia** te rekomendacje, dokonuje poprawek i podejmuje finalne decyzje. Jej praca nadal ma charakter osobisty – AI jest tylko narzędziem analitycznym, jak zaawansowany kalkulator ⁶⁵ ⁶⁶ .

Podkreślmy jednak granicę: **AI nie może całkowicie zastąpić uwagi i osądu pracownika**. Gdyby pracownik bezrefleksyjnie polegał na AI i np. przekopiował klientowi odpowiedź wygenerowaną przez chatbota z błędnymi danymi – poniesie konsekwencje tak, jakby sam popełnił błąd. AI bywa omylna i zdarza jej się **“halucynować” – generować treści pozornie wiarygodne, lecz fałszywe**. Badania wskazują, że użytkownicy często nie zauważają błędów, **zbyt ufając narzędziom AI (tzw. błąd automatyzacji)** ⁶⁷ ⁶⁸ . Dlatego pracownik musi używać AI z rozsądkiem: jako pomoc, ale **nie wyrocznie**. Firmy powinny uczulać personel, że **wyniki z AI należy weryfikować**, zwłaszcza gdy chodzi o informacje dla klienta czy dane wykorzystywane do podjęcia decyzji.

Granice korzystania z AI przez pracownika

Ostatnia ważna kwestia: **czy pracownik może być ukarany za używanie AI w pracy?** Tutaj decyduje **wewnętrzna polityka firmy** i okoliczności. **Jeśli pracodawca oficjalnie zakazał używania AI**, a pracownik mimo to korzysta z niej, może to być potraktowane jako **naruszenie obowiązków pracowniczych**. W skrajnych przypadkach – zwłaszcza gdy skutkiem jest poważne zagrożenie dla firmy (np. wyciek danych, ujawnienie tajemnicy) – **pracodawca ma prawo zwolnić takiego pracownika dyscyplinarnie** za ciężkie naruszenie obowiązków ⁶⁹ . Nawet jeśli firma **nie wprowadziła formalnego zakazu**, ale **działania pracownika spowodują negatywne skutki** (np. straci klienta przez błąd AI albo ujawni chronione informacje), to **musi liczyć się z konsekwencjami**, włącznie z wypowiedzeniem umowy z powodu utraty zaufania ⁶⁹ . Innymi słowy, **rozsądek i lojalność wobec pracodawcy wymagają, by pracownik korzystał z AI tylko w ramach wyznaczonych zasad**. Właśnie dlatego tak istotne jest wcześniejsze ustanowienie jasnej polityki – by obie strony wiedziały, co wolno.

Trzeba też wspomnieć o **monitorowaniu pracownika przy użyciu AI** – np. niektóre firmy kusi śledzenie aktywności pracowników przez algorytmy (analiza korespondencji, kamera z rozpoznawaniem twarzy itp.). To jednak podlega ograniczeniom prawnym (RODO, prawo pracy, prawo do prywatności). Monitoring musi być proporcjonalny i transparentny. AI nie może np. podejmować **samodzielnie decyzji o zwolnieniu pracownika** na podstawie samych statystyk efektywności – pracodawca musi

zapewnić czynnik ludzki w ocenie wyników, by uniknąć błędów i dyskryminacji. Ta zasada zostanie jeszcze wzmocniona przez AI Act, który dla systemów AI używanych do oceny pracowników czy rekrutacji będzie nakładał określone obowiązki (np. dokumentowanie takiego systemu, zapewnienie nadzoru człowieka). Już teraz jednak Urząd Ochrony Danych Osobowych czy Państwowa Inspekcja Pracy bacznie przyglądają się technologiom monitoringu – warto zachować ostrożność i umiar, **stawiając na AI raczej w roli asystenta niż „elektronicznego kierownika”**.

Podsumowując: Z punktu widzenia prawa pracy **AI to narzędzie, a nie pracownik**. Pracodawca może usprawniać pracę AI i nawet redukować etaty, ale musi przestrzegać przepisów o wypowiedzeniach. Pracownik z kolei może korzystać z AI, o ile robi to **lojalnie i z zachowaniem kontroli**, nie łamiąc zakazów firmy ani nie narażając jej na szkodę. Współpraca człowieka z AI powinna przypominać tandem, gdzie AI zwiększa możliwości pracownika, a nie go zastępuje.

Propozycja: jeden czy dwa filmy?

Temat **“Jak wdrożyć AI w firmie zgodnie z prawem?”** jest dość obszerny, dlatego warto rozważyć formę prezentacji. Możliwe są dwie opcje:

- **Jeden dłuższy film (~10 minut):** obejmujący całość zagadnień w jednym materiale – od definicji i przepisów, przez RODO, po prawo pracy. Taka forma daje widzom pełen obraz za jednym razem, ale wymaga utrzymania ich uwagi przez cały okres trwania filmu i bardzo klarownej struktury, by nie zgubili wątku.
- **Dwa krótsze filmy (ok. 5 minut każdy):** podzielenie tematu na dwie części może ułatwić przyswojenie informacji. **Propozycja podziału:** część **I** – aspekty techniczno-prawne: definicja AI, polityka w firmie, zgodność z RODO, dostawcy AI, odpowiedzialność pracodawcy; część **II** – aspekty kadrowe: AI a prawo pracy, relacja pracownik-AI, personalne konsekwencje używania AI. W ten sposób widzowie zainteresowani konkretnie np. kwestiami RODO obejrzą część I, a osoby ciekawie się HR-owymi dylematami – część II. Oczywiście można zachęcić do obejrzenia obu, by mieć pełny obraz.

Rekomendacja: Ze względu na ilość informacji skłaniałbym się ku **dwóm filmom**, co pozwoli lepiej zgłębić każdy blok tematyczny bez pośpiechu. W pierwszym odcinku można spokojnie wyjaśnić podstawy prawne i praktyczne wskazówki wdrożenia AI, a w drugim skupić się na konkretnej sytuacji pracownika i pracodawcy. Jeśli jednak publiczność kanału woli kompleksowe, jednorazowe materiały, jeden 10-minutowy film również da się zrealizować – kluczem będzie wtedy wyraźne rozdzielanie segmentów i podsumowanie najważniejszych punktów po każdej sekcji, by utrwalić wiedzę. Wybór formatu warto dostosować do preferencji widzów i ich czasu, jaki chcą poświęcić na jeden materiał.

ütfen, en arabic note

1 3 4 AI Act - definicja AI - czym jest wg prawa?

<https://lome.legal/system-ai-definicja-obowiazki-ai-act/>

2 6 40 42 44 45 49 50 51 52 54 Czym jest shadow AI i jak może zostać wykorzystane?

<https://poradnikprzedsiebiorcy.pl/-shadow-ai-czyli-pracownik-wykorzystujacy-chatgpt-w-pracy-a-rod-i-prywatnosc>

5 24 25 26 27 56 Korzystanie z AI i zjawisko Shadow AI w polskich firmach - CRN

<https://crn.pl/aktualnosci/55-proc-polskich-pracownikow-ukrywa-przed-pracodawca-korzystanie-z-ai/>

7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 28 29 30 Wewnętrzna polityka AI firmy w praktyce. Co powinna zawierać? - Legalis Księgowość Kadry Biznes

<https://biz.legalis.pl/wewnetrzna-polityka-ai-firmy-w-praktyce-co-powinna-zawierac/>

31 32 41 46 47 48 67 68 ChatGPT i Microsoft Copilot w urzędzie – legalność wg RODO i opinii EROD 28/2024?

<https://odo24.pl/wiedza/pytania-i-odpowiedzi-wpis.chatgpt-i-microsoft-copilot-w-urzedzie-legalnosc-wg-rod-i-opinii-erod-28-2024>

33 34 36 37 38 39 43 53 Dane w OpenAI API – gdzie trafiają i jak to uregulować?

<https://www.przewodnikporodo.pl/transfery-danych-miedzynarodowe/dane-w-openai-api-gdzie-trafiaja-i-jak-to-uregulowac>

35 Korzystanie z ChatGPT a RODO

<https://sylwiaczub.pl/korzystanie-z-chatgpt-a-rod/>

55 57 58 59 60 61 62 63 64 65 66 Sztuczna inteligencja w miejscu pracy - Porady.pl

<https://porady.pl/sztuczna-inteligencja-w-miejscu-pracy/>

69 Sztuczna inteligencja w pracy a kwestia zatrudnienia

<https://poradnikprzedsiebiorcy.pl/-sztuczna-inteligencja-w-pracy-czy-jej-stosowanie-moze-prowadzic-do-zwolnien>