
Pracownicy już używają ChatGPT

*Polityka AI dla małej firmy — AI Act i RODO krok po kroku,
z gotowymi dokumentami*

Spis treści

Zanim zaczniesz: jak korzystać z tej książki	3
Dla kogo jest ta książka	3
Czym ta książka NIE jest	3
Jak jest zbudowana	3
Ramki, które spotkasz w tekście	4
Załączniki	5
Stan prawny i aktualizacje	5
CZĘŚĆ I — ZROZUM	8
1. Co się dzieje w Twojej firmie, kiedy nie patrzysz	9
Trzy sceny z życia małej firmy	9
To nie jest wyjątek — to norma	9
Cztery ryzyka, o które naprawdę chodzi	10
Co to znaczy dla Ciebie	11
2. Trzy przepisy, które Cię dotyczą — w jednej tabeli	13
Dwie role: dostawca i podmiot stosujący	14
Czego NIE musisz — żeby nie robić za dużo	15
Koniec próbki	18

Zanim zaczniesz: jak korzystać z tej książki

Ta książka ma jeden cel: **po jej przeczytaniu i wykonaniu kroków masz w firmie porządek w sprawie sztucznej inteligencji** — na papierze i w praktyce. Nie musisz rozumieć, jak działają modele językowe. Musisz podjąć kilkanaście decyzji, wypełnić kilka wzorów i raz na kwartał sprawdzić, czy nadal są aktualne.

Dla kogo jest ta książka

- Prowadzisz firmę zatrudniającą od jednej do kilkudziesięciu osób (biuro rachunkowe, gabinet, kancelaria, agencja, sklep internetowy, firma usługowa, warsztat, mała produkcja).
- Ty albo Twoi ludzie korzystacie — oficjalnie lub nie — z ChatGPT, Claude, Gemini, Copilota, Canvy z funkcjami AI, narzędzi do transkrypcji spotkań, chatbota na stronie albo programu rekrutacyjnego, który „sam ocenia kandydatów”.
- Nie masz działu prawnego, działu IT ani inspektora ochrony danych na etacie (albo masz, ale chcesz wiedzieć, o co go zapytać).
- Słyszysz o „AI Act”, „RODO”, „karach 35 milionów euro” i chcesz wiedzieć, **co z tego naprawdę dotyczy Twojej firmy i co masz mieć na papierze**.

Czym ta książka NIE jest

WAŻNE

To nie jest porada prawna. Książka ma charakter informacyjny i edukacyjny. Opisuje stan prawny na dzień **23 sierpnia 2026 r.** i pokazuje, jak w praktyce spełnić obowiązki typowej małej firmy. Monaltro jest biurem rachunkowym i firmą wdrażającą rozwiązania cyfrowe — **nie jest kancelarią prawną, radcą prawnym ani doradcą podatkowym.** Jeśli Twoja sytuacja jest nietypowa (np. używasz AI do oceny kandydatów, zdolności kredytowej klientów albo przetwarzasz dane medyczne), skonsultuj wypełnione dokumenty z radcą prawnym lub inspektorem ochrony danych. W książce zaznaczamy wprost miejsca, w których taka konsultacja jest wskazana.

Jak jest zbudowana

Książka ma trzy części i czternaście załączników.

Część	Co robisz	Ile czasu
I. Zrozum (rozdziały 1–4)	Czytasz. Dowiadujesz się, co Ci grozi, które przepisy Cię dotyczą, od kiedy i kto to kontroluje. Robisz test „czy mnie to dotyczy”.	ok. 60 minut
II. Zrób (rozdziały 5–11)	Siedem kroków. Każdy ma cel, czas, listę kontrolną i gotowy wzór dokumentu. Pierwszy efekt (rejestr narzędzi i decyzje) masz po jednym popołudniu; komplet po 3–4 tygodniach.	12–20 godzin łącznie, rozłożone
III. Utrzymaj (rozdziały 12–16)	Przegląd kwartalny, kalendarz terminów do 2028 r., ścieżka dla firm z „wysokim ryzykiem”, odpowiedzi na najczęstsze pytania, słownik, źródła.	1–2 godziny na kwartał

Każdy z siedmiu kroków kończy się sekcją **„Zanim przejdiesz dalej”** z polami do odhaczenia. Jeśli czegoś nie możesz odhaczyć — nie idź dalej, tylko wróć do instrukcji kroku. To nie jest formalność: kolejne kroki zakładają, że poprzednie są zrobione.

Ramki, które spotkasz w tekście

UWAGA

UWAGA — pułapka, w którą wpada większość firm. Przeczytaj dwa razy.

PRZYKŁAD

PRZYKŁAD — jak to wygląda w konkretnej firmie: w biurze rachunkowym, w sklepie internetowym, w agencji, w gabinecie.

WAŻNE

WAŻNE — fakt prawny z podanym źródłem (numer artykułu i link). Na tym możesz się oprzeć.

WZÓR

WZÓR — fragment do skopiowania: zdanie do polityki, komunikat dla klientów, treść maila do dostawcy.

Załączniki

Wzory dokumentów są w dwóch miejscach: w treści książki (żebyś widział/a, jak wyglądają) i jako osobne, edytowalne pliki DOCX w katalogu [załączniki/](#). Wypełniasz pola oznaczone [WSTAW: ...]. Wszystkie dokumenty są napisane tak, żeby firma 5-osobowa mogła je przyjąć bez zmian, a firma 40-osobowa — po drobnych uzupełnieniach.

Załącznik	Dokument	Używasz w kroku
A	Ankieta inwentaryzacyjna (anonimowa)	1
B	Rejestr narzędzi AI	1, 2
C	Polityka korzystania ze sztucznej inteligencji (wzór)	4
D	Lista kontrolna umowy powierzenia (DPA) i transferu danych	3
E	Zapytanie do dostawcy o zgodność z AI Act i RODO	3
F	Agenda i skrypt szkolenia (60 minut)	5
G	Lista obecności i test wiedzy	5
H	Komunikaty chatbota i voicebota (art. 50 ust. 1)	6
I	Rejestr treści AI i wzory etykiet	6
J	Procedura kontroli redakcyjnej tekstów AI	6
K	Aneks dla agencji i freelancerów	6
L	Klauzula licencyjna i arkusz wkładu człowieka	6
M	Procedura postępowania z incydem	7
N	Lista kontrolna przeglądu kwartalnego	12

Stan prawny i aktualizacje

Przepisy o AI zmieniają się szybko. Ta wersja (1.0.0) uwzględnia:

- rozporządzenie (UE) 2024/1689 (AI Act) w brzmieniu po zmianach wprowadzonych rozporządzeniem (UE) 2026/1744 (tzw. AI Omnibus, obowiązuje od 27 lipca 2026 r.),
- polską ustawę z dnia 3 lipca 2026 r. o systemach sztucznej inteligencji (Dz.U. 2026 poz. 1003),
- finalne wytyczne Komisji Europejskiej do art. 50 AI Act (20 lipca 2026 r.) i Kodeks praktyk dotyczący przejrzystości treści generowanych przez AI (10 czerwca 2026 r.),
- RODO i praktykę polskiego organu ochrony danych.

Kolejne wersje książki będą odnotowywane w dzienniku zmian na końcu. Rozdział 12 pokazuje, które daty wpisać do kalendarza i gdzie sprawdzać zmiany samodzielnie.

CZEŚĆ I — ZROZUM

1. Co się dzieje w Twojej firmie, kiedy nie patrzysz

Trzy sceny z życia małej firmy

Biuro rachunkowe, wtorek, 16:40. Księgowa ma do opisanie trzydzieści faktur kosztowych nietypowego klienta. Otwiera darmowego ChatGPT w przeglądarce, wkleja treść faktur — z nazwami kontrahentów, numerami NIP, kwotami — i prosi o tabelę z podziałem na kategorie kosztów. Dostaje ją w dwadzieścia sekund. Jest zadowolona. Nikt jej tego nie zabronił, bo nikt nie pomyślał, że trzeba.

Agencja marketingowa, czwartek. Grafik robi baner dla klienta z branży meblowej. Nie ma zdjęcia salonu, więc generuje fotorealistyczne wnętrza w Canvie. Klient jest zachwycony. Baner trafia do kampanii na Facebooku. Trzy dni później Meta odrzuca reklamę: „treść zawiera materiały generowane przez AI, które nie zostały ujawnione”. Kampania stoi, klient pyta, co się stało.

Firma produkcyjna, 30 osób. Kadrowa testuje program, który „sam ocenia CV” i układa kandydatów w ranking. Kupiła go, bo oszczędza jej trzy godziny dziennie. Nie wie, że w załączniku III do unijnego rozporządzenia o sztucznej inteligencji taki system jest wymieniony z nazwy jako „wysokiego ryzyka” i że w grudniu 2027 r. zaczną obowiązywać dla niego konkretne obowiązki — w tym poinformowanie pracowników i zapewnienie nadzoru człowieka.

Żadna z tych osób nie zrobiła niczego w złej wierze. Każda z nich rozwiązywała realny problem swojej pracy. I każda wystawiła firmę na ryzyko, o którym właściciel dowie się ostatni.

To nie jest wyjątek — to norma

Zjawisko ma nazwę: **shadow AI** — korzystanie z narzędzi sztucznej inteligencji, o których firma nie wie albo których nie zatwierdziła. Liczby, które warto znać:

- W badaniu Microsoft i LinkedIn *Work Trend Index 2024* (31 tys. pracowników w 31 krajach) **52%** pracowników zadeklarowało, że używa AI w pracy, a z tej grupy **78%** przynosi do firmy własne narzędzia — nie te, które dała im firma.¹
- Według raportu IBM *Cost of a Data Breach 2025* w **20%** organizacji, które miały wyciek danych, do incydentu przyczyniły się niezatwierdzone narzędzia AI; taki wyciek kosztował średnio o **670 tys. USD** więcej. Organizacje, które miały spisane zasady korzystania z AI, ponosiły koszty naruszeń o **40%** niższe.²

1. Microsoft & LinkedIn, *2024 Work Trend Index*

Annual Report: AI at work is here. Now comes the hard part, maj 2024,

<https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>

Ostatnia liczba jest najważniejsza w tej książce. **Firma, która ma zasady, traci mniej** — nie dlatego, że zasady są magiczne, tylko dlatego, że ludzie wiedzą, co wolno, a co nie, i mają komu zgłosić problem.

Cztery ryzyka, o które naprawdę chodzi

Nie musisz znać się na AI, żeby zrozumieć, co może pójść nie tak. Ryzyka są cztery i każde z nich ma swoją „szufladę” w przepisach.

1. Dane osobowe wychodzą z firmy (RODO)

Kiedy pracownik wkleja do darmowego narzędzia AI treść umowy, listę klientów, CV kandydata albo korespondencję z pacjentem, **przekazuje dane osobowe firmie trzeciej** — najczęściej spoza Unii Europejskiej — bez umowy, bez podstawy prawnej i bez Twojej wiedzy. Z punktu widzenia RODO to Ty jesteś administratorem tych danych i Ty odpowiadasz.

Ryzyko nie polega na tym, że „ktoś w Kalifornii przeczyta umowę”. Polega na tym, że:

- w darmowych planach konsumenckich treść rozmów **może być wykorzystywana do trenowania modeli**, jeśli użytkownik tego nie wyłączył,
- nie masz umowy powierzenia przetwarzania (art. 28 RODO), więc nie masz nawet prawa tam tych danych wystać,
- nie wiesz, czy i kiedy dane zostały usunięte,
- jeśli dojdzie do wycieku, nie dowiesz się o nim — a masz 72 godziny na zgłoszenie do Prezesa UODO.

2. Tajemnica firmy i tajemnice klientów (umowy, NDA)

Cennik, marże, plany, kod źródłowy, dokumentacja techniczna klienta, strategia przetargowa — to nie są dane osobowe, więc RODO ich nie chroni. Chroni je **umowa z klientem** (klauszula poufności) i prawo o zwalczaniu nieuczciwej konkurencji. Jeśli Twój pracownik wklei dokumentację klienta do publicznego narzędzia, a klient się dowie, problem nie jest „regulacyjny” — jest handlowy i może skończyć się utratą klienta lub karą umowną.

3. Nieoznaczone treści i chatbot, który udaje człowieka (AI Act, art. 50)

Od **2 sierpnia 2026 r.** obowiązują w całej Unii przepisy o przejrzystości: chatbot musi się przedstawić jako AI, a treści typu deepfake (fotorealistyczne obrazy, wideo i audio wygenerowane przez AI) muszą być oznaczone. Platformy reklamowe (Meta, Google) wymuszają to po swojemu — odrzucając reklamy. Ryzyko to nie tylko kara od organu nadzoru (w Polsce: KRIŚI), ale przede wszystkim **zatrzymana kampania i utrata zaufania**, kiedy klient odkryje, że „zdjęcie salonu” nigdy nie istniało.

2. IBM, Cost of a

Data Breach Report 2025,

<https://www.ibm.com/reports/data-breach>

4. Decyzje o ludziach podejmowane przez maszynę (AI Act, wysokie ryzyko)

Jeśli AI ocenia kandydatów do pracy, decyduje o premiach, ocenia zdolność kredytową klientów albo egzaminuje uczniów — wchodzisz w kategorię „**wysokiego ryzyka**” z własnym reżimem obowiązków (od 2 grudnia 2027 r.). Większości małych firm to nie dotyczy. Ale firmy, których dotyczy, zwykle o tym nie wiedzą — bo kupiły „program do rekrutacji”, a nie „system AI wysokiego ryzyka”.

Co to znaczy dla Ciebie

Przepisy o AI nie wymagają od małej firmy rzeczy niemożliwych. Wymagają **trzech prostych rzeczy**, które i tak warto mieć:

1. **Wiedzieć, czego używasz** — rejestr narzędzi (krok 1).
2. **Ustalić i spisać zasady** — polityka AI, umowy z dostawcami, komunikaty dla klientów (kroki 2–4, 6).
3. **Nauczyć ludzi** — krótkie, udokumentowane szkolenie (krok 5) i procedura na wypadek wypadki (krok 7).

Reszta tej książki to instrukcja, jak to zrobić w 3–4 tygodnie, bez prawnika na etacie.

UWAGA

Najczęstszy błąd właściciela: zakaz. Reakcją na pierwszą wpadkę bywa polecenie „od dziś nikt nie używa ChatGPT”. To nie działa — pracownicy przechodzą na prywatne telefony i przestają mówić o tym, co robią. Shadow AI nie znika, tylko schodzi głębiej do cienia. Celem nie jest zakaz, tylko **kanal**: zatwierdzone narzędzia, jasne kategorie danych i prosty sposób zgłaszania problemów.

2. Trzy przepisy, które Cię dotyczą — w jednej tabeli

Zacznijmy od uporządkowania słownictwa, bo w mediach wszystko zlewa się w jedno „prawo o AI”. Dla małej firmy w Polsce liczą się trzy akty prawne:

Akt	Co to jest	Czego dotyczy w Twojej firmie	Kto kontroluje
AI Act — rozporządzenie (UE) 2024/1689 ³	Unijne rozporządzenie — obowiązuje bezpośrednio, bez „wdrażania” do prawa polskiego. Od 27 lipca 2026 r. zmienione tzw. AI Omnibusem. ⁴	Kompetencje pracowników (art. 4), zakazane praktyki (art. 5), przejrzystość — chatboty i treści AI (art. 50), systemy wysokiego ryzyka (rozdz. III).	KRIBSI (w Polsce)
RODO — rozporządzenie (UE) 2016/679 ⁵	Ochrona danych osobowych — obowiązuje od 2018 r. i niczego w nim nie zmieniono z powodu AI.	Wszystko, co dzieje się z danymi osobowymi w narzędziach AI: podstawa prawna, umowa powierzenia, transfer poza EOG, informowanie, wycieki.	Prezes UODO
Ustawa o systemach sztucznej inteligencji z 3 lipca 2026 r. (Dz.U. 2026 poz. 1003) ⁶	Polska ustawa „obslugująca” AI Act: powołuje organ nadzoru, określa tryb kontroli i kar, piaskownicę regulacyjną, opinie indywidualne.	Do kogo zgłaszać, kto Cię skontroluje, jak używać wiążącą opinię o swojej sytuacji.	KRIBSI

3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie sztucznej inteligencji, tekst polski:

<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/pol>

4. Rozporządzenie (UE) 2026/1744 (tzw. Digital Omnibus on AI), Dz.Urz. UE z 24.07.2026, w mocy od 27.07.2026:

<https://eur-lex.europa.eu/eli/reg/2026/1744/oj/pol>

5. Rozporządzenie (UE) 2016/679 (RODO), tekst polski:

<https://eur-lex.europa.eu/eli/reg/2016/679/oj/pol>

6. Ustawa z dnia 3

lipca 2026 r. o systemach sztucznej inteligencji, Dz.U. 2026 poz. 1003:

<https://eli.gov.pl/eli/DU/2026/1003/ogl> (ISAP:

<https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20260001003>)

Do tego dochodzą przepisy, które nie są „o AI”, ale AI je uruchamia: **prawo autorskie** (czy treść wygenerowana przez AI jest Twoja), **regulaminy platform** (Meta, Google, TikTok — oznaczanie kreacji AI) i **prawo pracy** (informowanie pracowników o systemach, które ich oceniają). Omawiamy je w kroku 6 i rozdziale 13.

Dwie role: dostawca i podmiot stosujący

AI Act dzieli świat na tych, którzy AI **robią**, i tych, którzy AI **używają**. To najważniejsze rozróżnienie w tej książce, bo od niego zależy, ile masz obowiązków.

WAŻNE

Art. 3 pkt 3 AI Act — „dostawca” to podmiot, który *rozwija system AI* (lub zleca jego rozwój) i *pod własną nazwą lub znakiem towarowym wprowadza go do obrotu lub oddaje do użytku*.

Art. 3 pkt 4 — „podmiot stosujący” to podmiot, który *wykorzystuje system AI, nad którym sprawuje kontrolę*, z wyjątkiem użytku osobistego, pozazawodowego.

Źródło: rozporządzenie (UE) 2024/1689, art. 3.

Po polsku:

Sytuacja	Rola	Co to oznacza
Zespół korzysta z ChatGPT Business, Copilota, Gemini, Claude	podmiot stosujący	Obowiązki: kompetencje (art. 4), nieużywanie do zakazanych celów (art. 5), RODO. Art. 50 — tylko jeśli publikujesz deepfake lub prowadzisz chatbota dla klientów.
Masz chatbota na stronie/WhatsAppie zbudowanego z gotowego narzędzia (Tidio, Intercom, Meta Business Agent)	podmiot stosujący	Jak wyżej + obowiązek, żeby bot informował, że jest AI (art. 50 ust. 1 — formalnie zapewnia to dostawca, ale to Ty odpowiadasz za ustawienia i komunikat).
Generujesz grafiki, wideo, lektora AI do marketingu	podmiot stosujący	Art. 50 ust. 4 — oznaczanie deepfake (krok 6).
Kupujesz program do oceny CV / scoringu klientów	podmiot stosujący systemu wysokiego ryzyka	Rozdział 13 — obowiązki od 2 grudnia 2027 r.
Budujesz i sprzedajesz klientom własnego chatbota / narzędzie AI pod własną marką	dostawca	Znacznie szerszy reżim (dokumentacja, znakowanie maszynowe treści — art. 50 ust. 2). Ta książka tego nie obejmuje — potrzebna konsultacja prawna.

PRZYKŁAD

Agencja marketingowa, która uruchamia klientom chatboty na bazie gotowej platformy, zwykle pozostaje podmiotem stosującym (lub pomaga klientowi, który nim jest). Ale agencja, która **pod własną marką** oferuje „nasz asystent AI” zbudowany na API modelu, może stać się **dostawcą**. Granica zależy od tego, czyja nazwa jest na produkcie i kto go „oddaje do użytku”. Jeśli jesteś blisko tej granicy — to jeden z dwóch przypadków w tej książce, w których od razu kierujemy do prawnika (drugi to wysokie ryzyko).

Czego NIE musisz — żeby nie robić za dużo

Większość małych firm to podmioty stosujące, które używają gotowych narzędzi do codziennej pracy. Dla nich **nie istnieje** obowiązek:

- rejestrowania firmy w jakiegokolwiek „bazie AI” (rejestr w art. 49 AI Act dotyczy dostawców systemów wysokiego ryzyka i organów publicznych),
- sporządzania „dokumentacji technicznej” systemu, oceny zgodności ani oznakowania CE (to obowiązki dostawców),
- powoływania „pełnomocnika ds. AI” (taka funkcja w przepisach nie istnieje; inspektor ochrony danych to osobna instytucja z RODO, wymagana tylko w określonych przypadkach),
- przeprowadzania oceny skutków dla praw podstawowych (art. 27 AI Act — tylko podmioty publiczne, świadczące usługi publiczne oraz stosujące AI do oceny zdolności kredytowej lub ubezpieczeń na życie i zdrowotnych),
- „certyfikowania” pracowników — art. 4 wymaga *wspierania rozwoju kompetencji*, nie egzaminów państwowych (o tym w kroku 5).

Co **musisz** — to pięć rzeczy, które składają się na resztę tej książki: wiedzieć, czego używasz; mieć zasady; mieć umowy z dostawcami; przeszkolić ludzi; informować klientów, gdy rozmawiają z AI lub oglądają treści AI.

Koniec próbki

To był wstęp i pierwszy rozdział. Pełna wersja to **16 rozdziałów** prowadzących przez siedem kroków — od anonimowej ankiety wśród pracowników po przegląd kwartalny — oraz **14 gotowych dokumentów w plikach DOCX i Markdown**: ankieta inwentaryzacyjna, rejestr narzędzi AI, wzór polityki korzystania z AI, lista kontrolna umowy powierzenia, zapytanie do dostawcy (PL i EN), agenda i skrypt szkolenia, lista obecności z testem wiedzy, komunikaty chatbota, rejestr treści AI z wzorami etykiet, procedura kontroli redakcyjnej, aneks dla agencji, klauzula licencyjna, procedura postępowania z incydemem i lista kontrolna przeglądu kwartalnego.

Pełna wersja e-booka wraz z załącznikami: <https://sklep.monaltro.pl/>