localize.pl

PRZEWODNIK DLA FIRM

AI Act w Twojej firmie

Co sprawdzić, w jakiej kolejności i które obowiązki są po Twojej stronie. Dla firm działających na rynku UE.

Localize.pl — Agenor Hofmann-Delbor
Stan prawny: **29 lipca 2026**

Jak czytać ten przewodnik. Trzy zasady, od których wszystko się zaczyna:

1. **Liczy się zastosowanie narzędzia, a nie jego nazwa.** Ten sam produkt, np. Copilot firmy Microsoft, używany do redakcji tekstu i do wsparcia rekrutacji to dwa kompletnie różne przypadki.
2. **Kluczowe jest zrozumienie, jak klasyfikować rolę organizacji.** Dostawca rozwiązania AI ma zupełnie inne obowiązki niż firma, która korzysta z gotowego narzędzia. Możesz też mieć obie role naraz w różnych systemach.
3. **Kategorie się nakładają, ale wymagają odrębnych testów.** Będą potrzebne testy w kategorii zakazów, wysokiego ryzyka i przejrzystości.

W skrócie: 7 rzeczy, które trzeba wiedzieć

1. **AI Act może Cię dotyczyć**, nawet jeśli Twoja firma tylko używa zewnętrznych narzędzi AI i ich nie wytwarza. Zakres obowiązków zależy od **konkretnego zastosowania** i od **Twojej roli**. Inne ma dostawca, a inne firma, która jedynie korzysta z gotowego narzędzia.
2. **Od 2 sierpnia 2026** stosuje się tzw. obowiązki przejrzystości z art. 50. **Nie każdy z nich dotyczy każdego**, a każdy ustęp artykułu dotyczy innej roli. Który dotyczy Ciebie, sprawdzisz w rozdziale 4.
3. **Polska ustawa o systemach sztucznej inteligencji jest już ogłoszona:** ustawa z dnia 3 lipca 2026 r., **Dz.U. 2026 poz. 1003**, ogłoszona 27 lipca 2026. Data wejścia w życie to co do zasady czternasty dzień od ogłoszenia, czyli **11 sierpnia 2026**. Ustawa powołuje organ nadzoru: **KRiBSI**, Komisję Rozwoju i Bezpieczeństwa Sztucznej Inteligencji. Wniosek o interwencję tej instytucji może złożyć każdy, czyli np. klient, pracownik, albo... konkurent. Choć pełny rozruch KRiBSI może zająć trochę czasu, trzeba zaznaczyć, że obowiązki z tytułu AI Act stosuje się zgodnie z datami rozporządzenia, czyli w dużej części — już.
4. **Zakazy obowiązują od lutego 2025.** Jeden z nich dotyczy rozpoznawania emocji **w miejscu pracy i w edukacji**, czyli pracowników, kandydatów i uczniów. Co ciekawe, **analiza emocji klientów nie jest objęta tym zakazem**, ale podlega obowiązkowi informacyjnemu i wymogom RODO. Kara za praktykę zakazaną wynosi do 35 mln EUR lub 7% obrotu.
5. **Obowiązki dla systemów wysokiego ryzyka przesunięto.** Wchodzą w życie 2 grudnia 2027 (rekrutacja, ocena pracowników, scoring, edukacja).
6. **Od lutego 2025 trzeba wspierać kompetencje AI** u osób pracujących z tymi narzędziami (art. 4). Przepisy stwierdzają, że środki mają być **proporcjonalne**. Choć możliwości jest więcej, najprostszym sposobem, by spełnić ten wymóg, jest odbycie szkolenia i uzyskanie poświadczenia (elektroniczne wystarczy w zupełności).
7. **Nikt nie wymaga od Ciebie certyfikatu w zakresie AI Act.** Musisz jedynie **wiedzieć, czego używasz, i mieć należytą dokumentację w tym zakresie.** I tutaj fundamentem świętego spokoju będzie tzw. Rejestr zastosowań AI.

1. Czy to na pewno dotyczy mojej firmy?

Sprawdźmy to w prosty sposób. Zadaj sobie pięć poniższych pytań:

- Czy na Twojej stronie albo infolinii funkcjonuje chatbot lub voicebot?
- Czy publikujesz teksty, obrazy, wideo lub głos wygenerowane przez AI (opisy produktów, posty, reklamy, lektor, dubbing, awatary)?
- Czy ktoś w firmie używa ChatGPT, Copilota, Gemini, Claude lub podobnego narzędzia do pracy?
- Czy używasz narzędzi wspierających rekrutację, ocenę pracowników, scoring klientów lub wykrywanie nadużyć?
- Czy sprzedajesz produkt lub usługę, w której jest komponent AI?

Do objęcia wymogami AI Act **wystarczy, że tylko na jedno z tych pytań odpowiesz „tak"**. Pamiętaj, że samo posiadanie narzędzia zakupionego lata temu, które obecnie ma funkcje AI (np. MS 365), nie oznacza, że mamy do czynienia z powyższymi przypadkami.

Przewodnik jest w głównej mierze przeznaczony dla firm z siedzibą w UE lub działających na rynku unijnym. AI Act może jednak objąć także dostawcę albo podmiot stosujący spoza Unii, jeżeli wprowadza system na rynek unijny albo wynik działania systemu jest wykorzystywany w UE.

2. Kalendarz AI Act

Data	Zakres	Kogo dotyczy
2 lut 2025	Zakazane praktyki + obowiązek wspierania kompetencji AI u pracowników	**wszystkich**
2 sie 2025	Obowiązki twórców modeli AI (GPAI)	dostawców modeli
2 sie 2026	Przejrzystość (art. 50): chatbot się przedstawia, treści AI są oznaczane, zakres zależny od roli	zależnie od roli i zastosowania
2 gru 2026	**Koniec ulgi na znakowanie maszynowe dla starszych systemów + nowe zakazy (NCII/CSAM)**	firm z GenAI
2 gru 2027	Systemy wysokiego ryzyka: rekrutacja, HR, scoring kredytowy, ubezpieczenia, edukacja	wybranych branż
2 sie 2028	AI wbudowane w produkty regulowane (maszyny, wyroby medyczne, zabawki)	producentów

Niewątpliwie najrozsądniejszym założeniem jest traktowanie AI Act tak, jakby już obowiązywał w całości, dzięki czemu proces dostosowania będzie dawać długoterminowe efekty.

3. Cztery kategorie regulacyjne, czyli co sprawdzić

> **Ważne:** to nie są elementy jednego procesu. Zakaz, wysokie ryzyko i obowiązek przejrzystości sprawdza się **osobno** i nie ma znaczenia, że mogą się nakładać. Jedno narzędzie używane do dwóch różnych rzeczy może więc mieć dwie różne kwalifikacje.

Praktyki zakazane

Tu żarty się kończą, bo kara wynosi do 35 mln EUR lub 7% obrotu. Przykłady zastosowań wymagających sprawdzenia:

- **rozpoznawanie emocji pracownika, kandydata lub ucznia**. Zakaz dotyczy miejsca pracy i instytucji edukacyjnych (poza względami medycznymi i bezpieczeństwa). Kwalifikacja zależy od tego, **czyich emocji** dotyczy, **z jakich danych** system wnioskuje (biometryczne czy bezpośrednio treść rozmowy) i **w jakim kontekście**. I nie zawsze jest to oczywiste, bo zwykła analiza sentymentu transkrypcji to co innego niż system rozpoznawania emocji,
- ocenianie klientów lub pracowników „ogólną punktacją zaufania" i wyciąganie z tego konsekwencji w niezwiązanym obszarze,
- systemy manipulujące decyzją klienta w sposób wykorzystujący jego słabości i potencjalnie działający na jego szkodę.

> **Analiza emocji klientów** (np. w call center) **co do zasady nie wpada w ten zakaz**, ponieważ dotyczy on miejsca pracy. Sytuacja ta natomiast podlega obowiązkowi poinformowania osób (art. 50 ust. 3) i obowiązującym już od dawna przepisom RODO. To rozróżnienie bywa często mylone, więc pamiętaj, by dobrze się przyjrzeć temu zagadnieniu w ramach organizacji.

Systemy wysokiego ryzyka

Te, o dziwo, są dozwolone, ale pod warunkami. Musi istnieć dokumentacja, musi być nadzór człowieka, zapewniona dbałość o jakość danych, a do tego logi.

Przykłady: automatyczna selekcja CV kandydatów, ocena i awanse pracowników, scoring kredytowy, ocena ryzyka w ubezpieczeniach na życie i zdrowotnych, systemy oceniania w edukacji.

Obowiązek przejrzystości

Gdy czytasz ten przewodnik, masz już obowiązek w zakresie przejrzystości. Czas więc upewnić się, że należycie oznaczasz treści (i nie dotyczy to wyłącznie tagów widocznych dla botów).

Przykłady: chatbot, voicebot, generowane opisy i artykuły, syntetyczny lektor, AI dubbing, awatary, obrazy z generatora w reklamie.

Zastosowania o minimalnym ryzyku

Tu nie pojawiają się dodatkowe obowiązki z tytułu AI Act, poza dwoma obowiązkami przekrojowymi: wspieraniem kompetencji AI i przepisami o ochronie danych.

Przykłady: filtr spamu, autouzupełnianie, rekomendacje produktów, tłumaczenie maszynowe do użytku **wewnętrznego**.

4. Co konkretnie musisz mieć zrobione

> **Zacznij od ustalenia roli.** Art. 50 ma cztery ustępy i **każdy dotyczy kogoś innego**. Ust. 1 i 2 definiują **dostawcę** systemu, a ust. 3 i 4 odnoszą się do **podmiotu stosującego**, czyli firmy, która z systemu korzysta. Jeżeli kupujesz gotowe narzędzie od zewnętrznego dostawcy, część poniższych obowiązków leży więc po jego stronie, nie po Twojej.

4.1. Chatbot musi się przedstawić (art. 50 ust. 1, obowiązek dostawcy)

System przeznaczony do bezpośredniej interakcji z ludźmi musi jasno informować, że jest rozwiązaniem AI i to już **przy pierwszej interakcji**. Musi to uczynić w sposób czytelny i dostępny (a więc nie drobnym drukiem w regulaminie). Są wyjątki, gdy jest to oczywiste, ale zawsze bezpieczniej trzymać się powyższej reguły.

Dobrze: „Cześć, jestem asystentem AI Localize.pl. Odpowiadam automatycznie."
Źle: „Cześć, jestem Anna, w czym mogę pomóc?"

> Jeśli wystawiasz chatbota **pod własną nazwą** — także zbudowanego na cudzym API — to w tym momencie najprawdopodobniej jesteś jego **dostawcą** i ten obowiązek należy do Ciebie.

4.2. Oznaczanie maszynowe treści (art. 50 ust. 2, obowiązek dostawcy narzędzia)

Tu pojawia się obowiązek technicznego oznaczania treści syntetycznych w formacie odczytywalnym maszynowo (tagi, metadane C2PA, watermark, dane o pochodzeniu). Odpowiada za to **dostawca systemu generatywnego**, z wyjątkami określonymi w art. 50 ust. 2.

Co z tego wynika dla Ciebie jako użytkownika narzędzia? W ramach tzw. należytej staranności należy zweryfikować, czy narzędzie ma w ogóle funkcje oznaczania, co na ten temat mówią warunki licencji i czy Twój proces obróbki materiału nie usuwa metadanych. Sprawdź przede wszystkim ostatni element procesu i co rzeczywiście trafia do odbiorcy.

> Powyższe trzeba traktować jako **rozsądną praktykę i element zarządzania ryzykiem**, bo nie wynika wprost z art. 50 ust. 2. I tak warto to zrobić.
>
> Dla pewności sprawdź też kalendarz AI Act dla systemów, które były na rynku przed wdrożeniem rozporządzenia, bo w niektórych przypadkach możesz mieć jeszcze trochę czasu.

4.3. Deepfake (art. 50 ust. 4, obowiązek podmiotu stosującego)

Obowiązek ujawnienia powstaje, gdy materiał spełnia **definicję deepfake'u**. I tu diabeł tkwi w szczegółach, bo definicja mówi jedynie, że deepfake w sposób fałszywy sprawia wrażenie **autentycznego przedstawienia istniejącej osoby, obiektu, miejsca, podmiotu lub wydarzenia**. Przykładowo: różowy, latający pomidor wielkości miasta nie mógłby istnieć, ale pies grający na pianinie łapami już tak (nawet jeśli jest to nieludzko trudne dla psa).

Syntetycznego lektora, awatara i AI dubbing również oceniamy według tej definicji. Nie każdy materiał syntetyczny jest deepfakiem. Przykładowo: wygenerowany głos czytający Twój własny tekst produktowy zwykle nie udaje autentycznego nagrania konkretnej osoby. I nie mamy wówczas podstaw, by uznać materiał za deepfake.

Gdy test wypada negatywnie, **dobrą praktyką komunikacyjną jest dobrowolne ujawnienie**. Takie podejście buduje zaufanie i zdejmuje ryzyko zarzutu wprowadzenia w błąd. Nie jest to obowiązkiem, rzecz jasna, ale warto je wdrożyć.

4.4. Teksty publiczne o sprawach ważnych społecznie

Jeśli publikujesz teksty informujące opinię publiczną o sprawach interesu publicznego i są one generowane przez AI, sprawa jest jasna — trzeba ten fakt ujawnić. Tu od razu **wyjątek:** jeśli materiał przeszedł redakcyjną kontrolę człowieka, który bierze za niego odpowiedzialność, wtedy obowiązek znika. Trzeba jednak mieć ten proces wyraźnie opisany i udokumentowany.

4.5. Kompetencje AI (art. 4)

Od 2 lutego 2025 dostawcy i podmioty stosujące AI powinny podejmować tzw. **proporcjonalne środki wspierające rozwój kompetencji AI** u osób pracujących z tymi systemami w ich imieniu. Tu również kluczem będzie możliwość pokazania dowodu zastosowania wspomnianych środków. Może to być szkolenie z poświadczeniem uczestnictwa, instrukcja stanowiskowa, materiały edukacyjne, onboarding, ćwiczenia, konsultacje itp. Zalecany jest co najmniej test, który zostawia potwierdzenie sprawdzenia kompetencji. **Zakres zawsze dopasuj do ról, wiedzy, kontekstu użycia i ryzyka.**

> **Czy przepis mówi, jak ma wyglądać szkolenie?** Nie, nie ma żadnego narzuconego formatu szkolenia, corocznego cyklu ani wymaganej listy obecności. Dobrze jednak wewnętrznie na potrzeby firmy zdefiniować **własny standard** w ramach dobrej praktyki. Nawet jeśli brak takiego standardu nie stanowi naruszenia AI Act.

5. Rejestr systemów AI

Rozporządzenie nie nakazuje wprost „prowadzenia rejestru" każdej firmie, ale **bez rejestru znacznie trudniej będzie wykazać realizację pozostałych obowiązków**. Jeśli zamierzasz w sprawie AI Act zrobić tylko niezbędne minimum, to ten dokument jest właśnie tym, na czym warto się skupić.

Minimalny zakres kolumn:

Kolumna	Po co
Nazwa systemu / narzędzia	identyfikacja
Dostawca i wersja	odpowiedzialność, zmiany
Do czego jest używany	podstawa klasyfikacji
Dział i właściciel biznesowy	kto odpowiada
Nasza rola (dostawca / podmiot stosujący)	zakres obowiązków
Poziom ryzyka + uzasadnienie	dowód świadomej decyzji
Czy przetwarza dane osobowe	powiązanie z RODO
Czy wchodzi w interakcję z ludźmi / generuje treści	art. 50
Nadzór człowieka: kto i na czym polega	art. 14 / art. 26
Data oceny i data następnego przeglądu	aktualność

Gotowy szablon dostaniesz też w ramach audytu w Localize.pl, ale swobodnie możesz zbudować własny w arkuszu. Musi tylko być aktualny i mieć właściciela.

6. Siedem obszarów ryzyka, które warto sprawdzić

> Poniższa lista to **obszary do sprawdzenia**, które wynikają z konstrukcji przepisów, a kolejność jest przypadkowa.

1. **„Nie używamy AI"**. Gdy jednak sprawdzisz dokładniej, okazuje się, że dział marketingu generuje opisy produktów, HR filtruje CV w systemie rekrutacyjnym, a support ma podpowiedzi w helpdesku. Brak rejestru sprzyja powstawaniu zjawiska „Shadow AI".
2. **Chatbot bez informacji, że jest botem**. Zwykle najprostsze do naprawienia (wystarczy jeden komunikat w interfejsie) i najłatwiejsze do wychwycenia przez kogokolwiek z zewnątrz. Zanim zaczniesz szukać rozwiązania, sprawdź, czy na pewno jesteś dostawcą tego chatbota.
3. **Narzędzia „analityki jakości rozmów"**. Tu sprawdź, czy system **wnioskuje o emocjach z danych biometrycznych** i **czyje to są emocje**. Analiza dotycząca **pracowników** może być zakazana, ale analiza dotycząca **klientów** podlega tylko obowiązkowi informacyjnemu z art. 50 ust. 3 i RODO. To dwie różne sytuacje o zupełnie różnych skutkach.
4. **Wklejanie danych klientów do publicznych modeli**. Tu powstaje przede wszystkim ryzyko naruszenia przepisów RODO i tajemnicy przedsiębiorstwa. Kluczem będzie ustanowienie polityki wewnętrznej organizacji.
5. **„To dostawca odpowiada"**. To prawda, ale jeśli tworzysz system (także na cudzym API) i oferujesz go **pod własną nazwą**, możesz od tej pory być jego **dostawcą** w rozumieniu art. 3 pkt 3. Osobna kwestia to art. 25, który dotyczy **przejęcia obowiązków dostawcy przy systemach wysokiego ryzyka**, m.in. po zmianie marki, istotnej modyfikacji lub zmianie przeznaczenia. To więc dwie różne podstawy. Ustal najpierw, jaki system oferujesz i czy na pewno jest systemem wysokiego ryzyka.
6. **Brak jakiegokolwiek śladu po działaniach kompetencyjnych**. Sprawdź, jakie dokumenty lub rejestry możesz pokazać, by potwierdzić, **co i dla kogo zrobiono**.
7. **Wdrożenie AI do oceny pracowników bez poinformowania załogi**. Niezależnie od przepisów RODO, przy systemach wysokiego ryzyka tu pojawia się osobny obowiązek informacyjny wobec pracowników i ich przedstawicieli (art. 26 ust. 7).

7. Plan minimum na 30 dni

Tydzień	Działanie	Efekt
1	Spisz wszystkie narzędzia AI używane w firmie (bezpośrednio zapytaj każdy dział + przejrzyj faktury za usługi SaaS)	rejestr v1
2	Dla każdego zastosowania ustal **swoją rolę** i wykonaj trzy osobne testy: podleganie pod zakaz / klasyfikacja systemu wysokiego ryzyka / art. 50	mapa ryzyka
3	Zrealizuj te obowiązki z art. 50, **które faktycznie Cię dotyczą** wg roli: komunikat w chatbocie, weryfikacja oznaczania u dostawcy, ujawnienia przy materiałach spełniających definicję deepfake'u	przejrzystość wg roli
4	Wyznacz osobę odpowiedzialną, przyjmij prostą politykę AI, zaplanuj proporcjonalne działania kompetencyjne i zapisz, co zrobiono	art. 4 + ład

To całkiem realny zakres dla firmy o wielkości do kilkuset osób. W dużej mierze **zdejmuje ryzyko z obszarów, które są najbardziej widoczne na zewnątrz**.

8. Kiedy potrzebujesz pomocy z zewnątrz

Jeśli masz mało narzędzi, żadne z nich nie dotyczy HR/finansów/zdrowia, nie budujesz własnych produktów AI, to z pewnością poradzisz sobie we własnym zakresie.

W innym przypadku warto sięgnąć po audyt. Ma to sens szczególnie, gdy:

- używacie AI w rekrutacji, ocenie pracowników, scoringu klientów lub ubezpieczeniach,
- wystawiacie narzędzie AI klientom pod własną marką (wtedy jesteście dostawcą, nie użytkownikiem),
- macie klientów korporacyjnych, którzy pytają partnerów biznesowych o zgodność z AI Act,
- pracujecie na danych osobowych na dużą skalę,
- nikt w firmie nie ma czasu, chęci ani pewności, żeby ten proces przeprowadzić.

9. Słowniczek

- **Dostawca** — tworzy system AI i wprowadza go do obrotu lub oddaje do użytku pod swoją nazwą.
- **Podmiot stosujący** — używa systemu AI w działalności zawodowej. W praktyce większość firm.
- **GPAI** — model ogólnego przeznaczenia (GPT, Claude, Gemini, Llama).
- **Deepfake** — treść wygenerowana lub zmanipulowana przez AI, przedstawiająca osoby, przedmioty lub zdarzenia tak, że fałszywie sprawia wrażenie autentycznej.
- **KRiBSI** — Komisja Rozwoju i Bezpieczeństwa Sztucznej Inteligencji, polski organ nadzoru rynku AI.
- **FRIA** — ocena skutków dla praw podstawowych, wymagana dla części podmiotów przy systemach wysokiego ryzyka.
- **C2PA** — standard oznaczania pochodzenia treści cyfrowych (metadane odczytywalne maszynowo).

Materiał przygotowany przez Localize.pl. Stan prawny: 29 lipca 2026 (po Digital Omnibus i po ogłoszeniu ustawy z dnia 3 lipca 2026 r. o systemach sztucznej inteligencji, Dz.U. 2026 poz. 1003). Dokument ma charakter informacyjny i nie stanowi porady prawnej.