

Checklista oceny dostawcy narzędzia AI

Wypełnij przed zatwierdzeniem narzędzia | Narzędzie: _____ | Dostawca: _____ |
Data: _____

Lista pytań jest kompilacją autora na podstawie ogólnej struktury pytań inicjalnych UODO (2026), listy OWASP Top 10 for LLM Applications 2025 oraz wymogów rozporządzenia o sztucznej inteligencji. Nie jest wzorem opublikowanym przez żaden z tych organów ani poradą prawną. Oficjalne listy UODO: uodo.gov.pl.

Najpierw: do czego narzędzie ma służyć?

UODO zaleca, by najpierw ustalić, jaki problem rozwiązuje narzędzie i na jakich danych będzie pracować, a dopiero potem oceniać zgodność. Wpisz:

Zastosowanie	
Dział / użytkownicy	
Klasa danych (zielone / żółte / czerwone)	
Czy w grę wchodzi dane osobowe?	
Czy wynik wpływa na decyzje o osobach?	

A. Dane i umowa

Pytanie do dostawcy	Dlaczego pytamy	Odpowiedź dostawcy	Ocena (OK / ? / NIE)
Czy dostawca używa naszych danych (zapytań, plików) do trenowania modeli? Czy można to wyłączyć i gdzie jest to zapisane w umowie?	Dane firmy nie powinny zasilać modelu dostępnego dla innych.		
Gdzie dane są przetwarzane i przechowywane (kraj, region)? Jak długo?	Transfer poza EOG wymaga podstaw prawnych.		
Czy dostawca zapewnia możliwość usunięcia danych i historii? W jakim terminie?	Kontrola nad cyklem życia danych.		
Czy są konta firmowe z zarządzaniem użytkownikami, logowaniem jednokrotnym (SSO) i dziennikiem aktywności?	Bez tego nie kontrolujemy dostępu po odejściu pracownika.		
Co się dzieje z danymi po zakończeniu umowy?	Ryzyko pozostania danych u dostawcy.		

B. RODO

Pytanie do dostawcy	Dlaczego pytamy	Odpowiedź dostawcy	Ocena (OK / ? / NIE)
Czy dostawca podpisze umowę powierzenia przetwarzania danych (art. 28 RODO), jeśli wprowadzamy dane osobowe?	Bez umowy nie wprowadzamy danych osobowych.		
Kim są podwykonawcy dostawcy i czy publikuje ich listę?	Łańcuch przetwarzania.		

Pytanie do dostawcy	Dlaczego pytamy	Odpowiedź dostawcy	Ocena (OK / ? / NIE)
Czy zastosowanie wymaga oceny skutków dla ochrony danych (DPIA)? Kto ją przeprowadzi?	Zależy od skali i rodzaju danych; ustala to inspektor lub prawnik.		
Czy musimy poinformować osoby, których dane dotyczą, o użyciu narzędzia?	Obowiązki informacyjne.		

C. Bezpieczeństwo

Pytanie do dostawcy	Dlaczego pytamy	Odpowiedź dostawcy	Ocena (OK / ? / NIE)
Czy dostawca ma certyfikaty lub raporty (np. ISO/IEC 27001, SOC 2) i czy może je udostępnić?	Podstawowe potwierdzenie dojrzałości bezpieczeństwa.		
Czy dostawca informuje klientów o incydentach? W jakim terminie?	Musimy znać termin, by spełnić własne obowiązki.		
Szyfrowanie danych w spoczynku i w transmisji?	Standard minimalny.		
Czy narzędzie chroni przed wstrzykiwaniem poleceń (prompt injection) i ujawnianiem informacji z poleceń systemowych? Jak?	Pozycje na liście OWASP Top 10 for LLM Applications 2025.		

D. Uprawnienia i integracje (dla narzędzi agentowych)

Pytanie do dostawcy	Dlaczego pytamy	Odpowiedź dostawcy	Ocena (OK / ? / NIE)
Do jakich systemów narzędzie ma dostęp (poczta, dyski, CRM, finanse)? Czy zakres można ograniczyć do odczytu?	OWASP: nadmierna sprawczość (excessive agency).		
Czy akcje o skutkach zewnętrznych (wysłanie maila, płatność, zmiana danych) wymagają zatwierdzenia człowieka?	Człowiek odpowiada za skutki.		
Czy jest dziennik wszystkich działań agenta?	Możliwość ustalenia, co się stało.		
Czy produkt rzeczywiście działa agentowo, czy to przemianowany chatbot lub automatyzacja?	Gartner opisuje zjawisko „agent washing”.		

E. Zgodność z AI Act i odpowiedzialność

Pytanie do dostawcy	Dlaczego pytamy	Odpowiedź dostawcy	Ocena (OK / ? / NIE)
Do jakiej kategorii dostawca zalicza system (zakazany, wysokiego ryzyka, ograniczonego ryzyka, minimalnego)? Na jakiej podstawie?	Obowiązki firmy zależą od zastosowania, nie tylko od narzędzia.		

Pytanie do dostawcy	Dlaczego pytamy	Odpowiedź dostawcy	Ocena (OK / ? / NIE)
Czy narzędzie będzie używane do rekrutacji, oceny lub zarządzania pracownikami?	Takie zastosowania mogą należeć do obszaru wysokiego ryzyka (załącznik III). Wymaga konsultacji prawnej.		
Czy narzędzie generuje treści (obrazy, wideo, tekst) publikowane na zewnątrz? Czy oznacza je maszynowo?	Obowiązki przejrzystości (art. 50).		
Jak umowa rozkłada odpowiedzialność za błędy narzędzia? Czy jest limit odpowiedzialności dostawcy?	Wobec klienta odpowiadamy my.		

F. Koszty i ciągłość

Pytanie do dostawcy	Dlaczego pytamy	Odpowiedź dostawcy	Ocena (OK / ? / NIE)
Jaki jest pełny koszt (licencje, limity użycia, opłaty za dodatkowe zapytania)?	Gartner wskazuje niejasne koszty wśród przyczyn porzucania projektów AI.		
Co zrobimy, jeśli dostawca zmieni warunki lub wycofa produkt? Czy możemy wyeksportować nasze dane i konfigurację?	Ryzyko uzależnienia.		

Decyzja

Decyzja	☐ Zatwierdzone ☐ Zatwierdzone z ograniczeniami ☐ Odrzucone ☐ Do wyjaśnienia
Ograniczenia (klasy danych, użytkownicy, zakres)	
Osoba oceniająca / data	
Termin kolejnego przeglądu	