DGP | Dziennik Gazeta Prawna

ZACKIEWICZ & PARTNERS

Lista kontrolna dla zarządu

10 pytań, które powinien zadać sobie każdy zarząd przed wprowadzeniem sztucznej inteligencji
Zaznacz pytania, na które możesz odpowiedzieć twierdząco. Każde „nie" lub „w trakcie" to obszar wymagający podjęcia działań regulacyjnych przed wdrożeniem lub kontynuacją używania systemów AI w organizacji.

Pytanie	Tak	Nie / w trakcie
01. Czy wiem, jakie systemy AI są używane lub planowane w mojej organizacji? Dotyczy zarówno rozwiązań własnych, jak i narzędzi SaaS z komponentem AI (Copilot, ChatGPT Enterprise, narzędzia rekrutacyjne, chatboty obsługi klienta, systemy scoringowe).	☐	☐
02. Czy wykluczyliśmy stosowanie zakazanych praktyk AI oraz oceniliśmy, które z używanych systemów AI są systemami wysokiego ryzyka? AI Act bezwzględnie zakazuje wybranych praktyk (m.in. social scoring, rozpoznawanie emocji w pracy i edukacji, biometryczna kategoryzacja danych wrażliwych, nieukierunkowane pozyskiwanie wizerunków z internetu). Z kolei systemy wysokiego ryzyka (m.in. HR, scoring kredytowy, biometria, dostęp do usług kluczowych) mogą wymagać oceny zgodności przed wdrożeniem lub dalszym stosowaniem.	☐	☐
03. Czy organizacja wie, czy jest dostawcą, operatorem, czy stosującym AI w rozumieniu AI Act? Rola determinuje zakres obowiązków. Błędna kwalifikacja oznacza błędnie zidentyfikowane obowiązki compliance i realną ekspozycję na kary (do 35 mln euro lub 7 proc. obrotu).	☐	☐
04. Czy w zarządzie lub na poziomie C-suite ktoś formalnie odpowiada za AI governance? AI Act nakłada na organizacje obowiązki nadzoru i kompetencji, które w praktyce wymagają przypisania ról i odpowiedzialności. Brak takiego przypisania stanowi słabość governance, którą organy nadzoru mogą uwzględniać przy ocenie zgodności.	☐	☐
05. Czy zapewniamy pracownikom odpowiedni poziom kompetencji w zakresie AI (AI literacy)? AI Act zobowiązuje dostawców i podmioty stosujące AI do zapewnienia odpowiedniego poziomu kompetencji AI u osób zajmujących się obsługą i użytkowaniem systemów. Wymaga to szkoleń dostosowanych do roli, wiedzy technicznej i kontekstu wykorzystania AI.	☐	☐

DGP | Dziennik Gazeta Prawna

ZACKIEWICZ & PARTNERS

Lista kontrolna dla zarządu

Pytanie	Tak	Nie / w trakcie
06. Czy pracownicy i klienci są informowani o interakcji z AI i przetwarzaniu ich danych w tym kontekście? AI Act nakłada obowiązek transparentności (systemy generatywne, deepfake, chatboty). RODO wymaga zaktualizowanych klauzul informacyjnych. Brak informacji = podwójne ryzyko regulacyjne.	☐	☐
07. Czy wdrożono zasady korzystania z AI przez pracowników? Pracownik wpisujący dane klientów do publicznego LLM naraża organizację na naruszenie RODO i tajemnic przedsiębiorstwa oraz odpowiedzialność kontraktową wobec klientów.	☐	☐
08. Czy oceniono ryzyka cyberbezpieczeństwa specyficzne dla AI (prompt injection, data poisoning, model inversion)? AI wprowadza nowe wektory ataku nieobecne w standardowych analizach ryzyka. Brak uwzględnienia AI w ocenie ryzyka ICT może być zakwestionowany przez organ nadzoru.	☐	☐
09. Czy umowy z dostawcami AI zawierają klauzule wymagane przez AI Act i RODO? Standardowe ToS dostawców często nie spełniają wymogów umowy powierzenia z art. 28 RODO ani obowiązków operatora według AI Act. Akceptacja bez negocjacji = ryzyko po stronie zamawiającego.	☐	☐
10. Czy organizacja jest gotowa wykazać zgodność z AI Act w razie kontroli lub incydentu? Audyty, logi decyzji AI, dokumentacja techniczna systemów wysokiego ryzyka – to warunki konieczne do osiągnięcia compliance. Brak dokumentacji = brak możliwości obrony.	☐	☐