Autonomiczne AI dla firm regulowanych: RODO i unijny akt o AI

20 maja 2026

Firmy działające pod nadzorem regulacji chcą korzyści płynących z nowoczesnego AI, ale zwykła droga wysyła dane osobowe i poufne do modelu w chmurze prowadzonego przez podmiot trzeci. W świetle RODO i unijnego aktu o AI ta droga dokłada ciężaru prawnego do każdego wdrożenia. Uruchomienie AI na własnej infrastrukturze usuwa większość tego ciężaru u źródła. Ten dokument opisuje, w jaki sposób.

Problem z drogą przez chmurę

Gdy zapytania i dokumenty opuszczają twoją sieć, aby dotrzeć do hostowanego modelu, dostawca modelu staje się kolejną stroną twoich danych. Rodzi to pytania, na które regulowany nabywca musi odpowiedzieć: jaka jest podstawa prawna, kto jest podmiotem przetwarzającym, gdzie znajdują się dane i jak można to audytować. Na każde z nich da się odpowiedzieć, ale każde dokłada umów, ocen i ryzyka. Autonomiczne, lokalne AI odpowiada na większość z nich, po prostu nie pozwalając danym wyjść na zewnątrz.

RODO

RODO łatwiej spełnić, gdy dane osobowe pozostają w obrębie granicy samego administratora.

- Brak zewnętrznego podmiotu przetwarzającego dla modelu. Ponieważ model działa na twojej infrastrukturze, do wnioskowania nie ma zewnętrznego podmiotu przetwarzającego dane osobowe w twoim imieniu ani łańcucha umów powierzenia i dalszych transferów, którym trzeba by zarządzać.
- Brak transferów międzynarodowych. Dane, które nigdy nie opuszczają twojej siedziby, nie są przekazywane do innego kraju, więc reguły transferu, które

komplikują AI w chmurze, nie mają zastosowania.

- Minimalizacja danych i miejsce przechowywania z założenia. Indeks wyszukiwania i logi znajdują się tam, gdzie je umieścisz, w twojej jurysdykcji i pod twoimi regułami przechowywania.
- Czytelniejsza podstawa prawna. Bez wtórnego wykorzystania danych podstawą przetwarzania jest cel, który już masz, a nie nowy, tworzony przez wysłanie danych do dostawcy.

Unijny akt o AI

Akt o AI nakłada obowiązki dotyczące przejrzystości, zarządzania, prowadzenia dokumentacji i nadzoru człowieka, skalowane do ryzyka systemu. Wdrożenie lokalne samo w sobie nie klasyfikuje ani nie certyfikuje systemu, ale ułatwia spełnienie tych obowiązków.

- Przejrzystość i dokumentacja. Ponieważ modele, indeks i logi są wewnątrz twojej granicy, możesz widzieć i przechowywać dokumentację, której oczekuje akt, zamiast polegać na podsumowaniach dostawcy.
- Nadzór człowieka. System działa tam, gdzie są twoi ludzie i mechanizmy kontroli, więc nadzór jest kwestią twoich własnych procesów, a nie konsoli dostawcy.
- Zarządzanie. Jedna granica do nadzorowania jest prostsza niż zestaw zewnętrznych integracji, co czyni ocenę i monitorowanie wymagane przez akt bardziej wykonalnymi.

Poufność i reguły branżowe

Poza tymi dwiema regulacjami praca w sektorze regulowanym wiąże się z NDA klientów i regułami branżowymi, w finansach, ochronie zdrowia, sektorze publicznym i usługach prawnych. Materiał przetwarzany na miejscu pozostaje w ramach poufności, którą już obiecałeś, i nie staje się kwestią mechanizmów kontroli dostawcy.

Weryfikowalne, a nie deklarowane

Zgodność to ocena prawna dokonywana w twoim kontekście, a ten dokument nią nie jest. Empisto dostarcza architekturę, która czyni tę ocenę łatwiejszą, a dowody

dostępnymi: platforma działa wewnątrz twoich murów, nie ma wychodzącej ścieżki dla twoich danych i jest otwarta na niezależny audyt sposobu przetwarzania danych oraz działania sieci. Zaufanie ma opierać się na tych dowodach, a nie na słowie dostawcy.