7 lucruri concrete pe care proprietarii de IMM nu le știu despre AI

Nu mituri, fapte, obligații și date curente din 2025-2026, direct relevante pentru firma ta.

01 Din februarie 2025 ai o obligație legală activă: instruirea echipei în AI (Art. 4, AI Act)

02 Din 2 august 2026 trebuie să spui clar clienților când vorbesc cu un AI, nu cu un om

03 Ești responsabil legal pentru ce spune chatbot-ul firmei tale: „AI-ul a greșit” nu e apărare

04 Cele mai grele obligații din AI Act nu se aplică ție dacă doar cumperi unelte AI gata făcute

05 Angajații tăi folosesc deja AI, chiar dacă firma n-a aprobat nicio unealtă („shadow AI”)

06 AI-ul greșește cu încredere, ca regulă, nu ca excepție rară

07 80% dintre proiectele AI eșuează, dar aproape niciodată din cauza tehnologiei

#1

Din februarie 2025 ai o obligație legală activă: instruirea echipei în AI (Art. 4, AI Act)

Explicație

Articolul 4 din Regulamentul UE privind AI e în vigoare din 2 februarie 2025 și obligă orice firmă care folosește sisteme AI, nu doar cele care le construiesc, să asigure un nivel „suficient” de educație AI pentru angajați și pentru oricine operează AI în numele firmei. Nu există un curs sau certificat obligatoriu: o instruire internă documentată e, de regulă, suficientă, dar lipsa completă a oricărei măsuri te lasă expus. Din 2 august 2026, infrastructura de supraveghere și aplicare a devenit complet operațională în fiecare stat membru UE, iar nerespectarea intră sub regimul general de sancțiuni (până la 15 milioane EUR sau 3% din cifra de afaceri globală, pragul mai mic aplicându-se IMM-urilor).

Ce trebuie să faci

→ Dacă echipa ta folosește ChatGPT, Copilot sau orice alt instrument AI la muncă, obligația se aplică deja firmei tale.

→ Un document intern și o sesiune de instruire documentată sunt, de regulă, suficiente. Nu e nevoie de curs formal.

→ Lipsa oricărei măsuri devine factor agravant dacă apare altă problemă legată de AI în firmă.

#2

Din 2 august 2026 trebuie să spui clar clienților când vorbesc cu un AI, nu cu un om

Explicație

Articolul 50 din AI Act a intrat în aplicare pe 2 august 2026. Obligația de transparență cere ca orice persoană care interacționează cu un chatbot sau alt sistem AI să fie informată clar că vorbește cu o mașină, dacă acest lucru nu e deja evident din context. Aceeași regulă se aplică și conținutului generat sau modificat semnificativ de AI (postări, imagini, articole) pe care firma îl publică: trebuie marcat corespunzător ca fiind produs cu AI.

Ce trebuie să faci

→ O notă vizibilă pe chat („Acest asistent este operat de AI”) acoperă cerința de bază.

→ Verifică dacă furnizorul instrumentului tău AI include deja marcaj automat în output. Dacă nu, cere clarificare în contract.

→ Conținutul generat de AI publicat pe rețele sociale sau site are nevoie, la rândul lui, de o etichetă vizibilă.

#3

Ești responsabil legal pentru ce spune chatbot-ul firmei tale: „AI-ul a greșit” nu e apărare

Explicație

Într-un caz canadian din 2024 (Moffatt v. Air Canada), chatbot-ul companiei a inventat o politică de reducere pentru bereavement care nu exista. Compania a susținut că nu răspunde, pentru că „AI-ul a făcut o greșeală”. Tribunalul a respins complet acest argument și a obligat compania să onoreze promisiunea chatbot-ului. Un tribunal german a decis similar în 2026, obligând o companie medicală să răspundă pentru afirmații greșite ale propriului chatbot despre calificările personalului. Curțile tratează tot mai des output-ul unui chatbot ca fiind comunicarea oficială a firmei, nu o entitate separată.

Ce trebuie să faci

→ Orice informație greșită oferită de un chatbot al firmei tale (preț, politică, promisiune) poate deveni obligație contractuală reală.

→ Un disclaimer generic („AI-ul poate greși”) reduce, dar nu elimină, expunerea legală.

→ Fluxurile cu risc financiar sau contractual (oferte, rambursări, politici) au nevoie de verificare umană înainte să ajungă la client.

#4

Cele mai grele obligații din AI Act nu se aplică ție dacă doar cumperi unelte AI gata făcute

Explicație

Legea face o distincție esențială între „provider” (cine construiește și lansează un sistem AI pe piață) și „deployer” (cine folosește un sistem AI cumpărat de la altcineva). Majoritatea covârșitoare a IMM-urilor sunt deployeri. Asta înseamnă că obligațiile grele, evaluare de conformitate, marcaj CE, înregistrare în baza de date UE, nu se activează automat doar pentru că echipa ta folosește un instrument AI popular. Ele vizează aproape exclusiv sistemele de „risc ridicat” (recrutare, scoring de credit, educație, infrastructură critică), nu un asistent de scriere sau un chatbot obișnuit de suport pentru clienți.

Ce trebuie să faci

→ Verifică întâi dacă ești „provider” sau „deployer”: majoritatea IMM-urilor sunt deployeri, cu obligații mult mai ușoare.

→ Obligațiile grele vizează aproape exclusiv domeniile de risc ridicat (recrutare, credit, educație), nu uneltele AI obișnuite.

→ Fii sceptic dacă cineva îți vinde un „pachet complet de conformitate AI Act” pentru un simplu chatbot de suport.

#5

Angajații tăi folosesc deja AI, chiar dacă firma n-a aprobat nicio unealtă („shadow AI”)

Explicație

Studii din 2026 arată că între 45% și 68% dintre angajați folosesc regulat unelte AI neaprobate la muncă, iar aproximativ 11% din datele lipite în astfel de unelte sunt sensibile: cod sursă, date de clienți, documente financiare. Diferența cea mai izbitoare e „decalajul de încredere”: 78% dintre conducerile de firme cred că au o imagine clară asupra folosirii AI în companie, dar doar aproximativ 23% dintre angajați confirmă că firma chiar știe ce unelte folosesc de fapt. AI-ul e deja în firma ta, întrebarea e doar dacă îl vezi sau nu.

Ce trebuie să faci

→ Un audit simplu de vizibilitate („ce unelte AI folosiți deja?”) e primul pas, nu o măsură disciplinară.

→ Oferirea unei alternative aprobate, cu funcționalitate similară, reduce puternic folosirea neautorizată.

→ Datele de clienți sau financiare introduse în conturi gratuite ies din controlul firmei, adesea ireversibil.

#6

AI-ul greșește cu încredere, ca regulă, nu ca excepție rară

Explicație

„Halucinația”, un răspuns care sună convingător, dar e inventat, nu e un bug ocazional, ci o caracteristică structurală a modelelor generative actuale. Studiile raportează rate de eroare între 0,7% și aproape 30% în funcție de domeniu, iar pe întrebări juridice specifice ratele urcă la 69-88%. Exemple concrete: Google a pierdut aproximativ 100 de miliarde de dolari în capitalizare bursieră după ce chatbot-ul Bard a inventat un fapt într-o demonstrație live, iar un avocat american a fost sancționat cu 5.000 de dolari după ce a depus la instanță citate juridice complet fictive, generate de AI.

Ce trebuie să faci

→ Orice output AI cu impact financiar, legal sau medical are nevoie de verificare umană înainte de folosire.

→ Ratele de eroare cresc puternic pe domenii specializate (juridic, medical). Nu presupune acuratețe uniformă.

→ Un sistem care răspunde pe baza documentelor firmei tale (nu doar din memoria modelului) reduce, dar nu elimină, riscul.

#7

80% dintre proiectele AI eșuează, dar aproape niciodată din cauza tehnologiei

Explicație

Cercetarea RAND, pe peste 2.400 de inițiative AI din companii, arată o rată de eșec de peste 80%, de două ori mai mare decât la proiectele IT obișnuite. Într-o analiză pe 140 de implementări concrete, doar 23% dintre eșecuri au fost cauzate de performanța modelului, calitatea datelor sau complexitatea integrării. Restul de aproape 80% s-au datorat strategiei neclare, guvernanței slabe și managementului schimbării, adică lipsei unui obiectiv măsurabil și a adopției reale în echipă, nu unei limitări tehnice a AI-ului în sine.

Ce trebuie să faci

→ Motivul eșecului rareori e „AI-ul nu a fost suficient de bun”: de obicei e lipsa unui obiectiv clar sau a adopției interne.

→ Un singur proces bine definit și măsurat bate un proiect AI ambițios fără obiectiv clar.

→ Cere oricărui furnizor o metrică de succes stabilită dinainte (ore economisite, erori reduse), nu doar „implementare AI”.