LOOK SMART

BUSINESS CONSULTANCY

AI SUB CONTROL

Guvernanța inteligenței artificiale în companie,
dincolo de termenele care se mută

Ghid executiv

Actualizat la 5 iunie 2026

www.looksmart.ro
office@looksmart.ro
+4.0743.332.318

Notă editorială și metodologie

Acest ghid se adresează membrilor consiliilor de administrație, directorilor generali, directorilor financiari, directorilor de resurse umane și responsabililor de conformitate și risc care trebuie să ia, în lunile următoare, decizii concrete privind utilizarea inteligenței artificiale în organizațiile lor. Scopul lui nu este unul juridic exhaustiv, ci unul de management: să transforme un cadru de reglementare complex într-o agendă de acțiune clară și aplicabilă.

Materialul a fost construit pe surse primare și pe repere internaționale recunoscute: Regulamentul (UE) 2024/1689 privind inteligența artificială și pachetul de modificări „Digital Omnibus" aflat în proces legislativ, standardul ISO/IEC 42001:2023 pentru sistemele de management al inteligenței artificiale, cadrul NIST AI Risk Management Framework și Principiile OECD privind inteligența artificială, precum și orientarea metodologică a marilor firme de consultanță în privința integrării AI în modelul operațional și a guvernanței responsabile.

Am evitat în mod deliberat cifrele și procentele neverificabile. Acolo unde formulăm afirmații cantitative, ele provin din texte normative sau din surse care pot fi consultate; acolo unde realitatea este în mișcare sau incertă, o spunem explicit. Trei astfel de incertitudini structurează întregul material și trebuie reținute de la început.

- **Incertitudine 1 - calendarul.** La data redactării, pachetul „Digital Omnibus" care amână o parte dintre termenele AI Act nu este încă adoptat formal. Statutul lui se poate schimba; orice decizie operațională trebuie raportată la data de mai sus și reverificată periodic.
- **Incertitudine 2 - autoritățile din România.** Desemnarea autorităților naționale competente și de supraveghere a pieței în România nu poate fi confirmată cu certitudine la data redactării și trebuie verificată înainte de orice demers oficial.
- **Incertitudine 3 - standardele.** Standardele tehnice armonizate (CEN-CENELEC) care vor operaționaliza cerințele pentru sistemele cu risc ridicat sunt încă în dezvoltare și pot fi publicate aproape de termenele de aplicare, lăsând timp scurt de adaptare.

Prezentul ghid are caracter informativ și nu substituie consultanța juridică, financiară sau de specialitate într-o speță concretă. Drepturile de autor și condițiile de utilizare sunt detaliate în partea finală.

Rezumat executiv

În iunie 2026, companiile europene se află într-un moment de incertitudine controlată în privința aplicării Regulamentului european privind inteligența artificiale. Deși termenul inițial pentru sistemele cu risc ridicat era 2 august 2026, un acord politic provizoriu din mai 2026 indică o amânare până în 2027–2028. Acordul nu este însă adoptat formal la data redactării, ceea ce creează o dilemă reală pentru conducere: ne pregătim acum sau așteptăm clarificarea legislativă?

Studiul pleacă de la o poziție clară: **incertitudinea calendarului nu schimbă natura riscului și nici responsabilitatea managementului**. Arhitectura fundamentală a regulamentului rămâne neschimbată - o abordare bazată pe risc, cu obligații diferențiate în funcție de rolul companiei, și cerințe privind supravegherea umană, calitatea datelor, transparența și controlul operațional. În paralel, anumite obligații se aplică deja, independent de eventualele amânări: interdicțiile privind practicile de inteligență artificială deosebit de dăunătoare, obligația de alfabetizare în domeniul AI a personalului și cerințele pentru sistemele de uz general, inclusiv modelele generative.

În acest context, guvernanța inteligenței artificiale nu mai este o temă tehnologică sau juridică izolată, ci o responsabilitate directă a conducerii executive și a consiliului, la intersecția dintre risc, performanță și strategie. Organizațiile care acționează din timp obțin avantaje concrete - reducerea riscurilor operaționale și reputaționale, încredere sporită din partea clienților și a partenerilor, adoptare controlată și mai rapidă a tehnologiei și o poziționare competitivă mai bună într-un mediu reglementat. Cele care amână se expun unui risc dublu: neconformare într-un interval comprimat și, mai grav, pierderea controlului asupra unei tehnologii deja prezente în organizație.

Ghidul oferă o abordare orientată spre acțiune pentru a înțelege aplicabilitatea regulamentului, a cartografia utilizarea AI în companie, a construi un cadru de guvernanță robust și a defini un plan de implementare pe douăsprezece luni. În centrul lui stă un model propriu, **Look Smart AI Governance Framework**, și un capitol dedicat impactului asupra principalelor zece industrii.

Guvernanța AI nu este despre a respecta un termen care se mută, ci despre a controla o tehnologie care îți influențează deja deciziile.

1. Contextul: de ce acum

1.1 Momentul iunie 2026: între incertitudine și responsabilitate

Rareori cadrul de reglementare și realitatea operațională evoluează simultan, în ritm accelerat. Inteligența artificială este astăzi deja integrată în procese critice ale organizațiilor - de la recrutare și evaluarea performanței, până la relația cu clienții, marketing și decizii financiare. În același timp, regulamentul european încearcă să impună reguli clare pentru utilizarea acestei tehnologii, iar evoluțiile din mai 2026 introduc o zonă de ambiguitate: există un acord politic pentru amânarea unor termene, dar el nu este încă adoptat formal, iar prevederile existente rămân, teoretic, aplicabile.

Această situație creează o tensiune strategică reală la nivel executiv: este justificată amânarea pregătirii în absența certitudinii legislative? Din perspectiva managementului, răspunsul este negativ, din trei motive. Primul, expunerea există deja: inteligența artificială este folosită în organizație, adesea fără un control formal. Al doilea, arhitectura reglementării nu se schimbă - în discuție este doar calendarul. Al treilea, timpul de implementare este aproape întotdeauna subestimat: construirea unui cadru de guvernanță funcțional durează, în practică, între șase și optsprezece luni.

Prin urmare, întrebarea corectă nu este „când intră în vigoare?”, ci „**cât control avem astăzi asupra modului în care se folosește inteligența artificială în organizație?**”.

1.2 De ce guvernanța AI este o temă de consiliu, nu de IT

O eroare frecventă este tratarea inteligenței artificiale ca pe o inițiativă tehnologică izolată. În realitate, impactul ei este transversal: atinge resursele umane prin recrutare și evaluare, deciziile comerciale și de marketing, analiza financiară și riscul de credit, precum și relația cu clienții. Această transversalitate transformă AI într-o temă de guvernanță corporativă, de management al riscului și de responsabilitate executivă.

Conform bunelor practici definite de NIST, prin AI Risk Management Framework, și de standardul ISO/IEC 42001, gestionarea inteligenței artificiale trebuie integrată în sistemele de control deja existente, nu tratată separat. Utilizarea necontrolată generează riscuri directe pentru conducere - decizii opace sau discriminatorii, erori automate propagate la scară, încălcări de reglementare și pierderea încrederii. În acest context, responsabilitatea nu mai poate fi delegată exclusiv către IT sau către departamentul juridic; **guvernanța AI devine o extensie firească a responsabilității consiliului și a conducerii executive**.

2. Ce este, de fapt, regulamentul: arhitectură și domeniu de aplicare

2.1 Abordarea bazată pe risc și cele patru niveluri

Regulamentul nu tratează toate sistemele de inteligență artificială la fel, ci le ierarhizează după riscul pe care îl prezintă pentru drepturile și siguranța persoanelor. Distingem patru niveluri. **Riscul inacceptabil** cuprinde practicile interzise, eliminate complet din piață. **Riscul ridicat** acoperă sistemele care pot afecta semnificativ viața oamenilor - de exemplu în ocuparea forței de muncă, accesul la servicii esențiale sau evaluarea bonității - și atrage cele mai stricte obligații. **Riscul limitat** impune în principal obligații de transparență, iar **riscul minim**, în care intră marea majoritate a aplicațiilor uzuale, rămâne în esență neîngrădit.

Pentru management. *Prima sarcină a conducerii nu este conformarea, ci încadrarea corectă. Majoritatea sistemelor folosite de o companie obișnuită se vor situa la risc limitat sau minim; efortul de guvernanță trebuie concentrat acolo unde riscul este real, nu distribuit uniform.*

2.2 Cine ești în lanț: furnizor, implementator, importator

Obligațiile diferă radical în funcție de rolul companiei. Furnizorul dezvoltă sistemul AI sau îl pune pe piață sub numele său. Implementatorul (în limbajul regulamentului, „deployer") este organizația care utilizează un sistem AI în activitatea sa profesională. Importatorul și distribuitorul intermediază punerea pe piață. Majoritatea companiilor din România nu produc inteligență artificială, ci o folosesc; sunt, așadar, implementatori, iar obligațiile lor sunt mai reduse decât ale furnizorilor, dar nu inexistente - în special pentru sistemele cu risc ridicat.

2.3 Aplicabilitate extinsă și relația cu protecția datelor

Regulamentul se aplică și unor companii din afara Uniunii Europene, atunci când rezultatele sistemelor lor sunt utilizate în Uniune. La fel de important, el nu înlocuiește legislația privind protecția datelor, ci se aplică în paralel cu aceasta: un sistem AI care prelucrează date cu caracter personal trebuie să respecte simultan cerințele regulamentului privind inteligența artificială și pe cele ale Regulamentului general privind protecția datelor. O guvernanță bine gândită tratează cele două cadre împreună, pentru a evita munca dublă.

Pentru management. *Întrebarea „suntem doar utilizatori, deci nu ne privește?" este o capcană. Și utilizatorii au obligații, iar folosirea unui sistem AI extern nu transferă integral răspunderea către furnizor.*

3. Punctul de cotitură din mai 2026: ce s-a schimbat și ce nu

În noiembrie 2025, Comisia Europeană a propus pachetul „Digital Omnibus", menit să simplifice cadrul digital al Uniunii, inclusiv regulamentul privind inteligența artificială. După un prim tur de negocieri eșuat la sfârșitul lunii aprilie 2026, instituțiile europene au revenit la masă și au ajuns, la începutul lunii mai 2026, la un acord politic provizoriu, confirmat ulterior de reprezentanții statelor membre în Consiliu.

3.1 Ce s-a amânat

Acordul provizoriu amână aplicarea regimului pentru sistemele cu risc ridicat din anexa privind domeniile sensibile până la 2 decembrie 2027, iar pentru inteligența artificială încorporată în produse deja reglementate sectorial până la 2 august 2028. De asemenea, termenul pentru obligațiile de marcare a conținutului generat artificial este împins spre finalul anului 2026, iar termenele pentru spațiile naționale de testare în condiții reale sunt și ele decalate. Toate aceste date au, însă, statut provizoriu până la adoptarea formală.

3.2 Ce nu s-a schimbat

Esențial pentru orice decizie de management: arhitectura regulamentului a rămas neclintită. Clasificarea pe niveluri de risc, regimul de evaluare a conformității, pista dedicată modelelor de uz general și rolul de supraveghere al Oficiului European pentru Inteligența Artificială rămân toate în picioare. La fel, interdicțiile privind practicile dăunătoare și obligația de alfabetizare în domeniul AI nu au fost atenuate. Cu alte cuvinte, ceea ce s-a amânat este un set de termene, nu logica de fond a reglementării.

3.3 Scenariul pe care managementul trebuie să îl rețină

Dacă pachetul de amânare nu este adoptat formal înainte de 2 august 2026, prevederile originale ale regulamentului, inclusiv obligațiile pentru risc ridicat, devin aplicabile de la acea dată, așa cum au fost scrise. Această posibilitate, oricât de improbabilă ar părea, transformă pregătirea din opțiune în prudență elementară.

Pentru management. *Tratați noile termene ca pe o ipoteză de planificare credibilă, nu ca pe o certitudine. Construiți cadrul de guvernanță astfel încât să fie valabil în ambele scenarii - cu sau fără amânare - și veți fi protejați indiferent de deznodământul legislativ.*

4. Ce se aplică deja, indiferent de amânare

Dincolo de dezbaterea privind termenele pentru risc ridicat, trei categorii de obligații sunt deja relevante și nu sunt afectate de amânare. Ele formează „minimul de igienă" pe care orice organizație ar trebui să îl asigure acum.

4.1 Practicile interzise

Anumite utilizări ale inteligenței artificiale sunt complet interzise, fiind considerate incompatibile cu valorile fundamentale - de exemplu manipularea comportamentală care exploatează vulnerabilități, sau punctajul social generalizat. Aceste interdicții sunt deja în vigoare.

Pentru management. *Verificați rapid dacă vreun instrument folosit în organizație se apropie de zona interzisă. Este o verificare scurtă, dar cu miză mare: aici nu există perioadă de grație.*

4.2 Alfabetizarea în domeniul AI

Regulamentul cere organizațiilor să asigure un nivel suficient de competență în domeniul inteligenței artificiale pentru personalul care dezvoltă sau utilizează astfel de sisteme. Această obligație nu a fost atenuată de pachetul de amânare și are un corespondent practic imediat: un program de formare adaptat rolurilor, de la utilizatorii ocazionali de instrumente generative până la echipele care iau decizii pe baza rezultatelor AI.

Pentru management. *Alfabetizarea AI este obligația cea mai ușor de îndeplinit și cea mai vizibilă. Un program de formare bine construit este, în același timp, conformare și pârghie de adoptare responsabilă a tehnologiei.*

4.3 Modelele de uz general și inteligența artificială generativă

Obligațiile pentru furnizorii de modele de uz general se aplică din 2025, însoțite de un cod de bune practici elaborat la nivel european. Pentru companiile care folosesc modele generative de la terți, relevanța este indirectă, dar concretă: trebuie să știe ce instrumente folosesc angajații, în ce condiții și cu ce date, și să impună reguli clare de utilizare.

Pentru management. *Cele mai multe organizații folosesc deja inteligență artificială generativă, fără o politică explicită. Stabilirea unor reguli simple de utilizare este una dintre cele mai urgente și mai ieftine măsuri de control.*

5. Ești în domeniul de aplicare? Cartografiere, decalaj și maturitate

5.1 Inventarul: nu poți guverna ce nu vezi

Primul pas concret este inventarierea sistemelor de inteligență artificială folosite în organizație. Sună banal, dar este pasul pe care cele mai multe companii îl ratează, pentru că o bună parte a inteligenței artificiale este „ascunsă” în aplicații existente - module de selecție a candidaților în softurile de resurse umane, motoare de recomandare în platformele comerciale, funcții de scoring sau de detectare a fraudei.

La acestea se adaugă utilizarea instrumentelor generative direct de către angajați. Rezultatul inventarului ar trebui consemnat într-un registru intern al sistemelor AI, prima livrare tangibilă de guvernanță.

5.2 Clasificarea pe niveluri de risc

Odată identificat fiecare sistem, el trebuie încadrat pe niveluri de risc. Aici atenția se concentrează asupra cazurilor cu risc ridicat relevante pentru companii: instrumentele folosite în ocuparea forței de muncă, cele care condiționează accesul la servicii esențiale și cele de evaluare a bonității. Clasificarea nu este un exercițiu juridic abstract, ci fundamentul pe care se construiește întregul efort ulterior: ea decide unde se cheltuiește, de fapt, energia de conformare.

5.3 Unde sunt companiile azi față de unde ar trebui să fie

Realitatea observată în piață, confirmată de practica internațională, arată un decalaj consistent. Multe organizații nu au un inventar al sistemelor AI și, în consecință, nu știu cu exactitate unde folosesc inteligență artificială. Puține au politici interne formale, iar utilizarea instrumentelor generative se face frecvent fără un cadru de control. Acest decalaj nu este, în primul rând, o problemă de conformare, ci una de control managerial: o tehnologie care influențează decizii este folosită fără ca cineva să răspundă explicit de ea.

Pentru management. *Decalajul real nu este între companie și lege, ci între ceea ce folosește deja organizația și ceea ce controlează efectiv conducerea. Acesta este spațiul pe care guvernanța îl recuperează.*

5.4 Un model de maturitate pentru autopoziționare

Pentru a transforma diagnoza în direcție, propunem un model de maturitate în cinci niveluri. El permite conducerii să se autoevalueze rapid și să stabilească ținta realistă pentru următoarele douăsprezece luni.

Nivel	Denumire	Descriere
1	Ad-hoc	Inteligența artificială este folosită izolat, fără vizibilitate sau control. Nimeni nu răspunde formal.
2	Conștientizat	Organizația știe că folosește AI și recunoaște nevoia de control, dar nu a structurat încă un cadru.
3	Structurat	Există inventar, clasificare de risc și primele politici. Responsabilitățile încep să fie atribuite.
4	Guvernat	Guvernanța AI este integrată în managementul riscului, auditul intern și conformitate, cu supraveghere umană și monitorizare.
5	Optimizat	Controlul AI este o capabilitate continuă, care susține adoptarea responsabilă și avantajul competitiv.

Cele mai multe organizații se situează astăzi între nivelurile unu și doi. O țintă rezonabilă pentru următoarele douăsprezece luni este nivelul trei, cu un parcurs clar către nivelul patru.

6. Obligațiile pe niveluri de risc și trei scenarii din practică

6.1 Sistemele cu risc ridicat

Pentru sistemele încadrate la risc ridicat, regulamentul cere un set coerent de măsuri: un proces de management al riscului pe întreg ciclul de viață, guvernanța datelor folosite la antrenare și utilizare, documentație tehnică și jurnalizare, supraveghere umană semnificativă, precum și niveluri adecvate de acuratețe, robustețe și securitate. Implementatorii au obligații proprii, mai reduse decât ale furnizorilor, dar reale - în special asigurarea supravegherii umane și utilizarea sistemului conform instrucțiunilor.

6.2 Obligațiile de transparență

Pentru sistemele cu risc limitat, obligația principală este transparența: utilizatorul trebuie să știe când interacționează cu o inteligență artificială, iar conținutul generat artificial trebuie marcat ca atare. Este o cerință cu impact direct asupra marketingului, comunicării și relației cu clienții.

6.3 Furnizor sau implementator: cine ce datorează

Aspect	Furnizor	Implementator (utilizator)
Documentație tehnică	Întocmește și menține	Păstrează ce primește; o pune la dispoziție la cerere
Supraveghere umană	Proiectează sistemul pentru a o permite	O asigură efectiv în utilizare
Conformitate și marcaj	Realizează evaluarea conformității	Folosește sistemul conform instrucțiunilor
Monitorizare	Supraveghere ulterioară punerii pe piață	Monitorizează funcționarea și semnalează incidentele

Pentru management. *Înainte de a discuta obligații, stabiliți rolul: sunteți furnizor sau implementator pentru fiecare sistem? Răspunsul schimbă complet lista de sarcini și, adesea, costul conformării.*

6.4 Trei scenarii din practică

Recrutare (resurse umane). O companie folosește un instrument care preselectează automat candidații. Pentru că vizează ocuparea forței de muncă, sistemul intră, ca regulă, în categoria de risc ridicat.

Organizația trebuie să asigure supraveghere umană reală asupra deciziilor, să verifice absența discriminării și să poată explica modul în care se ajunge la o preselecție.

Marketing (inteligență artificială generativă). O echipă de marketing generează texte și imagini cu instrumente generative. Riscul este, de regulă, limitat, dar apare o obligație clară de transparență: conținutul generat artificial trebuie marcat, iar interacțiunile automate cu clienții trebuie să fie recognoscibile ca atare.

Finanțe (scoring). Un sistem evaluează automat bonitatea clienților. Evaluarea creditului este unul dintre cazurile explicit sensibile, cu risc ridicat. Aici se cer guvernanța datelor, testarea pentru părtinire, documentarea deciziilor și posibilitatea unei intervenții umane - cu atât mai mult cu cât aceleași date intră și sub incidența protecției datelor.

7. Modelul Look Smart - AI Governance Framework

Pentru a transforma cerințele regulamentului dintr-o listă de obligații într-un sistem operațional coerent, **Look Smart** propune un model integrat de guvernanță a inteligenței artificiale, construit pe cinci piloni. Modelul este aliniat cu standardul ISO/IEC 42001 și cu cadrul NIST și are o singură ambiție: să facă guvernanța AI funcțională, nu declarativă.

1. AI Visibility - vizibilitate completă

Organizația trebuie să știe unde și cum folosește inteligența artificială: inventarul tuturor sistemelor, inclusiv al celor încorporate în aplicații, identificarea utilizării instrumentelor generative de către angajați și ținerea unui registru centralizat. Fără vizibilitate nu există control.

2. Risk & Classification - evaluare și clasificare

Fiecare sistem este evaluat și încadrat pe niveluri de risc, cu identificarea cazurilor cu risc ridicat și a impactului asupra persoanelor și operațiunilor. Nu toate sistemele sunt egale, iar tratamentul trebuie diferențiat în consecință.

3. Control & Oversight - control și supraveghere

Se definesc responsabilitățile, supravegherea umană semnificativă, politicile și procedurile interne, precum și mecanismele de validare și audit. Inteligența artificială nu elimină responsabilitatea, ci o amplifică.

4. Operational Integration - integrare operațională

Guvernanța AI nu funcționează ca un strat separat. Ea trebuie integrată în procesele existente de management al riscului, audit intern, conformitate și guvernanță IT. Aici se află, de altfel, ADN-ul **Look Smart**: nu construim o structură paralelă, ci întărim sistemele de control pe care compania le are deja.

5. Continuous Assurance - asigurare continuă

Inteligența artificială nu este un sistem static. Sunt necesare monitorizarea performanței, detectarea abaterilor, gestionarea incidentelor și actualizarea continuă a modelelor și a controalelor. Controlul AI nu este un proiect cu final, ci o capabilitate permanentă.

Pentru management. *Cei cinci piloni nu se implementează simultan și nici perfect din prima. Ordinea contează: vizibilitate, apoi clasificare, apoi control, integrare și, în final, asigurare continuă. Fiecare pas creează fundamentul pentru următorul.*

8. Guvernanța AI ca avantaj de business, nu doar conformare

Majoritatea materialelor tratează regulamentul exclusiv ca pe o problemă de conformare și de risc. Este o abordare incompletă. Firmele de consultanță de prim rang - McKinsey, Boston Consulting Group, Bain - converg de ani de zile asupra unei idei simple: inteligența artificială creează valoare doar atunci când este integrată în modelul operațional și guvernată responsabil. Guvernanța responsabilă nu este o frână, ci condiția adoptării la scară.

Companiile care construiesc devreme un cadru de guvernanță obțin avantaje concrete. Își reduc riscurile operaționale și reputaționale, pentru că știu ce folosesc și cum. Câștigă încredere din partea clienților și a partenerilor mari, care cer tot mai des dovezi de control. Adoptă tehnologia mai repede și mai sigur, fiindcă au reguli clare în loc de interdicții reflexe sau de haos tăcut. Și se poziționează mai bine într-un mediu în care reglementarea devine un criteriu de selecție în relațiile dintre companii.

8.1 Responsabilitatea conducerii

Regulamentul prevede sancțiuni semnificative - în cazurile cele mai grave, până la treizeci și cinci de milioane de euro sau șapte la sută din cifra de afaceri globală anuală. Le menționăm o singură dată și fără dramatism, pentru că miza reală pentru conducere nu este amenda, ci responsabilitatea strategică de a ține sub control o tehnologie care ia sau influențează decizii în numele organizației. Privită astfel, guvernanța AI este o extensie a datoriei de diligență a consiliului, alături de riscul financiar, operațional și reputațional.

Pentru management. *Reformulați tema în interiorul organizației: nu „cum evităm amenda”, ci „cum ne asigurăm că deciziile luate cu ajutorul AI sunt corecte, explicabile și sub control”. Prima formulare produce conformare minimală; a doua produce capabilitate.*

9. Impactul pe principalele zece industrii

Regulamentul se aplică tuturor, dar nu uniform. Sectoarele diferă prin gradul de expunere la cazurile cu risc ridicat și prin maturitatea adoptării. Le prezentăm în ordinea importanței expunerii, cu ceea ce fiecare are de știut și de făcut.

1. Servicii bancare și financiare. Este sectorul cu cea mai directă expunere, pentru că evaluarea bonității este un caz explicit de risc ridicat, la care se adaugă detectarea fraudei și consultanța automatizată. Băncile și instituțiile financiare trebuie să inventarieze modelele de scoring și de decizie, să le integreze în guvernanța de risc a modelelor pe care o au deja și să asigure documentare, testare pentru părtinire și intervenție umană.

2. Asigurări. Stabilirea prețurilor și evaluarea eligibilității, în special pentru asigurările de viață și de sănătate, intră în zona de risc ridicat. Asigurătorii trebuie să clasifice sistemele de subscriere și tarifare, să demonstreze absența discriminării și să asigure transparența față de clienți, păstrând în același timp coerența cu cerințele privind protecția datelor.

3. Energie și utilități. Sistemele care contribuie la gestionarea infrastructurii critice sunt tratate cu exigență ridicată. Operatorii trebuie să identifice utilizările AI în conducerea rețelelor și a proceselor esențiale, să asigure supraveghere umană robustă și reziliență, în strânsă legătură cu obligațiile de securitate cibernetică ce le revin oricum.

4. Sănătate și dispozitive medicale. Inteligența artificială încorporată în dispozitive medicale și în instrumente de diagnostic se află în categoria de risc ridicat, suprapunându-se peste reglementarea dispozitivelor medicale. Furnizorii și unitățile medicale trebuie să alinieze conformitatea AI cu cea a dispozitivelor și să păstreze supravegherea clinică umană asupra deciziilor.

5. Producția industrială. Aici, inteligența artificială apare frecvent ca o componentă de siguranță a echipamentelor și în controlul calității sau mentenanța predictivă. Producătorii trebuie să identifice utilizările relevante pentru siguranță, care urmează regimul produselor reglementate, cu un orizont de aplicare mai îndepărtat, și să trateze cu prioritate sistemele cu impact asupra securității lucrătorilor.

6. Automotive și mobilitate. Funcțiile de asistență și siguranță urmează regimul componentelor de siguranță din produse reglementate, cu termene proprii. Constructorii și furnizorii din lanț trebuie să asigure conformitatea sistemelor cu impact asupra siguranței și trasabilitatea documentației pe tot lanțul de aprovizionare.

7. Tehnologie, software și telecomunicații. Companiile din acest sector sunt adesea, în același timp, furnizori și implementatori, iar produsele lor încorporează tot mai mult modele de uz general.

Ele trebuie să clarifice cu precizie rolul pe care îl au pentru fiecare funcție, să gestioneze obligațiile aferente modelelor de uz general și să transmită contractual cerințele relevante către clienți și parteneri.

8. Retail, comerț electronic și bunuri de consum. Predomină sistemele de recomandare, de personalizare a prețurilor și de marketing, situate în general la risc limitat, cu accent pe transparență. Comercianții trebuie să marcheze conținutul generat artificial, să facă recognoscibile interacțiunile automate cu clienții și să evite practicile care ar putea fi considerate manipulatoare.

9. Construcții și infrastructură. Inteligența artificială pătrunde în proiectarea asistată și modelarea informației despre clădire, în estimarea costurilor și pregătirea ofertelor, precum și în monitorizarea siguranței pe șantier. Cele mai multe utilizări se situează la risc limitat, dar instrumentele de recrutare și de monitorizare a lucrătorilor pot intra la risc ridicat. Companiile din construcții ar trebui să concentreze guvernanța asupra acestor instrumente de resurse umane și asupra calității datelor folosite în estimări și licitații.

10. Imobiliare și administrarea proprietăților. Evaluarea automată a proprietăților și selecția chiriașilor sunt zonele sensibile; selecția care condiționează accesul la locuință se poate apropia de regimul serviciilor esențiale. Companiile trebuie să clasifice aceste instrumente, să asigure nediscriminarea și transparența și să păstreze decizia umană în cazurile cu impact asupra persoanelor.

Pentru management. *Indiferent de sector, regula este aceeași: expunerea reală vine, cel mai adesea, din instrumentele de resurse umane și din cele care condiționează accesul la un serviciu. Începeți cartografierea de acolo.*

10. Dimensiunea românească și suprapunerea cu alte reglementări

Regulamentul este direct aplicabil în România, însă punerea lui în practică depinde și de cadrul național. Statele membre desemnează autorități competente și de supraveghere a pieței; la data redactării, situația desemnării acestora în România trebuie verificată înainte de orice demers oficial, motiv pentru care recomandăm confirmarea ei la momentul publicării și actualizarea periodică a acestei informații.

La fel de important, regulamentul privind inteligența artificială nu funcționează izolat. El se intersectează cu regimul protecției datelor și cu legislația de securitate cibernetică, mai ales pentru companiile care operează infrastructuri sau servicii esențiale. O guvernanță inteligentă tratează aceste cadre împreună, cu o singură funcție de risc care le acoperă pe toate, evitând structurile paralele și munca dublă.

Pentru management. *Nu construiți o guvernanță AI separată de cea de protecție a datelor și de securitate. Aceleași date, aceleași procese și, în bună măsură, aceiași oameni sunt implicați; integrarea reduce costul și crește coerența.*

11. Deciziile consiliului în 90 de zile, opțiuni strategice și foaie de parcurs

11.1 Deciziile pe care conducerea le poate lua în următoarele 90 de zile

Executivii nu caută concepte, ci decizii. Următoarele cinci decizii pot fi luate rapid și deblochează tot restul demersului:

- desemnarea unui responsabil pentru guvernanța inteligenței artificiale;
- aprobarea inițierii unui registru al sistemelor AI;
- stabilirea unei poziții clare privind utilizarea instrumentelor generative în companie;
- definirea pragurilor de risc care declanșează o analiză aprofundată; și
- alocarea unui buget minim pentru un program de alfabetizare AI.

Niciuna nu necesită certitudine legislativă, iar împreună mută organizația de la nivelul „ad-hoc” la un control vizibil.

11.2 Trei posturi strategice, comparativ

Postură	Avantaje	Limite și riscuri
Pregătire integrală acum	Control deplin, avantaj competitiv, adoptare sigură a tehnologiei.	Efort și cost inițial mai mari; necesită angajament al conducerii.
Pregătire minimă, pe ce e deja în vigoare	Cost redus; acoperă obligațiile imediate și reduce riscul evident.	Lasă descoperite cazurile cu risc ridicat; presiune mare dacă termenele revin.
Așteptare	Niciun efort pe termen scurt.	Risc dublu: neconformare în interval comprimat și pierderea controlului asupra AI deja folosite.

Recomandarea noastră este postura intermediară spre integrală: acoperiți acum ce este deja aplicabil - practici interzise, alfabetizare, reguli pentru instrumentele generative - și construiți în paralel inventarul și clasificarea, astfel încât trecerea la cerințele pentru risc ridicat să fie o continuare firească, nu un efort de criză.

11.3 Foaia de parcurs pe douăsprezece luni

În primul trimestru se realizează inventarul sistemelor AI, se desemnează responsabilul și se stabilesc regulile pentru instrumentele generative.

În al doilea trimestru se finalizează clasificarea de risc, se lansează programul de alfabetizare și se redactează politica internă de utilizare a inteligenței artificiale.

În al treilea trimestru se implementează mecanismele de supraveghere umană și de control pentru sistemele cu risc ridicat și se integrează guvernanța AI în managementul riscului și auditul intern. În al patrulea trimestru se pune în funcțiune monitorizarea continuă, se testează răspunsul la incidente și se evaluează maturitatea atinsă. Planul rămâne valabil indiferent de calendarul legislativ final.

12. Concluzie: de la conformare la capabilitate

Incertitudinea privind termenele nu este o scuză pentru pasivitate, ci un test de maturitate managerială. Companiile care tratează guvernanța inteligenței artificiale ca pe o bifă de conformare vor rămâne mereu în urma propriei tehnologii. Cele care o tratează ca pe o capabilitate strategică - vizibilitate, control, integrare, asigurare continuă - câștigă încredere, viteză și acces la piețe și parteneriate care cer, tot mai des, dovezi de control responsabil.

Guvernanța AI nu este o obligație de bifat, ci o infrastructură de control pentru o tehnologie care redefinește modul în care organizațiile iau decizii.

13. Despre Look Smart și cum vă putem sprijini

Look Smart este un boutique premium de consultanță în management și afaceri, înființat în 2009, cu birouri la București și Bruxelles. Lucrăm cu un portofoliu deliberat restrâns de clienți, implicându-ne ca partener pe termen lung, integrat în realitatea fiecărei afaceri, nu ca un furnizor extern. Partenerii noștri au condus și au consiliat organizații din industrii reglementate și complexe operațional, iar această experiență o aducem direct în fiecare proiect.

Servicii relevante pentru această temă

Sprijinim companiile pe exact pașii descriși în acest ghid: cartografierea utilizării inteligenței artificiale și construirea registrului de sisteme, clasificarea pe niveluri de risc, proiectarea cadrului de guvernanță și integrarea lui în managementul riscului, auditul intern, conformitatea și guvernanța IT, precum și programul de alfabetizare AI a echipelor.

Acoperim guvernanța corporativă și managementul riscului, transformarea digitală, securitatea informației și reziliența cibernetică, precum și consultanța executivă la nivel de conducere.

Ceea ce ne diferențiază este că nu ne oprim la recomandări. Ducem lucrurile până la implementare, alături de echipele dumneavoastră, până când guvernanța inteligenței artificiale devine o capabilitate care funcționează în practică, nu un document care rămâne în sertar.

Contact

Telefon: +40 743 332 318

E-mail: office@looksmart.ro

Web: https://www.looksmart.ro

LinkedIn: https://be.linkedin.com/company/look-smart-europe

Birouri: București · Bruxelles

Vă invităm la o discuție confidențială, fără caracter angajant, pentru a evalua împreună unde se află organizația dumneavoastră și care ar fi primii pași rezonabili.

Anexe

Anexa 1 - Autoevaluare în cinci întrebări

Răspunsul „nu” la oricare dintre întrebări indică o zonă de vulnerabilitate care merită atenția conducerii.

1. Știm toate sistemele de inteligență artificială folosite în organizație, inclusiv instrumentele generative folosite de angajați?
2. Avem o clasificare pe niveluri de risc a acestor sisteme?
3. Avem politici interne clare pentru utilizarea inteligenței artificiale?
4. Există supraveghere umană semnificativă acolo unde AI influențează decizii?
5. Am asigurat un program de alfabetizare în domeniul AI pentru personalul relevant?

Anexa 2 - Glosar de termeni

Termen	Explicație
Furnizor	Entitatea care dezvoltă un sistem AI sau îl pune pe piață sub numele său.
Implementator (deployer)	Organizația care utilizează un sistem AI în activitatea sa profesională.
Sistem cu risc ridicat	Sistem care poate afecta semnificativ siguranța sau drepturile persoanelor și care atrage cele mai stricte obligații.
Model de uz general (GPAI)	Model AI cu utilizări largi, care poate fi integrat în numeroase aplicații, inclusiv modelele generative.
Supraveghere umană	Capacitatea unei persoane de a înțelege, controla și, la nevoie, corecta funcționarea unui sistem AI.

Anexa 3 - Surse și referințe

- Regulamentul (UE) 2024/1689 privind inteligența artificială. Pachetul „Digital Omnibus” și acordul politic provizoriu privind modificarea termenelor (în proces legislativ, iunie 2026).
- Standardul ISO/IEC 42001:2023 - sisteme de management al inteligenței artificiale.
- NIST AI Risk Management Framework și profilul pentru inteligența artificială generativă.
- Principiile OECD privind inteligența artificială.
- Comunicatele Consiliului Uniunii Europene și ale Oficiului European pentru Inteligența Artificială.
- Orientarea tematică a firmelor de consultanță McKinsey, Boston Consulting Group și Bain privind integrarea AI în modelul operațional și guvernanța responsabilă.

Sursele au fost consultate la data redactării, iunie 2026.