AI ORGANISATIONAL READINESS ACCELERATOR

CBRNE LTD

Inventar integrat Q&A privind conformarea cu EU AI Act

Guvernanța AI în administrația publică: AI Act, cerințe și pași imediat următori

Pe baza webinariilor Progress Foundation with sprijin ANFP din 12 iunie și 9 iulie 2026

Document pregătit ca material de follow-up pentru webinariile dedicate guvernanței AI în administrația publică, organizate de Fundația Progress, cu experți CBRNE-AI ORA, în colaborare cu ANFP, în baza protocolului de colaborare dintre ANFP și Fundația Progress, pentru diseminarea unor informații relevante pentru dezvoltarea competențelor digitale în administrația publică.

Prezentatori:

Dr. Irina Marsh - expert în etică, guvernanță AI, conformitate și standardizare; Ethics and Governance Lead pentru CBRNE-AI ORA. LinkedIn: https://uk.linkedin.com/in/irinamarsh

Mihai Nămoloșanu - specialist în sisteme AI, software și guvernanță tehnică CBRNE-AI ORA; Lead Auditor ISO/IEC 42001. LinkedIn: https://ro.linkedin.com/in/mihainamolosanu

Contact: aiora.romania@cbrneltd.com

©CBRNE/AI ORA

Notă de transparență privind utilizarea AI

AI

Aceast raport a fost pregătit de echipa CBRNE-AI ORA cu sprijinul unor instrumente AI pentru structurare, redactare, reformulare și claritate editorială. Conținutul, selecția informațiilor, interpretarea și concluziile au fost revizuite și validate de experți umani.

AI nu a fost folosit pentru luarea unor decizii automate privind participanții și nu au fost analizate date personale ale participanților prin instrumente AI.

Introducere

Acest inventar integrat reunește și organizează întrebările primite în cadrul celor două webinarii ANFP privind guvernanța AI în administrația publică, susținute la 12 iunie și 9 iulie 2026.

Scopul documentului este de a oferi administrației publice un material practic de orientare privind utilizarea AI, conformarea cu EU AI Act, protecția datelor, securitatea, achizițiile, calitatea răspunsurilor generate și dezvoltarea AI literacy.

Răspunsurile oferă orientare generală, exemple și puncte de plecare. Ele reprezintă perspectiva și expertiza autorilor și nu constituie opinie juridică. Fiecare instituție trebuie să își adapteze abordarea în funcție de activitate, tipurile de date utilizate, nivelul de digitalizare, procedurile interne, rolurile interne și riscurile specifice.

Baza de lucru

Documentul sintetizează întrebările și comentariile transmise de participanți în cadrul celor două webinarii „Guvernanța AI în administrația publică: AI Act, cerințe și pași imediat următori", desfășurate in 12 iunie 2026 și 9 iulie 2026.

Pentru webinarul din 12 iunie 2026, au fost înregistrate 48 de întrebări și comentarii deschise. Raportul inițial de follow-up a selectat 10 întrebări reprezentative, care sunt integrate în prezentul inventar în clusterele tematice comune.

Pentru webinarul din 9 iulie 2026, au fost analizate 169 de întrebări și comentarii deschise, multe dintre ele vizând teme similare: legalitatea utilizării AI, protecția datelor, AI literacy, riscurile de halucinații, achizițiile, infrastructura și utilizările concrete în instituțiile publice.

Pentru a evita repetarea răspunsurilor și pentru a oferi un material mai ușor de parcurs, întrebările din cele două webinarii au fost integrate într-un singur inventar Q&A, organizat în cinci clustere tematice. Pentru fiecare cluster sunt incluse o orientare generală, întrebări reprezentative, răspunsuri detaliate și resurse utile.

Răspunsurile oferă orientare generală, exemple și puncte de plecare. Ele nu reprezintă opinii juridice și nu înlocuiesc analiza internă, tehnică sau legală adaptată fiecărei instituții.

AI poate sprijini administrația publică dacă este folosit cu discernământ, cu reguli clare și responsabilitate umană. Acesta este firul comun al răspunsurilor de mai jos.

Cluster	Întrebări recurente	Mesaj principal
1. AI Act, legalitate și guvernanță instituțională	Legalitatea utilizării AI, AI Act, obligații, coduri de practică, termene, proceduri interne.	AI nu este interzis în administrația publică, dar trebuie folosit într-un cadru controlat, documentat și proporțional.
2. Protecția datelor, confidențialitate și securitate	GDPR, date personale, date publice, securitate cibernetică, acuratețe și responsabilitate.	Datele personale și documentele interne nu trebuie introduse în instrumente neaprobate; DPO, IT și juridic trebuie implicați.
3. Implementare practică, achiziții și infrastructură	PC-uri vechi, platforme AI, achiziții, modele naționale, utilizări în UAT-uri și instituții mici.	AI trebuie introdus pornind de la nevoi, date, infrastructură și capacitate instituțională, nu ca soluție izolată.
4. Riscuri, calitatea răspunsurilor și impact	Halucinații, erori, răspundere, impact asupra muncii, marja de eroare, control uman.	AI poate asista, dar nu trebuie să devină autoritate finală în decizii administrative, juridice sau cu impact asupra cetățenilor.
5. AI literacy, cursuri și competențe	Traininguri, certificări, cursuri pentru funcționari, competențe pe roluri.	AI literacy trebuie tratată ca pregătire practică pe roluri, nu ca informare generală unică pentru toată lumea.

Cluster 1. AI Act, legalitate și guvernanță instituțională

Întrebările din acest cluster arată că participanții vor să înțeleagă dacă folosirea AI în instituțiile publice este permisă, ce obligații devin relevante și ce documente interne ar trebui pregătite. Răspunsul de bază este că AI nu este interzisă în administrația publică. Problema nu este utilizarea în sine, ci lipsa unui cadru de control: cine folosește AI, în ce scop, cu ce date, cu ce verificare și cu ce responsabilitate.

AI Act este un regulament european și se aplică direct în statele membre, asemănător GDPR. Totuși, fiecare stat membru trebuie să organizeze arhitectura națională de supraveghere, rolurile autorităților și regimul aplicabil sancțiunilor, inclusiv pentru autoritățile publice. În România, ANCOM a comunicat că a fost propusă de Guvernul României, prin Memorandum, să exercite rolul de autoritate națională de supraveghere și punct național unic de contact pentru aplicarea AI Act. Pe lângă ANCOM, arhitectura națională propusă include și autorități cu roluri sectoriale sau specializate: ANSPDCP pentru domenii sensibile legate de date personale, biometrie, drepturi fundamentale și alte zone cu impact asupra persoanelor; BNR și ASF pentru sistemele AI utilizate în sectorul financiar; ADR ca autoritate de notificare pentru organismele de evaluare a conformității; precum și alte autorități de supraveghere sectorială pentru sisteme AI integrate în produse reglementate, de exemplu în zona dispozitivelor medicale, echipamentelor tehnice, echipamentelor radio, protecției consumatorilor sau transporturilor.

În practică, aceasta înseamnă că instituțiile publice trebuie să urmărească atat aplicarea AI Act la nivel european, cat și modul în care România își clarifică mecanismele naționale de supraveghere, raportare, cooperare între autorități și aplicare a sancțiunilor.

Pentru instituții, primul pas nu este o politică foarte complexă, ci o guvernanță minimă: inventarierea utilizărilor AI, clasificarea riscurilor, reguli interne, AI literacy pe roluri, întrebări standard pentru furnizori și mecanisme de verificare umană.

Întrebări selectate și răspunsuri

1. Este legal să folosim AI în instituțiile publice?

Da, dar nu oricum. Utilizarea AI este permisă dacă respectă legislația aplicabilă, inclusiv AI Act, GDPR, regulile de securitate cibernetică, normele privind documentele și procedurile interne. Pentru utilizările cu risc redus, cum ar fi sumarizarea unor documente publice sau structurarea unor idei, AI poate fi folosită ca instrument de sprijin, cu verificare umană. Pentru utilizări care afectează drepturi, servicii publice, evaluări sau decizii administrative, nivelul de control trebuie să fie mult mai ridicat.

2. Este obligatorie folosirea AI în administrația publică?

Nu. AI Act nu obligă instituțiile publice să folosească AI. Regulamentul stabilește condiții pentru situațiile în care AI este dezvoltată, achiziționată, pusă în funcțiune sau utilizată. Decizia de a folosi AI trebuie să pornească de la nevoi reale, valoare publică, capacitate instituțională și riscuri.

3. Ce se schimbă în perioada 2026-2028?

În 2026 devin relevante în practică supravegherea și aplicarea mai clară a AI Act, precum și obligațiile de transparență pentru anumite sisteme și conținut generat sau modificat cu AI. În contextul acordului politic privind AI Omnibus, cerințele pentru anumite sisteme high-risk stand-alone, inclusiv din educație, ocupare, migrație, infrastructură critică sau biometrie, se aplică de la 2 decembrie 2027, iar cele integrate în produse reglementate de la 2 august 2028. Aceste termene înseamnă că instituțiile au o perioadă de pregătire, dar trebuie sa inceapa acum.

4. Care sunt elementele minime care ar trebui reglementate în administraţia publică pentru utilizarea AI?

Înainte de reguli complexe, instituţiile au nevoie de câteva repere simple. Cel mai important este ca utilizarea AI să nu rămână invizibilă (Shadow AI). O instituţie trebuie să ştie unde se foloseşte AI, în ce scop, cu ce date şi de către cine.

Un punct de plecare realist ar fi un set scurt de reguli interne privind utilizarea AI. Aceste reguli nu trebuie să blocheze inovaţia, dar trebuie să prevină utilizările riscante, mai ales atunci când sunt implicate date personale, documente interne sau decizii care pot afecta cetăţenii.

Câteva elemente minime ar fi utile:

- o evidenţă internă a utilizărilor AI;
- reguli clare privind datele care nu pot fi introduse în aplicaţii AI publice;
- obligaţia de verificare umană a rezultatelor generate de AI;
- reguli pentru folosirea instrumentelor aprobate de instituţie;
- cerinţe minime pentru achiziţia de soluţii AI;
- instruire de bază pentru personal.

Un registru intern al utilizărilor AI poate fi simplu la început. Nu trebuie să fie un sistem complicat. Important este ca instituţia să poată răspunde la câteva întrebări: ce instrumente AI folosim, în ce scop, ce date intră în sistem, cine verifică rezultatele şi cine răspunde dacă apare o problemă.

5. Există un cod de practică național pentru AI în administrația publică?

Nu există, în acest moment, un cod unic național obligatoriu pentru toate instituțiile publice. Există însă ghiduri, coduri și instrumente europene, inclusiv Codul de Practică privind transparența conținutului generat de AI. Instituțiile pot începe cu politici interne simple, adaptate activității lor, și le pot actualiza pe măsură ce se clarifică arhitectura națională de implementare.

6. Puteţi furniza un set minim de reguli pentru un cod de bune practici la nivelul instituţiei?

Da, dar cu o precizare importantă: un cod de bune practici trebuie adaptat fiecărei instituţii. Două instituţii publice pot avea acelaşi tip de activitate generală, dar date, riscuri şi proceduri foarte diferite.

Un cod util nu trebuie să fie lung. Dimpotrivă, în prima etapă este mai bine să fie clar, scurt şi uşor de aplicat. Scopul nu este să creeze încă un document formal, ci să ofere personalului repere concrete.

Un set minim de reguli ar putea include:

- Nu folosiţi AI pentru activităţi neaprobate de instituţie.
- Nu introduceţi date personale, date confidenţiale sau documente interne sensibile în aplicaţii AI publice.
- Nu trataţi răspunsul AI ca răspuns final.
- Verificaţi informaţiile generate înainte de a le folosi.

- Nu folosiţi AI pentru interpretări juridice finale sau decizii administrative fără validare umană competentă.
- Informaţi cetăţeanul atunci când interacţionează cu un sistem AI, de exemplu un chatbot.
- Raportaţi utilizările neautorizate, erorile sau incidentele.
- Folosiţi doar instrumentele aprobate instituţional pentru activităţi care implică date interne.

Aceste reguli trebuie completate acolo unde apar riscuri mai mari: achiziţii, resurse umane, servicii publice digitale, comunicare publică, control, inspecţie sau procese cu impact direct asupra cetăţenilor.

Resurse utile:

- Comisia Europeană – AI Act: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
- AI Act Service Desk – Timeline: https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act
- AI Act Service Desk – Article 4 AI literacy: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-4
- AI Act Service Desk – Article 99 Penalties: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-99
- ANCOM – Cod de bune practici privind transparența conținutului generat de AI: https://www.ancom.ro/despre-noi/media/comunicate-de-presa/cod-de-bune-practici-privind-transparenta-continutului-generat-de-inteligenta-artificiala/
- Comisia Europeană – AI Literacy: Questions & Answers: https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers

Cluster 2. Protecția datelor, confidențialitate și securitate

Acest cluster reunește întrebări despre GDPR, date personale, date publice, confidențialitate, securitate cibernetică și siguranța răspunsurilor generate. Mesajul principal este simplu: un instrument AI nu este sigur doar pentru că este folosit pe scară largă. Siguranța depinde de furnizor, contract, setări, locația procesării, retenția datelor, controlul accesului și modul în care instituția gestionează utilizarea.

Datele personale, petițiile, documentele interne, informațiile confidențiale sau datele sensibile nu ar trebui introduse în aplicații AI publice sau neaprobate. Chiar și datele publice trebuie tratate atent dacă, prin agregare sau context, pot genera riscuri suplimentare. DPO-ul, IT-ul, juridicul și securitatea cibernetică trebuie implicate înainte ca AI să fie folosit în fluxuri instituționale care implică date.

Întrebări selectate și răspunsuri

1. **Cum se împacă AI în instituțiile publice cu GDPR?**

AI și GDPR pot fi compatibile, dar numai dacă sunt clarificate fluxurile de date, temeiul legal, rolurile actorilor, retenția, transferurile, drepturile persoanelor vizate și măsurile de securitate. În practică, instituția trebuie să știe ce date intră în sistem, unde ajung, dacă sunt stocate, dacă sunt folosite pentru antrenare și cine are acces la ele.

2. **Dacă folosim AI pentru a răspunde la diverse adrese din instituţie, este posibil ca date cu caracter personal să ajungă la AI. Este corect? Sunt aceste date în siguranţă?**

Da, este posibil. Dacă un angajat copiază într-o aplicaţie AI o adresă, o petiţie, un document intern sau un email care conţine date personale, acele date ajung în sistemul respectiv.

De aceea, instituţiile publice trebuie să fie foarte prudente. Datele personale nu trebuie introduse în aplicaţii AI publice sau neaprobate. Faptul că un instrument este uşor de folosit nu înseamnă că este potrivit pentru date instituţionale.

Dacă datele sunt sau nu în siguranţă depinde de multe aspecte:

- cine este furnizorul;
- unde sunt procesate datele;
- dacă datele sunt stocate;
- dacă datele sunt folosite pentru antrenarea modelului;
- cine are acces la ele;
- ce măsuri de securitate există;
- ce prevede contractul;
- dacă există o bază legală pentru prelucrare;
- dacă este necesară o evaluare DPIA.

DPO-ul instituţiei trebuie implicat înainte ca AI să fie folosit în procese care includ date personale. În unele cazuri poate fi nevoie şi de implicarea departamentului IT, juridic, securitate cibernetică şi management.

Pentru uz curent, o regulă simplă este utilă: nu introduceţi în AI public ceea ce nu aţi trimite unui destinatar extern neautorizat.

3. **Putem încărca în ChatGPT date publice, dacă ele sunt deja disponibile online?**

Faptul că o informație este publică nu înseamnă automat că poate fi încărcată în orice instrument AI, în orice scop. Trebuie analizat contextul, scopul prelucrării, posibilele combinații de date, termenii platformei și riscurile de reutilizare. Pentru date cu adevărat publice și

nesensibile, utilizarea poate fi mai puțin riscantă, dar trebuie să existe reguli interne și verificare.

4. **Cum poate o primărie mică să implementeze responsabil AI?**

O instituție mică poate începe cu pași simpli: inventar al utilizărilor, reguli scurte privind datele interzise în aplicații publice, instruire de bază, identificarea câtorva utilizări cu risc redus și consultarea DPO/IT înainte de orice flux cu date personale. Nu este nevoie ca prima etapă să fie tehnic complexă; important este să existe control și responsabilitate.

5. **Este AI sigur din punct de vedere cibernetic şi corect din punct de vedere al datelor furnizate?**

AI nu este automat sigur şi nu este automat corect. Siguranţa şi corectitudinea depind de instrument, de furnizor, de date, de setările folosite şi de modul în care instituţia controlează utilizarea.

Riscurile cibernetice pot apărea din mai multe direcţii. Pot exista aplicaţii neaprobate, acces necontrolat, scurgeri de date, vulnerabilităţi ale infrastructurii, manipularea prompturilor sau integrarea necorespunzătoare cu sisteme interne.

Riscurile privind corectitudinea sunt la fel de importante. AI poate produce răspunsuri greşite, incomplete, depăşite sau părtinitoare. Dacă datele pe care se bazează sunt greşite sau incomplete, rezultatul poate fi la rândul lui problematic.

Pentru reducerea acestor riscuri, instituţiile pot începe cu măsuri clare:

- folosirea doar a instrumentelor aprobate;
- verificarea furnizorilor înainte de achiziţie;
- controlul accesului;
- loguri şi trasabilitate;
- testarea sistemelor înainte de utilizare;
- verificarea umană a rezultatelor;
- instruirea personalului;
- reguli de raportare a incidentelor.

AI trebuie tratat ca un instrument util, dar nu neutru şi nu lipsit de risc. Valoarea lui depinde de felul în care este introdus şi controlat.

6. **Cum prevenim scurgerile de informații?**

Prin reguli clare: nu se introduc date personale sau documente interne în instrumente neaprobate, se folosesc doar platforme aprobate, se limitează accesul, se verifică setările de confidențialitate, se păstrează trasabilitate pentru utilizările importante și se instruiește

personalul. O regulă practică: nu introduceți într-un AI public ceea ce nu ați trimite unui destinatar extern neautorizat.

7. Care sunt cele mai bune practici pentru introducerea şi utilizarea AI în instituţiile publice, respectând securitatea, protecţia datelor şi AI Act?

Pentru multe instituţii, primul pas nu ar trebui să fie achiziţia unei aplicaţii AI, ci clarificarea nevoilor şi a riscurilor. AI este util atunci când răspunde unei probleme reale, nu atunci când este introdus doar pentru că tehnologia este disponibilă.

O abordare prudentă ar putea începe cu o evaluare internă: unde se folosesc deja instrumente AI, ce nevoi are instituţia, ce tipuri de date sunt implicate şi ce nivel de risc apare. Această etapă ajută la identificarea utilizărilor informale, inclusiv a situaţiilor de tip Shadow AI, unde personalul foloseşte instrumente neaprobate fără ca instituţia să ştie.

După această evaluare, instituţia poate începe cu utilizări cu risc redus. De exemplu:

- redactarea unor texte nesensibile;
- sumarizarea unor documente publice;
- sprijin în structurarea unor note interne;
- traduceri preliminare;
- pregătirea unor materiale de comunicare;
- organizarea informaţiei deja publice.

Utilizările care implică date personale, răspunsuri oficiale, interpretări juridice sau decizii administrative trebuie tratate separat şi cu un nivel mai ridicat de control.

AI literacy este esenţială. Personalul trebuie să înţeleagă nu doar cum se foloseşte un instrument AI, ci şi unde sunt limitele lui. Instruirea trebuie adaptată pe roluri. Managementul are nevoie de o înţelegere strategică şi de risc. Juridicul şi DPO-ul trebuie să înţeleagă protecţia datelor şi conformitatea. IT-ul trebuie să evalueze securitatea şi integrarea. Personalul operaţional are nevoie de reguli clare şi exemple concrete.

Resurse utile:

- European Data Protection Board (EDPB) – Artificial Intelligence: https://www.edpb.europa.eu/topics/ai-and-technology/artificial-intelligence_en
- EDPB – Guidelines, recommendations and best practices: https://www.edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en
- ENISA – Artificial Intelligence Cybersecurity Challenges: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges

- AI Act Service Desk – Article 15 Accuracy, robustness and cybersecurity: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-15
- Comisia Europeană – AI Act: Regulatory framework: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
- Comisia Europeană – AI Literacy: Questions & Answers: https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers

Cluster 3. Implementare practică, achiziții și infrastructură

Întrebările din acest cluster arată o preocupare practică: cum introducem AI în instituții care au niveluri diferite de digitalizare, echipamente vechi, resurse limitate sau proceduri încă neclare? Răspunsul este că AI nu trebuie introdusă ca soluție izolată. Ea trebuie conectată la date, infrastructură, securitate, achiziții, competențe și obiective instituționale reale.

Multe instrumente AI funcționează în cloud și nu depind de performanța calculatorului local. Totuși, asta nu înseamnă că infrastructura nu contează. Contează conexiunea, securitatea, autentificarea, controlul accesului, integrarea cu sistemele existente și capacitatea instituției de a verifica rezultatele.

Întrebări selectate și răspunsuri

1. **Cum putem folosi AI dacă avem sisteme PC vechi? Nu riscăm să ne dezvoltăm mai repede într-o direcţie şi să rămânem blocaţi în alta?**

Întrebarea este foarte importantă, pentru că reflectă realitatea multor instituţii publice. Există situaţii în care se discută despre AI, dar instituţia are încă echipamente vechi, sisteme neintegrate sau procese digitale incomplete.

Totuşi, folosirea AI nu depinde întotdeauna de un calculator performant. Multe instrumente AI funcţionează în cloud, iar procesarea are loc pe serverele furnizorului, nu pe PC-ul local. Din acest punct de vedere, vechimea calculatorului nu este întotdeauna cea mai mare barieră.

Problemele reale pot fi altele:

- conexiuni nesigure;
- lipsa autentificării adecvate;
- lipsa controlului accesului;
- sisteme vechi care nu comunică între ele;
- lipsa competenţelor digitale;
- lipsa regulilor interne;
- lipsa unei strategii de modernizare.

AI nu trebuie introdus ca o soluţie izolată. Dacă instituţia nu are o fundaţie digitală minimă, AI poate crea confuzie, riscuri şi aşteptări nerealiste.

O abordare echilibrată ar fi să se înceapă cu utilizări simple, cu risc redus, care nu implică date personale sau procese critice. În paralel, instituţia trebuie să îşi evalueze infrastructura, securitatea, datele şi competenţele interne.

AI poate ajuta, dar nu poate înlocui digitalizarea de bază. Cele două trebuie gândite împreună.

2. Putem achiziționa platforme precum Claude, ChatGPT sau Copilot în instituții publice?

Da, în principiu, dar achiziția trebuie tratată ca achiziție de tehnologie cu implicații de date, securitate, conformitate și dependență de furnizor. Instituția trebuie să verifice contractul, procesarea datelor, locația datelor, retenția, setările de confidențialitate, logurile, suportul tehnic, drepturile de audit și condițiile de utilizare. Nu este suficient ca instrumentul să fie cunoscut sau popular.

Pentru administrația publică, este importantă și discuția despre suveranitate tehnologică: unde sunt procesate datele, ce control are instituția asupra configurației, cât de ușor poate schimba furnizorul și dacă există alternative europene sau soluții care pot fi operate într-un cadru mai controlat. Aceasta nu înseamnă că platformele globale nu pot fi folosite, ci că alegerea lor trebuie justificată, documentată și însoțită de măsuri de guvernanță.

În practică, achiziția ar trebui să pornească de la câteva întrebări: pentru ce scop vrem platforma, ce date vor fi introduse, cine o va folosi, ce rezultate vor fi acceptate, cine verifică outputul și cum se păstrează trasabilitatea. Pentru utilizări cu date personale, date sensibile sau impact asupra cetățenilor, DPO-ul, IT-ul, juridicul și managementul trebuie implicați înainte de achiziție.

3. Cât de aproape suntem de introducerea obiectivelor AI în strategiile de digitalizare ale României?

AI va deveni tot mai greu de separat de digitalizarea administraţiei publice. În realitate, instituţiile care îşi actualizează strategiile de digitalizare vor trebui să includă şi obiective legate de AI.

Totuşi, aceste obiective trebuie formulate concret. Nu ajută prea mult o strategie care spune doar că instituţia va utiliza AI. Este nevoie de obiective legate de date, infrastructură, competenţe, securitate, guvernanţă, achiziţii şi impact asupra serviciilor publice.

România este într-o etapă de tranziţie. Există discuţii şi paşi instituţionali pentru aplicarea AI Act şi pentru clarificarea responsabilităţilor naţionale. În acelaşi timp, multe instituţii se confruntă încă cu probleme de bază în digitalizare. De aceea, abordarea trebuie să fie realistă.

Pentru o instituţie publică, întrebarea practică nu este doar ce va apărea în strategia naţională, ci ce poate face instituţia în următoarele luni:

- să își evalueze nivelul de pregătire pentru AI;
- să identifice procese unde AI ar putea ajuta;
- să clarifice ce date are și cât de bune sunt;
- să pregătească personalul;
- să stabilească reguli interne;
- să înceapă cu proiecte-pilot cu risc redus;
- să măsoare impactul înainte de extindere.

AI poate sprijini servicii publice mai eficiente, dar doar dacă este conectat la nevoi reale și la o fundație digitală solidă.

4. Putem avea un model AI național sau instituțional, adaptat legislației române?

Este posibil ca, în timp, instituțiile să dezvolte sau să achiziționeze soluții AI adaptate unor nevoi publice specifice. Totuși, un model național sau sectorial cere date de calitate, guvernanță, responsabilitate, actualizare, securitate și evaluare continuă. Un astfel de model nu este doar un proiect tehnic, ci și un proiect de infrastructură publică, competențe, finanțare și guvernanță.

La nivel european, discuția se leagă de suveranitatea tehnologică: capacitatea Europei de a dezvolta, găzdui și controla infrastructuri, modele, date și servicii AI în acord cu valorile și regulile europene. Există deja inițiative europene pentru consolidarea ecosistemului AI, precum harta startup-urilor AI din Europa, care arată existența unui ecosistem divers de furnizori, produse și specializări AI. Această hartă poate fi utilă pentru instituții atunci când vor să înțeleagă piața și să caute alternative europene sau parteneri specializați.

Un exemplu interesant este modelul elvețian *Apertus,* dezvoltat de EPFL, ETH Zurich și Swiss National Supercomputing Centre. Apertus este prezentat ca un model lingvistic mare, deschis, transparent și multilingv, disponibil pentru cercetare, industrie și societate. Relevanța lui nu este că România ar trebui să copieze direct modelul elvețian, ci că arată o posibilă direcție: modele mai transparente, dezvoltate cu implicarea cercetării publice și gândite ca infrastructură de interes public.

Pentru multe instituții, o etapă mai realistă decât antrenarea unui model de la zero este folosirea unor soluții de tip RAG, care răspund pe baza unor documente aprobate și controlate de instituție. Această abordare poate sprijini adaptarea la legislația română și la procedurile interne, dar trebuie în continuare testată, monitorizată și verificată de experți umani.

5. Ar trebui ca instrumentele AI să fie plătite de instituție?

Pentru utilizări instituționale, este de preferat ca instrumentele să fie aprobate și gestionate instituțional. Faptul că un angajat folosește un cont personal sau o versiune gratuită poate crea

riscuri de date, securitate, trasabilitate și responsabilitate. Totuși, nu orice utilizare necesită imediat abonamente scumpe; prima etapă este evaluarea nevoilor și a riscurilor.

6. Care este un prim pilot realist pentru administrația publică?

Un pilot bun pornește de la o problemă clară, risc redus și date nesensibile: sumarizare de documente publice, structurarea informației, pregătirea unor drafturi interne nesensibile, suport pentru comunicare sau căutare în documente aprobate. Pilotul trebuie să aibă scop, responsabil, reguli, criterii de evaluare și verificare umană.

Resurse utile:

- Comisia Europeană – Strengthening Europe's Tech Sovereignty: https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty
- Comisia Europeană – AI Gigafactories: https://commission.europa.eu/topics/competitiveness/competitiveness-coordination-tool-projects/ai-gigafactories_en
- European AI Startup Landscape: https://www.ai-startups-europe.eu/
- ETH Zurich – Apertus: a fully open, transparent, multilingual language model: https://ethz.ch/en/news-and-events/eth-news/news/2025/09/press-release-apertus-a-fully-open-transparent-multilingual-language-model.html
- Sifted – Switzerland unveils national LLM in tech sovereignty push: https://sifted.eu/articles/switzerland-national-llm
- NIST AI Risk Management Framework: https://www.nist.gov/itl/ai-risk-management-framework
- ENISA – AI Cybersecurity Challenges: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
- OWASP – Top 10 for LLM Applications, util pentru proiecte-pilot cu AI generativ: https://owasp.org/www-project-top-10-for-large-language-model-applications/
- AI ORA – Start AI Assessment: https://aiora.co.uk/start-ai-assessment/

Cluster 4. Riscuri, calitatea răspunsurilor și impact

Întrebările despre halucinații, erori, răspundere și impact asupra locurilor de muncă arată că participanții înțeleg atât potențialul AI, cât și limitele sale. AI generativ poate produce răspunsuri bine formulate, dar greșite, incomplete, depășite sau scoase din context. În administrația publică, această problemă este importantă deoarece un răspuns greșit poate ajunge într-un document oficial, într-o comunicare cu cetățeanul sau într-o analiză internă.

Principiul de bază este controlul uman. AI poate asista, dar nu trebuie să decidă singur în situații juridice, administrative sau cu impact asupra drepturilor cetățenilor. Valoarea AI crește

atunci când instituția definește clar sarcinile permise, sursele folosite, cine verifică și cum se documentează utilizarea.

Întrebări selectate și răspunsuri

1. Cum se pot controla răspunsurile automate care conțin halucinații?

Halucinaţiile sunt unul dintre cele mai cunoscute riscuri ale AI generativ. Un sistem AI poate produce un răspuns care sună corect, este bine formulat, dar conţine informaţii greşite, inventate sau scoase din context.

În administraţia publică, acest risc este important. Un răspuns greşit poate ajunge într-un document oficial, într-o comunicare către cetăţean sau într-o analiză internă. De aceea, AI nu trebuie folosit ca autoritate finală.

Controlul halucinaţiilor se face prin mai multe măsuri combinate:

- verificare umană;
- limitarea tipurilor de sarcini permise;
- folosirea unor surse aprobate;
- testarea instrumentului înainte de utilizare;
- păstrarea unei evidenţe pentru utilizările importante;
- instruirea personalului să recunoască răspunsurile nesigure.

La nivel tehnic, unele soluţii pot fi construite astfel încât să răspundă pe baza unui set controlat de documente. De exemplu, arhitecturile de tip RAG, adică Retrieval Augmented Generation, pot ajuta sistemul să caute răspunsul într-o bază de documente aprobată de instituţie. Acest lucru poate reduce riscul, dar nu îl elimină complet.

Regula practică rămâne simplă: dacă răspunsul are consecinţe juridice, administrative sau publice, trebuie verificat de o persoană competentă înainte de utilizare.

2. Mă pot baza pe AI dacă amestecă articole de lege sau răspunde vag?

Nu. Dacă AI oferă un răspuns vag, amestecă articole de lege sau face trimiteri neclare, acel răspuns nu trebuie folosit ca bază pentru o decizie sau pentru un punct de vedere oficial.

Modelele de limbaj pot formula texte foarte convingătoare, dar asta nu înseamnă că înţeleg corect ierarhia actelor normative, aplicabilitatea unei prevederi sau contextul juridic al unei speţe. Ele pot combina informaţii, pot omite detalii esenţiale sau pot inventa referinţe.

AI poate fi folosit ca sprijin preliminar. De exemplu, poate ajuta la:

- structurarea unei întrebări;
- identificarea unor teme de analiză;
- reformularea unui text;

- pregătirea unei liste de aspecte care trebuie verificate;
- sumarizarea unui document public.

Dar interpretarea juridică trebuie făcută de o persoană competentă. În administrația publică, răspunsurile oficiale, deciziile administrative și punctele de vedere juridice nu trebuie externalizate către un instrument AI.

O formulare utilă pentru uz intern ar putea fi: AI poate ajuta la pregătirea unei analize, dar nu poate înlocui analiza.

3. Cine răspunde dacă folosim un răspuns AI greșit la locul de muncă?

Răspunderea nu se transferă către instrumentul AI. În activitatea instituțională, responsabilitatea rămâne la persoana și instituția care verifică, semnează, transmite sau folosește documentul. De aceea, este esențială verificarea umană și păstrarea unei evidențe pentru utilizările importante.

4. Cum va schimba AI locurile de muncă din administrația publică?

AI poate reduce sarcinile repetitive și poate sprijini redactarea, sumarizarea, căutarea sau analiza preliminară. În același timp, va crește nevoia de roluri legate de date, guvernanță, verificare, achiziții tehnologice și control. Cel mai probabil, AI va schimba conținutul muncii, nu va elimina nevoia de judecată profesională și responsabilitate umană.

5. Cum evaluăm riscurile înainte de utilizare?

O evaluare simplă poate începe cu câteva întrebări: care este scopul utilizării AI, ce date sunt folosite, cine este afectat, dacă rezultatul influențează o decizie, dacă există verificare umană, dacă este implicat un furnizor extern, dacă există loguri și ce se întâmplă dacă răspunsul este greșit.

Evaluarea trebuie să pornească de la impact, nu doar de la tehnologie. Același instrument AI poate avea risc redus dacă este folosit pentru reformularea unui text public, dar risc ridicat dacă este folosit pentru prioritizarea dosarelor, analiza eligibilității sau sprijinirea unei decizii administrative.

Pentru instituțiile publice, riscul trebuie tratat cu prudență atunci când sunt implicate date personale, drepturi, beneficii, acces la servicii, HR, educație, control, inspecție sau relația cu cetățenii. În astfel de cazuri, sunt necesare documentare, verificare umană și implicarea rolurilor relevante: juridic, DPO, IT și management.

Un prim pas practic este o grilă scurtă de triere: risc minim, obligații de transparență, utilizare sensibilă sau posibil high-risk. Această clasificare ajută instituția să decidă dacă utilizarea poate continua, dacă are nevoie de controale suplimentare sau dacă trebuie analizată mai detaliat.

Resurse utile:

- Comisia Europeană – AI Literacy: Questions & Answers: https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
- Comisia Europeană – AI Act: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
- AI Act Service Desk – Annex III High-risk AI systems: https://ai-act-service-desk.ec.europa.eu/en/ai-act/annex-3
- AI Act Service Desk – Article 14 Human oversight: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-14
- ENISA – AI Cybersecurity Challenges: https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges
- NIST – AI Risk Management Framework şi AI RMF Playbook, utile pentru evaluarea şi gestionarea riscurilor AI: https://www.nist.gov/itl/ai-risk-management-framework; https://airc.nist.gov/airmf-resources/playbook/

Cluster 5. AI literacy, cursuri și competențe

Participanții au întrebat frecvent despre cursuri, certificate, instruire instituțională și pregătire practică. Acest interes este important deoarece AI literacy este deja prevăzută în AI Act. Articolul 4 se aplică din 2 februarie 2025 și cere furnizorilor și utilizatorilor/deployerilor să ia măsuri pentru un nivel suficient de cunoștințe și competențe pentru personalul care folosește sau operează sisteme AI în numele organizației.

AI literacy nu se concentrează pe cunoștințe tehnice avansate. Înseamnă ca persona ocupand un rol trebuie să înțeleagă suficient ce este AI, ce poate și ce nu poate face, ce riscuri poate produce, ce date nu trebuie introduse în instrumente AI, când este necesară verificarea umană și când este nevoie de escaladare.

Din august 2026 începe etapa de supraveghere și aplicare mai clară a acestei obligații la nivel național. Asta nu înseamnă că, din prima zi, toate instituțiile vor fi automat controlate. În practică, controalele pot apărea gradual, pe măsură ce autoritățile naționale își organizează activitatea, emit orientări și răspund la sesizări sau incidente. Omnibus reformulează obligația de AI literacy dintr-o obligație de a „asigura un nivel suficient" într-o obligație mai flexibilă de a „lua măsuri pentru a sprijini dezvoltarea" AI literacy, fără un nivel de competență uniform sau garantat pentru fiecare persoană.

Pentru instituțiile publice, riscul practic este acesta: dacă apare o sesizare, un incident sau o întrebare formală privind utilizarea AI, instituția va trebui să poată arăta ce măsuri rezonabile a luat. De exemplu: dacă a început să identifice utilizările AI existente, inclusiv utilizările informale de tip *Shadow AI;* dacă are un inventar minim al instrumentelor folosite, al scopurilor de utilizare și al tipurilor de date implicate; dacă a informat personalul; dacă are reguli minime de utilizare AI; dacă a identificat rolurile expuse; dacă a oferit instruire adaptată; și dacă există mecanisme de verificare, control uman, documentare și escaladare.

De aceea, AI literacy nu trebuie tratată ca un curs unic sau ca o simplă bifă administrativă. Este o măsură de guvernanță care arată că instituția înțelege unde se folosește AI, cine îl folosește, în ce scop și ce nivel de pregătire este necesar pentru utilizare responsabilă.

Întrebări selectate și răspunsuri

1. Ce reguli vor fi aplicabile începând cu 3 august 2026 în legătură cu AI literacy?

Obligaţia privind AI literacy nu începe în 2026. Ea se aplică deja din 2 februarie 2025, conform AI Act.

Articolul 4 din AI Act cere furnizorilor şi utilizatorilor de sisteme AI să ia măsuri pentru a asigura un nivel suficient de cunoştinţe şi competenţe în rândul persoanelor care operează sau utilizează sisteme AI în numele organizaţiei. Omnibus reformulează obligația de AI literacy dintr-o obligație de a „asigura un nivel suficient" într-o obligație mai flexibilă de a „lua măsuri pentru a sprijini dezvoltarea" AI literacy, fără un nivel de competență uniform sau garantat pentru fiecare persoană. Cu alte cuvinte, nu este suficient ca instituţia să pună la dispoziţie un instrument AI. Trebuie să se asigure că persoanele care îl folosesc înţeleg ce fac, care sunt riscurile şi unde trebuie să ceară verificare sau aprobare.

Data de 3 august 2026 este relevantă pentru etapa de supraveghere şi aplicare mai clară a AI Act. Autorităţile naţionale competente vor avea un rol mai bine definit în aplicarea cadrului legal. Din acest motiv, instituţiile publice ar trebui să trateze AI literacy ca pe o obligaţie deja activă, nu ca pe un subiect de pregătit abia în 2026.

Paşi utili pentru instituţii:

- identificarea personalului care foloseşte sau poate folosi AI;
- instruire de bază pentru toţi utilizatorii;
- instruire specifică pentru roluri cu risc mai mare;
- reguli interne privind utilizarea AI;
- evidenţa participării la instruiri;
- actualizarea periodică a materialelor, pentru că tehnologia evoluează rapid.

2. Vom fi instruiți instituțional cum să folosim AI?

Aceasta ar trebui să devină o prioritate pentru instituții. AI literacy nu trebuie tratată ca un curs unic, identic pentru toată lumea, ci ca un program adaptat rolurilor, instrumentelor AI folosite și riscurilor reale din organizație.

Managementul are nevoie de înțelegere strategică și de risc; DPO și juridicul au nevoie de protecția datelor și conformitate; IT-ul are nevoie de securitate, integrare și control tehnic; achizițiile au nevoie de întrebări clare pentru furnizori; personalul operațional are nevoie de reguli practice, exemple și limite clare.

Cele mai utile programe sunt cele interne sau adaptate instituției, pentru că pornesc de la contextul concret: ce instrumente AI sunt folosite, ce date sunt implicate, ce activități sunt permise, unde este nevoie de verificare umană și când trebuie escaladată o situație.

3. Există cursuri recunoscute sau diplome internaționale pentru etica AI?

Există tot mai multe programe și certificări în zona de AI governance, etică AI, risk management și conformitate. Ele pot fi utile, mai ales pentru roluri specializate sau pentru persoane care vor coordona activități de AI governance în instituție.

În contextul AI Act și al modificărilor propuse prin Omnibus, accentul nu cade pe obținerea unei certificări formale obligatorii pentru fiecare angajat, ci pe capacitatea organizației de a demonstra că a luat măsuri rezonabile și proporționale pentru dezvoltarea AI literacy.

Aceste măsuri pot include programe interne de formare, participarea angajaților la cursuri adaptate rolurilor lor, sesiuni de informare, ghiduri interne de utilizare AI, evidența instruirilor și actualizarea periodică a competențelor.

Q&A-ul Comisiei Europene privind Articolul 4 precizează că nu este necesar un certificat formal, fiind suficiente dovezi interne ale trainingurilor sau ale altor inițiative de ghidare. În aceeași direcție, textul Omnibus propune ca furnizorii și deployerii să ia măsuri pentru dezvoltarea AI literacy, fără a fi obligați să garanteze un nivel specific de competență pentru fiecare persoană.

Certificarea poate fi importantă și valoroasă, dar nu este, în sine, singura dovadă de conformitate. Într-un domeniu care evoluează rapid, formarea continuă este esențială, fie prin programe interne, fie prin cursuri externe adaptate funcțiilor și riscurilor instituției.

4. Se pot organiza cursuri pentru funcționarii publici centrali sau locali?

Da. Experiența webinarului arată că există o nevoie clară de training aplicat, nu doar de informare generală. Pentru administrația publică, cele mai utile cursuri sunt cele care combină explicațiile despre AI Act cu exemple concrete din activitatea instituțiilor.

Cursurile pot fi organizate pentru funcționari publici centrali sau locali și pot fi structurate pe roluri: management, juridic/DPO, IT/data, achiziții, HR, comunicare, audit, relația cu cetățenii sau personal operațional.

Un avantaj al programelor organizate la nivel instituțional este că pot fi adaptate la instrumentele AI folosite efectiv, la politicile interne, la tipurile de date procesate și la riscurile specifice instituției. Astfel, instruirea devine mai utilă decât un curs generic, pentru că răspunde direct la întrebările oamenilor: ce pot folosi, ce nu pot folosi, ce date pot introduce, cine verifică și cine răspunde.

5. Vor fi suporturi de curs sau certificate?

Acest lucru depinde de organizator și de formatul sesiunii. Pentru webinare de informare, materialele pot fi distribuite ca pachet de follow-up: prezentare, întrebări și răspunsuri, resurse utile și recomandări pentru pașii următori.

Pentru programe de training structurate, se poate avea în vedere un certificat de participare și o listă a competențelor sau temelor acoperite. Un astfel de certificat poate fi util pentru evidența internă a instruirii și pentru a arăta că instituția a început să ia măsuri de AI literacy.

Totuși, din perspectiva AI Act, esențial nu este doar certificatul, ci existența unui efort documentat și proporțional: cine a fost instruit, pe ce teme, pentru ce roluri, cu ce legătură față de instrumentele AI folosite și ce reguli interne au fost comunicate. Certificatul poate susține acest efort, dar nu înlocuiește guvernanța internă.

6. Pot exista cursuri practice pentru audit, HR sau alte funcții specifice?

Da, aceasta este una dintre direcțiile cele mai utile. AI literacy generală trebuie completată cu sesiuni pe funcții, pentru că riscurile și întrebările sunt diferite.

Pentru HR, cursurile pot aborda utilizarea AI în recrutare, evaluare, managementul competențelor și riscul de discriminare. Pentru audit, pot aborda trasabilitatea, documentarea, verificarea utilizărilor AI și controlul intern. Pentru achiziții, pot include întrebări pentru furnizori, cerințe contractuale, date, securitate și responsabilitate. Pentru DPO și juridic, accentul poate fi pe GDPR, DPIA, transparență, bază legală și drepturile persoanelor afectate.

Aceste cursuri sunt mai utile dacă sunt construite pe scenarii reale sau probabile din instituție. Astfel, participanții nu primesc doar informații generale, ci învață cum să aplice AI Act, regulile interne și principiile de utilizare responsabilă în activitatea lor concretă.

Resurse utile:

- AI Act Service Desk – Timeline for the implementation of the EU AI Act: https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act
- AI Act Service Desk – Article 4, AI literacy: https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-4
- Comisia Europeană – AI literacy, Questions & Answers: https://digital-strategy.ec.europa.eu/en/faqs/ai-literacy-questions-answers
- Comisia Europeană – AI talent, skills and literacy: https://digital-strategy.ec.europa.eu/en/policies/ai-talent-skills-and-literacy
- Comisia Europeană – Repository of AI literacy practices: https://digital-strategy.ec.europa.eu/en/policies/repository-ai-literacy-practices
- Comisia Europeană – Living repository to foster learning and exchange on AI literacy: https://digital-strategy.ec.europa.eu/en/library/living-repository-foster-learning-and-exchange-ai-literacy
- Comisia Europeană – Digital Omnibus on AI Regulation Proposal: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-ai-regulation-proposal
- Mishcon de Reya – EU AI Act simplified? Unpacking the AI Omnibus agreement: https://www.mishcon.com/news/eu-ai-act-simplified-unpacking-the-ai-omnibus-agreement-of-may-2026
- AI ORA – AI Assessment: https://aiora.co.uk/start-ai-assessment/
- Progress Foundation și AI ORA în România: https://www.progressfoundation.ro/fundatia-progress-colaboreaza-cu-ai-ora-pentru-a-sprijini-pregatirea-responsabila-pentru-ai-in-romania/

Concluzie

Întrebările primite arată că administrația publică nu pornește de la zero: există interes, utilizări informale, nevoi practice și preocupări reale privind datele, legalitatea, securitatea, calitatea răspunsurilor și responsabilitatea pentru deciziile care pot afecta cetățenii. În același timp, tocmai această utilizare deja existentă face necesară guvernanța. Chiar și acolo unde instituția nu a achiziționat oficial instrumente AI, personalul poate folosi deja aplicații disponibile public, pe conturi personale sau în afara unui cadru instituțional clar.

Riscul principal nu este doar utilizarea AI, ci utilizarea AI fără vizibilitate, reguli și control. Fără un inventar minim al utilizărilor AI, instituția nu poate ști ce instrumente sunt folosite, ce date sunt introduse, cine verifică rezultatele și unde pot apărea riscuri juridice, operaționale sau reputaționale. Acest lucru este important mai ales în administrația publică, unde răspunsurile,

documentele, evaluările sau recomandările pot avea impact direct asupra cetățenilor și asupra încrederii publice.

O concluzie importantă privește și AI literacy. Pregătirea personalului nu trebuie înțeleasă ca un curs tehnic general sau ca o certificare formală obligatorie pentru fiecare angajat, ci ca o măsură de guvernanță adaptată rolurilor și riscurilor instituției. Managementul, DPO-ul, juridicul, IT-ul, achizițiile, HR-ul, comunicarea și personalul operațional au nevoie de repere diferite, în funcție de instrumentele AI folosite, de datele procesate și de impactul activității asupra cetățenilor.

În contextul AI Act și al clarificărilor aduse prin Omnibus, accentul cade pe capacitatea instituției de a arăta că a luat măsuri rezonabile și proporționale: a informat personalul, a oferit instruire adaptată, a stabilit reguli interne, a identificat utilizările AI, inclusiv Shadow AI, și a creat mecanisme de verificare, documentare, control uman și escaladare. Certificatele pot fi utile ca evidență a participării, dar nu înlocuiesc pregătirea continuă și integrarea AI literacy în practica organizațională.

Pentru instituții, prioritatea imediată nu este o soluție tehnică spectaculoasă, ci un set de pași practici și realiști: inventar AI, reguli interne de utilizare acceptabilă, AI literacy pe roluri, implicarea DPO/IT/juridic, verificare umană, documentare minimă și pilotare controlată. Este important ca instituțiile să înceapă cu utilizări cu risc redus, să testeze, să învețe și să extindă treptat, pe baza unor criterii clare de siguranță, utilitate și conformitate.

Aceste măsuri pot reduce riscurile și pot pregăti instituțiile pentru aplicarea AI Act și pentru o adopție AI responsabilă. În același timp, ele pot transforma AI dintr-o utilizare informală și fragmentată într-un instrument gestionat instituțional, integrat în procese, conectat la obiectivele de digitalizare și folosit în mod transparent, sigur și orientat spre interesul public.

Echipa de experți

Materialele au fost pregătite cu contribuția experților implicați în webinarii și în activitățile AI ORA România. Pentru a vedea echipa AI ORA în ansamblu, consultați pagina Echipa AI ORA. Echipa AI ORA

Dr. Irina Marsh - expert în etică, guvernanță AI, conformitate și standardizare; Responsible AI Integration Lead / Ethics and Governance Lead în echipa AI ORA. LinkedIn

Mihai Nămoloșanu - specialist în sisteme AI, software și guvernanță tehnică în echipa AI ORA; AI technology consultant și Lead Auditor ISO/IEC 42001. LinkedIn

Dr. Florin Silviu Bondar - expert în strategie AI, leadership, transformare instituțională și evaluarea valorii/ROI pentru adoptarea AI în echipa AI ORA. LinkedIn

Camelia Crișan, PhD – CEO al Fundației Progress, cu expertiză în educație digitală, dezvoltare de competențe, leadership și proiecte naționale precum CODE Kids, utilizarea AI în zona de resurse umane, cu accent pe competențe, etică, responsabilitate și implicațiile instituționale ale adoptării AI.LinkedIn

Despre CBRNE, AI ORA şi Progress Foundation

CBRNE Ltd

CBRNE Ltd este o companie din Marea Britanie care oferă expertiză în domenii precum rezilienţă organizaţională, guvernanţă, etică, conformitate şi implementarea responsabilă a tehnologiilor emergente.

Prin iniţiativa AI ORA, CBRNE sprijină organizaţiile să înţeleagă, să evalueze şi să adopte AI într-un mod practic şi responsabil.

Website: https://cbrneltd.com/

AI ORA

AI ORA înseamnă AI Organisational Readiness Accelerator. Iniţiativa sprijină organizaţiile să treacă de la interesul pentru AI la acţiune practică.

Procesul AI ORA include AI literacy, discovery, roadmap şi implementation. În funcţie de nevoile organizaţiei, AI ORA poate sprijini evaluarea nivelului de pregătire, instruirea echipelor, guvernanţa AI, identificarea cazurilor de utilizare, planificarea adopţiei, data engineering şi dezvoltarea de soluţii AI personalizate.

Website: https://aiora.co.uk/

Progress Foundation

Progress Foundation este o organizaţie din România cu experienţă în educaţie, tehnologie, cercetare, inovaţie şi dezvoltarea capacităţii instituţionale.

Prin colaborarea cu AI ORA, Progress Foundation sprijină pregătirea responsabilă pentru AI în România şi contribuie la conectarea expertizei locale cu metodologii practice de AI readiness şi adopţie responsabilă.

Website: https://www.progressfoundation.ro/

Despre colaborarea Fundația Progress - AI ORA

Fundația Progress și AI ORA colaborează pentru a sprijini pregătirea responsabilă pentru AI în România, prin informare, AI literacy, evaluare de readiness și sprijin practic pentru organizații în înțelegerea AI Act, a guvernanței AI și a pașilor de adopție responsabilă.

Fundația Progress aduce experiența sa în educație digitală și dezvoltare de competențe în comunități, inclusiv prin CODE Kids, una dintre cele mai mari mișcări naționale de programare și robotică pentru copii, desfășurată prin rețeaua bibliotecilor publice și în colaborare cu comunitățile locale. Prin această colaborare, experiența de lucru cu administrația locală și cu ecosistemele de învățare comunitară este conectată la nevoia actuală de AI literacy și guvernanță AI în administrația publică.

Website: Fundația Progress x AI ORA

Contact

Pentru întrebări suplimentare sau pentru o discuţie despre pregătirea instituţiei pentru utilizarea responsabilă a AI, ne puteţi contacta la: **aiora.romania@cbrneltd.com**

Persoane de contact:

- Dr. Irina Marsh
- Mihai Nămoloşanu