



Atelier Unseen

Date personale, confidențialitate și informații sensibile

Clasificarea informațiilor, GDPR, confidențialitate și riscurile utilizării AI

Obiectivele lecției

Diferențierea datelor personale, categoriilor speciale, informațiilor confidențiale și secretelor comerciale.
Aplicarea principiilor GDPR la utilizarea AI.
Identificarea informațiilor care nu trebuie introduse în instrumente neaprobată.
Stabilirea rolurilor interne și a nivelului de aprobare.
Documentarea deciziei și a măsurilor de protecție.

De ce promptul este o operațiune de date

Intrare

Prompturile, fișierele, imaginile și conectorii pot conține date personale sau confidențiale.

Prelucrare

Furnizorul poate genera jurnale, metadate, copii temporare sau rezultate derivate.

Ieșire

Rezultatul poate reproduce, deduce sau combina informații sensibile.

Harta informațiilor

Categorie	Exemple	Regulă
Publice	Comunicate, ghiduri publicate	Verifici sursa și actualitatea
Personale	Nume, email, telefon, identificatori	Scop, temei, minimizare
Speciale	Sănătate, biometrie, opinii, sindicat	Condiții stricte și aprobare
Confidențiale	Contracte, prețuri, strategie	Mediu controlat sau nu se folosesc
Securitate	Parole, tokenuri, vulnerabilități	Nu se introduc în prompturi

Date personale versus date anonime

Date personale

Identificarea poate fi directă sau indirectă. Eliminarea numelui nu este suficientă dacă funcția, localitatea, proiectul sau alte detalii permit identificarea.

Date anonime

Anonimizarea trebuie să fie ireversibilă în mod rezonabil. Pseudonimizarea și mascarea reduc riscul, dar datele pot rămâne personale.

Principiile GDPR aplicate AI

Principiu	Aplicare în AI
Legalitate și transparență	Scop, temei, informare și utilizare echitabilă
Limitarea scopului	Nu reutilizezi automat datele pentru alt scop
Minimizare	Folosești strict informațiile necesare
Exactitate	Verifici inputul și corectezi outputul
Limitarea stocării	Controlezi istoricul, proiectele și logurile
Integritate și confidențialitate	Conturi aprobate, acces, MFA, criptare
Responsabilitate	Păstrezi dovada deciziei și măsurilor

Confidențialitate dincolo de GDPR

Secrete comerciale

Strategii, know-how, liste de clienți, prețuri și condiții negociate.

Drepturi de autor

Documente, imagini, cod, baze de date și materiale protejate.

Securitate

Parole, chei API, tokenuri, configurații și vulnerabilități.

Riscuri specifice instrumentelor AI

Risc	Exemplu	Control
Istoric și loguri	Conversații păstrate în cont	Retenție și ștergere
Conectori	Acces la Drive, email sau CRM	Cel mai mic privilegiu
Shadow AI	Cont personal neaprobat	Politică și blocare
Reidentificare	Date mascate insuficient	Test de reidentificare
Transferuri	Furnizori și subprocesatori	Contract și garanții
Partajare	Link public sau captură	Controlul exportului

Rolurile interne

1

Utilizator

Clasifică, minimizează,
verifică și raportează.

2

Manager

Aprobă scopul și nivelul de
risc.

3

IT/Security

Controlează accesul,
logurile și incidentele.

4

DPO

Analizează temeiul,
drepturile și DPIA.

5

Juridic

Verifică AI Act, contractele și
confidențialitatea.

6

Achiziții

Evaluează furnizorul și
condițiile serviciului.

Când este necesară o evaluare suplimentară

Date sensibile

Categorii speciale, angajați, clienți, sănătate, biometrie.

Impact ridicat

Profilare, decizii despre persoane, monitorizare sau scoring.

Integrare amplă

Conectori, sisteme interne, volume mari și furnizori externi.

Studiu de caz: contract confidențial

Întrebare	Răspuns corect
Este necesar contractul integral?	Nu. Folosești strict clauzele necesare.
Conține date personale?	Da, posibil nume, email, cont și semnături.
Conține secrete comerciale?	Da, prețuri și condiții negociate.
Soluție	Curățare, instrument aprobat, acces limitat, verificare.

Checklist înainte de utilizare

Am clasificat informația?

Pot folosi date fictive sau agregate?

Instrumentul și contul sunt aprobate?

Am dreptul să transmit materialul?

Am eliminat datele inutile și metadatele?

Este necesară aprobarea DPO, juridic, IT sau manager?

Pot verifica și documenta rezultatul?

Principiul lecției

Nu întreba doar dacă AI poate procesa informația. Întreabă dacă organizația are dreptul, controlul și măsurile necesare pentru acea prelucrare.