Modificări ale Legislației privind Protecția Datelor cu Caracter Personal

Dispoziții Generale

Cazac Dumitru

Head of Legal Section, Phd, Senior Lawyer

Sursa și Originea Legislației privind Protecția Datelor cu Caracter Personal în RM

1. **Legea nr. 133 din 08.07.2011 – Directiva 95/46/CE** a Parlamentului European şi a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi libera circulație a acestor date

2. **Legea nr. 195 din 25.07. 2024** (în vigoare din 23.08.2026) - **Regulamentul (UE) 2016/679** al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date.

Principalele diferențe dintre Directiva 95/46/CE și GDPR: o perspectivă orientată spre afaceri

Directiva 95/46/CE

- **Obliga statele membre să transpună prevederile în legislația națională, ceea ce a dus la interpretări și aplicații diverse.**
- **Se aplica în principal entităților stabilite în UE.**
- **Acorda drepturi pentru acces, rectificare și opoziție împotriva prelucrării datelor personale (mai puține).**
- **Permitea consimțământul implicit în anumite contexte.**
- **Obliga operatorii de date să notifice autoritățile naționale cu privire la activitățile de prelucrare.**
- **Nu impunea notificarea în caz de breșe în sistemul de prelucrare și stocare a datelor.**
- **Lăsa sancțiunile la discreția legislațiilor naționale, ceea ce a dus la variații și aplicabilitate redusă.**

Principalele diferențe dintre Directiva 95/46/CE și GDPR: o perspectivă orientată spre afaceri

GDPR

- **Aplicabil direct în toate statele membre ale UE, fără a necesita transpunere în legislația națională.**
- **Introduce principii noi, precum responsabilitatea (“accountability”) și confidențialitatea prin design/implicit.**
- **Extinde drepturile persoanelor vizate, inclusiv dreptul la ștergere (“Right to be forgotten”), portabilitatea datelor și o transparență sporită.**
- **Necesită consimțământ explicit, informat și neechivoc pentru prelucrarea datelor.**
- **Înlocuiește notificările către autorități cu cerințe de documentație internă**
- **Introduce obligații stricte de notificare în caz de breșă de date, cu termen de 72 de ore.**
- **Stabilește un regim de sancțiuni armonizat, cu amenzi semnificative: până la 20 de milioane de euro sau 4% din cifra de afaceri globală anuală, ceea ce le face mult mai disuasive față de sancțiunile prevăzute de Directivă.**

Analiza principalelor schimbări introduse de GDPR

- **Uniformitate și standarde modernizate**

- **Extinderea domeniului de aplicare:**
  - Deși dispozițiile extrateritoriale ale GDPR se aplică nu doar entităților din UE, dar și acțiunilor care vizează prelucrarea datelor ale rezidenților (cetățenilor) UE (de exemplu, companiile care prestează servicii de export sau platforme digitale) trebuie să se alinieze cu GDPR pentru a rămâne competitive.
  - Sunt introduse definiții mai largi ale datelor personale, incluzând categorii moderne, precum adresele IP și datele de geolocație.

- **Drepturi sporite pentru persoanele vizate:**
  - Cetățenii vor beneficia de drepturi extinse, cum ar fi portabilitatea datelor și dreptul la ștergere, ceea ce crește obligațiile companiilor de a răspunde eficient la solicitările persoanelor vizate.
  - Obligațiile de transparență necesară cer notificări mai clare privind confidențialitatea atât în operațiunile interne, cât și în cele internaționale.

- **Cerințe mai stricte pentru consimțământ:**
  - Consimțământul liber exprimat, specific, informat și explicit nu este baza legală cea mai importantă pentru prelucrare. Din contra, consimțământul devine una dintre cele mai vulnerabile temeiuri legale de prelucrare, din perspectiva necesității demonstrării îndeplinirii criteriilor în momentul solicitării și recepționării acestuia.

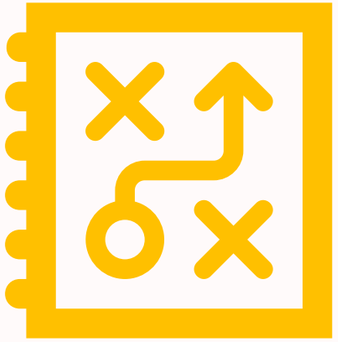
Analiza principalelor schimbări introduse de GDPR

- **Guvernanță internă:**
  - Toate companiile trebuie să mențină documentație internă cuprinzătoare și pot fi obligate să numească Responsabili pentru Protecția Datelor (DPO) în funcție de scara operațiunilor.
  - Evaluările Impactului asupra Protecției Datelor (DPIA) sunt încurajate pentru activități cu risc ridicat, chiar dacă nu sunt întotdeauna obligatorii din punct de vedere legal.

- **Notificări în caz de breșă de date:**
  - Companiile responsabile trebuie să notifice autoritățile de supraveghere prompt în caz de breșă (sau scurgeri de date), în termen de 72 de ore.

- **Sancțiuni:**
  - Directiva 95/46/CE lăsa sancțiunile la discreția statelor membre, ceea ce a dus la variații semnificative și, în multe cazuri, la amenzi neproporționale sau lipsa acestora.
  - GDPR introduce un regim armonizat de sancțiuni, cu amenzi semnificative: până la 20 de milioane de euro sau 4% din cifra de afaceri globală anuală, ceea ce le face mai disuasive. **(Conform Legii nr. 195 din 25.07.2024 - până la 2 000 000 de lei sau până la 2% din cifra totală de afaceri, luându-se în calcul cea mai mare valoare).**

Influența asupra Mediului de Afaceri din Moldova



Provocări:

Costuri de conformitate: Afacerile trebuie să investească în consultanță juridică, instruirea personalului și soluții tehnice pentru a asigura conformitatea.

Complexitate operațională: Adoptarea standardelor inspirate de GDPR, cum ar fi DPIA (Data Protection Impact Assessment) și RoPA, poate crește costurile administrative.

Oportunități:

Acces pe piață: Alinierea la principiile GDPR deschide uși către piețele UE și consolidează încrederea cu partenerii europeni.

Reputație îmbunătățită: Adoptarea practicilor robuste de protecție a datelor sporește încrederea clienților și credibilitatea corporativă.

Procese simplificate: Conformitatea standardizată reduce complexitățile în operațiunile transfrontaliere.

Situațiile (materiale) în care nu se aplică Legea

Reglementare veche (art.2):

Domeniul de acțiune al prezentei legi nu se extinde asupra:

prelucrării datelor cu caracter personal efectuate de către operatori exclusiv pentru nevoi personale sau familiale, dacă prin aceasta nu se încalcă drepturile subiecților datelor cu caracter personal.

Reglementare nouă (art. 2):

Prezenta lege nu se aplică prelucrării datelor cu caracter personal:

de către o persoană fizică în cadrul unei activităţi exclusiv personale sau domestice;

Aplicarea Extrateritorială:

Reglementare veche (art.2):

Domeniul de acţiune al prezentei legi se extinde asupra:

a) prelucrării datelor cu caracter personal efectuate în cadrul activităţilor desfăşurate de operatori aflaţi pe teritoriul Republicii Moldova;

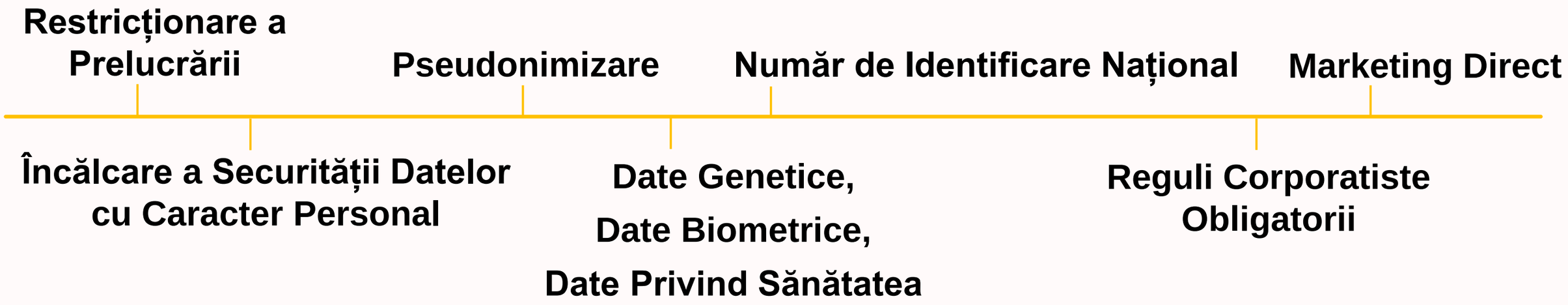
b) prelucrării datelor cu caracter personal efectuate de operatori aflaţi în afara teritoriului Republicii Moldova, cu utilizarea mijloacelor aflate pe teritoriul Republicii Moldova, cu excepţia cazului în care aceste mijloace nu sînt utilizate decît în scopul tranzitării pe teritoriul Republicii Moldova a datelor cu caracter personal care fac obiectul prelucrării respective;

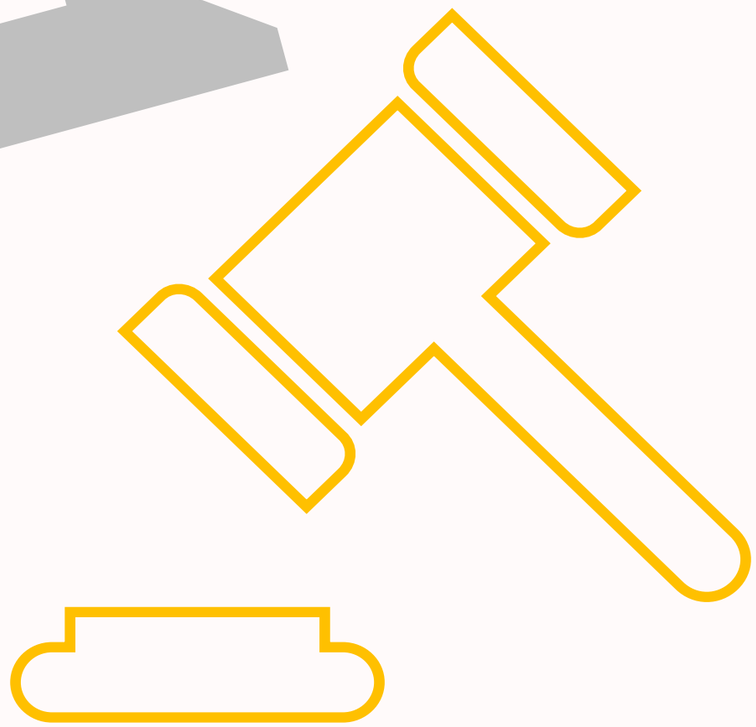
Reglementare nouă (art.3)

1) Prezenta lege se aplică prelucrării datelor cu caracter personal în contextul activităţilor unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Republica Moldova, indiferent dacă prelucrarea are loc sau nu pe teritoriul Republicii Moldova.
2) Prezenta lege se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Republica Moldova de către un operator sau o persoană împuternicită de operator care nu are sediu în Republica Moldova, atunci când activităţile de prelucrare sunt legate de:
   a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Republica Moldova, indiferent dacă se solicită sau nu efectuarea unei plăţi de către persoana vizată; sau
   b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Republicii Moldova.

Noțiuni Noi Introduse

În noțiunea date cu caracter personal au fost incluse expres
următoarele componente: nume, date de localizare, identificator online



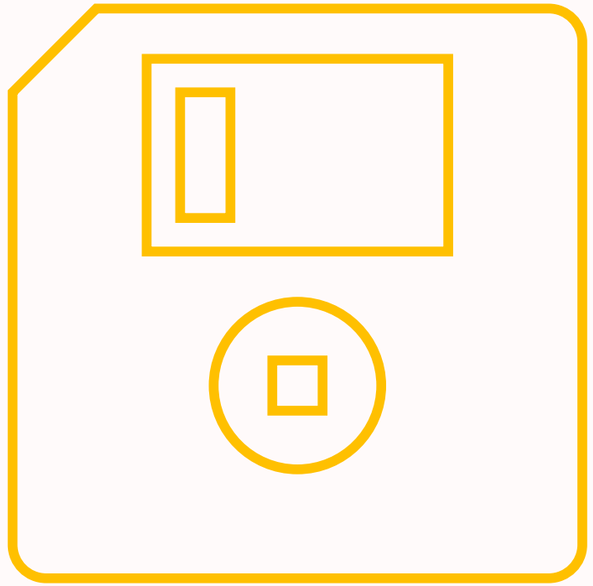


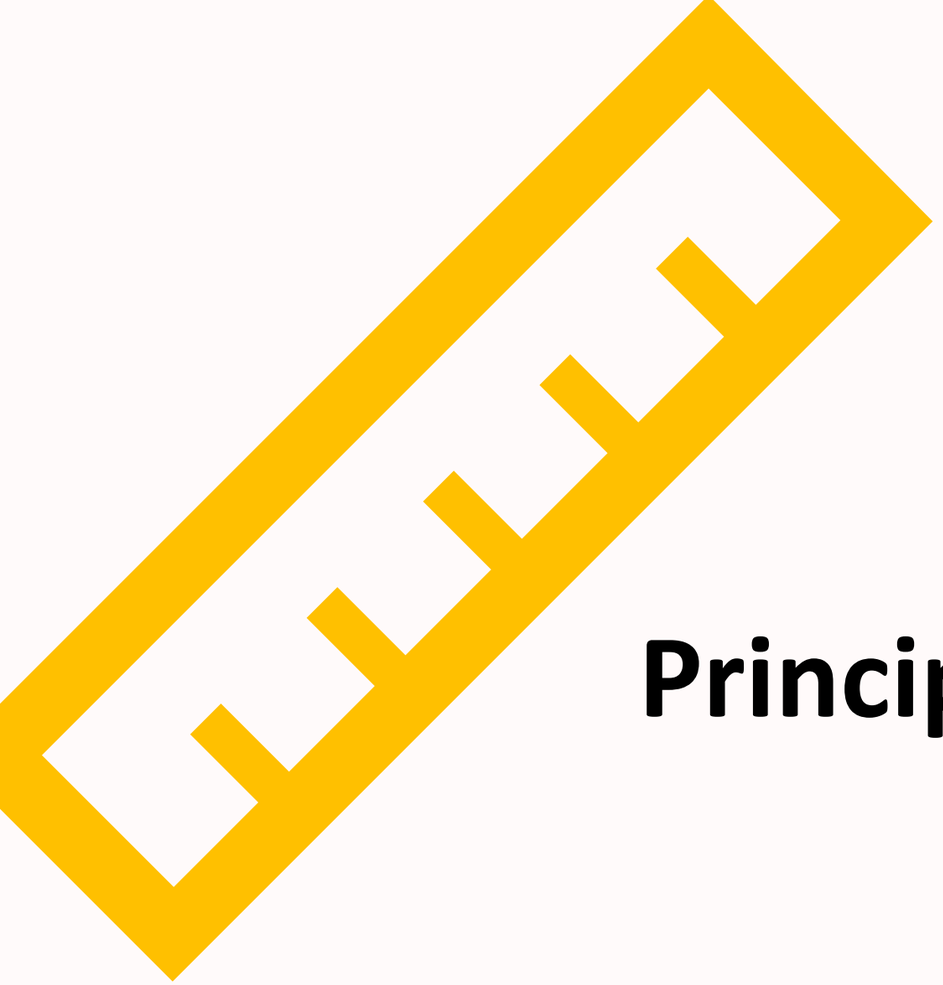
Principiul Legalității

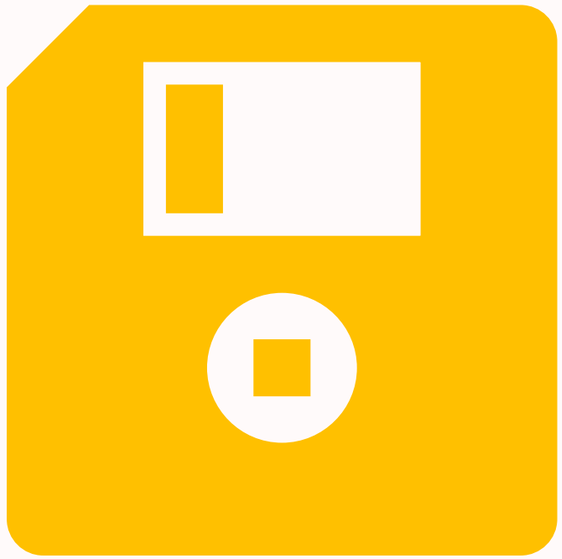
Principiul Echității și Transparenței

Principiul Limitării Legate de Scop

Principiul Reducerii la Minim a Datelor



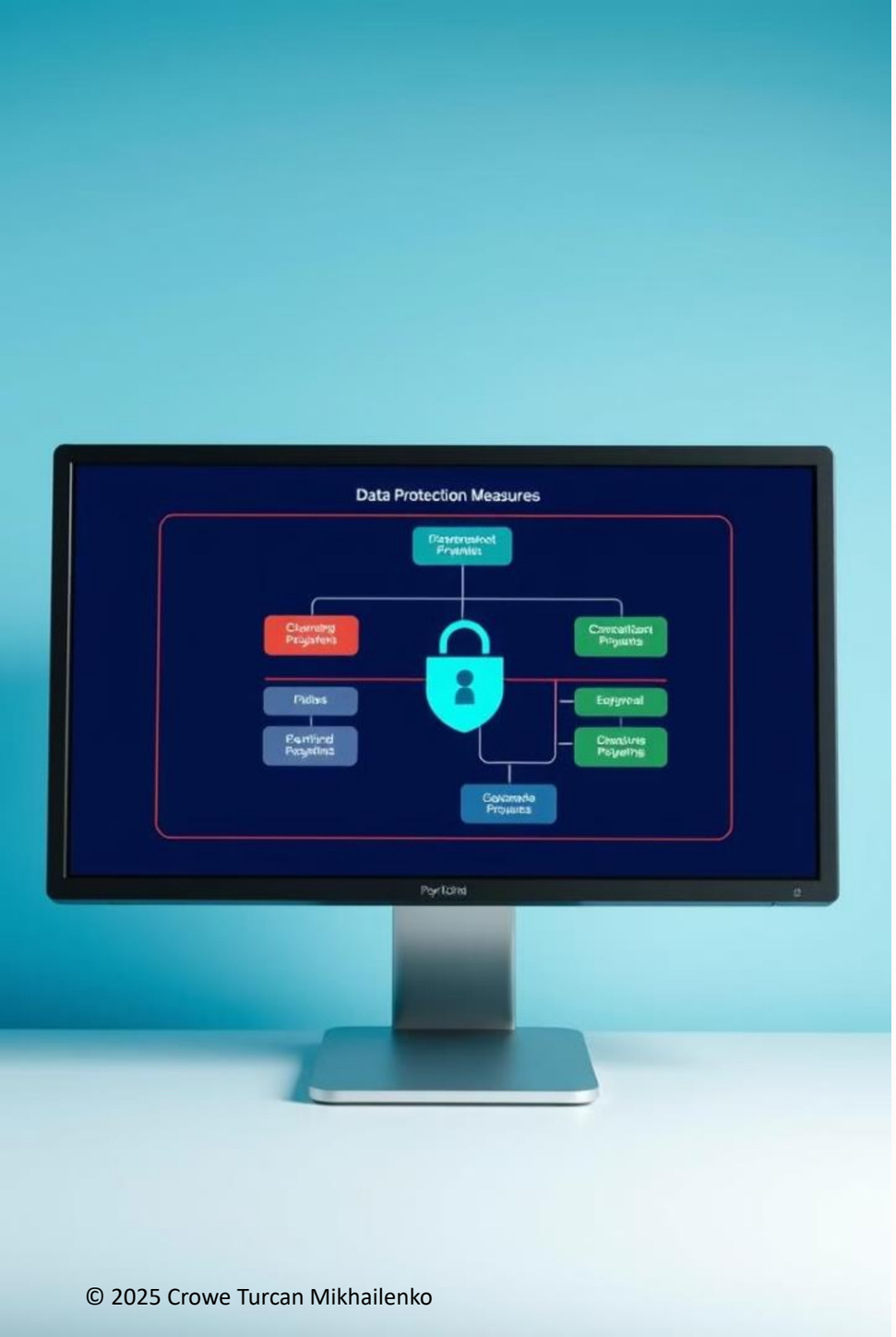




Principiul Exactității

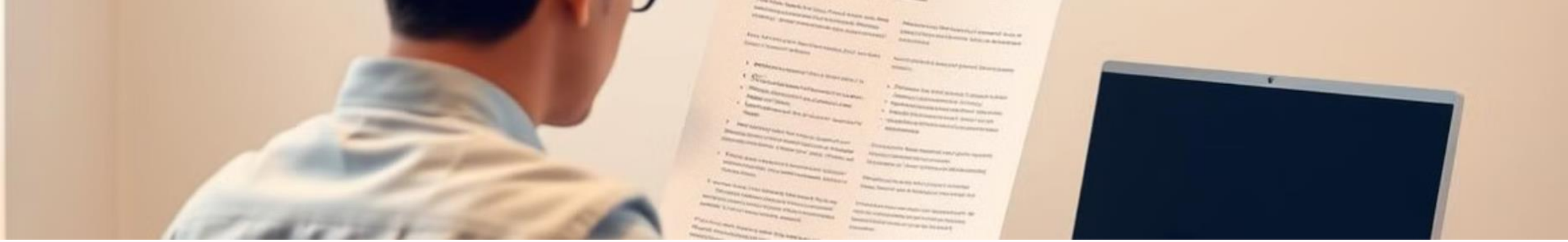
Principiul Limitării Legate de Stocare

Principiul Integrității și Confidențialității



Măsuri Tehnice și Organizatorice de Protecție a Datelor

- **Criptarea Datelor**
- **Controlul Accesului**
- **Backup-uri Regulate**
- **Politici Interne**
- **Instruirea Angajaților**
- **Prevenirea accesului neautorizat**
- **Gestionarea incidentelor de securitate:**
- **Pseudonimizarea și anonimizarea datelor**



Exemple:

Într-o clinică medicală:

Fișele pacienților sunt stocate electronic într-un sistem protejat prin parolă, iar accesul este permis doar medicilor autorizați.

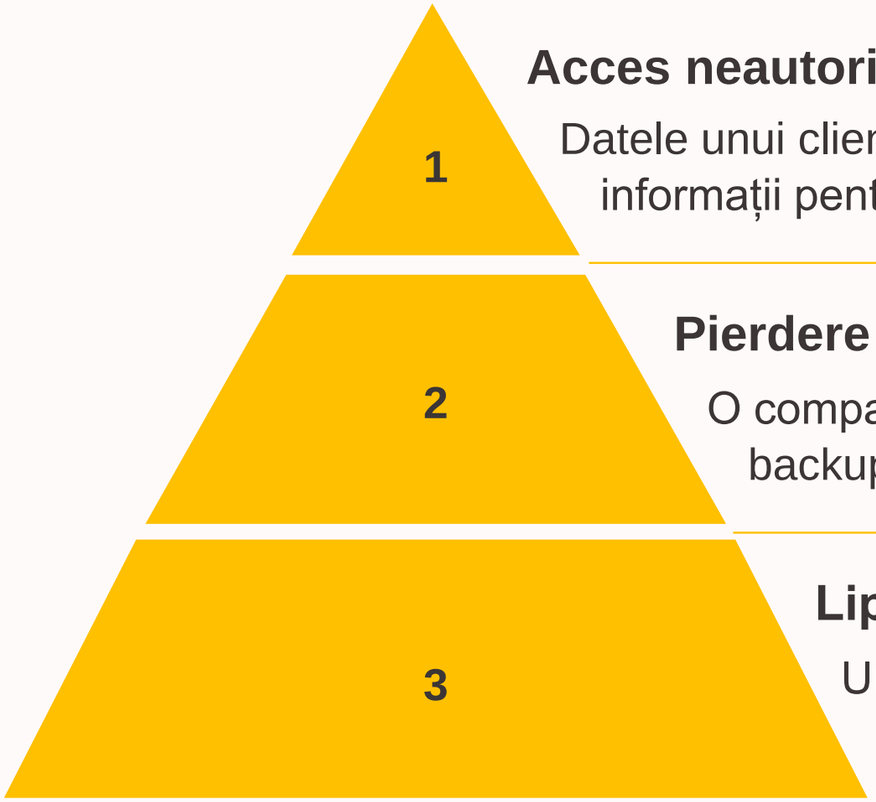
Datele transferate între medici și laboratoare sunt criptate pentru a preveni accesul neautorizat.

Într-o companie de recrutare:

CV-urile candidaților sunt stocate într-o bază de date securizată, cu acces limitat doar personalului de resurse umane.

Datele candidaților respinși sunt șterse conform politicii de retenție.

Încălcări ale Principiului Integrității și Confidențialității



Acces neautorizat:

Datele unui client sunt vizualizate de un angajat care nu are nevoie de aceste informații pentru a-și îndeplini sarcinile.

Pierdere de date:

O companie pierde datele financiare ale clienților pentru că nu a făcut backup-uri regulate.

Lipsa securității datelor:

Un laptop care conține date personale este pierdut, iar datele nu sunt protejate prin criptare.

Principiul Responsabilității

Încălcarea Principiului Responsabilității:

1

Lipsa transparenței:

O companie colectează date despre clienți fără a informa despre scopul și temeiul legal al prelucrării.

2

Documentație inexistentă:

O organizație nu păstrează evidențe ale activităților de prelucrare și nu poate demonstra conformitatea în cazul unui control.

3

Securitate insuficientă:

Datele angajaților sunt stocate într-un format neprotejat și accesibile oricărui angajat, ceea ce duce la pierderea încrederii și la potențiale sancțiuni

Concluzii și Recomandări

1

Prioritizarea Protecției Datelor

Protecția datelor cu caracter personal ar trebui să fie o prioritate pentru toate organizațiile.

2

Respectarea Cadrului Legal

Este esențial ca operatorii de date să respecte legislația privind protecția datelor.

3

Conștientizarea Angajaților

Este important ca angajații să fie conștienți de importanța protecției datelor.