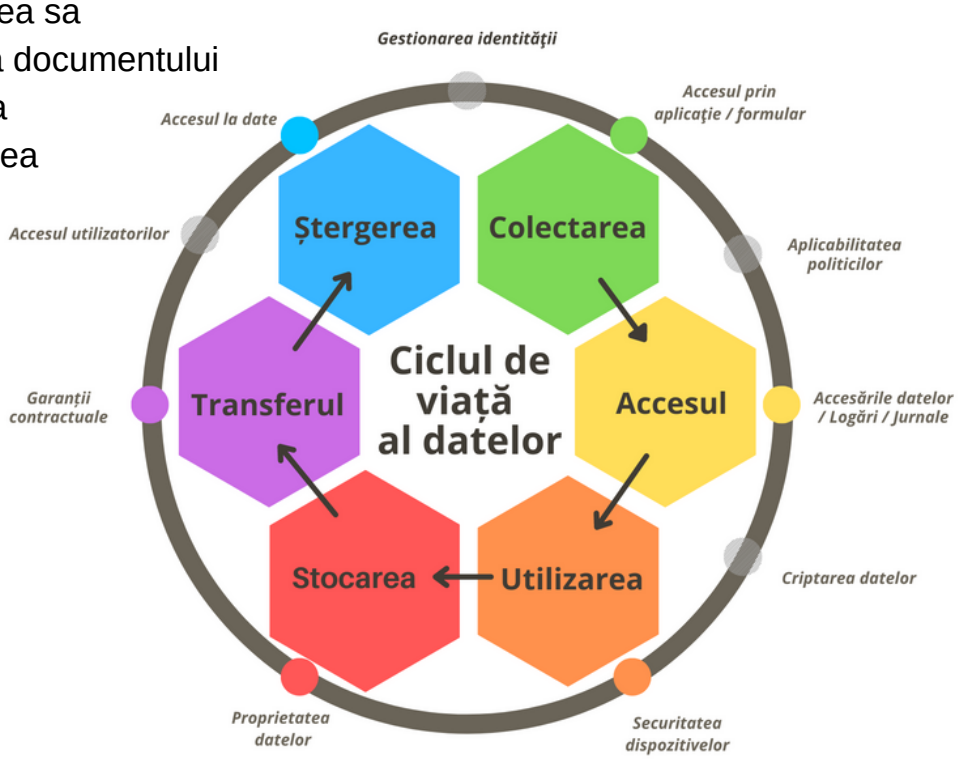
3.14 ORIENTĂRI PRIVIND DISTRUGEREA ÎN SIGURANȚĂ A DATELOR CU CARACTER PERSONAL

Explorarea celor mai bune practici pentru distrugerea în siguranță a documentelor care conțin date cu caracter personal, atât prin metode interne, cât și prin externalizarea serviciilor

Orice document (fizic sau electronic) care conține date cu caracter personal are un **„ciclu de viață”**. Astfel, vorbim despre:

- Crearea documentului
- Analiza / folosirea acestuia
- Distribuirea sa
- Utilizarea documentului
- Arhivarea
- Distrugerea



Pentru a ne asigura că respectăm întru totul normele privind protejarea vieții private și a datelor cu caracter personal este foarte indicat să acordăm o atenție sporită documentelor aflate în **ultimele faze ale ciclului de viață – arhivarea și mai ales distrugerea** acestora. În continuare vom dezvolta câteva practici în acest sens.

Prezenta Orientare se adresează operatorilor de date (unităților medicale, furnizorilor de servicii medicale, indiferent că sunt constituiți într-o entitate cu sau fără personalitate juridică). Medicii, în special cei cu atribuții de management sau de reprezentare a operatorului, vor avea în vedere această perspectivă, deoarece sunt parte a sistemului de resurse umane din cadrul operatorului.

Ce ar trebui să cunoașteți:

Orice informații vehiculăm pe suport de hârtie sau în format electronic se încadrează într-o categorie de date, care trebuie regăsite într-un nomenclator al operatorului, unde se menționează perioada de deținere a documentului și alte informații. Odată ce această perioadă este îndeplinită, se trece la operațiunea de distrugere a suportului de informație, operațiune la care se referă prezenta Orientare.

Distrugerea documentelor se poate realiza atât **direct** de dumneavoastră în cadrul unității medicale sau, atunci când este vorba de un volum mare de documente care trebuie distruse, se poate alege un **furnizor de servicii de distrugere** a acestora. Haideți să vedem ce trebuie însă să avem în vedere:

Metode interne de distrugere a datelor

- **Tocătoare de documente**: Utilizarea unor tocătoare de documente este o metodă eficientă pentru distrugerea în siguranță a documentelor în format fizic. Alegeți tocătoare care să taie documentele în fâșii înguste sau particule mici, pentru a face dificilă, dacă nu imposibilă, reconstituirea informațiilor.
    - **Exemplu**: Simpla aruncare la coșul de gunoi a unor documente expune unitatea medicală sau chiar pe dumneavoastră (în cazul nerespectării procedurilor și politicilor interne). În secțiunea cazuistică vom dezvolta o astfel de speță.

- **Demagnetizarea**: Pentru distrugerea datelor stocate pe suporturi magnetice (ex. CD-uri, hard disk-uri, benzi magnetice) demagnetizarea este o soluție eficientă.

Aceasta constă în utilizarea unui aparat de demagnetizare (degausser) pentru a distruge informațiile prin expunerea suportului la un câmp magnetic puternic.

  - **Exemplu**: Pierderea unui CD (nesecurizat) care conține rezultatele unor analize medicale ale unui pacient poate constitui un incident care să atragă sancțiuni mari!

- **Ștergerea securizată a datelor**: În cazul dispozitivelor de stocare electronică (ex. hard disk-uri, memorii flash) utilizați un software de ștergere securizată pentru a distruge ori suprascrie datele de mai multe ori, astfel încât să nu poată fi recuperate.
  - **Exemple**: CCleaner, Eraser, BitRaser sunt câteva exemple de astfel de softuri. Puteți alege orice soft identificați ca fiind facil pentru această activitate. Atenție! Vă rugăm să vă asigurați că furnizorul de soft respectă normele R.G.P.D. (adesea acest angajament este luat prin politica de confidențialitate publicată pe website sau informații relevante se pot găsi în termeni și condiții).

Servicii externalizate de distrugere a datelor

- **Evaluarea furnizorilor**: Dacă alegeți să externalizați procesul de distrugere a datelor, asigurați-vă că furnizorul ales respectă standardele R.G.P.D. și oferă garanții adecvate în ceea ce privește securitatea și confidențialitatea datelor. Cereți recomandări de la alți colegi care colaborează cu furnizori exemplari!
  - **Exemplu**: Așa cum menționam și mai sus, studiați angajamentele pe care aceștia și le iau pentru a respecta normele legale (detaliate în politica de confidențialitate sau termeni și condiții). Dacă nu își asumă nici un fel de răspundere pentru distrugerea securizată și în condiții de confidențialitate, dar să poată să și demonstreze acest lucru, evitați furnizorul de servicii respectiv!

- **Acorduri privind protecția datelor**: Încheiați un acord de confidențialitate și protecție a datelor cu furnizorul, care să detalieze responsabilitățile și obligațiile acestuia în legătură cu procesul de distrugere a datelor.
  - **Exemplu**: Cel mai adesea un furnizor responsabil va pune la dispoziția dumneavoastră un acord specific (operator-persoană împuternicită) pentru distrugerea acestor date.

- Urmăriți atent procesul detaliat pentru distrugere și felul în care acesta este documentat! În cazul în care nu vă este transmis un astfel de acord, solicitați unul ori folosiți unul generic pus la dispoziție în acest ghid (**Anexa 2 Model de acord de confidențialitate pe care să îl utilizați în relație cu colaboratorii persoane împuternicite**)

- **Monitorizarea activității furnizorului**: Solicitați rapoarte și documentație referitoare la procesele de distrugere și verificați ca procesele să fie duse la îndeplinire cu succes.
    - **Exemplu**: puteți solicita furnizorului filmări cu procesul de distrugere a documentelor.

- **Documente doveditoare ale distrugerii**: După ce datele au fost distruse în mod corespunzător, furnizorul ar trebui să vă ofere un document care să ateste eliminarea completă și sigură a datelor. Acest document poate fi folosit ca dovadă în cazul unor audituri sau controale privind protecția datelor.
    - **Exemplu**: Un astfel de document poate fi un raport, un proces verbal de distrugere, un certificat sau un alt document de asumare a acestei răspunderi a furnizorului.

Recomandări suplimentare

- **Politici și proceduri interne**: Elaborați politici și proceduri interne care să reglementeze modul în care datele cu caracter personal sunt distruse în cadrul cabinetului medical sau al unității medicale în care vă desfășurați activitatea. Asigurați-vă că aceste politici sunt respectate de întregul personal și că toți angajații sunt instruiți în legătură cu responsabilitățile lor privind protecția datelor.
    - **Exemplu**: Poate fi vorba despre o procedură operațională de distrugere a documentelor prin care se va constitui o comisie de distrugere a documentelor, care pe baza unui inventar al documentelor ce vor fi distruse, le vor distruge și vor documenta aceasta printr-un proces verbal de distrugere semnat de toți membrii comisiei.

- **Revizuirea periodică a datelor**: Stabiliți un program de revizuire periodică a datelor stocate pe documente pentru a identifica informațiile care nu mai sunt necesare și care trebuie distruse în mod corespunzător.
    - **Exemplu**: Unele documente trebuie păstrate pe o perioadă lungă de timp, fiind o obligație legală a unității medicale conform legislației în vigoare (Legea 16/1996 privind Arhivele Naționale), în timp ce pentru altele nu identificați un termen stabilit de lege.

În acest caz stabiliți intern un termen rezonabil pentru păstrarea datelor raportându-ne la scopul colectării datelor.

- **Consultarea responsabilului cu protecția datelor**: Dacă este cazul, adresați-vă responsabilului cu protecția datelor (DPO) din cadrul unității medicale, care să vă coordoneze procesul de distrugere a datelor cu caracter personal. În situația unor operatori de date cu personal medical extrem de restrâns, fără a avea angajat un DPO, cum ar fi unele cabinete medicale individuale sau SRL-uri, acestea pot fie singure să-și stabilească clar procedura, fie să apeleze la un consultant.

Cazuistică relevantă

Clinica Medicală "Sănătate Plus" este o unitate medicală privată care oferă o gamă largă de servicii medicale, de la consultări și analize de laborator până la intervenții chirurgicale. Într-o zi, sistemul informatic al clinicii a fost atacat de hackeri, care au reușit să acceseze și să sustragă date cu caracter personal ale pacienților, inclusiv nume, adrese, numere de telefon, istoric medical și detalii despre tratamentele prescrise.

Ca urmare a acestui incident, conducerea clinicii a luat măsuri pentru a îmbunătăți securitatea informațiilor stocate în sistemul lor. Aceste măsuri au inclus actualizarea software-ului de securitate, implementarea unor metode mai avansate de criptare a datelor și instruirea personalului cu privire la importanța protejării datelor cu caracter personal.

De asemenea, clinica a informat pacienții afectați despre incident și le-a oferit asistență pentru a le proteja identitatea și a preveni posibilele fraude.

Cu toate acestea, în pofida măsurilor luate, datele compromise au fost deja expuse și pot fi utilizate în moduri ilicite de către terțe părți. Autoritatea națională de protecție a datelor a deschis o investigație privind incidentul și, în urma constatărilor, a decis să sancționeze Clinica "Sănătate Plus" cu o amendă semnificativă pentru nerespectarea prevederilor legale privind protecția datelor cu caracter personal.

Cazuistică din activitatea Autorității de Supraveghere:

Medlife S.A. – amendă aplicată de A.N.S.P.D.C.P. 5000 euro

O persoană fizică a identificat documente care conțineau date cu caracter personal, inclusiv date sensibile, la coșul de gunoi al unei unități administrativ teritoriale. Documentele conțineau date ale pacienților Medlife S.A. În cadrul investigației s-a constatat că operatorul nu a implementat măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de confidențialitate și securitate corespunzător riscului prezentat de prelucrare, ceea ce a condus la accesarea ori divulgarea ilicită a datelor cu caracter personal ale clienților proprii MEDLIFE S.A. (nume, prenume, CNP, serviciul medical de care a beneficiat, analiza medicală efectuată, suma achitată, cont bancar) și ale angajaților săi (salariu avans) în perioada iulie 2020 – august 2020.

Sursa: *https://www.dataprotection.ro/?page=Comunicat_Presa_24_05_2022*

Cazuistică internațională:

British Pregnancy Advisory Service (BPAS) este o organizație caritabilă din Marea Britanie care oferă consiliere și servicii conexe procedurilor de avort. În anul 2012, BPAS a fost victima unui atac cibernetic, care a dus la accesarea ilegală a peste 9.000 de fișiere care conțineau informații personale și medicale despre pacienți. Informațiile furate includeau numele, adresa, data de naștere, numărul de telefon și istoricul medical al pacienților, precum și informații despre avorturile pe care le-au avut sau intenționau să le facă. Autoritățile au stabilit că BPAS nu a luat măsurile adecvate pentru a proteja aceste informații și pentru a preveni un astfel de atac.

Ca urmare, BPAS a fost amendată cu 200.000 de lire sterline de către Information Commissioner's Office (I.C.O.) autoritatea de supraveghere a protecției datelor din Marea Britanie, în noiembrie 2014.

Sursa: *https://www.thirdsector.co.uk/british-pregnancy-advisory-service-fined-200000-hacker-accessed-information/communications/article/1284156*