4.3 PRINCIPIILE PROTECȚIEI DATELOR

- Cunoașterea întregului corpus de principii ale prelucrării datelor medicale
- Înțelegerea modalității de aplicare generală a acestor principii
- Prezentarea normelor juridice de referință

Modalitatea de realizare a secțiunii:

În partea teoretică a ghidului dorința a fost să se creeze un interes și o conștientizare că activitatea medicală se bazează pe standarde juridice și etice încorporate organic prin intermediul unui mecanism exterior esenței activității medicale: protecția datelor cu caracter personal.

În această parte a ghidului se impune aprofundarea, în sensul precizării stricte a principiilor în materia protecției datelor cu caracter personal, așa cum acestea figurează în legislația de protecție a datelor. Ca urmare, această parte va avea un caracter și mai accentuat juridic. Din acest motiv, pentru a fi cât mai firesc înțelese, principiile sunt însoțite în mod constant de exemple care nu sunt neapărat prezentate în limbaj juridic, dar sunt realizate după o formulă logică, comună inclusiv domeniului juridic.

Am considerat util să se facă trimitere strict la o legislație corespunzătoare, însă aceste referiri trebuie înțelese doar ca un instrument doveditor al principiilor expuse, util în special atunci când este confruntat cineva cu suportul legal al problematicilor de protecție a datelor medicale.

Referitor la legislația de protecție a datelor, ghidul în mod intenționat nu urmărește să dezvolte problematici extrem de specifice domeniului juridic, cum ar fi relația dintre normele internaționale, normele Uniunii Europene și legislația națională; principii de interpretare a normelor juridice; rolul precedentelor judiciare asupra înțelegerii principiilor etc. Am considerat că acest ghid are ca adresabilitate în special practicienii și profesioniștii din sistemul medical și din sănătate, astfel că o consultanță strictă de specialitate în domeniul protecției datelor trebuie obținută prin a apela la specialiști.

Scopul principal al ghidului este orientarea și încorporarea conștientă a standardului de protecție a datelor în activitatea medicală, astfel încât să fie obținute rezultate, precum: **îmbunătățirea cunoștințelor, abilităților și performanțelor în activitatea medicală**; îmbunătățirea și garantarea **securității și calității profesiei și activității medicale**; creșterea nivelului de **comunicare, de cooperare și de lucru în echipă**; menținerea **încrederii în activitatea medicală și în profesioniștii din sectorul medical**, atât din partea publicului larg cât și în special în relația dintre medic și pacient.

Din perspectiva protecției datelor personale, una dintre consecințele parcurgerii ghidului este ridicarea progresivă dar constantă a conformității cu Regulamentul General privind Protecția Datelor, deoarece acesta stabilește implicit obligația de instruire pentru operatorii de date (ex. unități medicale - spitale, clinici, cabinete medicale).

Principiile de prelucrare a datelor medicale

I. **Un prim mod de abordare a datelor medicale** este acela care ia în considerare **contactul direct** cu acestea și **maniera** în care trebuie ele **prelucrate**. De aceea, într-o activitate medicală, trebuie să identificăm persoanele implicate în colectarea datelor, organizarea lor, valorificarea lor prin toate modalitățile. Medicul rămâne principalul personaj care generează și fructifică aceste date, însă activitatea presupune intervenția multor altor persoane, precum asistenți medicali, personal administrativ etc. **Răspunderea pentru aceste date revine operatorului de date (spitalului, cabinetului medical sau oricărei alte forme juridice de organizare a activității), însă persoanele fizice care lucrează cu aceste date în mod direct și palpabil trebuie să cunoască bine regulile de urmat pentru prelucrarea datelor cu caracter medical**. Primul principiu a fost dezvoltat și în partea introductivă a ghidului, însă aici este reluat în contextul „arhitecturii" de ansamblu a principiilor de protecție a datelor.

Orice persoană care prelucrează date referitoare la sănătate trebuie să respecte următoarele **principii**:

DATELE TREBUIE SĂ FIE PRELUCRATE ÎNTR-UN MOD TRANSPARENT, LEGAL ȘI ECHITABIL

Respectarea acestui principiu va asigura medicului stabilirea unei relații de încredere cu pacientul, va asigura calitatea și securitatea datelor medicale și va conduce la rezultate medicale de calitate.

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. a), dar el este precizat în mod specific în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată**.
Astfel vorbim despre:

- **Articolul 30^8 al legii 95/2006** stabilește obligația generală de prelucrare a datelor în conformitate cu prevederile legale, obligație care aparține cabinetelor medicale ambulatorii ale medicilor de familie şi de alte specialități, centre de diagnostic și tratament, centre medicale, centre de sănătate, laboratoare, precum și prin alte unități sanitare publice și private, unităților sanitare publice şi private cu paturi.

- **Articolul 40 al Legii 95/2006** stabilește temeiul legal al unei situații specifice de prelucrare, precum aceea de păstrare a datelor privind sănătatea de către autoritățile de sănătate publică, cu scopul întocmirii de statistici și limitează utilizarea lor pentru alte scopuri, dacă nu există o dispoziție legală în acest sens, consimțământul persoanei vizate, protejarea unui interes vital sau a unui interes public major, ori necesitatea efectuării urmăririi penale.

- **Articolul 108 al Legii 95/2006** are în vedere stabilirea regulilor de înființare și organizare a spitalelor de urgență, context în care stabilește norma de organizare pe linia de colectare a datelor, precizând explicit că modalitățile de colectare se vor stabili cu respectarea prevederilor legale în vigoare privind protecția datelor cu caracter personal.

- **Articolul 138 al Legii 95/2006** impune obligații specifice furnizorilor de servicii medicale de specialitate în ceea ce privește utilizarea datelor colectate rezultate din activitatea proprie, raportările de date către autoritățile publice și arhivarea acestora, conform prevederilor legale.

- **Articolul 145 al Legii 95/2006** stabilește interdicția generală de prelevare de organe, ţesuturi şi celule de la potenţiali donatori minori în viaţă, cu excepţia cazurilor prevăzute de această lege, stabilind garanții specifice acestei situații, garanții situate la nivelul consimțământului minorilor.

- **Articolul 346^5 al Legii 95/2006** referitor la DES, stabilește regula că Prelucrarea datelor cu caracter personal în cadrul DES, ca parte componentă a Platformei informatice din asigurările de sănătate, se realizează cu respectarea prevederilor Regulamentului General privind Protecția Datelor.

- **Articolul 346^6 al Legii 95/2006** cuprinde reguli privind conținutul dosarului medical și condițiile de accesare a acestuia, în special privind echitatea procedurilor bazate pe consimțământul pacientului.

- **Articolele 346^7, 346^8, 346^9 ale Legii 95/2006** stabilesc o serie de reguli privind accesul la datele și informațiile din DES, cazuri de acces fără a fi necesar consimțământul persoanei vizate și unele concepte specifice DES. Toate acestea sunt condiționate de respectarea prevederilor RGPD.

- **Articolul 346^11 al Legii 95/2006** ne indică concret **obligația medicilor** de a respecta principiile de deontologie și etică medicală, cu respectarea legii și a normelor de protecție a datelor cu caracter personal, ori de câte ori utilizează DES al pacienților. Totodată, se impune obligația asigurării dreptului la informare și a tuturor drepturilor specifice pacienților.

- **Articolele 661 și 662 ale Legii 95/2006** stabilesc condițiile pentru exprimarea **consimțământului informat**, inclusiv situațiile de excepție și răspunderile aferente medicilor, asistenților medicali sau moașelor pentru nerespectarea prevederilor privind consimțământul informat.

- **Articolul 696 al Legii 95/2006** evidențiază un **caz distinct de prelucrare a datelor medicale**, motivat de **scopul analizelor și monitorizării serviciilor de sănătate** decontate din fondul de asigurări de sănătate. Instituția abilitată prin lege pentru colectarea datelor și prelucrarea lor în scopurile menționate este **INMSS**.

- **Articolul 910 al Legii 95/2006** stabilește **principalele obligații de informare a pacienților de către furnizorii de servicii medicale**, informații necesare pentru asigurarea consimțământului informat, asigurarea căilor de recuperare a unor prejudicii de către pacienți, să asigure nediscriminatoriu asistență medicală, inclusiv transfrontalieră și să respecte confidențialitatea datelor cu caracter personal în conformitate cu prevederile legale în materie.

- **Legea drepturilor pacientului nr. 46/2003** Contractul Cadru și Normele de aplicare ale COCA – pentru contractele realizate de furnizorii de servicii medicale – medicină de familie, ambulatoriu de specialitate, spitale, farmacii, îngrijiri la domiciliu și îngrijiri paliative.

Exemplu de bună practică în respectarea principiului legalității, echității și transparenței prelucrării datelor medicale de către un medic:

- Un medic solicită în mod explicit consimțământul pacienților înainte de a utiliza datele lor medicale într-un studiu științific. Medicul ar trebui să informeze pacienții despre **scopul studiului, modul în care vor fi utilizate datele lor personale, drepturile lor de acces, rectificare și ștergere a datelor** și să le ofere opțiunea de a se retrage din studiu în orice moment.

Exemplu din cazuistică

Autoritatea Națională de Supraveghere (A.N.S.) din România a finalizat în luna decembrie 2022 două investigații la un cabinet stomatologic și la un medic stomatolog (colaborator al cabinetului stomatologic) ambii operatori de date cu caracter personal.

În cadrul investigațiilor efectuate, s-a constatat că operatorii au divulgat informații medicale referitoare la tratamentul ortodontic al petiționarului Autorității (A.N.S.), constând într-un set de fotografii și radiografii care se puteau corela cu numele persoanei, prin publicarea unui articol pe un blog de specialitate. Aceste informații au fost publicate atât în scop științific, cât și în scop comercial.

A.N.S. a aplicat cabinetului stomatologic sancțiunea contravențională a amenzii în cuantum de 4.919,2 lei pentru încălcarea articolului 33 din RGPD și a aplicat medicului stomatolog colaborator sancțiunea contravențională a amenzii în cuantum de 4.919,2 lei pentru încălcarea dispozițiilor art. 6 alin. (1) lit. a) și ale art. 9 alin. (2) lit. a) din RGPD. Principala fundamentare a aplicării amenzii a fost că operatorul medic stomatolog colaborator a prelucrat, inclusiv prin utilizare și dezvăluire, datele personale privind starea de sănătate a persoanei vizate, în cadrul unui articol postat pe blogul personal, **fără să prezinte dovezi privind obținerea consimțământului expres al persoanei implicate și fără informarea sa prealabilă.**

Acest exemplu evidențiază încălcarea atât a principiului legalității cât și a echității prelucrării datelor medicale ale pacienților.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.10** cu privire la **gestionarea cererilor persoanelor vizate** (pacienți / aparținători) cu privire la propriile informații
- **Orientarea 3.8** cu privire **la protejarea datelor în afara cadrului profesional** de desfășurare a activității

DATELE TREBUIE COLECTATE ÎN SCOPURI DETERMINATE, EXPLICITE ȘI LEGITIME ȘI NU TREBUIE PRELUCRATE ULTERIOR ÎNTR-UN MOD INCOMPATIBIL CU ACESTE SCOPURI

PRELUCRAREA ULTERIOARĂ ÎN SCOPURI DE ARHIVARE ÎN INTERES PUBLIC, ÎN SCOPURI DE CERCETARE ȘTIINȚIFICĂ SAU ISTORICĂ ORI ÎN SCOPURI STATISTICE NU ESTE CONSIDERATĂ INCOMPATIBILĂ CU SCOPURILE INIȚIALE, DAR TREBUIE SĂ EXISTE GARANȚII PENTRU RESPECTAREA DREPTURILOR ȘI LIBERTĂȚILOR PERSOANELOR

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. b), dar și acesta este precizat în mod specific în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată.**

Unul dintre exemplele ilustrative este reglementat de articolul 346^12 al Legii 95/2006 și se referă la **refuzul expres al pacienților de a li se utiliza dosarul electronic de sănătate**, precum și la utilizarea datelor din DES în scopuri de arhivare în interes public, cercetare științifică și scopuri statistice. Potrivit acestui articol pacienții care în mod expres refuză să accepte utilizarea DES, datele acestora nu vor putea fi introduse în DES, iar cele deja introduse pot fi complet anonimizate dacă pacientul solicită acest lucru, ceea ce înseamnă că nu vor mai putea fi corelate electronic cu identitatea pacientului. Această situație, chiar reglementată, evidențiază că natura sensibilă a datelor medicale justifică necesitatea ca datele să fie anonimizate dacă au fost introduse în DES, deoarece altfel principiul legitimității scopurilor prelucrării datelor nu ar fi respectat, deoarece **acordarea îngrijirilor medicale nu poate fi condiționată de „acordul" pacientului de a i se utiliza datele din DES**.

Exemplu de bună practică

- O bună practică în colectarea datelor personale în activitatea medicală ar putea fi ***utilizarea unui sistem de management al pacienților*** într-un spital. În acest context, scopurile determinate, explicite și legitime ale colectării datelor personale ale pacienților ar putea include:
    - Îmbunătățirea calității îngrijirii medicale oferite pacienților
    - Monitorizarea și prevenirea potențialelor riscuri și incidente în domeniul sănătății
    - Ușurarea comunicării între personalul medical și pacienți
    - Managementul eficient al resurselor spitalicești

Astfel, datele personale colectate ar trebui să fie limitate la informațiile necesare pentru atingerea acestor scopuri, precum numele, adresa, numărul de telefon, data nașterii, istoricul medical și diagnosticul. Datele nu ar trebui să fie prelucrate în moduri care nu sunt compatibile cu aceste scopuri, cum ar fi comercializarea sau utilizarea acestora în cercetări care nu sunt legate de îmbunătățirea sănătății pacienților.

Cu toate acestea, măsurile de siguranță ar trebui să fie sporite, informarea pacienților trebuie să fie extrem de completă și transparentă, iar după atingerea acestui scop principal, acela al îngrijirilor medicale spre exemplu, informațiile ar trebui anonimizate în cel mai scurt timp.

Exemplu din cazuistică

În cauza denumită Lindqvist (C-101/01), Curtea de Justiție a Uniunii Europene (CJUE) a examinat problematica publicării pe internet de către o persoană a unor date personale despre colegii săi dintr-o asociație cu caracter religios, inclusiv informații despre starea lor de sănătate. Aceste informații au putut fi accesate prin intermediul unei pagini web, deși la momentul colectării acestora scopul era exclusiv în interesul funcționării acelei asociații, iar membrii asociației nici nu fuseseră informați nici nu li se ceruse consimțământul pentru publicarea respectivelor date. Practic, scopul publicării pe site-ul web nu mai era compatibil cu scopul inițial pentru care datele au fost colectate. Curtea a constatat că publicarea informațiilor a încălcat principiul ca datele personale să fie colectate și prelucrate numai în scopuri determinate, explicite și legitime, conform Directivei 95/46/CE privind protecția datelor personale, care a fost înlocuită ulterior de Regulamentul General privind Protecția Datelor (GDPR).

O altă situație de încălcare a principiului colectării datelor a fost supusă investigației Autorității Naționale de Supraveghere, care a aplicat o amendă de aproximativ 2000 Euro unui centru medical, în luna noiembrie 2021 deoarece a dezvăluit date ale unui fost pacient unui alt operator, fără a-l informa sau a-i cere consimțământul.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.5** cu privire la **posibilitatea de fotografiere, realizarea de capturi video și alte imagini folosite în serviciul medical**

PRELUCRAREA DATELOR AR TREBUI SĂ FIE NECESARĂ ȘI PROPORȚIONALĂ ÎN RAPORT CU SCOPUL LEGITIM URMĂRIT ȘI AR TREBUI SĂ FIE EFECTUATĂ NUMAI PE BAZA CONSIMȚĂMÂNTULUI PERSOANEI VIZATE SAU PE UN ALT TEMEI LEGITIM

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. c) coroborat cu articolul 9, dar acesta este precizat în mod specific și în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată**. Astfel, vorbim despre:

- **Articolul 30^9 al Legii 95/2006** reglementează relația dintre ipoteza telemedicinei și drepturile pacientului, impunând garanții de informare a acestuia asupra a serviciilor disponibile, calității actului medical în contextul mijloacelor tehnice utilizate pentru transmisia de date, necesitatea garantării consimțământului liber și informat al pacientului. Pentru mai multe detalii, a se vedea **Orientarea 3.9** cu privire la **oferirea de servicii de telemedicină**

- **Articolul 101 al Legii 95/2006** reglementează asigurarea asistenței medicale private de urgență, pe baza consimțământului beneficiarului, chiar și atunci când aceasta se acordă pe baza unui contract cu asigurătorul privat.

- **Articolele 144 - 154 ale Legii 95/2006** stabilesc garanții specifice privind donarea de organe, țesuturi și celule de origine animală, astfel încât să fie asigurat consimțământul informat și liber al donatorului, demonstrarea și asigurarea legalității întregii proceduri. Sunt menționate inclusiv condițiile de prelevare de la persoane decedate.

- **Articolul 230 al Legii 95/2006** reglementează relația dintre asigurați, pe de o parte și asigurători și furnizorii de servicii medicale pe de altă parte. Printre drepturile asiguraților se numără și dreptul de a li se garanta confidenţialitatea privind datele, în special în ceea ce priveşte diagnosticul şi tratamentul, precum și dreptul la informaţie în cazul tratamentelor medicale.

- **Articolele 346^1 și următoarele ale Legii 95/2006** reglementează dosarul electronic de sănătate al pacientului, stabilind că acesta conține date și informații clinice, biologice, diagnostice şi terapeutice, personalizate, acumulate pe tot parcursul vieții pacienților. Se stabilesc situațiile de prelucrare electronică a datelor, când nu este necesar consimțământul pacientului, cum este cazul etapei de constituire a acestuia declarându-se activitate de utilitate publică de interes național, precum și situațiile de utilizare a datelor, bazate pe consimțământul pacientului. Sunt stabilite în detaliu categoriile de date prelucrate, procedurile de prelucrare, răspunderea pentru securitatea și încărcarea datelor în DES.

- **Articolele 653 și următoarele ale Legii 95/2006** reglementează problematica răspunderii civile a personalului medical, a psihologilor şi a furnizorilor de servicii conexe actului medical acordate persoanelor diagnosticate cu tulburări din spectrul autist în cadrul programelor naționale de sănătate curative, în toate cazurile această răspundere angajându-se atunci când nu s-au respectat condițiile prevăzute de lege pentru un consimțământ informat, dacă nu ne găsim în situația unor excepții în care consimțământul trebuie acordat de reprezentanții legali ai pacientului.

- Potrivit **articolului 661 al Legii 95/2006** vârsta legală pentru exprimarea consimțământului informat este de 18 ani. Minorii își pot exprima consimțământul în absența părinților sau reprezentantului legal, în următoarele cazuri:
    - situaţii de urgenţă, când părinţii sau reprezentantul legal nu pot fi contactaţi, iar minorul are discernământul necesar pentru a înţelege situaţia medicală în care se află
    - situaţii medicale legate de diagnosticul şi/sau tratamentul problemelor sexuale şi reproductive, la solicitarea expresă a minorului în vârstă de peste 16 ani.

În vederea obţinerii acordului scris al pacientului / reprezentantului legal al acestuia, după caz, psihologul are obligaţia să prezinte pacientului / reprezentantului legal al acestuia informaţii la un nivel ştiinţific rezonabil pentru puterea de înţelegere a acestuia.

Informaţiile trebuie să conţină: metodele utilizate, riscuri, alternative, modul de desfăşurare, frecvenţa, modul în care se poate retrage consimţământul dacă se doreşte acest lucru, limitele confidenţialităţii, inclusiv date privind posibilitatea înregistrării audio-video.

Exprimarea acordului informat este condiţionată de existenţa capacităţii depline de exerciţiu a persoanei cu tulburări din spectrul autist. Modelul de formular pentru consimțământ este stabilit prin Ordin al Ministrul Sănătății, tocmai pentru a garanta în mod specific nivelul de obligativitate și natura sensibilă a datelor medicale.

Exemplu de bună practică privind respectarea principiului prelucrării datelor medicale pe baza consimțământului informat, liber și demonstrabil

Spitalul X implementează un sistem de management al informațiilor medicale pentru a îmbunătăți calitatea serviciilor medicale și a eficientiza procesele interne. Înainte de a prelucra datele medicale ale pacienților, spitalul obține consimțământul scris al pacienților sau al reprezentanților legali ai acestora, în care sunt incluse informații detaliate despre scopul prelucrării datelor, drepturile persoanelor vizate și modalitățile de exercitare a acestor drepturi.

Spitalul limitează accesul la datele medicale doar personalului autorizat și prelucrează datele numai în măsura în care este necesar pentru scopurile medicale stabilite. De asemenea, spitalul implementează măsuri de securitate adecvate pentru a proteja datele pacienților de accesul neautorizat, pierdere sau distrugere.

Cazuistică în domeniu

Un caz notabil în care prelucrarea datelor medicale a fost realizată într-un mod care nu respecta consimțământul pacientului și a fost investigat de Information Commissioner's Office (ICO) din UK. Acest caz implică Royal Free NHS Foundation Trust și DeepMind, o companie de AI deținută de Alphabet, corporația-mamă a Google.

În 2015, **Royal Free NHS Foundation Trust** a încheiat un parteneriat cu **DeepMind** pentru a dezvolta o aplicație numită Streams, care avea ca scop să îmbunătățească tratamentul pacienților cu insuficiență renală acută.

În procesul de a dezvolta această aplicație, Royal Free a oferit DeepMind acces la datele medicale a aproximativ 1,6 milioane de pacienți fără a obține consimțământul explicit al acestora.

În 2017, ICO a finalizat o investigație asupra acestei colaborări și a concluzionat că transferul de date între Royal Free și DeepMind nu respecta legea privind protecția datelor din Marea Britanie. ICO a criticat Royal Free pentru lipsa de transparență și pentru că nu a informat corespunzător pacienții despre cum vor fi utilizate datele lor. Royal Free a fost obligat să efectueze modificări semnificative în ceea ce privește prelucrarea datelor și să își îmbunătățească practicile de protecție a datelor.

În urma acestui caz, DeepMind și Royal Free au luat măsuri pentru a se conforma recomandărilor ICO și a asigura protecția datelor pacienților. Acest caz a servit drept exemplu pentru organizațiile din domeniul sănătății și al tehnologiei în ceea ce privește importanța respectării legilor privind protecția datelor și obținerea consimțământului pacienților înainte de a utiliza datele lor în proiecte similare.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.13** privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- **Orientarea 3.16** privind **obținerea și gestionarea consimțământului persoanei vizate**

DATELE CU CARACTER PERSONAL AR TREBUI, ÎN PRINCIPIU ȘI ÎN MĂSURA ÎN CARE ESTE POSIBIL, SĂ FIE COLECTATE DE LA PERSOANA VIZATĂ

ÎN CAZUL ÎN CARE PERSOANA VIZATĂ NU ESTE ÎN MĂSURĂ SĂ FURNIZEZE DATELE ȘI ACESTE DATE SUNT NECESARE ÎN SCOPUL PRELUCRĂRII, ACESTEA POT FI COLECTATE DIN ALTE SURSE, DAR CU RESPECTAREA TUTUROR PRINCIPIILOR DE PROTECȚIE A DATELOR

Aceasta este o regulă care îmbunătățește managementul relației cu beneficiarul serviciilor de îngrijire medicală, dar reprezintă și o garanție a exactității datelor, reducând riscul apariției unor date inexacte și a erorilor medicale. Principiul este asumat la nivel european prin Recomandarea Comitetului de Miniștri a Consiliului Europei privind prelucrarea datelor de sănătate.

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. a) coroborat cu articolul 6 alin. 4, dar acesta este precizat în mod specific și în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată.**

- Spre exemplu, potrivit **articolului 346^1 al Legii 95/2006**, Dosarul electronic de sănătate al pacientului se constituie cu ocazia transmiterii primului document medical al acestuia în DES de către medicii care își desfășoară activitatea în unitățile prevăzute la art. 30 alin. (1), *fără consimțământul pacientului*, realizarea și implementarea acestuia fiind de *utilitate publică de interes naţional*.

- Potrivit **articolului 346^2** utilizarea dosarului electronic de sănătate are drept *scop prioritar creşterea calităţii şi eficienţei actului medical* prin accesul imediat la date şi informaţii medicale, precum şi furnizarea de date şi informaţii statistice necesare politicilor de sănătate, cu implicarea pacientului ca factor activ al protejării şi promovării propriei sănătăţi, prin completarea informaţiilor privind antecedentele personalei fiziologice şi patologicei regim de viaţă, precum şi prin consultarea directă a datelor medicale proprii din dosarul său de sănătate.

Exemplu de bună practică

Într-un centru de urgențe medicale, un pacient este adus în stare gravă și nu poate comunica sau furniza informații despre starea sa medicală. În acest caz, medicul de gardă decide să obțină informațiile medicale necesare ale pacientului de la medicul de familie al acestuia, pentru a asigura un tratament adecvat și în conformitate cu principiile de protecție a datelor.

Centrul de urgențe medicale are politici și proceduri clare privind accesarea datelor medicale ale pacienților în astfel de situații și garantează că acestea sunt respectate. De asemenea, centrul păstrează un registru al accesărilor și prelucrărilor efectuate în astfel de cazuri, pentru a putea fi verificate ulterior și a se asigura că datele personale ale pacienților sunt utilizate numai în scopul tratamentului lor medical.

Cazuistică în domeniu

Curtea de Justiție a Uniunii Europene a judecat în cauza F-46/09 (V & EDPS V. EUROPEAN PARLIAMENT) o cerere de anulare a unei decizii a Parlamentului European prin care se retrage o ofertă de angajare din 2008 făcută reclamantului pe motiv că nu este apt să fie angajat.

Serviciul medical al Comisiei stabilise că reclamanta nu era aptă; aceasta a formulat recurs, iar Comisia a confirmat concluzia. Aceasta a depus o plângere în temeiul articolului 90, pe care Comisia a respins-o, apoi o acțiune în justiție împotriva acestei decizii, pe care Tribunalul de Primă Instanță a respins-o.

În 2008, i s-a propus un post de agent contractual la Parlament. Parlamentul a solicitat și a primit o copie a dosarului său medical de la serviciul medical al Comisiei și, ulterior, și-a retras oferta pe motiv că nu era aptă să lucreze în niciuna dintre instituțiile UE. Reclamanta a depus o plângere împotriva acestei decizii, pe care Parlamentul a respins-o. În acțiunea în fața instanței, reclamanta a susținut că dosarul său medical colectat de Comisie ar fi trebuit să fie utilizat numai în ceea ce privește recrutarea sa de către Comisie. În plus, consilierul medical al Parlamentului ar fi trebuit să o examineze doar pe reclamantă și nu să se intereseze de istoricul său medical anterior.

În memoriul AEPD se afirmă că transferul a încălcat Regulamentul 45/2001. În primul rând, datele nu fac parte din dosarul medical al reclamantei în calitate de fost agent temporar și fost agent contractual al Comisiei. Manualul de procedură al serviciului medical al Comisiei nu indică scopurile pentru care datele medicale colectate în cadrul unei proceduri de recrutare sunt păstrate în arhivă pentru mai mult de 6 luni, nici condițiile în care acestea sunt accesibile.

În avizele adresate Parlamentului și Comisiei a recomandat ca, în cazul candidaților considerați inapți pentru angajare, datele medicale colectate în timpul procedurii de recrutare să fie păstrate doar pentru o perioadă limitată, care să corespundă perioadei în care este posibilă contestarea datelor sau a deciziei luate pe baza acestora. În plus, transferul este reglementat de articolul 7, fără a aduce atingere articolelor 4, 5, 6 și 10. Astfel, respectarea articolului 7 nu face ca transferul și utilizarea finală a datelor să fie legale în temeiul regulamentului în ansamblul său.

În temeiul articolului 10 alineatul (1), prelucrarea unor categorii speciale de date este interzisă, iar protecția acestor date are, pentru CEDO, o importanță fundamentală pentru exercitarea dreptului la viață privată, garantat de articolul 8 din Convenție. Reclamanta nu și-a dat consimțământul pentru transfer, în conformitate cu excepția prevăzută la articolul 10 alineatul (2).

În plus, Parlamentul nu a demonstrat că transferul era cu adevărat necesar pentru respectarea statutului, în sensul articolului 10 alineatul (2) litera (b). Ar fi fost posibil să se obțină informațiile într-un mod mai puțin intruziv. Odată primite de către Parlament, datele nu mai erau utilizate în scopul pentru care au fost colectate. Transferul și utilizarea datelor au încălcat articolul 4 alineatul (1) literele (b) și (e).

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.13** privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- **Orientarea 3.16** privind **obținerea și gestionarea consimțământului persoanei vizate**

DATELE PRELUCRATE TREBUIE SĂ FIE ADECVATE, RELEVANTE ȘI LIMITATE LA CEEA CE ESTE NECESAR ÎN RAPORT CU SCOPURILE ÎN CARE SUNT PRELUCRATE

ELE TREBUIE SĂ FIE EXACTE ȘI, ÎN CAZUL ÎN CARE ESTE NECESAR, SĂ FIE ACTUALIZATE

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. c) și d), dar acesta este precizat în mod specific și în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată**.

- **Articolele 280 și 281 ale Legii 95/2006** stabilește printre atribuțiile CNAS actualizarea Registrului unic de evidență a asiguraților, ceea ce dă expresie garantării principiului exactității datelor cuprinse în acest registru. Această atribuție se realizează pe cale ierarhică, pornind de la competențele teritoriale ale caselor de asigurări de a actualiza datele și a le transmite către CNAS.

- Potrivit **articolului 322 al Legii 95/2006** stabilirea calității de asigurat de către CNAS se face pe baza unor date puse la dispoziție de autoritățile publice pe baza unui protocol. Același protocol stabilește și termenele la care datele sunt actualizate în Platforma informatică din asigurările de sănătate. Chiar dacă același articol stabilește că responsabilitatea pentru corectitudinea datelor revine autorităților publice care le transmit, realitatea este că în temeiul articolului 5 alin. 2 din RGPD răspunderea aparține și CNAS sau caselor de asigurări de sănătate.

- O situație asemănătoare este prevăzută de **articolul 414 al Legii 95/2006**, acesta stabilind că printre atribuțiile CMR se numără și aceea de a actualiza permanent Registrul unic al medicilor.

- Totodată, **articolul 512^1** CMR are atribuția actualizării Registrului unic al medicilor stomatologi din România, informațiile cuprinse în acest titlu fiind colectate, verificate, introduse și actualizate de colegiile teritoriale. Faptul că legea stabilește responsabilitatea pentru realizarea acestor operaţiuni privind membrii înscrişi în colegiul teritorial aparține colegiilor teritoriale, din perspectiva responsabilității față de standardul de protecție a datelor încorporat de RGPD, responsabilitatea revine și CMR.

Exemplu de bună practică în actualizarea datelor medicale

O clinică medicală privată implementează un sistem de gestionare electronică a fișelor medicale ale pacienților. Acest sistem include un mecanism automat de revizuire și actualizare a informațiilor medicale ale pacienților. De exemplu, atunci când un pacient își efectuează analizele de sânge în laborator, rezultatele sunt transmise direct în sistemul informatic al clinicii și sunt adăugate automat la fișa medicală electronică a pacientului.

Clinica are politici și proceduri clare pentru personalul medical, care detaliază pașii necesari pentru a actualiza informațiile medicale ale pacienților. Aceste politici includ instrucțiuni cu privire la revizuirea periodică a informațiilor, verificarea acurateței și corectarea oricăror erori. În plus, clinica instruiește în mod regulat personalul medical în ceea ce privește aceste proceduri, pentru a se asigura că datele medicale ale pacienților sunt actualizate și gestionate corespunzător.

Cazuistică în domeniu

Cauza **P.T. împotriva Republicii Moldova** privește încălcarea regulii confidențialității datelor prin prelucrarea lor disproporționată. Acest caz se referea la dezvăluirea statutului HIV pozitiv al solicitantului într-un certificat care îl scutește de serviciul militar. Reclamantul s-a plâns că a fost nevoit să prezinte certificatul atunci când și-a reînnoit actele de identitate în 2011 și în alte situații, cum ar fi atunci când a solicitat un nou loc de muncă. Curtea a considerat că a avut loc o încălcare a articolului 8 (dreptul la respectarea vieții private) din Convenție, constatând că dezvăluirea faptului că este seropozitiv în armata militară a încălcat dreptul la viață privată al reclamantului. Curtea a remarcat în special că guvernul moldovean nu a specificat care "scop legitim" al articolul 8 din Convenție fusese urmărit prin dezvăluirea bolii reclamantului. În plus, nu au explicat de ce a fost necesar să includă informații sensibile despre reclamant într-un certificat care putea fi solicitat într-o varietate de situații în care starea sa medicală nu era aparent relevantă. În cazul reclamantului, Curtea a considerat că o astfel de ingerință gravă în drepturile sale a fost disproporționată.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.13** privitoare la **utilizarea datelor cu caracter personal în scopuri secundare decât cele în care au fost colectate inițial**
- **Orientarea 3.16** privind **obținerea și gestionarea consimțământului persoanei vizate**

MĂSURILE DE SECURITATE TREBUIE SĂ FIE ADECVATE, LUÂND ÎN CONSIDERARE CELE MAI RECENTE EVOLUȚII TEHNOLOGICE, NATURA SENSIBILĂ A DATELOR REFERITOARE LA SĂNĂTATE ȘI EVALUAREA RISCURILOR POTENȚIALE

ELE TREBUIE SĂ FIE STABILITE PENTRU A PREVENI RISCURI PRECUM ACCESUL ACCIDENTAL SAU NEAUTORIZAT LA DATELE CU CARACTER PERSONAL, DISTRUGEREA, PIERDEREA, UTILIZAREA, INDISPONIBILITATEA, INACCESIBILITATEA, MODIFICAREA SAU DIVULGAREA

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. f), dar acesta este precizat în mod specific și în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată**.

- **Articolul 30 al Legii 95/2006** referitor la asistența medicală, stabilește în mod specific pentru cabinete medicale ambulatorii ale medicilor de familie şi de alte specialităţi, centrele de diagnostic şi tratament, centrele medicale, centrele de sănătate, laboratoare, precum şi pentru alte unităţi sanitare publice şi private **obligația asigurării condiţiilor de securitate şi confidenţialitate** în procesul de transmitere a datelor medicale care urmează a fi introduse în dosarul electronic de sănătate a pacientului. Potrivit articolului 30^8 această obligație este pe tot parcursul procedurilor de colectare, prelucrare, utilizare şi stocare a datelor personale.

- Potrivit **articolului 346^4 al Legii 95/2006**, sistemul DES poate face obiectul *interoperabilităţii* cu registrele naționale de sănătate, *în condiţiile legii.*

- Potrivit **articolului 346^5 al Legii 95/2006**, în ceea ce privește prelucrarea datelor în sistemul DES, CNAS are obligația de a adopta *măsuri tehnice şi organizatorice adecvate* în vederea asigurării unui nivel corespunzător de securitate şi confidenţialitate a datelor, în acord cu prevederile art. 32 din Regulamentul general privind protecţia datelor.

- Importanța asigurării securității sistemului DES este reflectată prin aceea că, potrivit **articolului 346^6 al Legii 95/2006**, datele, informaţiile şi procedurile operaţionale necesare utilizării şi funcţionării DES se aprobă prin ordin al ministrului sănătăţii şi al preşedintelui CNAS, cu avizul ministerelor şi instituţiilor din sistemul naţional de apărare, ordine publică şi siguranţă naţională, respectiv Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Ministerul Justiţiei, Serviciul Român de Informaţii, Serviciul de Telecomunicaţii Speciale, Serviciul de Informaţii Externe, Serviciul de Protecţie şi Pază, în conformitate cu prevederile prezentei legi.

- La **articolul 346^7 al Legii 95/2006** sunt detaliate următoarele măsuri de securitate privind accesul pacienților sau al reprezentanților legali ai acestora la datele şi informaţiile din DES: stabilirea unei matrici de securitate şi a parolei de acces; exclusiv prin intermediul cardului naţional de asigurări sociale de sănătate cu codul PIN asociat acestuia şi a parolei de acces; eliberarea matricei de securitate se face, pe baza solicitării pacienților, de către medicii care deţin un certificat calificat eliberat în condiţiile prevăzute de lege; parola de acces este personalizată de fiecare pacient, este strict confidenţială, fiind un element de securitate cunoscut numai de pacient şi se utilizează în cadrul DES atât pentru cardul naţional de asigurări de sănătate, cât şi pentru matricea de securitate.

- Articolul **933 al Legii 95/2006** cuprinde referințe specifice asigurării securității dispozitivelor medicale și prelucării datelor în conformitate cu RGPD. Astfel, acest articol stabilește pentru utilizatorii dispozitivelor medicale următoarele obligații: de a utiliza dispozitivele medicale numai în scopul pentru care au fost realizate; de a se asigura că dispozitivele medicale sunt utilizate numai în perioada de valabilitate a acestora, când este cazul, şi că nu prezintă abateri de la performanţele funcţionale şi de la cerinţele de securitate aplicabile.

Exemplu de bună practică privind măsurile de securitate adecvate pentru protecția datelor medicale:

Un spital implementează un sistem de management electronic al fișelor medicale ale pacienților și pune în aplicare următoarele măsuri de securitate pentru a proteja datele cu caracter personal și pentru a preveni accesul accidental sau neautorizat, distrugerea, pierderea, utilizarea, indisponibilitatea, inaccesibilitatea, modificarea sau divulgarea:

- **Criptare**: Datele medicale ale pacienților sunt criptate în repaus și în tranzit, utilizând tehnologii de criptare moderne și puternice. Acest lucru asigură că informațiile rămân confidențiale și inaccesibile pentru persoanele neautorizate.
- **Controlul accesului**: Spitalul implementează o politică strictă de control al accesului, care prevede autentificarea cu doi factori pentru a accesa fișele medicale ale pacienților. Personalul medical are acces doar la informațiile necesare îndeplinirii responsabilităților lor profesionale și în conformitate cu principiul accesului minim.
- **Audit și monitorizare**: Sistemul de management al fișelor medicale include funcționalități de audit și monitorizare care înregistrează toate accesările și modificările fișelor medicale. Acest lucru permite identificarea rapidă a oricăror incidente de securitate și a oricăror încălcări ale politicilor de protecție a datelor.
- **Copii de rezervă și planuri de recuperare**: Spitalul efectuează copii de rezervă regulate ale datelor medicale ale pacienților și păstrează aceste copii într-o locație sigură și separată. Spitalul are, de asemenea, un plan de recuperare în caz de dezastre care asigură restaurarea rapidă și sigură a datelor în cazul pierderii sau distrugerii acestora.
- **Pregătirea personalului și actualizarea politicilor**: Spitalul asigură instruirea continuă a personalului medical în ceea ce privește politicile și procedurile de protecție a datelor și de securitate informatică. Aceste politici și proceduri sunt revizuite și actualizate periodic pentru a ține pasul cu evoluțiile tehnologice și pentru a aborda riscurile emergente.
- **Evaluarea riscurilor și testarea de penetrare**: Spitalul efectuează evaluări periodice ale riscurilor în ceea ce privește securitatea datelor medicale și utilizează teste de penetrare realizate de terți independenți pentru a identifica și remedia vulnerabilitățile în sistemul său de management al fișelor medicale.

Prin punerea în aplicare a acestor măsuri, spitalul se asigură că datele medicale ale pacienților sunt protejate în mod adecvat, în conformitate cu principiul menționat.

Cazuistică în domeniu

Speța 1: Incidentul Anthem, Statele Unite ale Americii (2015)

În 2015, Anthem Inc., una dintre cele mai mari companii de asigurări de sănătate din Statele Unite, a suferit o breșă masivă de securitate a datelor, rezultând în expunerea datelor personale și medicale ale aproximativ 78,8 milioane de persoane. Informațiile furate au inclus nume, date de naștere, adrese de e-mail, adrese de domiciliu, numere de asigurare socială, precum și detalii de sănătate.

Această breșă de securitate a reprezentat o încălcare a principiului legalității, transparenței și echității în prelucrarea datelor medicale, deoarece Anthem nu a reușit să protejeze în mod corespunzător informațiile personale și medicale ale pacienților săi, punând în pericol dreptul lor la confidențialitate și protecția datelor.

Ca urmare a incidentului, Anthem a fost investigat de autoritățile federale și statale, precum și de Departamentul de Sănătate și Servicii Umane al SUA (HHS). În 2018, Anthem a ajuns la o înțelegere cu HHS, acceptând să plătească o amendă de 16 milioane de dolari și să adopte un program de conformitate corectivă pentru a îmbunătăți securitatea datelor și a preveni astfel de incidente în viitor.

De asemenea, Anthem a ajuns la o înțelegere într-o acțiune colectivă inițiată de persoanele afectate de breșa de securitate, acceptând să plătească 115 milioane de dolari pentru a acoperi costurile legate de monitorizarea creditului și de protecția împotriva furtului de identitate pentru persoanele afectate.

Această speță reprezintă un exemplu concret de jurisprudență în care s-a constatat încălcarea principiului legalității, transparenței și echității și a securității în prelucrarea datelor medicale.

Speța 2: În 2017, în Statele Unite, firma **Medical Informatics Engineering** (MIE) și afiliata sa **NoMoreClipboard** (NMC), au fost implicate într-un caz de încălcare a datelor medicale.

În acest caz, informații personale și de sănătate ale a aproximativ 3,5 milioane de pacienți au fost expuse în urma unui atac cibernetic. Încălcarea a implicat date sensibile, precum nume, adrese, numere de securitate socială și informații medicale.

În urma investigațiilor, s-a constatat că MIE și NMC nu au implementat măsuri de securitate adecvate pentru a proteja datele pacienților și nu au respectat principiile de protecție a datelor personale.

În ianuarie 2019, MIE a acceptat să plătească o amendă de 100.000 de dolari pentru încălcarea legii federale privind protecția datelor medicale (HIPAA). De asemenea, în 2020, companiile au ajuns la un acord într-un proces colectiv și s-au angajat să plătească 900.000 de dolari pentru a încheia litigiile.

Acest caz a devenit un exemplu renumit privind încălcarea principiilor de protecție a datelor medicale și a subliniat importanța aplicării unor măsuri de securitate adecvate pentru a proteja informațiile sensibile ale pacienților.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.3** privind **regulile de acces la bazele de date electronice**

TREBUIE RESPECTATE DREPTURILE PERSOANEI ALE CĂREI DATE SUNT PRELUCRATE, ÎN SPECIAL DREPTUL DE ACCES LA DATE ȘI DREPTUL LA INFORMARE, RECTIFICARE, OPOZIȚIE ȘI ȘTERGERE

Texte legale aplicabile: RGPD impune respectarea și aplicabilitatea acestui principiu la articolul 5 alin. 1 lit. f), dar acesta este precizat în mod specific și în numeroase secvențe și ipoteze avute în vedere de legislația națională, în special de **Legea 95/2006 privind reforma în domeniul sănătății, republicată**.

- **Articolul 30^9 al Legii 95/2006** stabilește obligația unităților din sistemul de sănătate de a respecta drepturile pacienților, în special dreptul la informare, de a-şi exprima consimţământul în mod liber şi informat, dreptul la confidențialitate, garantarea securității sistemelor.

- În plus, drepturile pacienților sunt reglementate distinct de **Legea drepturilor pacientului nr. 46/2003**, cu modificările şi completările ulterioare.

- În mod detaliat **Legea 95/2006, la articolul 89**, enumeră categoriile de obligaţii care revin personalului şi cabinetelor de medicină de familie, o categorie distinctă fiind aceea a obligaţiilor faţă de pacienţi - prin îndeplinirea prevederilor specifice din actele normative care reglementează obligaţiile de etică şi deontologie profesională, precum şi din legislaţia privind drepturile pacientului, obligaţiile faţă de sistemul asigurărilor sociale de sănătate.

- Potrivit **articolului 146 al Legii 95/2006** în cazul prelevării de organe, ţesuturi sau celule, drepturile pacienților sunt configurate distinct, demonstrarea respectării acestora fiind obligație concretizată prin întocmirea unui formular specific aprobat prin ordin al ministrului sănătăţii.

- În mod distinct, **la articolul 165**, sunt avute în vedere drepturile pacienților în contextul desfăşurării activităţilor de învăţământ medico-farmaceutic, postliceal, universitar şi postuniversitar, precum şi al activităţilor de cercetare ştiinţifică medicală.

- Printre drepturile pe care le au asiguraţii, **articolul 230** enumeră dreptul la confidențialitate privind datele, în special în ceea ce priveşte diagnosticul şi tratamentul; dreptul la informaţie în cazul tratamentelor medicale.
- **Articolul 234** stabilește dreptul fiecărui asigurat de a fi informat cel puţin o dată pe an, prin casele de asigurări, asupra serviciilor de care beneficiază, precum şi asupra drepturilor şi obligaţiilor sale.
- **Articolul 421 al Legii 95/2006** stabilește obligaţiile membrilor CMR, ce decurg din calitatea lor specială de medici, printre care figurează și aceea de a respecta drepturile pacienților.

Exemplu de bună practică în prelucrarea datelor medicale, respectând drepturile persoanei ale cărei date sunt prelucrate:

O policlinică implementează un portal online securizat pentru pacienți, care le permite acestora să își gestioneze propriile date medicale și să își exercite drepturile în conformitate cu principiile protecției datelor. Următoarele **măsuri** sunt luate pentru a asigura **respectarea drepturilor pacienților:**

- **Accesul la date**: Pacienții se pot autentifica în portalul online securizat, utilizând un sistem de autentificare cu doi factori, pentru a accesa și vizualiza propriile lor fișe medicale.
- **Dreptul la informare**: La prima vizită a unui pacient în clinică, acesta primește un document informativ care explică în detaliu modul în care datele sale medicale vor fi prelucrate, scopul prelucrării, drepturile pe care le are și cum să le exercite.
- **Rectificarea datelor**: Pacienții pot solicita rectificarea oricăror date incorecte sau incomplete prin portalul online sau prin contactarea directă a clinicii. Personalul clinic este instruit să se asigure că astfel de solicitări sunt tratate în mod corespunzător și în timp util.
- **Opoziție**: Pacienții au dreptul să se opună prelucrării datelor lor medicale în anumite circumstanțe, cum ar fi atunci când datele sunt utilizate în scopuri de marketing. Policlinica respectă aceste solicitări și își actualizează politica de confidențialitate pentru a reflecta dreptul pacienților de a se opune.
- **Ștergerea datelor**: Pacienții pot solicita ștergerea datelor lor medicale în anumite situații, cum ar fi atunci când nu mai este necesară păstrarea datelor în scopul pentru care au fost colectate. Clinica se asigură că astfel de solicitări sunt tratate în conformitate cu legislația aplicabilă și într-un mod transparent.

Cazuistică în domeniu

Cauza Avilkina și alții împotriva Rusiei

Reclamanții făceau parte dintr-o organizație religioasă, Centrul administrativ al organizației Martorilor lui Iehova din Rusia. Aceștia au reclamat în special dezvăluirea dosarelor lor medicale către organele de urmărire penală din Rusia, în urma refuzului lor de a li se face transfuzii de sânge în timpul internării lor în spitale publice. În legătură cu deschiderea unei anchete privind legalitatea activităților organizației reclamante, autoritățile de urmărire penală au dat instrucțiuni tuturor spitalelor din Sankt Petersburg să raporteze refuzurile de transfuzii de sânge de către Martorii lui Iehova.

De asemenea, Curtea Europeană a Drepturilor Omului a considerat că a existat o încălcare a articolului 8 (dreptul la respectarea vieții private și de familie) din Convenție în ceea ce privește ceilalți doi reclamanți. Aceasta a constatat, în special, că nu a existat o nevoie socială urgentă de dezvăluire de informații medicale confidențiale despre aceștia. În plus, mijloacele utilizate de către procuror în desfășurarea anchetei, care implică divulgarea de informații confidențiale fără niciun avertisment prealabil sau posibilitatea de a obiecta, nu trebuiau să fie atât de opresive pentru reclamanți.

Prin urmare, autoritățile nu au făcut niciun efort pentru a găsi un echilibru echitabil între, pe de o parte, dreptul reclamanților la respectarea vieții lor private și, pe de altă parte, obiectivul procurorului de a proteja sănătatea publică.

Notă! Acest caz evidențiază aspecte practice și etice extrem de importante, deoarece se poate observa că nici măcar atunci când o solicitare de date medicale este efectuată de un magistrat, transmiterea acestora nu trebuie făcută înainte ca deținătorul să evalueze **necesitatea** transmiterii unor asemenea date, **legalitatea** solicitării, **proporționalitatea** cu obiectivul urmărit de acel magistrat. Ca urmare, **orice medic poate dintr-o perspectivă etică și, mai mult decât atât, bazându-se direct pe principiile R.G.P.D., să refuze orice solicitare de date medicale, indiferent de cine este formulată sau că ar exista un temei legal al acelei solicitări, dacă apreciază că nu este îndeplinit unul dintre criteriile** enunțate mai sus.

Cauza Vilnes și Alții împotriva Norvegiei
Aceasta privește unele reclamații ale scafandrilor că sunt handicapați ca urmare a scufundărilor în Marea Nordului realizate pentru companiile petroliere în perioada de pionierat a explorării petrolului (din 1965 până în 1990). Toți reclamanții s-au plâns de faptul că Norvegia nu a luat măsuri adecvate pentru a proteja sănătatea și viața scafandrilor de mare adâncime atunci când lucrau în Marea Nordului și, în ceea ce privește trei dintre reclamanți, în instalațiile de testare. De asemenea, toți aceștia au susținut că statul nu a reușit să le furnizeze informații adecvate cu privire la riscurile pe care le implică atât scufundările la mare adâncime, cât și cele de testare.

Curtea a considerat că a avut loc o încălcare a articolului 8 (dreptul la respectarea vieții private și a dreptului la viață privată) din Convenție, din cauza faptului că *autoritățile norvegiene nu s-au asigurat ca reclamanții să primească informațiile esențiale care să le permită să evalueze riscurile la sănătatea și viața lor* care rezultă din utilizarea tabelelor de decompresie rapidă. Această cauză completează jurisprudența Curții cu privire la accesul la informații în temeiul articolelor 2 și 8 din Convenție, în special în măsura în care stabilește o *obligație pentru autorități* de *a se asigura că angajații primesc informații esențiale care să le permită să evalueze riscurile profesionale pentru sănătatea și securitatea lor.*

Cauza K.H. și Alții împotriva Slovaciei
Curtea europeană a analizat problematica accesului pacienților la datele lor cu caracter medical, colectate și înregistrate de spitalul de tratament. Reclamantele, opt femei de origine romă, nu au mai putut concepe după ce au fost tratate la secțiile de ginecologie din două spitale diferite și au suspectat că aceasta era din cauză că fuseseră sterilizate în timpul șederii lor în acele spitale. Acestea s-au plâns că nu au putut obține fotocopii ale fișelor lor medicale. Curtea europeană a drepturilor omului a considerat că a avut loc o încălcare a articolului 8 (dreptul la viață privată și familială) din Convenție, întrucât reclamanților nu li s-a permis să facă *fotocopii ale fișelor lor medicale*.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.10** cu privire la **gestionarea cererilor persoanelor vizate cu privire la propriile informații**
- **Orientarea 3.11** cu privire la **gestionarea reclamațiilor angajaților respectiv pacienților**

II. Principiile privind protecția datelor cu caracter personal (enumerate anterior) ar trebui **să fie luate în considerare implicit** (privacy by default) și **încorporate încă de la proiectarea sistemelor informatice** care prelucrează date referitoare la sănătate (privacy by design). Conformitatea cu aceste principii ar trebui să fie revizuită periodic pe tot parcursul ciclului de viață al prelucrării. Operatorul ar trebui să efectueze, înainte de a începe prelucrarea și la intervale regulate, o **evaluare a impactului potențial al prelucrării** preconizate a datelor în ceea ce privește protecția datelor și respectarea drepturilor omului, inclusiv a măsurilor care vizează reducerea riscului.

Exemplu de bună practică privind respectarea principiilor "privacy by default" și "privacy by design":

O companie care dezvoltă software pentru spitale și alte instituții medicale, să numim această companie "MediTech", a creat un sistem de management electronic al fișelor medicale (EMR) care încorporează principiile de protecție a datelor personale încă de la proiectare. Acest sistem include următoarele caracteristici și măsuri de securitate:

- **Criptarea implicită**: Sistemul utilizează criptarea atât pentru datele aflate în repaus, cât și pentru datele în tranzit, asigurând confidențialitatea și integritatea datelor medicale.
- **Controlul accesului**: Accesul la datele medicale este strict limitat la personalul autorizat, în conformitate cu principiul accesului minim. Acest lucru este realizat prin implementarea unui sistem de autentificare cu doi factori și a unei politici de gestionare a permisiunilor bazată pe **roluri**.
- **Protecție încorporată**: Sistemul include măsuri de protecție încorporate, cum ar fi protecția împotriva atacurilor de tip SQL injection și protecția împotriva accesului neautorizat prin intermediul API-urilor.
- **Evaluarea impactului asupra protecției datelor**: MediTech efectuează evaluări regulate ale impactului asupra protecției datelor pentru a identifica riscurile potențiale și pentru a implementa măsuri de reducere a riscului.
- **Revizuirea periodică a conformității**: MediTech revizuiește periodic conformitatea cu principiile privind protecția datelor și efectuează actualizări ale sistemului EMR pentru a se asigura că rămâne în conformitate cu legislația și reglementările aplicabile.
- **Formarea și informarea utilizatorilor**: MediTech oferă instruire și suport pentru personalul medical care utilizează sistemul EMR, subliniind importanța protecției datelor personale și explicând modul în care sistemul asigură respectarea acestor principii.

Prin implementarea acestor măsuri și caracteristici în sistemul său de management electronic al fișelor medicale, MediTech asigură respectarea principiilor "privacy by default" și "privacy by design" și protejează datele medicale ale pacienților în conformitate cu legislația și reglementările privind protecția datelor.

Cazuistică în domeniu

Cazul Municipiul Bergen, Norvegia (2019)

La 19 martie, Autoritatea norvegiană pentru protecția datelor a aplicat o amendă administrativă de 1,6 milioane de coroane norvegiene, echivalentul a 170.000 de euro, municipalității din Bergen.

Incidentul se referă la fișierele informatice din sistemul informatic al municipalității, care conțineau datele personale a peste 35 000 de elevi și angajați ai școlilor primare ale municipalității. Din cauza unor măsuri de securitate insuficiente, aceste fișiere erau neprotejate și accesibile în mod deschis oricărui utilizator al sistemului, indiferent de tipul de autorizație. Acest lucru a permis utilizatorilor neautorizați să acceseze diversele sisteme informatice și datele personale ale școlii. Faptul că majoritatea persoanelor afectate erau copii și că municipalitatea a fost avertizată de mai multe ori (atât de către autoritate, cât și de către un denunțător intern) au fost considerate factori agravanți. Municipalitatea nu a făcut apel la decizie.

Autoritatea de supraveghere a datelor a constatat că municipiul Bergen nu a respectat principiile "privacy by design" și "privacy by default", întrucât nu a implementat măsuri tehnice și organizatorice adecvate pentru a proteja datele personale ale utilizatorilor. Concret, municipiul nu a asigurat restricționarea accesului la informațiile respective numai pentru personalul autorizat și nu a implementat mecanisme adecvate de autentificare și autorizare în sistemul său.

Acest caz demonstrează importanța implementării corespunzătoare a principiilor "privacy by design" și "privacy by default" în sistemul de prelucrare a datelor și consecințele nerespectării acestor principii în conformitate cu GDPR.

Cazul Haga District Court, Olanda (2019)

Autoritatea olandeză pentru protecția datelor ("AP") a anunțat, la 16 iulie 2019, că a impus o amendă de 460 000 EUR societății Stichting HagaZiekenhuis pentru încălcări ale securității în temeiul articolului 32 din Regulamentul general privind protecția datelor [Regulamentul (UE) 2016/679] ("GDPR").

În special, AP a evidențiat faptul că spitalul nu a pus în aplicare măsuri de securitate internă adecvate pentru a proteja dosarele pacienților, lucru care a fost dezvăluit după ce personalul medical a accesat fără motiv dosarele unui cunoscut cetățean olandez, ceea ce a dus la o anchetă.

În plus, AP a remarcat că, în cazul în care spitalul nu își îmbunătățește măsurile de securitate până la 2 octombrie 2019, va fi, de asemenea, supus unei sancțiuni de 100 000 euro la fiecare două săptămâni, cu un maxim de 300 000 euro. AP a subliniat că spitalul nu a reușit să implementeze controale cu privire la cine are posibilitatea de a accesa dosarele pacienților și să pună în aplicare un sistem care să necesite cel puțin autentificarea cu doi factori.

Deși acest caz nu se referă în mod specific la principiile "privacy by design" și "privacy by default", el subliniază importanța securității datelor în sectorul medical și consecințele nerespectării GDPR în acest context.

III. Operatorii de date și persoanele împuternicite care acționează sub responsabilitatea acestora ar trebui să ia toate măsurile adecvate pentru a-și îndeplini obligațiile în ceea ce privește protecția datelor și ar trebui să fie în măsură **să demonstreze** în special pentru autoritatea de supraveghere competentă că prelucrarea este în **conformitate** cu aceste obligații.

Exemplu de bună practică privind respectarea obligațiilor de protecție a datelor de către un spital:

Spitalul "XYZ" a implementat un program cuprinzător de conformitate cu protecția datelor pentru a se asigura că prelucrarea datelor personale, inclusiv a datelor medicale sensibile, este în conformitate cu legislația aplicabilă și cu GDPR. Acest program include următoarele componente:

- **Desemnarea unui responsabil cu protecția datelor (DPO)**: Spitalul a numit un DPO care supraveghează toate activitățile legate de protecția datelor și asigură conformitatea cu GDPR.
- **Politici și proceduri interne**: Spitalul a elaborat politici și proceduri clare și detaliate privind prelucrarea datelor personale, care sunt puse la dispoziția tuturor angajaților și colaboratorilor.
- **Formare și conștientizare**: Spitalul oferă instruire periodică angajaților și colaboratorilor cu privire la protecția datelor și responsabilitățile lor în cadrul programului de conformitate.
- **Controlul accesului și securitatea datelor**: Spitalul a implementat măsuri tehnice și organizatorice adecvate pentru a proteja datele personale, cum ar fi controlul accesului bazat pe roluri, criptarea datelor și monitorizarea activității în sistemele informatice.
- **Evaluarea impactului asupra protecției datelor (DPIA)**: Spitalul efectuează evaluări ale impactului asupra protecției datelor pentru orice prelucrare de date care prezintă un risc înalt pentru drepturile și libertățile persoanelor fizice.
- **Înregistrarea activităților de prelucrare**: Spitalul menține un registru al activităților de prelucrare a datelor, care include detalii despre scopul, natura și categoriile de date personale prelucrate.
- **Notificarea încălcărilor de securitate**: Spitalul a stabilit proceduri pentru notificarea promptă a încălcărilor de securitate către autoritatea de supraveghere competentă și persoanele vizate, conform cerințelor GDPR.

- **Monitorizarea și revizuirea periodică**: Spitalul efectuează revizuiri și audituri periodice ale programului său de conformitate cu protecția datelor pentru a identifica și aborda eventualele deficiențe și a se asigura că rămâne în conformitate cu legislația și reglementările aplicabile.

Prin implementarea acestui program cuprinzător de conformitate cu protecția datelor, spitalul "XYZ" își îndeplinește obligațiile în ceea ce privește protecția datelor și poate demonstra autorității de supraveghere competente că prelucrarea datelor personale este în conformitate cu aceste obligații.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.12** privind **modalitatea de răspuns în caz de încălcare a securității și confidențialității datelor pacientului sau a altei persoane vizate**

IV. Operatorii de date și persoanele împuternicite de către aceștia care nu sunt profesioniști din domeniul sănătății ar trebui să prelucreze datele referitoare la sănătate **numai în conformitate cu normele de confidențialitate și măsurile de securitate** care asigură un nivel de protecție **echivalent celui impus profesioniștilor din domeniul sănătății.**

Exemplu de bună practică privind respectarea normelor de confidențialitate și măsurile de securitate de către spitale pentru operatorii de date și persoanele împuternicite care nu sunt profesioniști din domeniul sănătății:

Spitalul "ABC" lucrează cu o companie externă de facturare și procesare a plăților, care are acces la anumite date referitoare la sănătate ale pacienților în scopul facturării serviciilor medicale. Pentru a asigura respectarea normelor de confidențialitate și a măsurilor de securitate, spitalul "ABC" și compania de facturare au implementat următoarele măsuri:

- **Acord de confidențialitate**: Spitalul "ABC" și compania de facturare au încheiat un acord de confidențialitate care prevede obligațiile părților în ceea ce privește protecția datelor referitoare la sănătate și responsabilitățile legate de păstrarea confidențialității acestor date.
- **Controlul accesului**: Compania de facturare are acces limitat la datele referitoare la sănătatea pacienților și poate prelucra aceste date numai în scopurile prealabile stabilite, cum ar fi facturarea și procesarea plăților. Accesul la date este restricționat în funcție de rolurile angajaților și necesitățile legitime de a accesa aceste informații.
- **Formare și conștientizare**: Spitalul "ABC" și compania de facturare oferă instruire periodică angajaților care lucrează cu date referitoare la sănătate în ceea ce privește normele de confidențialitate, măsurile de securitate și responsabilitățile lor în cadrul GDPR și a legislației naționale privind protecția datelor.
- **Măsuri tehnice și organizatorice de securitate**: Compania de facturare implementează măsuri de securitate adecvate pentru a proteja datele referitoare la sănătate, cum ar fi criptarea datelor în tranzit și la repaus, monitorizarea activității în sistemele informatice și protejarea fizică a serverelor și echipamentelor.
- **Audituri și revizuiri periodice**: Spitalul "ABC" efectuează audituri și revizuiri periodice ale măsurilor de confidențialitate și securitate implementate de compania de facturare pentru a se asigura că acestea respectă normele și măsurile de protecție adecvate.

Cazuistică în domeniu

Autoritatea Națională de Supraveghere din România a finalizat în luna februarie a anului curent (2023) o investigație la operatorul Tehnoplus Industry SRL în cadrul căreia a constatat încălcarea prevederilor art. 5 alin. (1) lit. a), c), e) și alin. (2), precum și ale art. 6 din Regulamentul General privind Protecția Datelor (RGPD) și a sancționată cu o amendă de aproximativ 5000 EURO.

Investigația s-a desfășurat ca urmare a unei plângeri prin care se reclama faptul că operatorul a prelucrat datele cu caracter personal ale petentului prin intermediul sistemului GPS instalat pe mașina sa de serviciu, fără să fi fost informat cu privire la monitorizarea autovehiculului, scopul și temeiul legal al acestei prelucrări și durata de stocare a datelor astfel colectate.

De asemenea, petentul a mai reclamat faptul că informațiile extrase din sistemul GPS au fost utilizate de operator în alt scop decât acela de a monitoriza mașina de serviciu atribuită acestuia.

În cadrul investigației efectuate s-a constatat faptul că Tehnoplus Industry SRL a prelucrat în mod excesiv (în afara orelor de serviciu) datele de localizare aferente petentului, angajat al operatorului, prin sistemul de monitorizare GPS instalat pe mașina acestuia de serviciu, fără să fi demonstrat că anterior a epuizat alte metode mai puțin intruzive pentru atingerea scopului prelucrării și fără a face dovada informării complete a petentului în legătură cu prelucrarea datelor prin intermediul sistemului GPS, încălcând astfel prevederile art. 5 alin. (1) lit. a), c) și (2) și art. 6 din RGPD.

Totodată, s-a constatat că operatorul a stocat datele din sistemul mai sus menționat, după expirarea duratei de stocare, fără să prezinte dovezi din care să rezulte că depășirea termenului de 30 de zile prevăzut de art. 5 din Legea nr. 190/2018 se bazează pe motive justificate, încălcând astfel dispozițiile art. 5 alin. (1) lit. e) și (2) din RGPD.

De asemenea, s-a constatat că operatorul a utilizat datele petentului din sistemul GPS în alt scop decât cel pentru care le colectase inițial.

În același timp, în temeiul art. 58 alin. (2) lit. d) din RGPD, s-au dispus față de societatea Tehnoplus Industry SRL:

- măsura corectivă de a asigura conformitatea cu RGPD a operațiunilor de colectare și prelucrare ulterioară a datelor personale, prin reevaluarea necesității atingerii scopurilor propuse prin folosirea datelor de localizare provenite din sistemul de monitorizare prin GPS instalate pe mașinile de serviciu ale angajaților operatorului și evitarea colectării excesive a datelor, prin raportare la obligațiile prevăzute de RGPD și de Legea nr. 190/2018;

- măsura corectivă de a asigura conformitatea cu RGPD a operațiunilor de colectare și prelucrare ulterioară a datelor personale, prin limitarea perioadei de stocare a datelor prin raportare la scopurile prelucrării datelor, conform obligațiilor prevăzute de RGPD și de Legea nr. 190/2018.

Pentru a ilustra pe larg diverse situații relevante specifice acestui principiu, vă rugăm să parcurgeți:

- **Orientarea 3.14 privind distrugerea în siguranță a datelor cu caracter personal**