Revista Română de Protecția Datelor

Editorial: av. dr. Andrei Săvescu, Managing Partner SAVESCU & ASOCIAȚII, președinte al SOCIETĂȚII de ȘTIINTE JURIDICE

Coordonator colectiv autori: av. Laurențiu Petre, Expert Data Protection, Partner SAVESCU & ASOCIATII, Director JURIDICE.ro

Autori: Andreea Coman, Alexandru Matei, Elena Tomacinschi, av. Alexandra Jivan, Partner în cadrul Hațegan Attorneys, Coordonator Practică de Data Protection

Manager proiect: Georgiana Istudor

Director Creație-Producție: Cristina Straton
Tehnoredactare: Simona Morărescu
Corectură: Elvira Panaitescu

Fotografii: Adobestock

Redacția: Bdul Națiunile Unite nr. 4, sector 5, București;
Telefon: 021.317.25.87,
E-mail: info@rs.ro; Internet: www.rs.ro
Corespondență:
Ghișeul ext. 3 – O.P. 39, sector 3, București

Publicație editată de:
RENTROP & STRATON

Președinte: George Straton
Director General: Octavian Breban

ISSN 2601 - 4289
ISSN-L 2601 - 4289

În această ediție:

Editorial

Instruire în domeniul protecției datelor cu caracter personal

IAPP (International Association of Privacy Professionals) este o ONG foarte prestigioasă, cu sediul în SUA.

Din conducerea ei fac parte profesioniști recunoscuți în domeniu, reprezentanți ai unor companii renumite care susțin asociația. Executive Committee: Citrix Systems (SUA), LinkedIn (SUA), Naspers (Africa de Sud), Intel (SUA), Mastercard (SUA). Board of Directors: The Walt Disney Company (SUA), Pfizer (SUA), Bank of America (SUA), Northrop Grumman Corporation (SUA), Citrix Systems (SUA), Prifender (SUA), Promontory (SUA), Nctm (Italia), Allianz (Germania), LinkedIn (SUA), Nymity (Canada), Mastercard (SUA), Naspers (SUA), Intel (SUA).

Această asociație americană organizează și în Europa cursuri de instruire în domeniul protecției datelor cu caracter personal și organizează examene (online), eliberând certificate corespunzătoare.

Transferul de date cu caracter personal dintr-o țară membră a Uniunii Europene către o țară terță se poate realiza atunci când Comisia Europeană a decis că țara terță asigură un nivel de protecție adecvat.

Comisia publică în Jurnalul Oficial al Uniunii Europene și pe site-ul său o listă a țărilor terțe în cazul cărora a decis că nivelul de protecție adecvat este asigurat. Lista țărilor non-UE în care nivelul de protecție este adecvat nu a fost încă întocmită.

În absența unei astfel de decizii privind caracterul adecvat al nivelului de protecție, transferul de date cu caracter personal către o țară terță poate avea loc numai în mod excepțional (în condițiile prevăzute de art. 49 GDPR).

Deși lista țărilor non-UE care asigură un nivel de protecție adecvat nu a fost încă întocmită, este încurajator faptul că asociația americană se implică activ în realizarea pregătirii specialiștilor europeni în protecția datelor. Unul dintre cele mai apreciate certificate eliberate de IAPP este Certified Information Privacy Manager.

av. dr. Andrei Săvescu,
Managing Partner SĂVESCU & ASOCIAȚII,
președinte al SOCIETĂȚII de ȘTIINȚE JURIDICE

Informaţii generale privind protecția datelor cu caracter personal pentru entități din sectorul sănătăţii

În lumea digitalizată în care trăim, protecția și confidențialitatea datelor cu caracter personal ale pacienților este mai importantă ca oricând. Semnificația crește chiar mai mult când vine vorba de un subiect delicat, și anume datele cu caracter personal privind sănătatea.

Acesta este motivul pentru care noua reglementare în privința protecției datelor cu caracter personal va avea un impact puternic asupra industriei de sănătate.

GDPR instituie un nivel mai ridicat de protecție pentru datele cu caracter personal privind sănătatea având în vedere că datele legate de sănătate reprezintă un subiect foarte sensibil și o inadecvată utilizare a lor poate avea un impact negativ asupra vieții sau reputației pacienților *(persoanelor vizate)*.

GDPR distinge între **trei categorii** de date cu caracter personal în sectorul sănătății, și anume:

1. Datele privind sănătatea – datele personale legate de sănătatea fizică sau psihică a unei persoane fizice, inclusiv asigurarea de servicii de îngrijire a sănătății, care dezvăluie informații despre sănătatea persoanei fizice.

2. Date genetice – datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice care furnizează informații unice despre fiziologia și sănătatea unei persoane fizice și care conduc, în special, la o analiză a unei probe biologice a persoanei fizice în cauză.

3. Datele biometrice - datele care rezultă din prelucrări tehnice specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a acelei persoane, cum ar fi imagini faciale sau date dactiloscopice.

Regulamentul conține, de asemenea, dispoziții despre cum trebuie prelucrate datele medicale în scop de cercetare medicală și studiu.

Cum va influența GDPR, medicul care activează în cadrul unui cabinet medical privat?

Medicii vor fi complet responsabili pentru datele sensibile ale pacienților săi *(în conformitate cu terminologia GDPR, aceștia vor deveni în același timp un operator de date cu caracter personal și persoană împuternicită de operator).*

Aceștia vor avea o mare responsabilitate, la fel ca și obligațiile pe care trebuie să le îndeplinească.

Operatorii de date cu caracter personal vor fi obligați să instituie măsuri speciale pentru a garanta că datele cu caracter personal sunt prelucrate în conformitate cu cerințele GDPR. În plus, ei vor avea obligația de a ține evidența tuturor activităților privind prelucrarea datelor cu caracter personal, pentru a fi în măsură să dovedească conformitatea cu GDPR.

Pacienții vor trebui să își exprime consimțământul cu privire la datele cu caracter personal care le aparțin și trebuie întotdeauna informați despre scopul prelucrărilor.

De asemenea, pacienții trebuie să aibă acces la datele lor, pentru a fi în măsură să le modifice sau actualizeze sau de a le retrage în orice moment.

Conform GDPR, pentru a fi obligatorie desemnarea unui DPO este necesară întrunirea următoarelor condiții, în mod cumulativ:
- operațiunile de prelucrare sunt **periodice;**
- operațiunile de prelucrare se referă la **date speciale cu caracter personal;**
- operațiunile de prelucrare se fac **pe scară largă;**
- operațiunile de prelucrare sunt **sistematice;**
- operațiunile de prelucrare reprezintă o **activitate principală** a operatorului *(prin natura, domeniul de aplicare și/scopurile operațiunilor).*

Astfel, cabinetele medicale, stomatologice, alți practicanți în domeniul sănătății și farmaciilor, cel mai probabil, vor fi nevoite să își desemneze un DPO. În orice caz, chiar și în ipoteza în care nu se procedează la desemnarea unui DPO, va trebui în aceeași măsură să fie asigurată conformitatea cu cerințele GDPR.

Persoana desemnată DPO poate fi un angajat existent, ale cărui atribuții sunt compatibile cu îndatoririle unui DPO, astfel încât să nu genereze un conflict de interese. *Spre exemplu*, acesta nu poate deține o poziție care să îl influențeze în stabilirea scopurilor și semificațiilor prelucrării datelor cu caracter personal.

Clinicile medicale pot partaja un DPO?

Da. Se poate numi un singur responsabil cu protecția datelor care să acționeze pentru un grup de autorități publice sau entități, luând în considerare structura organizatorică și dimensiunea lor.

Care sunt regulile de securitate în GDPR?

GDPR impune ca datele personale să fie procesate într-o manieră care să asigure securitatea lor. Acest lucru implică protecție împotriva prelucrărilor neautorizate sau ilegale și împotriva pierderii accidentale, distrugere sau deteriorare. Este nevoie să fie instituite măsuri tehnice și organizatorice corespunzătoare.

Este nevoie de consimțământul persoanei vizate pentru a prelucra date cu caracter personal în scopul exercitării activității de îngrijire a pacientului?

Nu neapărat. Trebuie să aveți o bază legală pentru a procesa datele cu caracter personal – consimțământul este un temei legal, dar există și alternative. Există șase temeiuri legale, niciunul dintre ele neavând prioritate față de altul. Care dintre aceste temeiuri va fi mai potrivit a fi utilizat va depinde de scopul pentru care prelucrați și natura relației pe care o aveți cu persoana vizată.

Consimțământul, conform GDPR, trebuie să fie liber exprimat, specific, informat și neechivoc, din care să rezulte o acțiune clară (o opțiune în acest sens). Dacă doriți să vă bazați pe consimțământ trebuie să fiți capabil să demonstrați că ați obținut consimțământul și faptul că persoanele vizate au dreptul oricând de a și-l retrage cu ușurință. Dacă sunteți o autoritate publică sau altă organizație cu o poziție dominantă în raport de persoana vizată poate fi dificil să demonstrați obținerea în mod valabil a consimțământului.

ȘTIAȚI CĂ?

Acordul pacientului pentru tratament sau pentru partajarea înregistrărilor medicale nu este echivalent cu consimțământul necesar a fi obținut potrivit GDPR.

În sectorul medical, datele personale ale pacienților sunt deținute în temeiul unei obligații de confidențialitate. Furnizorii de servicii medicale, în general, prelucrează date cu caracter personal pe baza acordului implicit pentru utilizarea datelor personale ale pacienților în scopul îngrijirii lor, fără a încălca obligația de confidențialitate.

În context, acordul implicit pentru îngrijirea directă este practica în această industrie la acest moment. Dar acest consimțământ implicit care are la bază obligația de confidențialitate nu este similar consimțământului pentru prelucrarea datelor cu caracter personal în baza unui temei legal prevăzut de GDPR.

Orice solicitare de obținere a consimțământului la tratament medical, în sine, nu înseamnă că reprezintă și o cerință pentru obținerea acordului asociat conform GDPR pentru prelucrarea datelor cu caracter personal, în situația în care alte baze legale ar fi mai susceptibile de a fi adecvate.

În sectorul sănătății, acordul, adesea, nu este baza legală cea mai potrivită în conformitate cu GPDR. Acest tip de presupunere a acordului implicit nu ar satisface standardul unui act de voință afirmativ clar – sau să fie calificat ca acord explicit pentru diverse categorii speciale de date, care includ datele cu caracter personal privind sănătatea (medicale). Furnizorii de asistență medicală ar trebui să identifice o altă bază legală (*de exemplu, interesul public poate fi mai adecvat).*

IMPORTANT!

În situația în care sunt prelucrate date speciale cu caracter personal – care includ datele personale privind starea de sănătate – nu este suficient să se justifice că prelucrarea se efectuează în baza unui temei legal. De asemenea, trebuie îndeplinită o condiție separată pentru prelucrarea datelor speciale cu caracter personal.

Datele speciale cu caracter personal conform GDPR sunt mai sensibile, motiv pentru care necesită o protecție sporită.

Pentru a procesa în mod legal categorii speciale de date, trebuie să se identifice o bază legală în conformitate cu articolul 6 din Regulament, similar prelucrării oricăror date cu caracter personal și o condiție separată, specifică pentru prelucrarea datelor de categorie specială în temeiul articolului 9 din Regulament.

Alegerea bazei legale în conformitate cu articolul 6 din Regulament nu dictează ce condiție din categoria celor prevăzute la articolul 9 din Regulament trebuie să se aplice, și vice-versa. *De exemplu*, dacă utilizați consimțământul ca temei legal, nu sunteți limitat la utilizarea acordului explicit pentru prelucrarea categoriilor speciale de date cu caracter personal în conformitate cu articolul 9 din Regulament. Ar trebui să se aleagă oricare condiție aplicabilă categoriei datelor speciale cu caracter personal, care este cea mai adecvată în circumstanțele date – deși în multe cazuri poate de asemenea exista o legătură evidentă între cele două. De exemplu, dacă baza legală este reprezentată de *interesele vitale* ale persoanei vizate, este foarte probabil că temeiul legal determinat de articolul 9 din regulament aferent *intereselor vitale* va fi unul adecvat.

Trebuie astfel să fie determinată situația care se aplică pentru prelucrarea datelor de categorie specială înainte de a începe această prelucrare sub imperiul GDPR și trebuie să documentați acest lucru.

Cum vom aborda cererile de rectificare a datelor cu caracter personal?

Persoanele vizate au dreptul de a avea datele personale rectificate în cazul în care sunt inexacte sau incomplete.

În cazul în care s-au furnizat date speciale cu caracter personal către terțe părți, acestea din urmă trebuie să fie informate

despre rectificare. De asemenea, trebuie să fie informate persoanele vizate despre terțele părți cărora au fost comunicate datele cu caracter personal.

Cu toate acestea, acest lucru nu se extinde la **opiniile medicale**, în cazul cărora datele înregistrate cu precizie reprezintă opinia în cauză.

Adesea este imposibil să se concluzioneze cu certitudine, probabil, până la momentul efectuării testelor, indiferent dacă un pacient suferă de o anumită afecțiune. Un diagnostic inițial (sau opinie exprimată în cunoștință de cauză) se poate așadar dovedi a fi incorect după examinarea mai extinsă sau după efectuarea unor teste suplimentare. Persoanele fizice ar putea dori ca diagnosticul inițial să fie eliminat pe motiv că acesta a fost, sau s-a dovedit a fi, inexact. Cu toate acestea, în cazul în care înregistrările despre un pacient reflectă cu exactitate diagnosticul medicului la un anumit moment dat, înregistrările nu pot fi calificate ca fiind inexacte, pentru că ele reflectă cu exactitate opinia particulară a medicului la acea vreme. În plus, înregistrarea diagnosticului inițial poate ajuta tratarea pacientului mai târziu.

Când este nevoie raportarea unei încălcări a datelor cu caracter personal?

O încălcare a datelor cu caracter personal reprezintă o violare a securității acestora, aptă să conducă la distrugeri accidentale sau ilicite, pierderi, modificare, divulgare neautorizată sau accesul la acestea.

Sub imperiul GDPR, o încălcare a securității datelor speciale cu caracter personal trebuie să fie notificată autorității de supraveghere în termen de 72 de ore, dacă nu este puțin probabil să conducă la un risc pentru drepturile și libertățile persoanelor fizice. Organizațiile trebuie să notifice pe cei în cauză, în cazul în care o încălcare este aptă a putea duce la un risc ridicat pentru drepturile și libertățile persoanelor vizate fără întârzieri nejustificate.

Dacă se apelează la o persoană împuternicită, și aceasta se confruntă cu o încălcare/incident de securitate, aceasta trebuie să informeze operatorul de date cu caracter personal fără întârziere, de îndată ce acestea cunosc încălcarea – operatorul este responsabil pentru raportarea către autoritatea de supraveghere a încălcărilor obligațiilor care decurg din GDPR.

Cum afectează dreptul de ștergere înregistrările medicale și stomatologice?

Este important a fi reținut faptul că nu există un *„drept de a fi uitat”* absolut.

Persoanele vizate pot cere ca datele lor personale să fie șterse – dar numai atunci când nu există niciun motiv imperios pentru continuarea prelucrării.

Cererile vor trebui să fie evaluate pe baza trăsăturilor proprii. Cu toate acestea, furnizorii de servicii medicale, de exemplu, vor avea probabil un motiv foarte bun pentru prelucrarea în continuare a datelor cu caracter personal pe care le dețin în scopul de a oferi îngrijire medicală.