REGULAMENTUL GENERAL PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL ÎN CADRUL ACTIVITĂȚII FARMACEUTICE DIN ROMÂNIA

Bianca Naghi, avocat senior coordonator D&B David și Baias SCA

Corina Bădiceanu, avocat D&B David și Baias SCA

Ce este Regulamentul General privind Protecția Datelor cu Caracter Personal?

Începând cu 25 mai 2018 intră în vigoare Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE ("**RGPD**" sau „**Regulamentul**").

Regulamentul se dorește a fi cea mai avansată și riguroasă legislație privind protecția datelor cu caracter personal din lume. RGPD vine pe fondul necesității de a nivela standardul de protecție al Statelor Membre (care au implementat în mod diferit o directivă pe aceeași temă în vigoare din 1995 și s-a constatat că la nivelul Statelor Membre cetățenii europeni nu beneficiază de aceleași drepturi).

Regulamentul a fost publicat în mai 2016. Statele Membre și toți operatorii au avut astfel o perioadă de 2 ani de zile pentru a se conforma noilor reguli și a implementa noile cerințe (acest timp de acomodare expiră în mai 2018).

Cui i se aplică Regulamentul General privind Protecția Datelor cu Caracter Personal?

Regulamentul se aplică și farmaciilor, indiferent de forma de organizare, indiferent de mărime, număr de persoane sau cifră de afaceri cât timp acestea prelucrează date cu caracter personal ale unor persoane fizice.

Aceasta deoarece Regulamentul se aplică oricărei persoane (juridice sau fizice) care prelucrează date cu caracter personal ale persoanelor fizice care rezidă în Uniunea Europeană în contextul unei activități comerciale sau de orice natură care se desfășoară conform legii. Sfera persoanelor care sunt excluse de la aplicarea Regulamentului este foarte restrânsă (de exemplu, RGPD nu se aplică persoanelor fizice care prelucrează date în scop personal, de exemplu pentru a menține o agendă cu persoane de contact).

Date cu caracter personal înseamnă informaţii despre o persoană a cărei identitate este fie clară în mod evident, fie poate fi, cel puţin, stabilită prin obţinerea unor informaţii suplimentare. Cu titlu de exemplu: numele, prenumele, adresa de corespondență, adresa de email, număr de telefon reprezintă date cu caracter personal pentru că

identifică în mod direct o persoană fizică. Pe de altă parte, numărul sau codul de client poate reprezenta o dată cu caracter personal dat fiind că oferă o informație unică care poate să ducă indirect la identitatea unei persoane fizice. Nu există o listă care să enumere toate datele cu caracter personal existente, astfel că analiza trebuie să se facă de la caz la caz.

Date cu caracter special reprezintă o categorie diferită de date și include doar următoarele: (1) date cu caracter personal care dezvăluie originea rasială sau etnică, (2) opiniile politice, (3) confesiunea religioasă sau convingerile filozofice sau (4) apartenența la sindicate, (5) date genetice, (6) date biometrice, (7) date privind sănătatea sau (8) date privind viața sexuală sau orientarea sexuală.

Prelucrare înseamnă orice operațiune sau set de operațiuni, care se desfășoară asupra datelor cu caracter personal, respectiv: colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terţi prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea. Cu titlu de exemplu: consemnarea unui număr de telefon sau a unei adrese pentru livrarea unui produs, prelucrarea datelor din rețetă pentru eliberare medicamente reprezintă operațiuni de prelucrare date cu caracter personal.

Din perspectiva Regulamentului, actorii importanți sunt operatorii și împuterniciții.

Operatorii sunt persoanele care determină scopul și mijloacele prelucrării. De exemplu, farmacia este operator atunci când prelucrează datele propriilor angajați sau clienți/pacienți.

Farmacia este operator de date cu caracter personal atunci când prelucrează date:

- ale propriilor angajați în scop de recrutare, încheiere și derulare rapoarte de muncă, îndeplinirea oricăror obligații legale referitoare la angajați (concedii, indemnizații, bonificații, cercetări disciplinare etc.)
- ale reprezentanților partenerilor pentru aprovizionare sau derulare activitate proprie,
- ale clienților atunci (a) când supraveghează video locația farmaciei, (b) când emite carduri de fidelitate, (c) eliberează tratament sau comercializează alte produse decât cele din categoria medicamentelor, (d) comunică disponibilitatea unor medicamente către clienți recurenți.

Împuterniciții sunt persoanele care ajută operatorul în implementarea prelucrării. De exemplu, o societate care ajută farmacia cu privire la înregistrarea angajaților în REVISAL și cu transferul salariului este împuternicit.

În România există o lege specială? Regulamentul se aplică direct în locul acesteia?

Este necesar să existe o legislație națională pentru a aplica Regulamentul?

În România, protecția datelor cu caracter personal este reglementată prin Legea 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date ("**Legea 677/2001**").

Autoritatea care aplică Legea 677/2001 se numește Autoritatea Națională de Supraveghere a Protecției Datelor cu Caracter Personal ("**ANSPDCP**"). Mai multe detalii despre autoritate și activitatea sa le puteți găsi la www.dataprotection.ro.

Regulamentul va abroga Legea 677/20o1 și se va aplica direct în România, fără să fie necesară o altă prevedere națională specială. La data la care redactăm acest articol, există 2 proiecte de lege în Parlament menite să aducă clarificări suplimentare Regulamentului:

(a) un proiect de modificare a legii de funcționare și organizare a ANSPDCP, care îi sporește competențele de investigație și sancționare (de exemplu, în baza proiectului de lege, autoritatea intenționează suplimentarea personalului și de asemenea intenționează să efectueze inspecții inopinate la fel ca și Consiliul Concurenței), și

(b) un proiect de lege menit să particularizeze anumite aspecte din Regulament la nivel național (de exemplu, se specifică regimul sancționatoriu diferit aplicabil autorităților publice față de cele private, se impun condiții suplimentare mai riguroase pentru situația în care se prelucrează numere de identificare unice în scop legitim, cum este cazul solicitării CNP sau serie și număr de CI pentru acces într-o clădire).

Mai multe detalii puteți vedea pe paginile de internet dedicate[1].

Protecția datelor cu caracter personal este un domeniu extrem de specific cu care nu m-am întâlnit în decursul activității. De ce aș începe să aprofundez cerințele Regulamentului?

Alături de standardul extrem de ridicat pe care îl impune, Regulamentul aduce un nivel de penalități care poate ajunge până la maxim 20 milioane EUR sau până la 4% din cifra de afaceri mondială a grupului de societăți (urmând să se aplice oricare dintre cele două este mai mare).

1A se vedea https://www.senat.ro/Legis/Lista.aspx?cod=21236 și http://www.dataprotection.ro/?page=Proiect_de_modificare_si_completare_a_Legii_nr_102_/_2005&lang=ro.

Subliniem că acest nivel este unul maxim și că în același timp, Regulamentul prevede și sancțiunea cu avertismentul. În acest sens, autoritatea din România a dat un comunicat de presă care subliniază că va înclina înspre a da avertismente înainte de a aplica sancțiunea cu amenda[2].

Chiar și așa, trebuie avut în vedere că maximul de amendă conform Legii 677/2001, legea din prezent este de 50.000 lei, adică de 2.000 de ori mai mic decât pragul maxim din Regulament.

Nu doar nivelul ridicat al amenzii determină societățile să aprofundeze și să înceapă implementarea Regulamentului ci și contextul curent (din ce în ce mai multe persoane fizice devin tot mai circumspecte în ceea ce privește datele lor personale – a se vedea scandalul Facebook – Cambridge Analytica).

Doresc să aplic Regulamentul la nivelul farmaciei. Care sunt pașii pe care trebuie să îi urmez?

Bineînțeles, este necesar să aflați mai multe detalii despre Regulament înainte de a începe orice activitate de implementare a acestuia dar vă oferim în cele ce urmează 6 pași principali și obligatorii de parcurs:

Pasul 1. *Identificarea responsabililor în cadrul farmaciei*
Pasul 2. *Redactarea unui plan de acțiune*
Pasul 3. *Crearea unei evidențe a prelucrărilor*
Pasul 4. *Asigurarea protecției datelor cu caracter personal și protejarea împotriva incidentelor de securitate*
Pasul 5. *Asigurarea respectării drepturilor persoanelor*
Pasul 6. *Asigurarea faptului că prelucrarea respectă principiile din Regulament*

Pasul 1. Identificarea responsabililor în cadrul farmaciei

Farmacii de talie mică: identificați persoana din cadrul companiei care poate să documenteze toate modalitățile în care farmacia prelucrează date cu caracter personal (care poate să răspundă la întrebări ca și cum se colectează datele, sub ce formă (fizic sau electronic se înregistrează), care sunt metodele de stocare sau ștergere, către cine se comunică date cu caracter personal și în ce mod etc.).

Farmaciile de talie medie sau mare: identificați o echipă de persoane care să se ocupe de cele menționate mai sus. Totodată, volumul activității (calculat atât din perspectiva

2A se vedea http://www.dataprotection.ro/?page=Obiective_RGPD&lang=ro.

numărului de clienți cât și a întinderii geografice) poate determina obligativitatea numirii unui Responsabil cu Protecția Datelor cu Caracter Personal. Nu există o formulă matematică care să fie aplicată și care să indice obligativitatea acestei poziții. Cu titlu de exemplu, autoritatea din România a specificat că nu este obligatorie numirea unui Responsabil cu Protecția Datelor la nivelul unui cabinet medical individual dar că este nevoie de această persoană la nivelului unui spital. Cert este însă că, dacă veți fi identificat ca fiind obligat să numiți un responsabil, lipsa acestuia reprezintă o încălcare gravă a Regulamentului.

Aveți posibilitatea ca Responsabilul cu Protecția Datelor să fie un angajat (alocat chiar și parțial acestui rol) sau să fie o persoană externă farmaciei pe care să o împărțiți cu alte farmacii/operatori. Autoritatea va vedea numirea acestei persoane drept un semn de bunăvoință la nivelul farmaciei în ceea ce privește efortul de conștientizare a Regulamentului.

Pasul 2. Redactarea unui plan de acțiune

Cei 6 pași pe care îi sumarizăm pot reprezenta un bun început de plan de acțiune deoarece ating principalele puncte ale Regulamentului.

Planul de acțiune ar mai putea cuprinde și efortul asumat de întreaga echipă la nivel de farmacie de cunoaștere și conștientizare a Regulamentului prin programe de pregătire. De asemenea, planul de acțiune ar mai trebui să cuprindă și notificarea persoanelor (în ce mod și prin ce canale, inventarierea împuterniciților și setarea unui cadru pentru incidentele de securitate – dat fiind că Regulamentul impune ca incidentele serioase de securitate să fie notificare autorității în termen de 72 de ore de la data luării la cunoștință).

Cu siguranță înainte de a începe implementarea Regulamentului trebuie să cunoașteți cel puțin:

- care sunt datele cu caracter personal pe care le prelucrați și cum și unde le puteți identifica,
- că farmacia este operator de date cu caracter personal,
- care sunt împuterniciții farmaciei,
- ce înseamnă raportat la propria activitate un incident de securitate serios.

Pasul 3. Crearea unei evidențe a prelucrărilor

Regulamentul impune redactarea și menținerea unei evidențe riguroase a prelucrărilor de date cu caracter personal doar pentru acei operatori care au mai mult de 250 de angajați. Cu toate acestea, implementarea Regulamentului cere o documentare a modului în care sunt prelucrate datele cu caracter personal.

Mai jos, vă recomandăm un model de evidență aplicabil pentru prelucrarea datelor cu caracter personal:

Statut Farmacie	Operator
Categorii de persoane și de date cu caracter personal	Pacienți Date de contact (nume, adresă, date de contact) Date de sănătate
Scopul prelucrării	Eliberare rețetă
Baza legală a prelucrării	Îndeplinirea obligaţiilor legale de eliberare a medicamentelor către populaţie / interes public, conform prevederilor HG 140/2018, Legii farmaciei nr. 266/2008, a Normelor privind înființarea, organizarea și funcționarea farmaciilor și drogheriilor, aprobate prin Ordinul Ministrului Sănătății nr. 962/2009, precum și Regulilor de bună practică farmaceutică adoptate prin Ordinul Ministrului Sănătății nr. 75/2010
Cum se colectează datele?	Prin rețetă pusă la dispoziție de pacient, prin propria persoană sau prin împuternicit
Cum se păstrează datele?	Sistem IT Email Fizic
Cât timp se păstrează datele?	Conform cu prevederile legale aplicabile
Cui i se dezvăluie datele?	Casa Națională de Asigurări de Sănătate

De menționat că acesta este o singură prelucrare și că la nivel de farmacie ar mai putea fi: prelucrare date în scop de eliberare card fidelitate, prelucrare client fidel în scop de notificare stoc, prelucrare date angajați sau colaboratori în scop de organizare muncă și executare contract individual de muncă, prelucrare date parteneri comerciali în scop de derulare activitate (sau a reprezentanților acestora dacă partenerii comerciali sunt persoane juridice) etc.

Pasul 4. Asigurați protecția datelor cu caracter personal și protejați-vă împotriva incidentelor de securitate

Cu riscul de a ne repeta, securitatea datelor cu caracter personal începe prin creșterea gradului de conștientizare al personalului care lucrează cu datele cu caracter personal prin educarea cu privire la riscurile de încălcare a confidențialității datelor și informarea angajaților despre măsurile implementate de farmacie pentru a face față acestor riscuri. Este foarte important ca la nivel de farmacie să existe sesiuni de informare, proceduri interne, responsabilități și verificări periodice.

De asemenea este important ca farmacia să implementeze o politică de clasificare a informațiilor prin care să se definească diferite niveluri de confidențialitate. Un rol

important îl joacă și regulile de securitate pe care trebuie să le respecte utilizatorii în sistemele informatice folosite (de a nu comunica parola unei terțe părți; de a nu instala, copia, edita sau distruge software fără autorizație; de a bloca calculatoarele de îndată ce utilizatorii părăsesc spațiul de lucru etc.).

Pasul 5. Asigurați respectarea drepturilor persoanelor

Regulamentul preia drepturile specifice ale persoanelor din legislația curentă (ba chiar le suplimentează cu dreptul la portabilitatea datelor). Sumarizăm drepturile persoanelor, precum și incidența lor în cadrul activității unei farmacii:

Drepturi specifice	**Detalii**
Dreptul de a fi informat	Orice persoană căreia i se prelucrează datele cu caracter personal are dreptul de a fi informată cu privire la coordonatele prelucrării. Informațiile care se vor pune la dispoziția acesteia sunt cele menționate în cadrul secțiunii cu evidența prelucrării (Pasul 3 de mai sus).
Dreptul de acces	Orice persoană poate solicita acces la datele personale proprii, în anumite condiții.
Dreptul de rectificare	Fiecare persoană poate cere actualizarea datelor cu unele corecte și la zi.
Dreptul de fi uitat (dreptul la ștergere)	De exemplu, atunci când persoana solicită ștergerea datelor în scop de marketing, farmacia va trebui să șteargă datele acesteia (însă dacă pentru persoana respectivă s-a realizat și prelucrarea unei rețete în scop de eliberare tratament, păstrarea acestor date va fi continuată în baza unei obligații legale pentru acest scop doar).
Dreptul de a restricționa prelucrarea	De exemplu, în cazul în care persoana consideră că datele pe care farmacia le deține sunt incorecte sau prelucrarea nu este legală.
Dreptul la portabilitatea datelor	Acest drept se aplică numai în anumite circumstanțe, de exemplu dacă prelucrarea datelor cu caracter personal este prin consimțământul persoanei vizate (în scop de marketing) sau a unui contract și se realizează prin mijloace automate.
Dreptul de a obiecta	Persoanele au dreptul să se opună prelucrării datelor. Într-un astfel de caz, va trebui să vă gândiți dacă nevoia farmaciei de a continua prelucrarea are prioritate asupra intereselor, drepturilor și libertăților persoanei respective. În cele mai multe cazuri, va trebui ca farmacia să păstreze datele dacă este vorba despre prelucrarea unei rețete în scop de eliberare tratament (minimul perioadei de stocare fiind cel prevăzut de lege).
Mecanismele de decizie automată	În general, acest drept este relevant pentru procesul de prelucrare al farmaciei doar în cazul în care se transmite mesaje comerciale personalizate către baza de date existentă

(inclusiv profiling-ul)	de clienți.

Subliniem faptul că farmacia trebuie să răspundă la toate cererile persoanelor în termen de maxim o lună de la data primirii (posibilitate de prelungire există însă doar pentru motive obiective excepționale).

Răspunsul trebuie oferit în mod gratuit, cu excepția cazului în care persoanele solicită în mod repetitiv sau se pot considera a fi de rea credință.

Pasul 6. Asigurarea faptului că prelucrarea respectă principiile din Regulament

Orice prelucrare de date cu caracter personal trebuie făcută cu respectarea următoarelor principii:

- legalitate, corectitudine şi transparență. Conform acestui principiu, farmacia trebuie să cunoască în mod continuu de ce prelucrează date cu caracter personal și care este necesitatea care impune o astfel de prelucrare (de exemplu, se prelucrează date pentru a elibera tratamentul sau se prelucrează date pentru a se raporta la CNAS). Totodată, prelucrarea trebuie să fie transparentă față de persoanele ale căror date se prelucrează (de exemplu, persoana trebuie să cunoască tot timpul care este traseul prelucrării, unde se stochează, către cine se dezvăluie etc.),

- limitarea scopului este unul dintre cele mai restrictive principii ale Regulamentului și impune ca datele cu caracter personal să se prelucreze doar în scopul declarat la colectare (de exemplu, este strict interzis ca o farmacie să dezvăluie fără consimțământul pacienților datele lor de sănătate unei societăți care efectuează studii de piață sau de consum anumite produse - ar fi posibil ca farmacia să dea unei astfel de companii date agregate care să nu dezvăluie identitatea persoanei fizice, dacă este în limita legii),

- minimizarea datelor înseamnă că farmacia nu trebuie să colecteze mai mult decât ceea ce este obligatoriu potrivit legii sau necesar pentru ducerea la îndeplinire a scopului prelucrării (de exemplu, ar putea fi excesiv solicitarea CNP pentru eliberarea unui card de fidelitate),

- exactitate, integritate şi confidenţialitate, respectiv datele cu caracter personal trebuie să fie corecte, integre, actualizate și complete.

- limită de stocare impune farmaciei să nu păstreze date cu caracter personal mai mult decât ceea ce este necesar sau impus de lege (de exemplu, datele de contact ale unei persoane care a solicitat ștergerea sa din baza de date de clienți

fideli nu ar mai trebui păstrate dacă nu există o obligație fiscal-contabilă de reținere, pe de altă parte datele din rețetă nu ar putea fi păstrate mai mult decât termenul legal prevăzut),

- răspundere, operatorul fiind cel care trebuie să își asume responsabilitatea că procesul de prelucrare este sigur și respectă Regulamentul.

Acestea sunt principalele etape în implementarea Regulamentului, însă acestea pot fi completate cu multe altele poate la fel de importante (cum ar fi de exemplu identificarea împuterniciților și încheierea unui contract care să impună reguli și cerințe specifice în materie de protecție a datelor).

În toate cazurile, trebuie să vă pregătiți pentru asumarea responsabilităților din cadrul Regulamentul cât mai eficient și cât mai cuprinzător, dat fiind că RGPD a fost pregătit încă din 2014 și se preconizează că a fi din ce în ce mai cunoscut la nivel de persoane ale căror date se prelucrează.