Iulian Boldea, Dumitru-Mircea Buda, Cornel Sigmirean (Editors)
MEDIATING GLOBALIZATION: Identities in Dialogue
Arhipelag XXI Press, 2018

GDPR IMPLEMENTATION IN HEALTHCARE SYSTEM

Lacrima Bianca Luntraru

Assist., PhD, "Petru Maior" University of Tîrgu Mureș

Abstract: The magnitude of technological developments and the globalization have been the main premises for adopting a set of general rules aimed at ensuring effective protection of personal data - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the use of personal data concerning the processing of personal data and the free movement of such data and repealing Directive 95/46 / EC (GDPR). It has been found that contemporary technology allows the use of personal data at an unprecedented level, with the risk that they may become public and cause serious harm, materializing the need for a regulation designed to provide increased protection.
In the present study, we attempted to map the main coordinates for the implementation of the Regulation in the medical system

Keywords: healthcare domain, liability,personal data, consent, privacy protection

1. Considerații introductive.

General Data Protection Regulation[1] reprezintă unul dintre cele mai actuale subiecte în toate domeniile de activitate, la nivelul Uniunii Europene, dată fiind aplicarea directă a acestui act normativ începând cu 25 mai 2018, dar mai ales, având în vedere numeroasele responsabilități instituite în sarcina operatorilor de date personale. Amploarea evoluțiilor tehnologice și globalizarea au fost principale premise ale adoptării acestui set de reguli generale ce vizează asigurarea unei protecții efective a datelor cu caracter personal, care sunt prelucrare prin mijloace automatizate sau care fac parte dintr-un sistem de evidență a datelor. S-a constat faptul că tehnologia contemporană permite utilizarea datelor cu caracter personal la un nivel fără precedent, existând riscul ca acestea să ajungă publiceși să cauzeze serioase prejudicii.

Ab initio, se impune a fi subliniat domeniul general de aplicare teritorială a GDPR, astfel cum acesta este statornicit prin dispozițiile art. 3: *Prezentul regulament se aplică prelucrării datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.*

(2) Prezentul regulament se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de:

a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată; sau

b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

[1] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția peroanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (GDPR), publicat în Jurnalul Oficial al Uniunii Europene nr. 119L din data de 4 mai 2016.

(3)Prezentul regulament se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internațional public.

În ceea ce privește *sistemul medical*, remarcăm faptul că acesta este afectat de multiple încercări în procesul de implementare a dispozițiilor instutite prin Regulament, dată fiind complexitatea acestui act normativ, caracterul de noutate, drepturile și obligațiile instituite, fiind practic nevoie de o reconstruire a întregului mecanism ce vizează prelucararea datelor în unitățiile spitalicești.

De la bun început trebuie subliniat faptul că ***toate instituțiile de sănătate, publice sau private, fac obiectul RGPD,*** fiind responsabile de prelucrarea datelor personale ale pacienților în cadrul acestora, precum și în ipotezele în care acționează ca și sub-contractant, cum ar fi spre exemplu, atunci când fac parte dintr-o grupare.

În vederea implementării dispozițiilor Regulamantului trebuie întreprinse numeroase acțiunii, care, în esență, se circumscriu inițiativei globale de gestionare a riscurilor,ce este inițiată de unitatea spitalicească respectivă pentru ameliorarea calității și securității îngrijirilor. Acestea se integrează în procedurile de conformitate ale instituției, respectiv, în cele ce vizează gestiunea riscurilor de securitate a sistemelor informatice utilizate.

Obligațiile care trebuie să fie luate în considerare variază în funcție de calificarea rolului instituției și natura tratamentului și a datelor utilizate. Se concretizează ***două perspective juridice***:

- De regulă generală, unitatea spitalicescă este responsabilă pentru multiplele prelucrări de date personale pe care le întreprinde, care pot sau nu să includă și aspecte ce țin de sănătatea persoanei vizate.
- În anumite cazuri, răspunderea unității se raportează la calitatea sa de sub-contractant, atunci când acționează în calitate de persoană împuternicită de operator.

2. Natura datelor prelucrate de unitatea spitalicească:

În primul rând, unitatea spitalicească prelucrează date personale, care nu sunt în mod neapărat date de sănătate, cum ar fi ,spre exemplu, datele privind identificarea persoanei, dar pentru care se aplică Regulamentul.

Potrivit dispozițiilor art. 4, pct. 1 din Regulament vor fi considerate **date cu caracter personal***orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.*

În general însă, spitatele colectează, generează și prelucrează date privind sănătatea, date genetice și date biometrice. Prin punctele 13,14 și 15 ale art. 4 din GDPR sunt stabilite în termeni exacții coordonatele tuturor acestor categorii de date, cupă cum urmează:

- „**date genetice"**reprezintă*datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză*;
- „**date biometrice**" *înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale*

ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

- „**date privind sănătatea**" *înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia.*

În acest context, se impune a fi subliniat faptul că, în acord cu prevederile considerentului 35 al GDPR, care are valoare normativă, este instituită obligația de interpretare a sintagmei ***date cu caracter personal privind sănătatea*** în sensul că acestea includ toate datele aflate în legătură cu starea de sănătate a persoanei vizate care dezvăluie informații despre starea de sănătate fizică sau mentală, trecută, prezente sau viitoare. Sunt avute în vedere:

- informațiile colectate în vederea înscrierii persoanei vizate la serviciile de asistență medicală sau în cadrul acordării servicilor respective persoanei fizice;
- orice număr, simbol sau semn distinctiv atribuit persoanei vizate în vederea identificării în scopuri medicale;
- informațiile rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale inclusiv datele genetice și eșantioanele de material biologic;
- orice informații privind o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea fiziologică sau biomedicală a persoanei vizate indiferent de sursa acestora adică dacă provin de la un medic sau de la un cadru medical ori de la un spital, un dispozitiv medical sau un test de diagnostic in vitro.

În privința acestor categorii de date – date privind sănătatea, date genetice și date biometrice, **Regulamentul instituie un principiu de interzicere a prelucrării lor, dată fiind sensibilitatea specifică.** Acest principiu este însă însoțit de numeroase excepții statornicite prin dispozițiile art. 9, potrivit căruia, în domeniul datelor viztae, prelucrarea este permisă în următoarele trei ipoteze:

1. există un consimțământ explicit în acest sens;
2. prelucrarea este *necesară* în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (3) al art. 9;
3. prelucrarea este *necesară* din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional.

Se impune a fi subliniat faptul că nu există o definiție generală, la nivelul regulamentului a termenului *necesar*, astfel încât ultimele ipoteze sunt susceptibile de interpretări. În vederea înlăturării oricăror discuții sau controverse este de preferat a fi utilizată în special prima ipoteză, cea a consimțământului explicit[2].

[2] În acest sens, J.P. Armstrong, A. Bywater, *What Healtcare Organizations should know about the GDPR*, prezentare publicată pe site-ul www.absolute.com/gdpr.

Bineînțeles, statul român are la îndemână posibilitatea de a legifera limitări sau condiții suplimentare referitor la datele specifice domeniul medical. În orice caz, ori de câte ori se va pune problema procesării datelor din sistemul medical în mod obligatoriu trebuie să fie respectate condițiile din Regulament (sau cel puțin una).

Instituțiile medicale trebuie să manifeste o atenție sporită în primirea, maparea și utilizarea datelor personale, dar mai ales în observarea îndeplinirii condițiilor sus-expuse.

3. Obligațiile unității spitalicești cu privire la protecția datelor de sănătate ale pacienților

În sarcina unității spitalicești se concretizează mai multe obligații referitoare la modalitățile de punere în practică a datelor cu caracter personal privind sănătatea[3].

În primul rând, intituția este obligată să respecte în totalitate și întocmai principiile generale privind asigurarea protecției datelor de sănătate – finalitate, pertinență și proporționalitate, conservare limitată, securitate și confidențialitate, respectarea dreptului persoanei.

În al doilea rând, unitatea spitalicească trebuie să își adapteze procedurile la prevederile Regulamentului, ceea ce presupune următoarele:

- *Trebuie ținută o documentație internă, care să vizeze descrierea modalități de prelucrare înterprise și măsurile de punere în conformitate a acestora cu prevederile noii reglementări.* În anumite cazuri, mai ales atunci când sunt vizate activități de cercetare, este necesară obținerea prealabilă a unei autorizații în acest sens, emisă de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

- *Trebuie să numească un responsabil cu protecția datelor personale*. Toate institutile publice sunt vizate de această obligație potrivit art.37, alin. (1), lit. a din Regulament. În ceea ce privesc instituțiile private, nu există obligația expresă în acest sens.Cu toate acestea, având în vedere dispozițiile art. 37, alin. (1), lit. c, ori de câte ori este vizatăprelucrarea datelor sensibile, precum cele menționate de prevederile art. 9, se concretizează această obligație și în sarcina operatorului respectiv. Deci, implicit și spitatele private au obligația de a-și numi un responsabil cu protecția datelor, obiectul lor de activitate raportându-se în genere la datele de sănătate, datele sensibile în general.

De altfel, în cuprinsul Ghidului orientativ de aplicare a Regulamentului General pentru Protecția Datelor destinat operatorilor, lansat în luna septembrie a anului 2017, Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal recomandă în mod insistent desemnarea unui responsabil cu protecția datelor chiar și în ipoteza în care entitatea vizată nu are obligație expresă în acest sens, având în vedere efectul benefic mai exact asigurarea respectării dispozițiilor Regulamentului. Se subliniază ideea că acest responsabil cu protecția datelor reprezintă un avantaj major pentru Operator în vederea înțelegerii și respectării obligațiilor ce sunt legiferate prin intermediul GDPR.

În mod efectiv, responsabilul cu protecția datelor are obligația de a informa și consilia operatorul cu privire la obligațiile instituite în sarcina sa de către legiuitor; obligația de a monitoriza respectarea regulamentului; obligația de a aduce la cunoștința operatorului concluziile studiilor de impact privind protecția datelor; obligația de a se perfecționa în domeniu; obligația de a coopera cu autoritatea pentru protecția datelor, de a reprezenta punctul de contact în relația cu aceasta.

- *Trebuie să asigure respectul drepturilor tradiționale ale persoanei cu privire la prelucrarea datelor sale* - dreptul de a fi informat asupra operațiunii de prelucrare, dreptul de acces al persoanei vizate, dreptul la rectificare, dreptul la restricționarea prelucrării pentru motive legitime.

[3] În acest sens, *Établissements de santé: préparez-vous au règlement européen sur la protection de donnés personnelles (RGPD*), prezentare susținută de L Agence Française de la Santé Numérique, RGPD Fiche : Impacts en établissement de santé – Novembre 2017.

Noi drepturi sunt prevăzute, cum ar fi, spre exemplu, dreptul la portabilitatea datelor sau dreptul de a fi uitat, care dobândesc uneori funcționalități specifice și trebuie să fie prevăzute în sistemele de informare folosite de instituție. Astfel, art. 20 legiferează dreptul la portabilitatea datelor statuând în sensul că persoana vizată are dreptul de primi datele personale ce o privesc și pe care le-a furnizat operatorului într-un format structurat accesibil, respectiv dreptul de a le transefar altui operator, fără obstacole. (art. 20)

În ceea ce privește dreptul de a fi uitat, acesta este statornicit prin disp. art. 17, care prevăd că persona vizată are dreptul la ștergerea tuturor datelor personale ce o privesc fără întârzieri nejustificate. (art. 17). Aceste se aplică oricărei prelucrări de date privind sănătatea, mai puțin în privința celor ce fac obiectul cercetărilor științifice. Excluderea se justifică din perspectiva preocupării de menajare a studiilor vizate, avându-se în vedere modalitatea în care exercitarea acestui drept ar afecta[4].

Se ridică o serie de probleme de implementare, fiind criticabilă modalitatea neclară în care este instituit acest drept. Operatorii de date personale vor fi puși în situația în care trebuie să dezvolte soluții tehnice complexe astfel încât orice ștergere a datei personale procesate, la cererea unei persoane, să fie posibilă.

- *Realizarea unei analize a impactului prelucrării datelor personale care vizează atât riscurile de securitate şi tehnice, precum şi riscurile juridice pentru persoane***,** înainte de a pune în aplicare anumite prelucrări,mai ales, acele care au legătură cu datele în masă, privind sănătatea.Este suficietă o singură evaluare pentru mai multe operațiuni de procesare similare, care prezintă același riscuri sau atunci când se extinde un serviciu și i se atribuie noi funcționalități. Totuși în măsura în care în aceste ipoteze pot fi identificate riscuri noi, trebuie realizată o nouă evaluare a impactului asupra vieții private.

- *Trebuie să se acorde o atenție sporită ipotezelor în care se încheie contracte de prestări servicii cu terții.*Din momentul în care unitatea spitalicească recurge la un prestator de servicii extern, iar acest lucru implică tratarea datelor personale de sănătate trebuie să fie încheiat cu prestatorul un contract, în cuprinsul căruia să fie precis individualizat conținutul obligațiilor ce incubă prestatorului, de regulă, o prezentare detaliată a dispozițiilor art 28 din Regulament.

În cazul în care, unitatea spitalicească nu are puterea de control asupra modalității de contractare sau asupra mijloacelor de lucru folosite de prestator, trebuie, pe cât posibil, ă fie instituită în orice mod posibil (declarații , convenții etc) obligația prestatorului de a garanta că va respecta principiile Regulamanetului.

- *Trebuie să se pună în practică proceduri care permit garantarea securității și confidențialității datelor personale în acord cu respectul politicii generale de securitate a sistemelor de informație din domeniul sănătății și să se respecte întocmai obligațiile legate de conservarea datelor* – să fixeze o durată de conservare, să organizeze o modalitate de arhivare, să se asigure capacitatea de restituire a datelor de sănătate.

- *Trebuie să se semnaleze Autoritatea Națională de supraveghere a Prelucrării Datelor cu Caracter Personal*cu privire la orice incident de securitate care implică datele personale.

4. Etapele implementării GDPR

În vederea implementării dispozițiilor regulamentului pot fi concretizate șase etape:

1. *Desemnarea unui responsabil cu protecția datelor în acord cu prevederile art. 37-39 din Regulament.*
2. *Cartografierea datelor personale – art. 30 din Regulament.*

[4] E. Vollebregt, *The new General Data Protection Regulation impact on medical devices industry*, articol publicat online la adresa www.medicaldeviceslegal.com

Printre procedurile inițiale care trebuie întreprinse în vederea implementării regulamentului se numără întocmirea evidenței activităților de prelucrare. Indiferent de profilul de activitate sau de natura datelor personale sau scopul prelucrarea acestora, dacă organizația are mai mult de 250 de angajați există obligația cartografierii prelucrării datelor cu Caracter Personal în temeiul articolului 30.Obligația se concretizează și în sarcina operatorilor din sistemul privat cu mai puțin de 250 de angajați însituațiile în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, sau dacă prelucrarea nu e ocazională sau include categorii speciale de date precum cele prevăzute de disp. art. 9.

Potrivit articolului 30, unitatea spitalicească trebuie să întocmească o evidență clară a următoarelor informații:

-Numele și datele de contact ale operatorului și, după caz, ale operatorului asociat ale reprezentantului operatorului și ale responsabilului cu producția datelor.

- Scopurile prelucrării.

- Descrierea categoriilor de persoane vizate și a categoriilor de date cu caracter personal.

- Categoriile de destinatari cărora le-a fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țările terțe sau organizații internaționale.

- Transferurile de date cu caracter personal către o țară terță sau organizație internațională, inclusiv identificarea țării terțe sau organizații internaționale respective și, în cazul transferurilor menționate la articolul 49 aliniatul (1) al doilea paragraf, documentația care dovedește existența unor garanții adecvate.

- Acolo unde este posibil termenele limită preconizate pentru ștergerea diferitelor categorii de date.

- Acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate de dispozițiile articolului 32.

În ipoteza unui control din partea autorităților de supraveghere competente toate aceste informații trebuie să fie puse la dispoziția organelor abilitate.

3. Stabilirea unor priorități pentru acțiunile care trebuie să fie puse în practică cu privire la riscurile inerente prelucrări datelor, asupra drepturilor și libertăților persoanelor vizate.

4. Gestiunea riscurilor – efectuarea unui studiu de impact asupra protecției datelor personale pentru fiecare dintre prelucrările întreprinse, susceptibilă de a creea riscuri.

5. Organizarea unei proceduri interne care să garanteze luarea în considerare protecției datelor la orice moment ținem cont de ansamblul evenimentelor care pot să survină cu privire la prelucrarea datelor.

6. Asigurarea că regulamentul este bine pus în practică și este în conformitate cu toate interpretările actualizate.

5. Scurte considerațiuni cu privire la criteriile consimțământului adecvat în termenii GDPR

Pornind de la regulile instituite în cuprinsul art. 9 cu privire la prelucrarea datelor sensibile și având în vedere faptul că în două din cele trei ipoteze în care este permisă această operațiune, se omite definirea unui termen esențial, și anume acela de *necesar*, apreciem că în domeniul medical, cel mai adesea se va recurge la tratarea datelor specifice doar în ipoteza în care există un consimțământ explicit în acest sens al persoanei vizate. În aceste condiții, am considerat oportun studiului nostru de a sublinia o serie de consideațiuni cu privire la caracteristiciile juridice pe care acest consimțământ trebuie să le îndeplinească.

Potrivit art. 4, pct. 11 din Regulament „*consimțământ*" al persoanei vizate înseamnă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate.

Din definiție, se deduce că este obligatorie concretizarea unui proces activ, care poate inclusiv să presupună încercuirea unei căsuțe speciale, alocate în acest sens pe un website. În orice caz, procesatorul de date personale trebuie să își asigure o dovadă concretă în sensul că, consimțământul a fost efectiv și în mod real exprimat. În termenii Regulamentului, se poate remarca că este permisă exprimarea consimțământului și anterior datei de 25 mai 2018, fiind considerat valabilpotrivit normelor instituite prin acesta, atâta timp cât sunt îndeplinite toate cerințele în acest sens. Pe de altă parte, în ipoteza în care consimțământul a fost exprimat anterior, însă nu se circumscrie condițiilor unui consimțământ explicit, nu va fi valabil, fiind necesară suplinirea omisiuniilor.

Totodată, consimțământul va fi considerat ca invalid în cazul în care există un dezechlibru evident între persoana vizată și operatorul de date. Acest aspect va fi dificil de implementat în practică, în special în ipotezele în care medicul prescrie utilizarea unui program pe care îl folosește spitalul pentru monitorizarea pacienților la distanță., cum ar fi cazul aparatelor care se poartă pe corp De cele mai multe ori pacientul aflat într-o astfel de situație nu va avea libertatea de a refuza procesarea datelor sale personale. Aceeași problemă se ridică și în ipoteza în care pacientul este subiectul unei cercetări științifice, cu mențiunea că în acest sens, există o serie de reglementări în cuprinsul art 89 și următoarele care permite anumite derogări.

În domeniul medical, se instituie o cerință expresă a consimțământului, și anume aceea de a fi explicit. Remarcăm faptul că legiutorul omite însă să definească acest *termen*, lăsând loc de interpretări și controverse, ceea ce în mod cert va afecta implementarea practică a consimțământului în domeniul medical. În orice caz, este general acceptat că un consimțământ explicit este cea mai riguroasă formă a acordului ce poate fi exprimată.

Termenul de explicit este definit în dicționarul explicativ al limbii române ca semnificând limpede, deslușit, lămurit, clar, fără dubiu fără echivoc[5]. Din perspectiva strict juridică, respectarea acestei cerințe presupune obținerea consimțământului în fața unei autorități cum ar fi, spre exemplu, un notar public. Însă termenul de explicit trebuie interpretat într-o manieră mai practică, astfel încât, consimțământul să poată fi exprimat și prin intermediul unui formular tipizat, care să conțină o serie de caracteristici care să demonstreze existența unui consimțământ real și complet, dar și limitele acesteia.[6]

Așadar, sectorul medical va trebui să acorde atenție maximă procesului de obținere a consimțământului, repectiv implementării unei metode cât mai adecvate obținerii acestuia.

Consimțământul exprimat trebuie să fie unul complex, care să acopere cât mai multe potențiale trensferuri de date cu caracter pesonal, inclusivcele internaționale sau stocarea datelor pe un cloud.

Este important de subliniat faptul că oodată ce a fost în mod corect emis consimțământul pacientului, nu mai este necesară o exprimare suplimentară privind prelucrarea secundară a datelor acesteia în sensul înscrierii într-un registru internet spre exemplu, cu condiția ca să fie respectate garanțiile adecvate.

[5]Academia Română, Institutul de lingvistică Iorgu Iordan, *Dicționarul explicativ al limbii române, ediția a II-a revăzută și adăugită,* Ed. Univers Enciclopedic Gold, București, 2012.

[6] În acest sens, G.Coca, O. Lazăr, *Despre confidențialitatea informațiilor și viața privată a pacienților*, lucrare publicată în volumul Sesiunii Științifice a Institutului de Cercetări Juridice Acad. Andrei Rădulescu, Simplificarea – imperativ al modernizării și ameliorării calității dreptului, 17 aprilie 2015, Ed. Universul Juridic, București, 2015.

6.Concluzii

Conformitatea cu GDPR reprezintă o prioritate majoră indiferent dacă sunt vizate unități spitalicești private sau publice .În acest sens trebuie adoptată o abordare proactivă, metodică și temeinică informată din toate perspectivele juridice, informatice sau de management.

Etapele implementării Regulamentului trebuie respectate întocmai și în permanență trebuie urmărită identificarea măsurilor de securitate ce se impun a fi implementate în vederea reducerii la minimum a riscurilor de acces neautorizat la date personale. Este introdus un nou instrument cu scopul a contribui la înlăturarea oricărui risc privind drepturile și libertățile peroanelor fizice – evaluarea impactului asupra protecției datelor anterior operațiunii de prelucrare.

În fine, întreaga reglementare se situează sub auspiciul principiului responsabilității, care presupune o serie de obligații ce incubă operatorului de date peresonale , menite să consolideze protecția drepturilor individuale, dar și să creeze oportunităț pentru alți profesioniști.