DANIEL-MIHAIL ŞANDRU
IRINA ALEXE
(Editori)

LEGISLAȚIA UNIUNII EUROPENE PRIVIND PROTECȚIA DATELOR PERSONALE

EDITURA UNIVERSITARĂ
Bucureşti, 2018

SUMAR

Punerea în aplicare a Regulamentului General privind Protecția Datelor 2016/679. Experiențe din România

The implementation of the General Data Protection Regulation 2016/679. Experience from Romania

Daniel-Mihail Şandru[1]
Irina Alexe[2]

Rezumat:

În continuarea activităților de cercetare din domeniul dreptului la o viață privată, respectiv al dreptului privind protecția datelor cu caracter personal, prezentul material reprezintă metodologic o cercetare privind consecințele intrării în vigoare a Regulamentului General privind Protecția Datelor (GDPR, acronimul englezesc) în România. Acest articol urmăreşte să pună în evidență efectele practice ale intrării în vigoare, cadrul normativ european, mult mai dezvoltat decât pare la prima vedere, precum şi eventualele implicații ale regulamentului, pentru judecătorul român.

Cuvinte cheie:

GDPR, judecător, protecția datelor, efecte practice, conformare; responsabil cu protecția datelor; sancțiuni.

Abstract:

In continuation of the research activities in the right to privacy field, namely the right to protect one's personal data, the present material is methodologically a research on the consequences of the General Data Protection Regulation's entry into force (also known as GDPR) in Romania. This article seeks to highlight the practical effects of the entry into force, the European normative framework, which is much more developed than it

[1] Prof. univ. dr. Universitatea Creştină „Dimitrie Cantemir", Universitatea din Bucureşti şi Universitatea Petru Maior, Tîrgu-Mureş; fondator şi coordonator al Centrului de Studii de Drept European (CSDE) din cadrul Institutului de Cercetări Juridice „Acad. Andrei Rădulescu" al Academiei Române; judecător ad-hoc la Curtea Europeană a Drepturilor Omului; adresa: Calea Victoriei, nr. 125, Sector 1, Bucureşti; e-mail: mihai.sandru@csde.ro mihaisandru.ro.

[2] Cercetător ştiințific asociat la Institutul de Cercetări Juridice „Acad. Andrei Rădulescu" al Academiei Române. Autor al unor volume şi articole în domeniu, ariile sale de interes vizează dreptul administrativ, dreptul constituțional şi dreptul european. Poate fi contactată la adresa irina_alexe@yahoo.com.

might seem at a first glance, as well as the possible implications of the regulation for the Romanian judge.

Keywords:
GDPR, judge, data protection, practical effects, compliance; data protection officer; sanctions.

I. Intrarea în vigoare a Regulamentului General privind Protecția Datelor

În continuarea activităților de cercetare din domeniul dreptului la o viață privată, respectiv al dreptului privind protecția datelor cu caracter personal, prezentul material reprezintă metodologic o cercetare privind consecințele intrării în vigoare a Regulamentului General privind Protecția Datelor (GDPR, acronimul englezesc). În precedentele două conferințe organizate în cadrul mureşean[3] am evidențiat teme centrale ale noului regulament, teme legate de fondul reglementării. Acest articol urmăreşte să pună în evidență efectele practice ale intrării în vigoare, cadrul normativ european, mult mai dezvoltat decât pare la prima vedere, precum şi eventualele implicații ale regulamentului, pentru judecătorul român.

Internetul şi noile tehnologii se găsesc într-un moment dual: pe de o parte dezvoltarea noilor tehnologii, pe de altă parte necesitatea reglementării. Reglementările se află şi ele (oarecum) la început, dar şi într-o stare de schimbare esențială, în mai multe domenii: neutralitatea internetului, protecția datelor, internetul lucrurilor (IoT). Protecția datelor este un subiect care a răsărit pe un teren neinclus în dezbaterile mari de până acum. Regulamentul privind protecția datelor reprezintă o declarație a drepturilor, chiar dacă teritorial ar părea cu efecte limitate. Cu toate acestea, datorită faptului că Regulamentul General privind Protecția Datelor se aplică tuturor cetățenilor europeni indiferent de sediul operatorilor, aplicarea teritorială devine în fapt globală. Protecția datelor pune în centru persoana

[3] Acest material a fost pregătit pentru Conferința Națională "*Impactul Regulamentului General privind Protecția Datelor (GDPR) în domeniul sănătății (ed. a III-a)*", organizată la data de 22 martie 2018, de Universitatea de Medicină şi Farmacie şi Universitatea Petru Maior, ambele din Tîrgu-Mureş. Ca urmare, majoritatea exemplelor din material sunt din domeniul medical, fără însă a le afecta aplicabilitatea în orice alt domeniu. Conferințele anterioare: *Conferința națională Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experienţelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679*, 17 martie 2017 şi Conferința internațională *Repere naționale şi internaționale în domeniul GDPR (Regulamentul General privind Protecția Datelor)*, 14 decembrie 2017, ambele organizate de Universitatea Petru Maior, Târgu-Mureş.

vizată, reglementările având rolul nu doar de a o proteja în fața valului de descoperiri tehnico-ştiinţifice, dar şi pentru a reglementa activitatea marilor organizații care prelucrează date cu caracter personal (magazine on-line, rețele sociale sau motoare de căutare).[4] În domeniul medical, regulamentul a explicitat pe larg, chiar în preambul, semnificația datelor cu caracter medical, printr-o listă exhaustivă de date: „Datele cu caracter personal privind sănătatea ar trebui să includă toate datele având legătură cu starea de sănătate a persoanei vizate care dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei vizate. Acestea includ informații despre persoana fizică colectate în cadrul înscrierii acesteia la serviciile de asistență medicală sau în cadrul acordării serviciilor respective persoanei fizice în cauză, astfel cum sunt menționate în Directiva 2011/24/UE a Parlamentului European şi a Consiliului[5]; un număr, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulară a acesteia în scopuri medicale; informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv din date genetice şi eşantioane de material biologic; precum şi orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea fiziologică sau biomedicală a persoanei vizate, indiferent de sursa acestora, ca de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro."

În România, directiva şi legea referitoare la protecția datelor s-au aplicat şi se interpretează de instanțele române, aspect dovedit de numărul mare de cauze soluționate.[6]

Nu toate problemele referitoare la informații, comunicare de informații publice sau confidențialitate sunt probleme de protecția datelor.

[4] Cei mai importanți jucători din mediul on-line FAMGA (Facebook, Apple, Microsoft, Google and Amazon) consideră că sunt dezavantajați de GDPR, însă sunt în căutarea soluțiilor tehnice şi a schimbării termenilor şi condițiilor pentru a se conforma regulamentului.

[5] Directiva 2011/24/UE a Parlamentului European şi a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45). Pe larg: **Gabriella Berki**, *Free Movement of Patients in the EU. A Patient's Perspective*, Intersentia, 2017.

[6] Peste 200 au fost analizate în: **Daniel-Mihail Şandru, Dragoş-Alin Călin, Constantin-Mihai Banu**, *Aplicarea şi interpretarea Directivei 95/46 de către instanțe române. Tipologii şi consecințe juridice*, în vol. **Irina Alexe, Nicolae-Dragoş Ploeşteanu, Daniel-Mihail Şandru (coordonatori)**, *Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experiențelor românești şi noile provocări ale Regulamentului (UE) 2016/679*, Editura Universitară, 2017, p. 41.

Toate acestea însă au implicații şi referitoare la protecția datelor. În special trebuie observate situațiile în care legi din domenii diferite (pază[7]) solicită informații care din punctul de vedere al regulamentul încalcă principiile referitoare la reducerea la minimum a datelor (art. 5 alin. 1 lit. c).

Potrivit art. 99 din regulament, intrarea în vigoare s-a făcut la 20 de zile de la publicarea în Jurnalul Oficial, urmând ca din 25 mai 2018 regulamentul să fie pus în aplicare.

II. Relația cu alte reglementări relevante

Regulamentul general privind protecția datelor face parte dintr-un sistem general de reglementare a informațiilor care se referă atât la domenii speciale de prelucrare a datelor cu caracter personal (datele în materie polițienească sau datele privind pasagerii) dar şi comerțul electronic. Relațiile dintre aceste acte normative, precum şi între acestea şi documentele soft law vor face obiectul aplicării şi interpretării de către instanțe (naționale sau europene) şi de autorități publice.

Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor şi privind libera circulație a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului[8].

Directiva are termen de transpunere 6 mai 2018, dar în România nu a fost discutată până în prezent. Potrivit GDPR, „protecția persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice şi al prevenirii acestora, precum şi libera circulație a acestor date, face obiectul unui act juridic specific al Uniunii.” (considerentul (19)) Regulamentul nu se aplică activităților de prelucrare în aceste scopuri, prelucrarea fiind reglementată printr-un „act juridic mai specific al Uniunii”, şi anume Directiva (UE) 2016/680. Statele membre au rol important în delimitarea competențelor precum şi a definirii anumitor direcții de aplicare între Regulamentul 679 şi Directiva 680.

Directiva (UE) 2016/681 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele

[7] Legea nr. 333/2003 *privind paza obiectivelor, bunurilor, valorilor şi protecția persoanelor,* modificată şi completată.
[8] JO L 119, 4.5.2016, p. 89–131.

pasagerilor (PNR) pentru prevenirea, depistarea, investigarea şi urmărirea penală a infracţiunilor de terorism şi a infracţiunilor grave[9].

Potrivit art. 13 din Directivă, aceasta nu aduce atingere aplicabilității Regulamentului „în ceea ce priveşte prelucrarea datelor cu caracter personal de către transportatorii aerieni, în special obligația acestora de a lua măsuri tehnice şi organizatorice adecvate pentru a proteja securitatea şi confidențialitatea datelor cu caracter personal".

Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității şi comunicațiilor electronice)[10].

Raportul acestei directive cu Regulamentul este subliniat în considerentul (173) în care se reaminteşte că este necesar ca aceste acte normative să fie puse în concordanță. Se pare că este o întârziere în adoptarea Regulamentului care să înlocuiască Directiva 2002/58.

Directiva 2000/31/CE privind anumite aspecte juridice ale serviciilor societății informaționale, în special ale comerțului electronic, pe piața internă (directiva privind comerțul electronic).

Regulamentul „nu aduce atingere aplicării Directivei 2000/31/CE, în special normelor privind răspunderea furnizorilor de servicii intermediari, prevăzute la articolele 12-15". De altfel, Directiva 2000/31 stipula că nu se aplică în „chestiunile referitoare la serviciile societății informaționale reglementate de Directivele 95/46/CE şi 97/66/CE".

Regulamentul nr. 45/2001 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile şi organele comunitare şi privind libera circulație a acestor date.[11]

Potrivit art. 1 alin. 3 „pentru prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile şi agențiile Uniunii, se aplică Regulamentul (CE) nr. 45/2001. Regulamentul (CE) nr. 45/2001 şi alte acte juridice ale Uniunii aplicabile unei asemenea prelucrări a datelor cu caracter personal se adaptează la principiile şi normele din prezentul regulament în conformitate cu articolul 98."[12]

---

[9] JO L 119, 4.5.2016, p. 132–149.

[10] Ediție specială în limba română, cap. 13, vol. 036, p. 63-73. Este în procedură de abrogare şi înlocuire cu un regulament. Detalii: http://eur-lex.europa.eu/procedure/EN/2017_3

[11] Ediție specială în limba română: Capitolul 13 Vol. 030, p. 142 – 164.

[12] Art. 98 are ca denumire marginală " *Revizuirea altor acte juridice ale Uniunii în materie de protecție a datelor*". Potrivit acestui articol, "dacă este cazul, Comisia prezintă propuneri legislative în vederea modificării altor acte juridice ale Uniunii privind protecția datelor cu caracter personal, în vederea asigurării unei protecții uniforme şi consecvente a persoanelor fizice în ceea ce priveşte prelucrarea. Acest lucru priveşte în special normele referitoare la

III. Forța juridică a actelor şi documentelor aplicabile în materia protecției datelor personale

Este semnificativ să discutăm forța juridică a diferitelor instrumente aplicabile în materia protecției datelor. Dacă despre regulament şi directivă[13] lucrurile sunt (relativ) clare, avizele şi documentele de lucru ale Grupului de Lucru art. 29[14] vor ocupa un loc central în analiză.

Temeiul esențial este art. 16 TFUE, urmat de art. 8 din Carta Drepturilor Fundamentale a Uniunii Europene (CDFUE).[15]

Forța juridică a opiniilor/ ghidurilor adoptate de Grupul de lucru art. 29 este aceea de recomandare. Însă, dacă observăm cauza *Grimaldi*,[16] documentele cu caracter de recomandare se impun instanțelor naționale. Recent a fost observat faptul că, deşi nu a fost citat, unul din documentele Grupului de lucru „Art. 29" a fost utilizat în cauza Nowak[17].

Preambulul Regulamentului este esențial pentru interpretarea şi aplicarea acestuia. Preambulul aduce, în unele situații, importante precizări, pe care Curtea de Justiție, le va utiliza la momentul potrivit.

Va fi foarte importat de stabilit raportul dintre regulament şi legislația specială, atunci când există un conflict normativ privind protecția datelor.[18]

---

protecția persoanelor fizice în ceea ce priveşte prelucrarea de către instituțiile, organismele, oficiile şi agențiile Uniunii, precum şi normele referitoare la libera circulație a acestor date."

[13] **Irina Alexe, Constantin Mihai Banu**, *De la directivă la regulament în reglementarea, la nivelul Uniunii Europene, a protecției datelor cu caracter personal*, în vol. **Irina Alexe, Nicolae-Dragoş Ploeşteanu, Daniel-Mihail Şandru (coordonatori)**, *Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experiențelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679*, Editura Universitară, 2017, p. 14 şi urm.

[14] Pentru o analiză a atribuțiilor Grupului de lucru „Art.29" dar şi a Comitetului European pentru Protecția Datelor, care îl va înlocui, a se vedea **Irina Alexe**, *Reforma instituțională, în materia protecției datelor, la nivel european*, în vol. **Andrei Săvescu,** *Regulamentul general privind protecția datelor. Comentarii şi explicații,* Editura Hamangiu, 2018 (în curs de publicare).

[15] Pentru o evidențiere a rolului Curții de Justiție în interpretarea articolelor din tratat şi CDFUE, a se vedea, **Adriana Maria Şandru**, *Privire critică asupra jurisprudenței Curții de Justiție a UE referitor la interpretarea art. 8 privind protecția datelor cu caracter personal din Carta drepturilor fundamentale a Uniunii Europene (CDFUE)*, Pandectele române, nr. 1/2018 (în curs de publicare).

[16] Cauza 322/88, Grimaldi / Fonds des maladies professionnelles, hotărârea din 13 decembrie 1989, ECR 1989 p. 4407, ECLI:EU:C:1989:646.

[17] C-434/16, Nowak, hotărârea din 20 decembrie 2017, ECLI:EU:C:2017:994.

[18] Alte obligații, care au natură juridică diferită de GDPR pot fi analizate separat, sau în contextul afectării datelor personale, dacă prin comportamentul reglementat se ajunge la încălcarea protecției datelor. De ex. obligația de confidențialitate este reglementată de art. 653 din Legea nr. 95/2006, potrivit căruia personalul medical răspunde civil şi pentru toate prejudiciile ce decurg din nesocotirea obligației de confidențialitate. A se vedea şi **Bianca Luntraru**, *Protecția datelor pacienților in sistemul medical*, în vol. **Irina Alexe, Nicolae-**

IV. Starea de fapt în privința protecției datelor cu caracter personal.

Starea de fapt, reflectată în multe articole ştiinţifice, dar şi în practica din România şi alte state, este incertitudinea. Sunt prea multe dispoziții vechi care, coroborate cu puținele noutăți, dau o astfel de rezultantă. Este subliniată în primul rând necesitatea pregătirii, nu doar a operatorului şi a desemnării unui responsabil pentru protecția datelor dar şi a salariaților care operează în mod direct cu datele personale, iar în domeniul medical aproape a tuturor salariaților.[19]

Sunt multe cercetări sociologice din care rezultă că organizațiile nu sunt pregătite. Oricare ar fi sursa cercetării, de mai mică sau de mai mare amploare, concluziile sunt aceleaşi: gradul de pregătire a angajaților este scăzut, pregătirea organizațiilor pentru desemnarea unui responsabil cu protecția datelor este abia la început şi nu se cunosc dispozițiile esențiale ale Regulamentului 679/2016.

Astfel, într-o cercetare la nivel mondial,[20] care a avut în vedere răspunsurile a 745 de respondenți, reies câteva cifre:

– 78% consideră conformarea la normele de protecție şi de confidențialitate a datelor personale un motiv tot mai puternic de îngrijorare;

– 60 % dintre respondenții cu societăți în Uniunea Europeană au un plan de respectare a normelor GDPR;

– la nivel mondial, 33% dintre respondenți au în derulare un plan de aliniere la GDPR.

Un sondaj [21] arată că 78% din angajații din domeniul medical nu au cunoştințe despre securitate cibernetică sau protecția datelor.

În Irlanda mai puțin de 2 din 5 participanți la un sondaj sunt siguri că sunt pregătiți pentru GDPR. În timp ce majoritatea participanților consideră că principala problemă în aplicarea Regulamentului sunt proprii salariați, doar 18% au urmat programe de pregătire.[22]

Dragoş Ploeşteanu, Daniel-Mihail Şandru (coordonatori), *Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experiențelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679*, Editura Universitară, 2017, p. 247.

[19] A se vedea: **Bernadette John**, *Are you ready for General Data Protection Regulation?*, BMJ, 2018, p. 360; Articolul evidențiază rolul GDPR în domeniul medical.

[20] *EY - Global Forensic Data Analytics Survey 2018*, disponibil la adresa http://www.ey.com/gl/en/services/assurance/ey-global-forensic-data-analytics-survey-2018, p. 25-27. Sondajul s-a desfăşurat în perioada octombrie-noiembrie 2017.

[21] MediaPro a realizat sondajul ”2017 State of Privacy and Security Awareness Report” https://healthitsecurity.com/news/78-of-healthcare-workers-lack-data-privacy-security-preparedness. Interviul a fost realizat în SUA cu peste 1000 de respondenți.

[22] Sondajul a fost realizat de Irish Computer Society şi National Data Protection şi este disponibil la adresa http://www.techcentral.ie/less-2-5-sure-prepared-gdpr/

Potrivit unui alt studiu, care indică într-o oarecare măsură şi direcţiile de dezvoltare a domeniului protecţiei datelor, se arată că 79% dintre cetăţenii europeni nu sunt la curent cu intrarea în vigoare a GDPR. Cu toate acestea, 82% dintre aceştia spun că vor încerca să-şi protejeze drepturile, să aplice GDPR, ori să solicite ştergerea datelor.[23]

V. Drepturile şi obligaţiile operatorilor

Etapele pentru conformarea la cerinţele GDPR.

Dacă modificările GDPR nu sunt multe faţă de dispoziţiile directivei, totuşi acestea sunt foarte importate. De la amenzi, la probarea îndeplinirii principiilor, trecând prin numirea unui responsabil cu protecţia datelor şi resurse pentru satisfacerea drepturilor persoanelor vizate (portabilitate, ştergerea datelor, dreptul la acces). În consecinţă conformarea cu noile reguli de protecţia datelor este esenţială atât pentru evitarea unor sancţiuni, dar, în unele situaţii, şi pentru mai buna funcţionare a organizaţiei.

Prima etapă este a stabilirii dacă organizaţia prelucrează **date cu caracter personal**[24] la un nivel la care să atragă obligativitatea desemnării unui responsabil cu protecţia datelor. Dacă desemnarea DPO este obligatorie, următoarele etape ar trebui parcurse împreună cu acesta. Dacă desemnarea DPO nu este obligatorie potrivit reglementărilor, însă organizaţia are dubii cu privire la desemnarea acestuia, este mai bine să fie desemnat unul.[25]

Stabilirea tipurilor de conţinut de date cu caracter personal. Nu trebuie evitată nicio sursă de date dintre cele pe care organizaţia le deţine. Trebuie stabilite locurile fizice în care sunt depozitate datele cu caracter personal sau sursele electronice. În acest din urmă caz trebuie stabilite atât sursele cu date personale cât şi persoanele care au acces la aceste date. Va fi realizată o listă, pe departamente, cu persoanele care vor avea acces la anumite fluxuri de informaţii. Angajaţii care operează cu datele cu caracter personal trebuie instruiţi în mod special, atât în privinţa operaţiunilor curente cât şi în privinţa limitelor competenţelor acestora. Trebuie observat

---

[23] EU Consumers Poised to Take Back Control of Personal Data from Businesses, According to Pega Survey on GDPR, https://www.pega.com/about/news/press-releases/eu-consumers-poised-take-back-control-personal-data-businesses-according

[24] ”Date cu caracter personal” înseamnă orice informaţii 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 identităţii sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale (art. 1 lit. a).

[25] **Irina Alexe**, *Principalele noutăţi privind responsabilul cu protecţia datelor, incluse în GDPR*, Pandectele române, nr. 1/2018 (în curs de publicare).

unde sunt ţinute atât datele fizice (pe hârtie) cât şi datele informatice, atât în cloud (dacă accesul este gratuit riscurile sunt aproape toate în sarcina operatorului) sau pe servere, cât şi stocate în calculatoarele organizației. În cazul în care există un contract pentru cloud/ servere, acesta trebuie să se refere expres la securitate şi riscuri legate de protecția datelor. Operatorul ar trebui să cunoască datele fizice cu privire la servere pentru a nu avea probleme referitoare la prelucrarea datelor sau transferul datelor în afara UE.

Verificarea surselor datelor cu caracter personal deținute/ obținute de organizație înainte de intrarea în vigoare a Regulamentului. Dacă până la intrarea în vigoare a regulamentului nu există posibilitatea stabilirii surselor deținerii datelor cu caracter personal, se va verifica dacă aceste date sunt prelucrate în condiții de legalitate (art. 6) precum şi dacă sunt respectate celelalte principii GDPR (art. 5).

Sunt cel puțin două categorii de date: ale propriilor angajați şi ale terților (clienți). În privința salariaților, regulamentul are reglementări proprii mergând până la declararea ca dată sensibilă apartenența la un sindicat, problemă pe care angajatorul va trebui să o rezolve, conform art. 9. În cadrul relației angajator angajat trebuie observate şi alte date sensibile, cum ar fi cele medicale, de orice natură; de exemplu, cele care privesc motivele absențelor pentru recuperarea medicală. Transmiterea diagnosticului către angajator este în afara protecției datelor personale,[26] cu excepțiile rezultate din interpretarea art. 9 alin. 2 lit. h. Datele cu caracter personal ale clienților sunt foarte importante mai ales dacă acestea sunt utilizate în vederea obținerii de beneficii de către organizația care le deține. Toate modalitățile de prelucrare a datelor cu caracter personal trebuie să fie atent realizate. În toate situațiile, înainte de utilizarea unui soft, aceste modalități trebuie evaluate printr-o procedură care să evalueze riscurile,[27] precum şi fluxul de date.

Desemnarea DPO se realizează conform prevederilor legale pentru personalul angajat, în cadrul raporturilor de muncă, sau în afara raporturilor de muncă, prin încheierea unui contract de servicii prevăzut de art. 37 alin. 6.[28] De asemenea, este necesar ca, indiferent de modalitatea de desemnare a

[26] A se vedea: HM Revenue & Customs, *Guidance Statutory Sick Pay: employee fitness to work*, disponibil la adresa https://www.gov.uk/guidance/statutory-sick-pay-employee-fitness-to-work. Bolile şi GDPR sunt elemente surpriză pentru economiştii care calculează „Full-time equivalent (FTE)" sau „whole time equivalent (WTE)".

[27] De exemplu, cunoscutul snapchat a fost identificat ca nefiind sigur pentru pacienți. **Sohini Patel, Susan Bewley, Nathan Hodson**, *Snapchat is not for sharing*, BMJ 2016; 352.

[28] **Irina Alexe**, *Responsabilul cu protecția datelor (DPO) - funcționar public sau personal contractual?*, RRDM, nr. 2/2018 (în curs de publicare).

unui responsabil cu protecția datelor (în cadrul sau în afara raporturilor de muncă – funcționar public, personal contractual sau parte a unui contract de servicii, cu normă întreagă sau *part-time*, prevăzându-i un post distinct în cadrul organizației, sau prin cumul de funcții, ori desemnându-l ca şef al unei structuri specializate, sau ca reprezentant unic al unui grup de societăți, ori ca reprezentant unic al mai multor autorități sau organisme publice), acestuia să îi fie asigurate toate resursele, precum şi garanțiile necesare, prevăzute de Regulament, pentru a-şi îndeplini sarcinile.

Certificarea DPO. Certificarea cea mai sigură provine din încredere şi cunoştințele DPO dar deocamdată, în România, certificarea DPO este la început. Primul pas a fost făcut în luna noiembrie 2017 când ocupația de responsabil pentru protecția datelor a fost inclusă în Clasificarea Ocupațiilor din România (COR) însă până la certificare calea este lungă şi se aşteaptă cu nerăbdare parcurgerea acesteia.

Raporturile cu **împuternicitul** sunt raporturi contractuale, care nu-l exonerează total de răspundere pe operator. Împuternicitul trebuie să ofere garanții suficiente, în sensul regulamentului, iar contractul dintre operator şi persoana împuternicită trebuie să conțină cel puțin cerințele prevăzute de regulament, ce vizează elementele esențiale ale contractului, drepturile şi obligațiile părților, confidențialitatea sau interzicerea delegării activității delegate, fără acordul prealabil al operatorului.

Modificarea structurii organizaționale. Ulterior desemnării unui DPO, organizația trebuie să-şi modifice actele interne: regulament de organizare şi funcționare, regulament de organizare internă, organigramă, contract colectiv de muncă. DPO trebuie „amplasat" în relație apropiată cu conducerea organizației, într-o organizare autonomă.[29] În unele situații trebuie concepută şi relația cu alte entități de profil, cum este situația în domeniul medical.[30]

Relația cu autoritatea de protecția datelor, mai precis, în România relația cu Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal este foarte importantă şi trebuie să aibă în vedere:

- comunicarea datelor de contact ale responsabilului cu protecția datelor;

[29] Cu privire la raportul dintre responsabilul cu protecția datelor (DPO) şi personalul tehnic (aşa numitul departament IT): **Laurence Eastham**, *Data Protection: ICO Charges under the GDPR*, 30.10.2017, https://www.scl.org/blog/10043-data-protection-ico-charges-under-the-gdpr

[30] **Louise H. K. Blume, Nico J. H. W. van Weert, Jamiu O. Busari, Annemiek M. V. Stoopendaal, Diana M. J. Delnoij**, *What hospitals need to know about guidelines—A mixed-method analysis of guideline implementation in Dutch hospitals*, Journal of Evaluation in Clinical Practice, vol. 23, 6/2017, p. 1266–1273.

- notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal.

În raport cu autoritatea, operatorul are dreptul a de fi consiliat. Deşi considerentul (129) din Preambul se referă la persoane vizate, acesta nu exclude şi o relație coerentă cu operatorii şi împuterniciții (”competențe de autorizare şi de consiliere, în special în cazul plângerilor depuse de persoane fizice”). În cadrul art. 36 „autoritatea de supraveghere oferă consiliere în scris operatorului”, în anumite condiții şi în anumite termene. În special alin. 3 din art. 58 enumeră tipurile de competențe în materia consilierii.

Fără a intra în detalii prind sancțiunile, trebuie remarcat faptul că, pe de o parte, Regulamentul[31] stabileşte condiții generale pentru impunerea amenzilor administrative, iar pe de altă parte, realizează o tipologie a sancțiunilor. Rolul autorităților naționale va fi foarte important în aplicarea Regulamentului. Şi, desigur, al Curții de Justiție, în eventuale cereri privind pronunțarea unor decizii preliminare.[32]

Verificarea conformării cu GDPR din punctul de vedere al prelucrării datelor. Acest lucru priveşte îndeosebi consimțământul în situațiile art. 6 lit. a dar şi în celelalte situații în care prelucrarea s-a realizat fără acordul persoanei vizate. Conformarea se referă la numirea DPO, realizarea procedurilor şi a fluxurilor de date; fiecare element al regulamentului trebuie respectat.

Programele informatice de conformare. Dincolo de toate aceste reglementări, mai mult sau mai puțin detaliate, trebuie să avem în vedere că nu există rețete de verificare şi aplicare universale. Bineînțeles, indicatori şi chestionare privind gradul de conformare, disponibile în număr foarte mare pe internet, ar putea fi utile. Însă toate acestea au o limitare serioasă care provine din specificul fiecărei organizații. Niciun produs software nu este pe deplin util dacă nu a fost pregătit pentru o anumită entitate, după ce au fost stabilite fluxurile de informații şi procedurile proprii. Şi, în toată ecuația, cu toate softurile achiziționate, cea mai importată resursă sunt oamenii pregătiți pentru prelucrarea legală a datelor cu caracter personal.

---

[31] **Irina Alexe**, *Regimul sancționator prevăzut de Regulamentul (UE) 2016/679 privind protecția datelor cu caracter personal*, Curierul Judiciar, nr. 1/2018, p. 36.

[32] Pentru trimiterile preliminare din România, a se vedea: **Daniel-Mihail Şandru**, *Importanța trimiterilor preliminare în materia protecției datelor cu caracter personal. Cauze semnificative şi experiențe românești*, Revista Română de Drept al Afacerilor, nr. 4/2017, p. 157-167.

VI. Drepturile şi obligaţiile persoanelor vizate

Drepturile persoanelor vizate nu sunt absolute.[33] Acest drept la protecția datelor intră în conflict cu alte drepturi, uneori dreptul la protecția datelor fiind mai puțin preferat între valorile sociale protejate în legislație. Explicațiile derivă din faptul că, mai ales în actuala stare a tehnicii şi mai ales a dezvoltării internetului, o insularizare a ființei umane este (aproape) imposibilă, sau cu efecte foarte complicate. Internetul a introdus celeritate şi comoditate dar a adus şi riscurile care sunt presupuse de accesul la această rețea informațională. Cu atât mai mult în constituirea comunităților virtuale, unde persoanele vizate renunță de bunăvoie la propria protecție a vieții private.[34]

Începând cu 25 mai persoanele vizate vor solicita aplicarea GDPR. Poate nu va fi o presiune din partea autorităților publice, a Comisiei Europene sau a autorităților naționale, cât fi din partea persoanelor vizate.

Regulamentul prevede în considerentul 59 exercitarea de către persona vizată a dreptului la acces, a dreptului la rectificarea şi ştergerea datelor precum şi exercitarea dreptului la opoziție.[35]

O persoană vizată ar trebui să aibă drept de acces la datele cu caracter personal colectate care o privesc şi ar trebui să îşi exercite acest drept cu uşurință şi la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare şi pentru a verifica legalitatea acesteia (considerentul (63)). Operatorul ar trebui să ia toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online şi al identificatorilor online. Un operator nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale (considerentul (64)).

---

[33] Considerentul (4) din Regulament. A se vedea şi analiza recentă din articolul **Lothar Determann**, *No One Owns Data*, UC Hastings Research Paper No. 265 (February 14, 2018), disponibil la https://ssrn.com/abstract=3123957

[34] Pe larg, **Daniel Mihail Şandru**, *Imposibila coexistență între protecția datelor şi comunitățile virtuale? Ce urmează?*, Pandectele române, nr.1/2018 (în curs de publicare). Referindu-se la controlul asupra informației, Pedro Cruz Villalón, afirmă că acesta este uneori irealizabil: ”din momentul în care un conținut informațional este postat pe internet, particularii se transformă imediat, voluntar sau involuntar, în distribuitori de informații prin rețele de socializare, prin comunicare electronică, prin linkuri, prin bloguri sau prin orice alte mijloace oferite de internet.” (par. 47 din Concluziile Avocatului General Pedro Cruz Villalón prezentate la 29 martie 2011 în cauzele conexate C-509/09 şi C-161/10).

[35] ”Operatorul ar trebui să ofere, de asemenea, modalități de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate şi cel târziu în termen de o lună şi, în cazul în care nu intenționează să se conformeze respectivelor cereri, să motiveze acest refuz.” (consid. 59)

Dreptul de a fi informat cu privire la încălcarea securității datelor (art. 34) este oarecum limitat pentru că regulamentul consideră că se poate face şi o informare publică atunci când costurile nu ar fi rezonabile.

Dreptul la ştergere trebuie realizat în limitele regulamentului şi trebuie verificată distincția dintre consimțământul acordat pentru încheierea contractului şi consimțământul privind prelucrarea datelor personale. Dreptul la ştergere nu ar trebui să fie exercitat abuziv; ştergerea (distrugerea) datelor se face cu responsabilitatea operatorului.[36]

”**Dreptul la portabilitatea datelor** are două componente: dreptul persoanei vizate de a primi ea însăşi datele (art. 20 alineatul 1 RGPD) şi dreptul de a solicita ca datele să fie transferate direct unui alt operator (art. 20 alineatul 2 RGPD).”[37]

VII. Interpretarea şi aplicarea Regulamentului 2016/697 de către instanțele române

Dreptul la ştergerea datelor („dreptul de a fi uitat”)

Într-o cauză soluționată definitiv,[38] instanța face referire la art. 8 alin. 1 şi 2 CDFUE, art. 17 alin. 1 din Regulament[39], după care se subliniază că „dispozițiile art. 17 din regulament reglementează „*dreptul de a fi uitat*”, drept ce constă în dreptul persoanelor de a cere eliminarea completă a datelor lor atunci când acestea nu mai sunt folositoare pentru scopurile în care au fost colectate ori chiar postate de bunăvoie, precum şi atunci când utilizatorul retrage consimțământul publicării lor.” În continuare se face referire la reglementarea națională (”Totodată, conform art. 14 alin. 1 lit. a) din Legea 677/2001”). Urmează şi motivarea instanței:

„Punând în balanță dreptul la viața privată şi la protecția datelor reclamantului şi dreptul la libertatea de exprimare, în speță, libertatea presei,

---

[36] Google, probabil cea mai mare organizație care prelucrează date cu caracter personal a raportat că a de-listat aproape două milioane şi jumătate de link-uri: **Nicolas Vega**, *Google gets 2.4M requests from Europeans to be 'forgotten'*, New York Post, 28.02.2018, By https://nypost.com/2018/02/27/google-gets-2-4m-requests-from-europeans-to-be-forgotten/. Desigur este o problemă de balanță a valorilor: libertatea de exprimare vs. dreptul la viață privată, problemă greu de rezolvat.

[37] **Andreea Lisievici**, Dreptul la portabilitatea datelor potrivit Regulamentului General privind Protecția Datelor, în vol. **Irina Alexe, Nicolae-Dragoş Ploeşteanu, Daniel-Mihail Şandru (coordonatori)**, *Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experiențelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679*, Editura Universitară, 2017, p. 146.

[38] Judecătoria Sectorului 3 București, Sentința civilă nr. 3731/27.03.2017, nepublicată, disponibilă la adresa http://rolii.ro/hotarari/590b19dde490098c890000ec

[39] Forma în care instanța (nota citată supra) face referire este foarte importantă întrucât aplică regulamentul: ” De asemenea, art. 17 alin. 1 din Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016, prevede că (...)”.

instanța consideră că primează primul drept la care s-a făcut referire. Astfel, având în vedere că articolul publicat la data de 27.09.2006, în care se face referire la numele reclamantului, nu mai este de actualitate şi nici nu prezintă informații care să fi fost de interes național şi care să fi prezentat o problemă îndelung mediatizată la acea dată, instanța consideră că nu se mai impune menținerea acestuia pe pagina de internet a publicației „România Liberă". Menținerea în continuare a articolului în spațiul on-line ar reprezenta o ingerință în dreptul reclamantului la protecția datelor ce nu mai este proporțională cu scopul urmărit.

Mai mult, instanța va avea în vedere şi faptul că pârâta a achiesat pretențiilor reclamantului, recunoscând că respectivul articol prezintă informații care, cu trecerea timpului (peste 10 ani) au dobândit caracter nesemnificativ."

Hotărârea aceasta, pronunțată după intrarea în vigoare a Regulamentului, dar înainte de punerea în aplicare, soluționează mai degrabă echitabil cererea decât să aibă în vedere aplicarea dispozițiilor legale.

Exceptarea persoanelor juridice de la aplicarea Regulamentului.

O altă cauză, care a opus Registrul Comerțului şi Autoritatea de protecție a datelor, a avut ca obiect anularea unui act administrativ (contestarea unei sancțiuni). Registrul Comerțului s-a apărat invocând că a aplicat reglementari europene,[40] şi în plus

„Consimțământul persoanei vizate nu era necesar conform art. 5 alin. 2 lit. c şi f din Legea nr. 677/2001. Judecătorul delegat este cel care stabileşte documentele care trebuie depuse pentru înregistrarea unei societăți, astfel încât susținerea intimatei cum că ar fi fost eliberate copii după înscrisuri care nu erau obligatorii a fi depuse în vederea efectuării înregistrărilor referitoare la modificarea sediului societății este neîntemeiată, întrucât ONRC nu are această atribuție. Publicitatea realizată prin registrul comerțului are la bază Directiva 2009/101/CE şi trebuie să permită terților să cunoască datele esențiale ale societăților comerciale şi alte informații privind societatea. Considerentul 14 din Regulamentul nr. 679/2016 privind protecția persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal prevede că acest regulament nu se aplică prelucrării datelor cu caracter personal care

[40] Tribunalul București, Secția a II a – Contencios Administrativ şi Fiscal, Sentința civilă nr. 24 din 08.01.2018, nepublicată, disponibilă la adresa http://rolii.ro/hotarari/5a7286f6e490095421000b3a; a se vedea şi Curtea de Apel Bucureşti, Secția de Contencios Administrativ şi Fiscal, Sentința civilă nr. 132/24.10.2017, disponibilă la adresa http://rolii.ro/hotarari/5a3099fbe49009580b000038