Logos Universality Mentality Education Novelty: Law
ISSN: 2284-5968 | e-ISSN: 2458-1046
Covered in: ERIH PLUS, HeinOnline, CEEOL, Index Copernicus, CrossRef, CrossCheck, J-GATE, Google Scholar, Ideas RePeC, Econpapers, Socionet, KVK, WorldCat.

2019, Volume 7, Issue 1, pages: 67-84 | doi: 10.18662/lumenlaw/20

Informing the Data Subject: Applying the Provisions in the (UE) 2016/679 Regulation. The Practitioner's Perspective

[Informarea persoanei vizate: aplicarea dispozițiilor din regulamentul (UE) 2016/679. Perspectiva practicianului]

Daniela SIMIONOVICI[1]

[1]Stefan cel Mare University of Suceava, Romania; LUMEN Research Center in Social and Humanistic Sciences, Iasi, Romania, dsimionovici@gmail.com

Abstract: Informing the data subject in the procedure required by Regulation (EU) 2016/679 on the protection of personal data is often confused by practitioners in GDPR with the process of obtaining informed consent. Apart from this, which gives rise to discussions on the necessity of requiring specialists in GDPR to do courses dedicated to the field, the issue of information raises a number of issues in practice, marked by blurring, non-uniform interpretations or even a void of interpretation, much as the current legal doctrine and not only is relatively poor in materials that concern the field of personal data protection, and the practice of the National Supervisory Authority for Personal Data Processing under the new EU Regulation is still in its infancy. This article aims to address a series of dilemmas encountered in the GDPR practice by providing theoretical explanations and examples to facilitate the access of practitioners to the essence of institutions that inform the target person.

Keywords: *personal data protection; informing the data subject; (UE) 2016/679 Regulation.*

How to cite: Simionovici, D. (2019). Informing the Data Subject: Applying the Provisions in the (UE) 2016/679 Regulation. The Practitioner's Perspective. *Logos Universality Mentality Education Novelty: Law, 7*(1), 67-84. doi:10.18662/lumenlaw/20

I. Introducere

Protecţia datelor cu caracter personal este un drept fundamental, aşa cum este prevăzut în Art. 8 din Carta drepturilor fundamentale a Uniunii Europene (PE, CUE, & CE, 2012), la fel ca demnitatea umană, dreptul la viaţă sau dreptul la integritate al persoanei. Protecţia datelor private, astfel cum s-a arătat în literatura de specialitate (Şandru, 2016), este un drept care ţine de protecţia dreptului mai larg la viaţă privată.

Datele cu caracter personal nu trebuie să fie doar protejate, ci şi folosite, adică prelucrate în mod corect.

Prin prevederile sale, Regulamentul (UE) 2016/679 şi toată legislaţia europeană şi naţională în domeniu se asigură că datele cu caracter personal, atât timp cât pot duce la identificarea persoanei vizate şi, mai ales dacă printr-o prelucrare necorespunzătoare prezintă orice fel de riscuri pentru persoana vizată, sunt prelucrate şi corect protejate, fie că sunt luate individual, ca identificatori sau în orice combinaţie a acestora, fie că sunt obţinute direct de la persoana vizată sau din orice altă sursă.

Sancţiunile foarte dure prevăzute de Regulament pentru încălcarea prevederilor sale referitor la protecţia datelor cu caracter personal ne fac să înţelegem cel puţin două lucruri:

– protecţia datelor cu caracter personal este un imperativ;

– protecţia datelor cu caracter personal este un imperativ pentru că încă nu este o normă internalizată şi trebuie reglementată „din afară".

În doctrina juridică (Ungureanu, 2018) s-a arătat că există două căi în care dreptul la protecţia datelor cu caracter personal poate fi apărat: calea administrativă, care presupune dreptul persoanei vizate de a formula o plângere către autoritatea naţională competentă, sau calea judiciară, care presupune dreptul persoanei de a sesiza instanţa cu privire la încălcarea drepturilor sale de către operatorul de date, persoanele care efectuează controlul activităţii acestuia sau chiar împotriva autorităţii de control.

Neglijenţa sau indiferenţa în ce priveşte modul cum tratăm şi folosim datele noastre cu caracter personal sau pe ale celorlalţi şi riscurile care decurg din aceste comportamente au impus apariţia unor mecanisme exterioare care să ne protejeze şi sub acest aspect. Se preconizează (Brkan, 2015) că, pe măsură ce Regulamentul va fi aplicat, gradul de conştientizare a publicului asupra dreptului la protecţia datelor cu caracter personal va creşte şi, pe cale de consecinţă, va creşte şi numărul de cazuri în care se va solicita o protecţie eficientă a acestui drept.

Punerea în aplicare a Regulamentului începând cu 25 mai 2018 a generat ample mişcări pentru conformarea cu prevederile sale şi în România,

datorită mediatizării cu accente de marketing stridente tocmai pe sancţiunile foarte dure prevăzute pentru nerespectarea drepturilor persoanelor privind protecţia datelor cu caracter personal (UE 2016/679: art. 83, alin. 4 şi 6).

Oferta mare de cursuri de pregătire în acest domeniu şi dobândirea competenţelor specifice domeniului nu înseamnă, însă, în mod necesar, că se realizează corespunzător şi conformarea cu prevederile Regulamentului.

Datorită experienţei dobândite ca practician în acest domeniu, am observat că mulţi operatori de date cu caracter personal, fie nu fac informarea persoanei vizate, fie solicită consimţământul persoanei vizate făcând doar o informare superficială a persoanei şi consideră că şi-au îndeplinit obligaţia de a informa persoana vizată despre ce urmează să se întâmple cu datele sale.

Mai mult, sunt operatori care substituie consimţământul cu informarea, adică fac confuzie între informarea persoanei vizate, ca fiind doar unul dintre drepturile persoanei vizate pe care operatorul este obligat să le respecte, şi solicitarea consimţământului persoanei pentru prelucrarea datelor cu caracter personal, care este doar unul din cele 6 temeiuri legale de prelucrare a datelor cu caracter personal.

Atunci când prelucrarea datelor se face în baza art. 6, alin. (1), lit. a „persoana vizată şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice" (UE 2016/679: art. 83, alin. 4 şi 6) şi lipseşte informarea, indiferent din ce cauze, sau informarea este incompletă sau chiar superficială, prelucrarea devine ilegală, consimţământul fiind viciat.

Se acordă foarte multă importanţă obţinerii consimţământului persoanei vizate, deşi prelucrarea datelor cu caracter personal se poate face şi pe alte temeiuri legale, şi nu se acordă atenţia cuvenită informării persoanei vizate, care este obligatorie, indiferent de temeiul în baza căruia se face acest lucru.

Această practică nu este doar sancţionată de Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP, n.d.a), ci ridică şi serioase probleme de etică.

II. Importanţa pregătirii profesionale adecvate a persoanei care îndeplineşte funcţia de DPO

Garantarea unui drept recunoscut şi legiferat ca fiind fundamental, cum este cel la protecţia datelor cu caracter personal, presupune nu doar aplicarea unor prevederi legale, ci şi o muncă susţinută pentru „traducerea" GDPR într-un limbaj accesibil oricui, fie operator, fie împuternicit al

acestuia, fie responsabil cu protecţia datelor sau persoană vizată, tocmai datorită unor prevederi „atipice". Aceasta deoarece, aşa cum s-a arătat în doctrină (Ungureanu, 2017), domeniul GDPR se află la graniţa dintre dreptul public şi dreptul privat, întrucât combină, foloseşte şi pune în aplicare instituţii şi mecanisme din mai multe ramuri ale dreptului: drept civil, penal, administrativ, drepturile omului etc.

Datorită GDPR a apărut pe piaţă o nouă categorie de profesionişti, cea a responsabililor cu protecţia datelor cu caracter personal, sau DPO (Data Protection Officer). Sarcinile şi responsabilităţile acestora sunt stabilite în Regulament şi, ceva ce în teorie ar fi trebuit să stabilească nişte repere clare, fixe, aproape rigide, în practică s-au dovedit a fi nişte jaloane mobile, flexibile.

În lucrarea de faţă nu ne propunem să clarificăm aspectele legate de ce înseamnă să fii DPO, ce ţi se permite sau eşti obligat de către lege să faci şi care e realitatea din practicarea efectivă a meseriei.

Articolul 37, alin. (5) din Regulament prevede: "Responsabilul cu protecţia datelor este desemnat pe baza calităţilor profesionale şi, în special, a cunoştinţelor de specialitate în dreptul şi practicile din domeniul protecţiei datelor, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la articolul 39".

Din acest articol înţelegem că, exceptând situaţiile de conflict de interese, aşa cum a încercat WP 29 să ofere nişte repere (CE, n.d.a), DPO poate fi orice angajat sau prestator de servicii care:

a) e preferabil, dar nu obligatoriu să aibă studii juridice, ca specializare de bază, iar nivelul studiilor nu este menţionat deloc în Regulament, nici măcar ca recomandare;

b) este apt din punct de vedere profesional să îndeplinească sarcinile de lucru ale unui DPO.

Relativ la nivelul studiilor DPO, în România s-a încercat o reglementare ordonată (care rămâne, însă, discutabilă în opinia noastră), prin definirea ocupaţiei de Responsabil cu protecţia datelor cu caracter personal, s-a creat şi aprobat standardul ocupaţional aferent de către Autoritatea Naţională pentru Calificări (ANC, 2018) prin care se stabileşte nivelul studiilor necesare ca fiind superioare şi s-a alocat un număr de cod acestei profesii în Codul Ocupaţiilor din România (MMJS, n.d.).

Responsabilul cu protecţia datelor cu caracter pesonal este persoana din organizaţie / societate / instituţie care este angajată sau care activează pe baza unui contract de prestări servicii, care este desemnată pe baza calităţilor profesionale, în special, a cunoştinţelor de legislaţie şi a practicilor privind

protecţia datelor şi care are capacitatea de a îndeplini sarcinile specifice profesiei, în conformitate cu art. 39 din Regulamentul 679/2016.

Ţinând cont de cele prezentate anterior, putem afirma că, în România, poate ocupa postul de Responsabil cu protecţia datelor cu caracter personal orice angajat sau prestator de servicii, absolvent de studii superioare, indiferent de specializarea de bază, care este capabil să execute sarcinile DPO, aşa cum sunt ele prevăzute în art. 39 din Regulament. Prestatorii de servicii GDPR sunt obligaţi, prin urmare, ca persoana pe care o desemnează pentru gestionarea contractelor de prestări de servicii GDPR şi îndeplinirea sarcinilor şi atribuţiilor DPO, pentru şi în numele beneficiarului, să fie absolvenţi de studii superioare.

După 25 mai 2018, chiar la o cercetare sumară pe internet, oferta de prestări servicii GDPR este făcută mai ales de case de avocatură şi / sau avocaţi independenţi, de societăţi comerciale sau persoane fizice specializate pe activităţi de contabilitate şi / sau de resurse umane, fără ca acestea să fie, în mod necesar, autorizate pentru această activitate, care este corespunzătoare codului CAEN 7490 Alte activităţi profesionale, ştiinţifice şi tehnice n.c.a. (Alte Activităţi…, n.d.), chiar dacă această încadrare poate fi considerată doar o soluţie de compromis. Domeniul protecţiei datelor cu caracter personal impune definirea unui cod CAEN specific.

La nivelul judeţului Iaşi, spre exemplu, sunt înregistrate cu acest cod CAEN un număr de 117 agenţi economici, cu o pondere de 0,19% din totalul agenţilor economici din judeţul Iaşi (Alte Activităţi…, n.d.). Dintre aceste 117 societăţi, la nivelul judeţului Iaşi, doar şapte oferă servicii GDPR, pe lângă activităţile de bază care constau, de fapt, în consultanţă şi servicii SSM, SU, PSI, ISCIR, resurse umane, medicina muncii sau contabilitate etc.

Un pas important şi care merită menţionat este mobilizarea mediului academic universitar pentru acreditarea de cursuri postuniversitare dedicate formării de specialişti în domeniul protecţiei datelor cu caracter personal şi aici amintim Universitatea „Petru Maior" din Târgu-Mureş (n.d.), Universitatea Danubius din Galaţi (n.d.) şi Universitatea „Ştefan cel Mare" din Suceava (n.d.), care sunt primele – iar, la data redactării prezentului articol, sunt chiar singurele – centre universitare din România care au făcut paşi concreţi în satisfacerea cererii de cursuri de formare în această profesie. Instruirea / educaţia formală în acest domeniu ar fi de dorit să fie o condiţie obligatorie pentru desfăşurarea activităţii de DPO. Domeniul este mult prea vast şi complex şi, fiind „deschis" şi practicienilor non-jurişti, care nu au formarea şi dexteritatea juriştilor în lucrul cu conceptele juridice, este de dorit ca instituţiile de învăţământ să îşi diversifice oferta educaţională, pentru

ca persoanele interesate să poată practica această profesie în mod corespunzător instruite.

Faptul că poate profesa în acest domeniu orice persoană care a absolvit studii superioare, că nu se solicită, pentru practicarea profesiei, niciun fel de competenţe specifice, dobândite în urma absolvirii unui curs de GDPR – DPO la un furnizor de formare profesională autorizat ANC, că oferta de cursuri de specialitate organizate de furnizorii de educaţie este extrem de redusă, poate fi una dintre cauzele pentru care pot apărea numeroase erori şi confuzie în practica efectivă de realizare a informării privind prelucrarea datelor cu caracter personal şi, ulterior, de obţinere a consimţământului informat. Regulile privind autorizarea cursurilor de formare profesională pot fi accesate pe site-ul oficial al Agenţiei Naţionale pentru Calificări (http://site.anc.edu.ro/).

III. Informarea persoanei vizate

Informarea persoanei vizate privind prelucrarea datelor cu caracter personal este doar unul dintre drepturile a căror respectare este impusă de Regulament şi este un întreg proces, obligatoriu, transparent, care presupune responsabilitatea operatorului de a face dovada că informarea s-a efectuat.

III.1. Informarea persoanei vizate în baza art. 13, atunci când datele sunt obţinute direct de la persoana vizată

Pentru o mai bună explicitare a modului cum ar trebui să se efectueze informarea persoanei vizate despre prelucrarea datelor sale cu caracter personal, atunci când datele sunt obţinute direct de la persoana vizată, vom face o serie de comentarii punctuale plecând de la textul articolul 13 din Regulament (UE 2016/679: art. 13).

Articolul 13 alin. 1 prevede următoarele: ”în cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obţinerii acestor date cu caracter personal, furnizează persoanei vizate toate informaţiile următoare” (UE 2016/679: art. 13). Prin sintagma „în momentul obţinerii acestor date” legiuitorul european a dorit să atragă atenţia supra faptului că este interzis a se începe colectarea datelor cu caracter personal ale persoanei vizate fără ca aceasta să fie informată despre ce operaţiuni urmează să efectueze operatorul cu aceste date. Sintagma „toate informaţiile” semnifică faptul că persoana vizată va primi de la operator toate informaţiile prevăzute în art. 13 şi, în situaţia în care nu este cazul efectuării unei anumite operaţiuni cu datele personale

colectate, aceasta nu înseamnă că operatorul o va elimina din informare, ci va preciza explicit că acea operațiune nu se va face.

O altă cerinţă a art. 1 este ca la momentul efectuării informării, persoanei vizate să i se comunice ”identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acestuia” (UE 2016/679: art. 13). În ceea ce priveşte comunicarea unor astfel de date în cazul persoanelor juridice care au calitatea de operator nu identificăm probleme deosebite, identitatea acestora referindu-se la numele complet al societăţii / organizaţiei / instituţiei, iar datele de contact sunt ale sediului / filialei / punctului de lucru persoană juridică unde se colectează şi se prelucrează datele.

Un caz particular îl reprezintă cel al unui ONG care oferă servicii / prestaţii sociale / medicale, cu sediul principal în / în afara UE, şi care deschide filiale în mai multe oraşe din România, iar aceste filiale au personalitate juridică proprie. Cade în sarcina acestor filiale să informeze persoanele vizate care solicită serviciile / prestaţiile oferite de organizaţie despre prelucrarea datelor cu caracter personal şi este responsabilitatea acestor filiale să asigure protecţia şi securitatea acestor date şi, implicit, se constituie un punct de contact pentru persoana vizată în ce priveşte exercitarea drepturilor acesteia, în conformitate cu prevederile Regulamentului. Prin urmare, persoana vizată va fi informată despre datele de contact ale filialei şi nu ale firmei care a înfiinţat filiala.

În cazul operatorilor persoane fizice, situaţia se dovedeşte a fi ceva mai delicată. Regulamentul obligă la declinarea identităţii, ceea ce înseamnă că operatorul persoană fizică ar trebui să se identifice prin nume şi prenume. Datele de contact, în cazul persoanelor juridice, includ şi adresa sediului unde se prelucrează datele cu caracter personal. Se pune întrebarea dacă persoana fizică este şi ea obligată să includă în datele de contact adresa exactă, mai ales când aceasta este adresa locativă a operatorului. Din prevederile Regulamentului reiese că trebuie să se furnizeze această informaţie dar, în acest caz, poate apărea problema siguranţei operatorului şi / sau a familiei sale, spre exemplu.

În ceea ce priveşte publicarea datelor reprezentantului operatorului sau a persoanei împuternicite de operator, în sensul Regulamentului, reprezentant „înseamnă o persoană fizică sau juridică stabilită în Uniune, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul articolului 27, care reprezintă operatorul sau persoana împuternicită în ceea ce priveşte obligaţiile lor respective care le revin în temeiul prezentului regulament” (UE 2016/679: art. 4). În cazul reprezentantului operatorului sau al persoanei împuternicite de operator care este persoană juridică, se precizează numele persoanei juridice şi datele de

contact ale acesteia. În cazul reprezentantului operatorului sau al persoanei împuternicite de operator care este persoană fizică, apare aceeaşi situaţie ca în cazul operatorului sau al persoanei împuternicite de operator care este el / ea însuşi / însăşi persoană fizică. Regulamentul obligă la oferirea anumitor date de contact şi nu specifică dacă acestea trebuie să fie cele personale ale operatorului, ale persoanei împuternicite de operator sau ale reprezentantului acestora. Ca urmare, în practică se încearcă evitarea folosirii numelui şi prenumelui reprezentantului operatorului sau al persoanei împuternicite de operator şi, cel mai adesea, se oferă o adresă de e-mail creată special pentru comunicarea cu respectiva persoană.

Art. 13 din Regulament prevede că se vor furniza şi "datele de contact ale responsabilului cu protecţia datelor, după caz" (UE 2016/679: art. 13). În această situaţie textul nu ridică probleme de interpretare, sens în care se oferă doar datele de contact ale DPO, adică o adresă de e-mail, preferabil dedicată lui sau activităţii specifice acestuia şi un număr de telefon de contact la care fie răspunde personal responsabilul cu protecţia datelor cu caracter personal, fie reprezentantul unui serviciu dedicat acestuia, care preia apelurile şi le transmite doar către DPO. Regulamentul nu prevede obligativitatea declinării identităţii DPO către persoana vizată. Identitatea responsabilului cu protecţia datelor se declină doar către Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în cazul completării şi transmiterii către aceasta a formularului de numire a responsabilului cu protecţia datelor cu caracter personal.

Sintagma „după caz" este inserată în text cu referire doar la operatorii obligaţi să desemneze un responsabil cu prelucrarea datelor cu caracter personal sau la cei care l-au desemnat în baza unei conduite care ţin de bune practici în domeniu. În această situaţie, persoana vizată va fi informată că „operatorul nu se încadrează în situaţiile prevăzute de Regulament privind obligativitatea numirii unui DPO". Aşa cum se aminteam mai sus, acest element nu trebuie eliminat din informare, ci se impune a se face precizarea că nu este necesar pentru o informare valabilă.

Art. 13 alin. 1 lit. c din Regulament impune ca în informare să fie incluse „scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării" (UE 2016/679: art. 13).

În practică, s-a observat că identificarea şi furnizarea scopurilor către persoana vizată, în aşa fel încât să se respecte prevederile Regulamentului, ridică serioase probleme multor operatori. Când operatorul îşi stabileşte scopurile prelucrării datelor cu caracter personal, acesta trebuie să respecte principiul limitării legate de scop, sens în care art. 5 alin. 1 lit. b detaliază că scopurile trebuie să fie "determinate, explicite şi legitime şi [datele – n.n.] nu

sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri" (UE 2016/679: art. 5 alin. 1 lit. b). Prin scopuri determinate, explicite şi legitime se înţelege că la momentul la care persoana vizată este informată asupra prelucrării datelor cu caracter personal, operatorul a determinat în mod vizibil / ştie care sunt scopurile pentru care prelucrează datele cu caracter personal şi menţionează acest lucru. Prelucrarea datelor cu caracter personal fără ca scopurile prelucrării să fie determinate este ilegală. Pentru determinarea scopurilor prelucrării, nu se admite utilizarea termenilor „orice", „oricâte", „oricăror", „toate" etc.

Faptul că datele nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopurile declarate înseamnă că operatorul trebuie să fie capabil, la momentul la care efectuează informarea persoanei vizate, să determine cât mai clar şi explicit scopurile prelucrării, întrucât se presupune că prelucrarea datelor cu caracter personal se face ca urmare a desfăşurării activităţii curente a operatorului, care are o strategie de funcţionare şi dezvoltare pe termen lung, deci poate defini scopurile prelucrării cât mai precis şi mai detaliat.

Faptul ca operatorul declară că va prelucra datele în scopuri legitime, în condiţiile legii nu este suficient. Operatorul trebuie să precizeze explicit care sunt aceste interese legitime şi să efectueze un test comparativ (Grupul de Lucru, 2014) prealabil prelucrării în interes legitim, deoarece „trebuie să se asigure că, urmărindu-şi interesele legitime, nu afectează în mod grav drepturile şi libertăţile persoanelor fizice în cauză; în caz contrar, societatea/organizaţia [...] nu se poate baza pe interese legitime ca justificare a prelucrării datelor şi trebuie găsit un alt temei juridic." (CE, n.d.b).

Pentru aplicarea corectă a unui test comparativ trebuie luaţi în considerare o serie de factori cheie care sunt detaliaţi într-un document special dedicat de Grupul de lucru pe articolul 29 prelucrării datelor cu caracter personal în temeiul interesului legitim, a cărui consultare o recomandăm ca fiind foarte utilă profesioniştilor în domeniul prelucrării datelor cu caracter personal, iar noi ne vom limita doar la o enumerare simplă a acestora:

a) evaluarea interesul legitim al operatorului;
b) impactul asupra persoanelor vizate;
c) echilibrul provizoriu;
d) garanţiile suplimentare (Grupul de Lucru, n.d.).

Un alt element pe care trebuie să îl conţină informarea este temeiul juridic al prelucrării, ceea ce înseamnă că, la momentul efectuării informării persoanei vizate, operatorul indică foarte clar articolul 6 şi litera din Regulament în baza căruia se face prelucrarea, precum şi legile specifice care guvernează activitatea operatorului şi legitimează scopurile prelucrării

declarate de operator. Conform art. 13 alin. 1 lit. d, „în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), [se vor indica – n.n.] interesele legitime urmărite de operator sau de o parte terţă" (UE 2016/679: art. 13). Regulamentul defineşte, î art. 13, ce se înţelege prin „interese legitime urmărite de operator": „un interes este cauza mai amplă pe care un operator o poate avea pentru prelucrare sau avantajul pe care operatorul îl obţine – sau pe care societatea l-ar putea obține – în urma prelucrării." (Grupul de Lucru, n.d.).

Operatorul este obligat să specifice interesele legitime pe care declară că le are pentru prelucrarea datelor cu caracter personal, iar acestea trebuie să îndeplinească următoarele condiţii (Grupul de Lucru, n.d.: 27) pentru a fi în conformitate cu prevederile Regulamentului:

a) să fie legale – operatorul trebuie să poată indica explicit legislația UE şi pe cea națională care justifică interesul său legitim;

b) să fie suficient de clar articulate pentru a permite efectuarea testului comparativ în raport cu interesul şi drepturile fundamentale ale persoanei vizate – interesul legitim declarat de operator trebuie formulat în termeni operaționali, clari şi cât mai specifici;

c) să reprezinte un interes real şi actual - operatorul trebuie să demonstreze că are un interes real şi actual pentru a prelucra datele şi nu unul speculativ.

Lit. e a art. 13 alin. 1 prevede că în informare se vor include menţiuni despre "destinatarii sau categoriile de destinatari ai datelor cu caracter personal" (UE 2016/679: art. 13), sens în care operatorul va specifica în mod clar şi explicit dacă nu dezvăluie / divulgă date cu caracter personal către terţi sau, dacă este cazul, va indica entitățile cărora le dezvăluie / divulgă datele cu caracter personal ale persanei vizate (spre exemplu, instituţii de stat - Inspectoratul Teritorial de Muncă, Agenția Națională de Administrare Fiscală – sau instituţii private - SC Transport Public SA, caz în care se vor adăuga mențiuni de tipul "pentru eliberarea legitimațiilor individuale de transport gratuit a persoanelor la evenimentul ...").

De asemenea, se va menționa, "dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională" (UE 2016/679: art. 13). Dacă nu există o asemenea intenție, operatorul va specifica asta expres; dacă există o asemenea intenție sau dacă activitatea operatorului presupune transferul de date cu caracter personal către o țară terță sau o organizație internațională, operatorul va preciza explicit persoanei acest lucru, împreună cu informații despre:

- existența sau absența unei decizii a Comisiei privind caracterul adecvat – în măsura în care un stat terț față de statele membre UE oferă un

nivel adecvat de protecţie a datelor cu caracter personal, nivel atestat printr-o decizie a Comisiei Europene, operatorul care transferă datele nu va fi nevoit să ofere persoanei vizate garanţii suplimentare privind maniera în care vor fi protejate datele sale personale, caz în care transferul datelor va fi asimilat acelor transferuri efectuate în interiorul graniţelor UE (CE, n.d.c). Emiterea unei astfel de decizii poate fi verificată pe site-ul Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal, unde sunt publicate ţările pentru care s-a emis o decizie privind caracterul adecvat al protecţiei datelor în ţara respectivă. În acest moment, la nivelul UE s-a adoptat o singura decizie privind caracterul adecvat al protecţiei datelor, în ceea ce priveşte Japonia (ANSPDCP, n.d.b);

- dacă nu există o decizie privind caracterul adecvat al protecției datelor, transferul de date nu este interzis, dar persoanele ale căror date se transferă trebuie să primească garanții adecvate că datele lor vor beneficia de protecţia corespunzătoare în statul în care se efectuează transferul, că drepturile pe care le au în UE în baza Regulamentului sunt opozabile statului în care se face transferul şi au căi de atac eficace pentru situaţia în care datele lor vor fi folosite inadecvat. Sunt considerate garanţii adecvate: instituirea unor reguli corporatiste obligatorii, acorduri contractuale cu destinatarul, care să conţină clauze contractuale standard aprobate de Comisia Europeană, aderarea la un cod de conduită sau la un mecanism de certificare, existenţa unor angajamente obligatorii şi executorii din partea destinatarului de a aplica garanţii adecvate (CE, n.d.c).
- dacă nu există nici decizie privind caracterul adecvat al protecției datelor şi lipsesc şi garanţiile adecvate, este necesar acordul explicit al persoanei de a i se transfera datele, după ce persoana este informată în mod complet cu privire la riscurile existente (CE, n.d.c).

Alin. 2 al art. 13 instituie o serie de elemente suplimentare care vor fi cuprinse de informările oferite de operator, elemente care au ca scop asigurarea unei prelucrări echitabile şi transparente.

- perioada pentru care vor fi stocate datele cu caracter personal – perioada de stocare a datelor cu caracter personal fie se regăseşte explicit într-o lege (spre exemplu, Legea arhivelor naţionale), fie poate fi dedusă dintr-o lege (spre exemplu, Legea voluntariatului, în art. 13, lit. d);

- criteriile utilizate pentru a stabili perioada de stocare a datelor, dacă această perioadă nu este prevăzută expres – în situaţiile în care operatorul nu are sau nu identifică un termen de stocare a datelor într-o lege, îşi poate stabili singur această perioadă, cu condiţia să respecte principiul limitării legate de stocare, care presupune să nu păstreze datele cu caracter personal mai mult decât este necesar pentru atingerea scopurilor pentru care au fost

colectate; condiţia impusă de Regulament este ca operatorul să informeze explicit persoana vizată despre aceste criterii şi cum le-a aplicat;

- operatorul este obligat să garanteze persoanei vizate drepturile de acces, rectificare, ştergere, restricţionare, opoziţie sau portabilitate, respectând prevederile articolelor din Regulament care reglementează în mod specific aceste drepturi;

- în cazul în care prelucrarea datelor se face pe baza consimţământului persoanei vizate, operatorul este obligat să garanteze acesteia dreptul de retragere a consimţământului, făcând menţiunea că retragerea consimţământului nu afectează legalitatea prelucrării efectuată anterior retragerii acordului (CE, n.d.c) şi că retragerea consimţământului se va face la fel ca acordarea acestuia, printr-o cerere scrisă adresată operatorului la sediul acestuia sau printr-un e-mail; se va preciza, de asemenea, expres faptul că după retragerea consimţământului, operatorul va înceta prelucrarea datelor;

- dreptul de a depune o plângere în faţa unei autorităţi de supraveghere - operatorul va furniza persoanei vizate datele de contact ale ANSPDCP.

- operatorul este obligat să furnizeze persoanei vizate informaţii explicite despre temeiul juridic în baza căruia prelucrează datele cu caracter personal, precum şi ce consecinţe pe care persoana vizată le va suporta dacă nu furnizează aceste date (CE, n.d.c); spre exemplu, în cazul raporturilor de muncă, dacă obligaţia de furnizare a datelor are caracter legal, angajatul are obligaţia legală de a depune la dosarul de angajare adeverinţa de la medicul de familie din care să reiasă că este apt de muncă, iar dacă refuză să furnizeze documentul, nu poate fi angajat; obligaţia poate avea caracter contractual, cum ar fi, spre exemplu, în cazul respectării dispoziţiilor privind sănătatea şi securitatea în muncă, care se includ obligatoriu în contractul individual de muncă, în fişa postului sau într-o anexă a contractului individual de muncă, parte integrantă a acestuia (angajatul este obligat să declare un anumit traseu de acasă spre serviciu şi retur, precum şi să anunţe orice schimbare de traseu; orice accident care are lor pe un traseu neanunţat angajatorului nu este considerat accident de muncă iar angajatorul este absolvit de orice responsabilitate); uneori, obligaţia de furnizare a datelor este necesară pentru încheierea unui contract (spre exemplu, în cazul depunerii la angajator a diplomelor care atestă îndeplinirea condiţiei studiilor de specialitate pentru un anumit post).

- în cazul în care operatorul prelucrează datele printr-un proces automatizat, care include şi crearea de profiluri, va furniza persoanei vizate toate informaţiile prevăzute de Regulament ”privind importanţa şi

consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată" (CE, n.d.c); dacă nu este cazul, operatorul va preciza expres acest aspect, fără a ignora in informare acest element, mai exact va menţiona că operatorul nu se încadrează la acea prevedere sau nu prelucrează datele în sensul prevăzut de respectivul articol.

- dacă operatorul, în momentul informării iniţiale a persoanei vizate nu a putut prevedea apariţia unor scopuri secundare ale prelucrării, după identificarea acestora, dar înainte de începerea prelucrării datelor pentru scopurile ulterioare identificate, este obligat să informeze persoana vizată asupra acestui fapt, cu alte cuvinte să reia informarea persoanei vizate, informare care se va face în mod extins, aşa cum a fost făcută şi informarea iniţială (CE, n.d.c).

III.2. Informarea persoanei vizate în baza art. 14, atunci când datele cu caracter personal nu au fost obţinute de la persoana vizată

Nu vom relua discuţiile făcute mai sus în cadrul acestui articol cu privire la menţiuni care sunt similare sau identice în textele articolelor 13 şi 14, limitându-ne în continuare la a analiza diferenţele dintre cele două texte de lege şi cum se traduc acestea în obligaţiile impuse operatorului.

Art. 14 din Regulament impune ca persoana ale cărei date sunt prelucrate să fie informată despre "categoriile de date cu caracter personal vizate" (UE 2016/679: art. 14), în funcţie de scopurile prelucrării. Dorim să atragem atenţia asupra următorului aspect: la sfârşitul enumerărilor nu recomandăm utilizarea acronimelor „etc.", „ş.a." sau „ş.a.m.d.". Utilizarea lor este ilegală în contextul respectării principiului reducerii la minimum a datelor, adică al utilizării doar a datelor strict necesare îndeplinirii scopurilor pentru care au fost colectate. Aceste acronime sugerează că datele prelucrate nu sunt doar cele declarate de operator, ci că acesta poate stoca şi utiliza şi orice alte date a obţinut, chiar dacă acestea nu sunt absolut necesare pentru atingerea scopurilor declarate de operator.

Operatorul este obligat să comunice şi să indice explicit sursa din care a obţinut datele cu caracter personal (UE 2016/679: art. 14): instituţii ale statului, persoane fizice sau juridice, internet, reţele de socializare sau alte surse, cum a fost cazul „Teleorman Leaks" mediatizat de jurnaliştii de la Rise Project (n.d.).

Conform alin. 3 al art. 14, informarea persoanei vizate trebuie să se facă într-un termen rezonabil, calculat de la data când sunt obţinute informaţiile cu caracter personal. Legea nu face nicio menţiune cu privire la care este în concret acest termen rezonabil, însă stabileşte limitarea în timp la maxim o lună, precum şi un criteriu în funcţie de care se va aprecia dacă în

interiorul acelei luni, termenul în care a fost făcută informarea a avut sau nu caracter rezonabil. Acest criteriu se referă la circumstanţele în care sunt prelucrate datele cu caracter personal.

Nu acelaşi este termenul dacă datele urmează a fi folosite în cadrul comunicării cu persoana vizată, caz în care informarea trebuie făcută cel târziu în momentul primei comunicări cu aceasta, caz în care, dacă această comunicare are loc mai devreme de termenul de o lună prevăzut la litera a, atunci informarea trebuie efectuată conform literei b. Suntem de părere că în cazul în care comunicarea se face mai târziu de o lună de la data preluării datelor, atunci informarea persoanei trebuie făcută în interiorul termenului de o lună, revenindu-se la regula instituită de litera a.

Textul stabileşte şi o a doua excepţie de la termenul de o lună instaurat prin dispoziţiile alin. 3 lit. a, mai exact situaţia când se intenţionează divulgarea datelor către un terţ, caz în care informarea trebuie făcută cel târziu la data divulgării. Iarăşi, considerăm că dacă această divulgare se face mai târziu de o lună de la colectarea datelor, se revine şi în acest caz la termenul instituit de alin. 3 lit. a.

Informarea este valabilă numai atât timp cât datele sunt prelucrate în scopul cu privire la care persoana a fost informată, astfel că, în conformitate cu art. 14 alin. 4, dacă pe parcurs operatorul intenționează să folosească datele şi în alte scopuri decât cele iniţiale, atunci este nevoit să efectueze din nou procedura informării, pentru aceste scopuri secundare, inclusiv prin punerea la dispoziția persoanei a oricăror alte informații relevante referitoare la modul cum vor fi prelucrate datele sale.

Alin. 5 al art. 14 instituie o excepţie de la regulile prevăzute de alin. 1-4 ale art. 14, o excepţie care are nuanţe speciale prin raportare la textul alin. 4: „persoana vizată deţine deja informaţiile" (UE 2016/679: art. 14). Aceasta nu înseamnă, prin prisma alin. 4, că textul permite efectuarea unor informări iniţiale neglijente, incomplete sau vagi, din care s-ar putea deduce că scopul prelucrării este mai larg decât cel expus expres în informare. Considerăm, mai degrabă, că această excepţie este o aplicaţie a principiului de drept „cine poate mai mult, poate şi mai puţin", iar excepţia devine aplicabilă în condiţiile în care prelucrarea are ca scop efectuarea unor activități de detaliu, incluse în scopul inițial şi legate intrinsec de acesta.

Tot în sens restrictiv trebuie interpretate şi dispoziţiile alin. 4 lit. b, care instituie nu una, ci trei excepţii de la regulile alin. 1-4 ale art. 14: prima este cazul în care furnizarea informațiilor suplimentare se dovedeşte fi imposibilă. Suntem de părere că simpla imposibilitate de contactare a persoanei vizate la datele de contact (domiciliu, email, număr de telefon etc.) furnizate inițial nu intră sub incidența excepției prevăzută la alin. 5 lit. b, iar

în acest caz comportamentul corect al operatorului ar fi să se abţină de la prelucrarea datelor în scopuri suplimentare.

O a doua excepţie este situaţia în care furnizarea informaţilor ar implica eforturi disproporţionate. Cum legea nu defineşte ce se înţelege prin eforturi disproporţionate, acestea vor fi analizate de la caz la caz şi va rămâne la latitudinea practicii să stabilească criteriile în funcţie de care un efort poate fi sau nu considerat disproporţionat. Cu toate acestea, textul de lege oferă o serie de exemple, şi spunem exemple datorită exprimării "cum ar fi", care indică faptul că enumerarea nu este limitativă: scopuri de arhivare. Această arhivare poate avea la bază interesul public, interesul statistic, cel de cercetare ştiinţifică sau cel istoric.

O menţiune specială se impune a fi făcută în ceea ce priveşte interesul de cercetare, atunci când aducem în discuţie cercetarea medicală pe subiecţi umani, cu atât mai mult cu cât această menţiune din text trebuie corelată cu o a treia excepţie instituită de lit. b a alin. 5, mai exact cea referitoare la situaţia în care informarea este de natură să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării. În situaţia în care persoana vizată este parte a unui eşantion de trial clinic cu efect placebo, spre exemplu, este imperios necesar să se asigure persoanei tratamentul adecvat bolii sale la nivelul cunoscut în medicină, în sens contrar operatorul încălcându-i acesteia drepturile, libertăţile sau interesele legitime, după caz, condiţie care, de altfel, este impusă de textul de lege pentru a se permite evitarea informării. De altfel, în toate cazurile în care există riscul ca aceste drepturi sau interese să fie încălcate, chiar dacă operatorul se află într-una dintre situaţiile de excepţie, acesta trebuie să renunţe la prelucrarea datelor.

O altă excepţie este cea prevăzută la lit. c, când obţinerea sau divulgarea datelor este prevăzută expres de lege. Acesta este, spre exemplu, cazul când informaţiile sunt puse la dispoziţia organelor de urmărire penală sau a altor instituţii ale statului cu atribuţii de control.

Secretul profesional este o ultimă excepţie prevăzută de la regula instituită de art. 14, atunci când confidenţialitatea este reglementată prin lege, care poate fi dreptul intern al statului sau dreptul Uniunii Europene.

Concluzii

Punerea în aplicare, la 25 mai 2018, a Regulamentului 679/2016 a scos în evidenţă câteva probleme în implementarea acestuia pentru care prezenta lucrare a încercat să ofere câteva soluţii. Una din probleme a fost legată de realizarea corectă a procesului de informare a persoanei vizate.

Am alocat un spaţiu amplu în lucrare detalierii paşilor de urmat în vederea efectuării corecte şi complete a informării persoanei vizate relativ la prelucrarea datelor cu caracter personal când datele sunt colectate de la persoana vizată şi când datele prelucrate sunt obţinute din alte surse decât de la persoana vizată.

Faptul că informarea corectă a persoanei vizate nu este un proces complet înţeles şi aplicat corespunzător de operatori este confirmat şi de Comunicatul de presă al ANSPDCP conţinând informaţii statistice referitoare la activitatea Autorităţii începând cu data de 25 mai 2018 şi până la data de 24 mai 2019, publicat în data de 31 mai 2019 (ANSPDCP, n.d.c). În cuprinsul lucrării s-a pus accent deosebit pe importanţa realizării corecte şi complete a informării persoanei vizate, ca pas obligatoriu în prelucrarea corespunzătoare a datelor cu caracter personal şi în obţinerea unui consimţământ cu adevărat informat.

În urma investigaţiilor efectuate de ANSPDCP au fost dispuse măsuri corective şi au fost acordate avertismente, măsurile corective vizând, printre altele, respectarea dreptului la informare a persoanelor vizate şi efectuarea unei informări complete. Am remarcat faptul că în comunicat nu se precizează că s-au aplicat şi amenzi, deşi încălcarea dreptului persoanei vizate la o informare corectă şi completă, conform art. 83, alin (5), lit. b), spre exemplu, este sancţionată de Regulament cu amenzi administrative de până la 20 000 000 EUR sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare, conform prevederilor art. 83, alin (5) din Regulamentul (UE) 2016/679.

În concluzie, indiferent de temeiul legal în baza căruia se face prelucrarea datelor cu caracter personal, procesul de informare a persoanei vizate este obligatoriu şi prealabil prelucrării acestor date, iar respectarea tuturor etapelor informării va garanta efectuarea unei informări corecte şi complete, protejând atât persoana vizată, cât şi operatorul.

Bibliografie

Alte activităţi profesionale ştiinţifice şi tehnice n.c.a. 7490. (n.d.). Disponibil la http://coduricaen.info/definitie-Alte-activitati-profesionale-stiintifice-si-tehnice-n-c-a-7490.html

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP). (n.d.a). Home. Disponibil la https://www.dataprotection.ro/

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP). (n.d.b). Protecţia adecvată a datelor cu caracter personal de

către Japonia. Disponibil la https://www.dataprotection.ro/?page=Protectia_datelor_de_catre_Japonia&lang=ro

Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP). (n.d.c). Comunicat de presă. Disponibil la https://www.dataprotection.ro/?page=Comunicat_de_presa_statistica_1_an_GDPR&lang=ro

Autoritatea Naţională pentru Calificări (ANC). (2018). Decizia nr. 74/19.03.2018 de aprobare a Standardului ocupaţional pentru profesia de Responsabil cu protecţia datelor cu caracter personal. Disponibil la http://www.anc.edu.ro/standarde_app/SO/Responsabil_cu_protectia_datelor_cu_protectia_datelor.pdf

Brkan, M. (2015). Data protection and European private international law. În *EUI Working Paper RSCAS 2015/40*. Badia Fiesolana, Italia: European University Institute.

Comisia Europeană (CE). (n.d.a). Justice and consumers. Disponibil la https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

Comisia Europeană (CE). (n.d.b). Ce înseamnă ”temeiul unui interes legitim”? Disponibil la https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_ro

Comisia Europeană (CE). (n.d.c). Ce norme se aplică dacă organizaţia mea transferă date în afara UE? Disponibil la https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_ro

Grupul de Lucru Privind Protecţia Persoanelor în ceea ce Priveşte Prelucrarea Datelor cu Caracter Personal. (2014). Avizul 06/2014 privind noţiunea de interese legitime ale operatorului de date prevăzută la articolului 7 din Directiva 95/46/CE, adoptat la 09.04.2014. Disponibil la http://www.dataprotection.ro/servlet/ViewDocument?id=1271

Ministerul Muncii şi Justiţiei Sociale (MMJS). (n.d.). Lista ocupaţiilor din COR în ordinea crescătoare a codurilor. Disponibil la http://www.mmuncii.ro/j33/images/Documente/Munca/COR/03052019_ISCO_08_lista_cresc_cod_ocupatii_cor.pdf

Parlamentul European, & Consiliul Uniunii Europene. (2016). 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 (Regulamentul general privind

protecţia datelor). Disponibil la https://www.dataprotection.ro/servlet/ViewDocument?id=1262

Parlamentul European, Consiliul Uniunii Europene, & Comisia Europeană (PE, CUE, & CE). (2012). Carta drepturilor fundamentale a Uniunii Europene. *Official Journal of the European Union, 2012/C 326/02*. Disponibil la https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=RO

Parlamentul României. (1996). Legea nr. 16/1996 a arhivelor naţionale. *Monitorul Oficial al Romîniei*, nr. 293, 2014, Aprilie 22.

Parlamentul României. Legea nr. 195/2001 a voluntariatului. *Monitorul Oficial al Romîniei*, nr. 276, 2007, Aprilie 25.

Rise Project, Conţinutul. Disponibil la https://www.riseproject.ro/articol/c-o-n-t-i-n-u-t-u-l/

Şandru, S. (2016). *Protecţia datelor personale şi viaţa privată*. Bucureşti, România: Hamangiu.

Ungureanu, C. T. (2017). Protecţia datelor cu caracter personal în contractele internaţionale. Analele Ştiinţifice ale Universitaţii „Al. I. Cuza" Iaşi LXIII (II), 135-154.

Ungureanu, C. T. (2018). Legal remedies for personal data protection in European Union. Logos Universality Mentality Education Novelty: Law, 6(2), 26-47. doi:10.18662/lumenlaw/10

Universitatea "Petru Maior" din Târgu Mureş, Centrul de Instruire şi Perfecţionare. (n.d.). Curs postuniversitar: Formare şi pregătire a responsabilului cu protecţia datelor cu caracter personal. Disponibil la http://cip.upm.ro/Curs-postuniversitar-Protectie-date-caracter-personal_c0033

Universitatea "Ştefan cel Mare" din Suceava. (n.d.). USV organizează un curs de formare pentru profesia de "Responsabil cu protecţia datelor cu caracter personal". Disponibil la http://www.usv.ro/index.php/ro/21/USV%20organizeaz%C4%83%20un%20curs%20de%20formare%20pentru%20profesia%20de%20%22Responsabil%20cu%20protec%C8%9Bia%20datelor%20cu%20caracter%20personal%22/2336/7/261

Universitatea Danubius din Galaţi. (n.d.). Responsabil cu protecţia datelor cu caracter personal – Curs postuniversitar de formare şi dezvoltare profesională continuă. Disponibil la http://www.univ-danubius.ro/nout%C4%83%C5%A3i/responsabil-cu-protec%C8%9Bia-datelor-cu-caracter-personal-%E2%80%93-curs-postuniversitar-de-formare-%C8%99i-dezvoltare-profesional%C4%83-continu%C4%83.html