Revista Universul Juridic ● nr. 6, iunie 2017, pp. 112-129

# PROCEDURI ŞI AUTORITĂȚI ÎN NOUL DREPT EUROPEAN AL PROTECȚIEI DATELOR CU CARACTER PERSONAL (I)

***Prof. univ. dr. Călina JUGASTRU***
Universitatea „Lucian Blaga" din Sibiu, Facultatea de Drept

**Abstract**

*Regulation (EU) No. 679/216 concerning the protection of individuals with regard to the processing of personal character data and the free movement of such data brings some novelty provisions. One of these has the role to designate the responsible with data protection - in cases specifically regulated; its appointment is an obligation of the entity where the personal data are processed. The importance of the new institution introduced by the Regulation can also be read in light of the consequences of the omission to appoint such a person responsible until 28 May 2018 (in cases where the law obliges the appointment), the sanction of the administrative fine being consistent.*

*The impact assessment procedure, in conjunction with the prior consultation, has the role of highlighting the risks of processing, in relation to the rights and freedoms of the persons concerned. Insofar as the activities requiring risk assessment will be rigorously identified (by the supervisor authorities), and the complex mechanism of safeguards, measures, mitigation / annihilation remedies will prove viable, the new impact assessment procedure can be converted into a useful and effective tool for all individuals involved in the processing of personal data.*

**Keywords**: *personal character data, Regulation no. 679/2016, international cooperation, DPO*

## Preliminarii

Între materiile aflate în perpetuă evoluție, protecția datelor personale ocupă un loc privilegiat şi sigur. „Privilegiat" – prin importanța cuvenită şi acordată acestui domeniu, mai ales după 2000, grație naturii fundamentale a dreptului ocrotit (dreptul la protecția datelor cu caracter personal). „Sigur" – datorită unei dinamici aflate sub semnul progresului tehnologiilor moderne de comunicare – iar evoluția în ritm rapid a acestora este o certitudine.

Iată că, într-un traiect ascendent, din punctul de vedere al preocupărilor centrate pe protecția datelor personale, anul 2016 a marcat adoptarea şi intrarea în vigoare a

două acte normative, diferit înveşmântate, sub aspect formal. În tiparul unui **regulament european**[1] care se va aplica începând cu 25 mai 2018 (interval de timp necesar şi rezonabil pentru ca statele membre să dispună măsurile preconizate), se găsesc regulile principale ale protecţiei, aplicabile cu titlu de normă-cadru. Necesitatea legiferării pe calea regulamentului este larg motivată şi are ca prim fundament asigurarea unui nivel consecvent, ridicat şi uniform de protecţie a drepturilor şi libertăţilor în spaţiul Uniunii. Înlăturarea obstacolelor din calea circulaţiei datelor are ca formulă optimă regulamentul. În timp ce reglementarea-cadru va înlocui aplicarea Directivei nr. 1995/46/CE începând cu mai 2018, prelucrarea datelor pe segmentul prevenirii infracţiunilor, urmăririi penale şi executării sancţiunilor penale este cuprinsă în **noua Directivă nr. 680/2016**, în vigoare din mai 2016[2]. Aceasta din urmă înlocuieşte Decizia-cadru 2008/977/JAI a Consiliului şi se preocupă de aspectele specifice dreptului penal şi dreptului procesual-penal. În ce măsură realitatea cotidiană a prelucrării datelor personale va concilia cele două reglementări – pe cale de regulament şi pe cale de directivă – aceasta este o chestiune ce va fi dezlegată de viitorul aplicării acestora.

Dificultăţile, deja conturate, ale interpretării-aplicării noilor prevederi ale dreptului european au determinat măsuri imediate. Între cele semnificative, menţionăm preocuparea de **elaborare a_ghidurilor destinate aplicării unitare a noului Regulament**. Grupul 29[3] a finalizat trei astfel de ghiduri, care concretizează propunerile ajustate în urma consultării publice din perioada decembrie

[1] Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 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 (JO L119/1 din 4 mai 2016).

[2] Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului (JO L119/89 din 4 mai 2016).

[3] Intrarea în vigoare a Directivei 1995/46/CE a prilejuit constituirea Grupului 29, organism european independent, cu caracter consultativ, format din reprezentanţii autorităţilor naţionale pentru protecţia datelor din statele membre ale Uniunii Europene, reprezentanţii autorităţilor create pentru instituţiile şi organismele comunitare, precum şi reprezentanţi ai Comisiei Europene. Activitatea Grupului 29 se circumscrie emiterii de opinii asupra nivelului de protecţie a datelor în statele membre şi în cele nemembre; emiterii de avize consultative asupra proiectelor de modificare a Directivei, asupra tuturor proiectelor de măsuri adiţionale sau specifice luate pentru apărarea drepturilor şi libertăţilor persoanelor fizice cu privire la prelucrarea datelor cu caracter personal, precum şi asupra altor proiecte de măsuri la nivel european, cu incidenţă asupra acestor drepturi şi libertăţi; emiterii de avize asupra codurilor de conduită elaborate la nivel european; emiterii de recomandări, precum şi alte documente asupra tuturor problemelor referitoare la protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal în cadrul Uniunii Europene, în vederea aplicării unitare a actelor normative naţionale care transpun directivele în materie (http://www.dataprotection.ro/?page=workgroup&lang=ro).

2016-ianuarie 2017: *Ghidul privind dreptul la portabilitatea datelor*; *Ghidul privind responsabilul pentru protecția datelor (DPO)*; *Ghidul privind identificarea autorității de supraveghere lider a unui operator sau împuternicit*[4].

Ghidurile menționate sunt un prim pas în armonizarea interpretării prevederilor regulamentare. Există o serie de noțiuni care necesită lămurire – oricum practica aplicării va aduce variabile cu repercusiuni importante, în privința domeniului de aplicare, categoriilor de date supuse prelucrării fără consimțământul persoanei vizate, drepturilor şi obligațiilor responsabililor şi persoanelor fizice supuse operațiunilor de prelucrare.

Ceea ce trebuie semnalat, dintru început, este faptul că Regulamentul consacră dreptul la protecția datelor cu caracter personal ca drept fundamental (considerentul 1). Beneficiarele protecției sunt persoanele fizice, pentru care Regulamentul creează spațiul de libertate, securitate şi justiție necesar în raport cu activitățile de prelucrare a datelor personale şi cu libera circulație a acestor date. Directiva nr. 1995/46/CE a vizat armonizarea nivelului de protecție a drepturilor şi libertăților fundamentale ale persoanelor fizice, fără să discute însă în termenii unui drept fundamental la protecția datelor cu caracter personal. Pasul înfăptuit de Regulament este semnificativ şi tranşează dezbaterile doctrinei cu privire la (eventuala) existență a unui drept subiectiv la protecția datelor personale[5].

Tot în rândul noutăților trebuie menționată instituirea unor obligații consolidate în sarcina responsabililor prelucrării (obligația de securitate, de exemplu), o mai riguroasă reglementare a consimțământului, suplimentarea garanțiilor oferite în cazul profilajului prin mijloace exclusiv automate, precum şi noi prerogative la dispoziția persoanelor vizate de prelucrare (dreptul la portabilitatea datelor, *droit à l'oubli*)[6].

Dintre procedurile şi autoritățile prevăzute de Regulamentul adoptat în anul 2016, ne vom opri la: desemnarea responsabilului cu protecția datelor, evaluarea impactului/consultarea prealabilă, autoritățile (naționale) de supraveghere

---

[4] Ghidurile pot fi consultate pe pagina Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, www.dataprotection.ro. În variantă preliminară, pe aceeaşi pagină poate fi accesat *Ghidul privind evaluarea impactului asupra protecției datelor*.

[5] A se vedea O. Ungureanu, C. Munteanu, *Dreptul la protecția datelor cu caracter personal, un drept autonom?*, în Revista Română de Drept Privat nr. 1/2014, p. 166-179.

[6] Drepturile persoanelor vizate constituie centrul de greutate al întregii legislații referitoare la protecția datelor cu caracter personal. Avem în vedere atât legislația internă (de exemplu, Legea franceză din 6 februarie 1978, cunoscută sub denumirea „Legea informatică şi libertăți"; Legea română nr. 677/2001 privind protecția persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date), cât şi Directiva 1995/46/CE, care îşi va înceta aplicabilitatea începând cu 25 mai 2018. Pentru comentarii cu privire la drepturile persoanelor vizate în actele normative menționate, a se vedea, C. Féral-Schuhl, *Cyberdroit. Le droit à l'épreuve de l'internet*, Dalloz, Paris, 2006, p. 34-36; A. Lepage, *Libertés et droit fondamentaux à l'épreuve de l'internet*, Litec, Paris, 2002, p. 26-31; S. Şandru, *Protecția datelor personale şi viața privată*, Editura Hamangiu, Bucureşti, 2016, p. 208-218; D. Gărăiman, *Dreptul şi informatica*, Ed. All Beck, Bucureşti, 2003, p. 295-296.

independente şi Comitetul european pentru protecţia datelor. Rolul autorităţilor nou instituite este major în ce priveşte menţinerea nivelului de protecţie a drepturilor şi libertăţilor fundamentale în ţările Uniunii, în condiţiile în care protecţia naţională a acestora şi, în mod special, ocrotirea vieţii private, sunt fragile.

Directiva nr. 680/2016 reglementează, de asemenea, responsabilul pentru protecţia datelor, evaluarea impactului şi consultarea prealabilă. Întrucât reglementarea noii Directive este similară celei din noul Regulament, vom dezvolta problematica, aşa cum se regăseşte în Regulamentul nr. 679/2016. Ca element particular, reţinem că dispoziţiile Directivei sunt adresate exclusiv protecţiei persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date.

Analizele dedicate responsabilului cu protecţia datelor şi evaluării impactului fac obiectul primei părţi a studiului (modalităţile de desemnare a responsabilului; cerinţele pentru numirea acestuia; funcţia şi sarcinile încredinţate de Regulament; operaţiunile supuse evaluării impactului; procedura consultării prealabile a autorităţii de supraveghere). Cea de a doua parte detaliază particularităţile desemnării şi statutul autorităţilor de supraveghere la nivelul statelor membre, respectiv structura şi atribuţiile Comitetului european pentru protecţia datelor.

**Responsabilul cu protecţia datelor (DPO)**

*„Data protection officer"* este reglementat cu titlu de noutate în dreptul european al prelucrării datelor cu caracter personal. Regulamentul stabileşte cazurile în care numirea responsabilului cu protecţia datelor este obligatorie, cerinţele legale cu privire la persoana responsabilului, funcţia şi sarcinile responsabilului cu protecţia datelor (art. 37-39). Sugestiv, responsabilul este indicat ca fiind noul „gardian" al prelucrărilor de date cu caracter personal[7].

***Desemnarea responsabilului pentru protecţia datelor***

Potrivit Regulamentului, numirea unui responsabil cu protecţia datelor este **obligatorie**, în cazurile expres menţionate:

a. atunci când *prelucrarea este efectuată de o autoritate sau un organism public*.

„Autoritate", „organism public" sunt termeni a căror accepţiune este determinată în conformitate cu dreptul intern. Sunt exceptate instanţele care acţionează în exerciţiul funcţiei lor jurisdicţionale.

b. atunci când *activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în operaţiuni de prelucrare care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o monitorizare periodică şi sistematică a persoanelor vizate pe scară*

[7] C. Timofte, *Ofiţerul de conformitate – noul „gardian" al prelucrărilor de date cu caracter personal*, material disponibil pe pagina http://dataprivacyblog.tuca.ro, accesată la data de 17 mai 2017.

*largă.* Împrejurarea că activitățile principale ale responsabilului prelucrării[8]/ împuternicitului[9] au în conținut operațiuni de prelucrare ce necesită monitorizare periodică şi sistematică a persoanelor vizate pe scară largă, este de natură să atragă obligativitatea numirii unui responsabil cu protecția datelor. Demersul explicării vocabularului se circumscrie sintagmelor: „activități principale", „monitorizare periodică şi sistematică", „persoane vizate pe scară largă".

**Activitățile principale** se raportează la obiectul de activitate al responsabilului prelucrării. În sectorul privat, activitățile principale ale unui operator se referă la activitățile sale de bază şi nu la prelucrarea datelor cu caracter personal drept activități auxiliare (considerentul 97). Precizarea *Ghidului privind responsabilul pentru protecția datelor (DPO)* este aceea că „activitățile principale" „nu ar trebui interpretate ca excluzând activitățile în care prelucrarea datelor reprezintă o parte indisolubilă a activității operatorului sau persoanei împuternicite de operator". Exemplificarea vizează domeniul medical, mai exact activitatea desfăşurată în unitățile spitaliceşti. În principal, spitalul oferă asistență medicală, însă eficiența şi calitatea îngrijirilor medicale presupun şi activitatea de prelucrare a datelor privind starea de sănătate a pacienților (prelucrarea dosarelor medicale). Pe cale de consecință, prelucrarea acestor date ar trebui să fie considerată a fi una dintre activitățile principale în orice spital, iar spitalele trebuie să desemneze un responsabil cu protecția datelor.

**Monitorizarea periodică şi sistematică** are unele repere, în ce priveşte lămurirea terminologiei, în partea introductivă a Regulamentului (considerentul 24 face referire la monitorizarea comportamentului persoanelor fizice). Pentru a se determina dacă o activitate de prelucrare poate fi considerată ca monitorizare a comportamentului persoanelor vizate, ar trebui să se stabilească dacă persoanele fizice sunt urmărite pe internet, inclusiv posibila utilizare ulterioară a unor tehnici de prelucrare a datelor cu caracter personal care constau în crearea unui profil al unei persoane fizice, în special în scopul de a lua decizii cu privire la aceasta, de a analiza sau de a face previziuni referitoare la preferințele personale, comportamentele şi atitudinile sale.

Rezultă fără dubiu că tehnicile care permit urmărirea conduitei utilizatorilor în mediul virtual sunt o formă de monitorizare a comportamentului persoanelor. Intră în această categorie, crearea de profiluri, publicitatea comportamentală, operarea unei rețele de telecomunicații; furnizarea de servicii de telecomunicații;

[8] „Responsabilul prelucrării" este „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile şi mijloacele prelucrării sunt stabilite prin dreptul Uniunii sau dreptul intern, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în dreptul Uniunii sau în dreptul intern" (art. 4 pct. 7 din Regulament).

[9] „Persoana împuternicită de responsabilul prelucrării" este „persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului" (art. 4 pct. 8 din Regulament).

email de direcţionare repetată; activităţi de marketing bazate pe date; profilare şi *scoring* în scopul evaluării riscurilor (de exemplu, în scopul de credit *scoring*, stabilirea primelor de asigurare, de prevenire a fraudelor, detectarea spălării banilor); urmărirea locaţiei prin aplicaţii mobile; publicitate comportamentală; monitorizarea wellness, fitness şi a datelor de sănătate prin intermediul dispozitivelor portabile; televiziune cu circuit închis; dispozitive conectate, spre exemplu, contoare inteligente, maşini inteligente ş.a.[10]

Credem că ipotezele arătate sunt relevante pentru spaţiul virtual, dar nu epuizează sfera comportamentului care poate fi supus monitorizării. Altfel, explicaţiile oferite de considerentul 24 al Regulamentului ar îngusta prea mult aria de aplicare a obligaţiei de desemnare a responsabilului cu protecţia datelor în raport cu primul caz în care funcţionează obligaţia legală. Monitorizarea conduitei persoanelor fizice are forme variate de manifestare, inclusiv în lumea „fizică", astfel că obligativitatea numirii acestuia funcţionează în toate situaţiile care întrunesc parametrii menţionaţi la lit. a), art. 37 din Regulament.

Monitorizarea periodică şi sistematică face apel la modul în care se manifestă în timp activitatea de supraveghere a celor vizaţi („periodic" – la anumite intervale de timp; „sistematic" – organizat, metodic, efectuat ca parte a unui plan).

c. atunci când *activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date*, menţionată la art. 9, *sau a unor date cu caracter personal privind condamnări penale sau infracţiuni*, conform art. 10.

Art. 9 alin. 1 prevede: „Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filosofice sau apartenenţa la sindicate şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viaţa sexuală sau orientarea sexuală ale unei persoane fizice". Textul instituie regula potrivit căreia prelucrarea datelor sensibile este interzisă. Alineatul 2 conţine situaţiile de excepţie, în care este legitimată prelucrarea, chiar în absenţa consimţământului celui vizat. Datele personale care se referă la condamnări penale sau infracţiuni se prelucrează sub controlul unei autorităţi de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii ori de dreptul intern care prevede garanţii adecvate pentru drepturile şi libertăţile persoanelor vizate (art. 10).

Aşadar, obiectul prelucrării este cel care determină numirea obligatorie a unui responsabil cu protecţia datelor. Fiind în discuţie datele cu caracter sensibil (sau datele „speciale"), este necesară prezenţa responsabilului – ceea ce ar putea constitui o garanţie în plus de protecţie pentru cei vizaţi.

---

[10] A se vedea, pentru exemplificări, *Ghidul privind responsabilul pentru protecţia datelor (DPO)*, p. 8, disponibil la adresa http://www.dataprotection.ro/servlet/ViewDocument?id=1384 (valabilă la data de 3 iunie 2017).

d. *în cazurile prevăzute fie de dreptul Uniunii Europene, fie de dreptul statului membru* (alte cazuri decât cele în care desemnarea responsabilului este obligatorie, conform Regulamentului)[11].

Desemnarea responsabilului pentru protecția datelor este o **facultate**, în ipoteza descrisă de art. 37 alin. 4 teza I. În alte cazuri decât cele reglementate ca fiind obligatorii (alin. 1, art. 37), operatorul sau persoana împuternicită de operator ori asociațiile şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna un responsabil pentru protecția datelor. Chiar de la primele observații pe marginea noului act normativ european, literatura de specialitate s-a pronunțat în favoarea numirii unui responsabil, chiar acolo unde legea nu obligă: „Chiar dacă Regulamentul nu prevede ca toți operatorii de date să desemneze un responsabil cu protecția datelor, ține de buna administrare a unei companii angajată în diverse operațiuni de prelucrare a datelor personale să creeze un astfel de rol. Sistemul sancțiunilor impuse de Regulamentul General pentru Protecția Datelor este usturător"[12].

***Desemnarea unui responsabil unic***

Regulamentul nr. 679/2016 prevede **două situații** în care este deschisă posibilitatea desemnării unui unic responsabil.

a. *Un grup de întreprinderi poate numi un responsabil unic pentru protecția datelor*; condiția cerută este ca responsabilul cu protecția datelor să fie uşor accesibil din fiecare întreprindere. Cerința accesibilității este impusă de sarcinile trasate responsabilului. Consilierea, monitorizarea şi cooperarea nu pot fi realizate decât atunci când responsabilul este accesibil fiecărei întreprinderi din grup. Nu numai întreprinderile, dar şi persoanele vizate trebuie să poată stabili contact cu responsabilul, în toate chestiunile relative la prelucrarea datelor lor şi la exercitarea drepturilor lor[13]. „*Grupul de întreprinderi*" trebuie înțeles ca entitate care exercită controlul şi întreprinderile controlate de aceasta (art. 4 pct. 18-19 din Regulamentul nr. 679/2016).

---

[11] În alte cazuri decât cele menționate la alin. 1, operatorul sau persoana împuternicită de operator ori asociațiile şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde dreptul Uniunii sau dreptul intern solicită acest lucru, desemnează un responsabil cu protecția datelor. Responsabilul cu protecția datelor poate să acționeze în favoarea unor astfel de asociații şi alte organisme care reprezintă operatori sau persoane împuternicite de operatori (art. 37 alin. 4).

[12] G. Zanfir Fortuna, *Toate autoritățile publice precum şi unii operatori de date privați, obligați să desemneze un responsabil cu protecția datelor din 2018*, articol disponibil la adresa https://www.juridice.ro/476072/toate-autoritatile-publice-precum-si-unii-operatori-de-date-privati-obligati-sa-desemneze-un-responsabil-cu-protectia-datelor-din-2018.html (accesat la 30 martie 2017).

[13] Prin „întreprindere" înțelegem persoana fizică sau juridică ce desfăşoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfăşoară în mod regulat o activitate economică. „Grup de întreprinderi" înseamnă o întreprindere care exercită controlul şi întreprinderile controlate de aceasta (art. 4 pct. 18 din Regulamentul nr. 679/2016).

b. De asemenea, *în cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, poate fi desemnat un responsabil cu protecţia datelor unic pentru mai multe dintre aceste autorităţi sau organisme*, luând în considerare structura organizatorică şi dimensiunea acestora. Varietatea activităţilor pe care le desfăşoară responsabilul cu protecţia datelor, în contextul funcţiei şi sarcinilor conferite de Regulament trebuie să se regăsească la fiecare nivel al structurii organizatorice a entităţii care l-a desemnat.

***Cerinţe pentru numirea responsabilului cu protecţia datelor***

Numirea responsabilului respectă **criteriul competenţei profesionale**, conform art. 37 alin. 5 din Regulament. În mod special, se va ţine seama de cunoştinţele sale de specialitate, de practica în domeniul protecţiei datelor personale, precum şi de capacitatea de a îndeplini sarcinile care îi revin.

Considerentul 97, teza ultimă, aduce unele precizări. *Nivelul necesar al cunoştinţelor de specialitate* va fi apreciat, în mod particular, în funcţie de operaţiunile de prelucrare a datelor efectuate şi de nivelul de protecţie impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Aceşti responsabili cu protecţia datelor, indiferent dacă sunt sau nu angajaţi ai operatorului, ar trebui să fie în măsură să îşi îndeplinească atribuţiile şi sarcinile în mod independent.

Trebuie reţinute şi explicaţiile *Ghidului* (p. 11), în sensul că nivelul de expertiză necesar nu este strict definit, dar trebuie să fie proporţional cu sensibilitatea, complexitatea şi volumul de date prelucrate de organizaţie. Se oferă exemplul operaţiunilor deosebit de complexe de prelucrare a datelor sau cazul în care este implicat un volum mare de date speciale – situaţii în care responsabilul cu protecţia datelor poate necesita un nivel mai ridicat de expertiză şi suport. Există, de asemenea, diferenţe, în funcţie de faptul transferării datelor cu caracter personal în afara Uniunii, în mod sistematic sau ocazional. Opţiunea pentru un anumit responsabil este necesar a fi configurată ţinând seama de aspectele de protecţie a datelor care apar în cadrul instituţiei/organizaţiei respective.

*Capacitatea de a îndeplini sarcinile* este o cerinţă care se referă la calităţile personale (integritatea profesională, respectarea regulilor de etică) şi poziţia responsabilului cu protecţia datelor în cadrul organizaţiei/instituţiei respective[14].

Aceşti responsabili cu protecţia datelor, indiferent dacă sunt sau nu angajaţi ai operatorului, trebuie să fie în măsură să îşi îndeplinească atribuţiile şi sarcinile în mod independent.

***Funcţia şi sarcinile responsabilului***

Sub genericul „Funcţia responsabilului cu protecţia datelor" (secţiunea 4, art. 38) este dezvoltată cerinţa/problema accesibilităţii responsabilului cu protecţia

[14] *Ghidul privind responsabilul pentru protecţia datelor, op. cit.*, p. 11.

datelor. Accesibilitatea este un aspect comun, atât situațiilor în care numirea este obligatorie, cât şi ipotezelor de desemnare facultativă.

Responsabilul cu protecția datelor are **rolul de punct de contact** (pentru responsabilul cu prelucrarea datelor, pentru persoanele vizate şi pentru autoritatea de supraveghere) în toate problemele referitoare la protecția datelor cu caracter personal. El poate oferi consultanță operatorului de date în realizarea studiului de impact, care este obligatoriu şi prealabil efectuării operațiunilor de prelucrare a datelor speciale[15].

De asemenea, persoanele vizate de prelucrare trebuie să fie informate de manieră a putea intra în legătură cu responsabilul cu protecția datelor. În acest sens, Regulamentul statuează că, în cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate o serie de informații obligatorii, între care datele de contact ale responsabilul cu protecția datelor (art. 13 alin. 1 pct. b). Aceleaşi informații se comunică persoanei vizate şi dacă datele cu caracter personal supuse prelucrării nu au fost obținute de la aceasta (art. 14 alin. 1 lit. b).

Ataşat rolului de punct de contact, toate informațiile referitoare identificarea responsabilului cu protecția datelor se păstrează în evidențele activităților de prelucrare.

Câteva ***precizări*** se desprind din redactarea textului de lege:

a. *numirea responsabilului cu protecția datelor este o prerogativă care aparține responsabilului cu prelucrarea datelor, persoanei împuternicite de acesta, asociațiilor şi alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori.* Responsabilul cu protecția datelor poate fi un angajat al operatorului sau persoanei împuternicite de operator ori poate să îşi îndeplinească sarcinile în baza unui contract de prestări servicii.

b. *responsabilul cu protecția datelor are îndatorirea de a se implica în mod corespunzător şi util în toate aspectele legate de protecția datelor cu caracter personal*. Acest tip de implicare traduce, de fapt, prezența sa efectivă în viața entităților care l-au desemnat. Ceea ce presupune informarea în timp util a responsabilului cu protecția datelor, cu privire la toate operațiunile de prelucrare preconizate la nivelul instituției sau organizației. În mod special, la momentul deciziilor ce implică aspecte de prelucrare a datelor cu caracter personal, este recomandabil să existe un

[15] Art. 35 alin. 1 din Regulamentul nr. 679/2016 prevede: „Având în vedere natura, domeniul de aplicare, contextul şi scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare".

aviz al responsabilului cu protecția datelor[16]. În mod cert, informarea persoanei responsabile cu protecția datelor trebuie să aibă loc ori de câte ori are loc încălcarea securității datelor[17]. Informarea completă este premisa îndeplinirii obligației de consiliere ce revine responsabilului cu protecția datelor, conform prevederilor Regulamentului.

c. *responsabilul cu protecția datelor este sprijinit, în realizarea funcției/sarcinilor care îi revin, de către responsabilul cu prelucrarea datelor sau persoana împuternicită de acesta*. Întâi de toate, sprijinul se va concretiza în asigurarea resurselor necesare pentru executarea acestor sarcini, precum şi pentru accesarea datelor cu caracter personal şi a operațiunilor de prelucrare. Resursele pot avea în vedere asigurarea echipamentelor specifice monitorizării activității de prelucrare a datelor, eventual asigurarea personalului necesar îndeplinirii rolului de punct de contact cu operatorul de date/persoanele vizate/autoritățile de profil naționale şi internaționale. Toate acestea presupun resurse financiare şi o infrastructură modernă, permanent adaptată evoluțiilor internaționale (relativ rapide).

Punerea în practică în mod optim a sarcinilor este condiționată şi de sprijinul oferit în menținerea/perfecționarea cunoştințelor de specialitate (stagii de perfecționare, achiziționarea lucrărilor de specialitate). O consultanță eficientă şi de înalt nivel implică o constantă conectare la realitatea internațională dinamică în materie de date personale.

Una dintre recomandările Grupului 29 este ca responsabilul cu protecția datelor să fie localizat pe teritoriul Uniunii, chiar dacă operatorul sau persoana împuternicită de operator este stabilită în afara acestui spațiu[18]. Totuşi, recomandarea nu exclude faptul că, în anumite situații în care operatorul sau persoana împuternicită de operator nu are sediul în Uniunea Europeană, un responsabil îşi poate îndeplini sarcinile într-un mod mai eficient dacă este localizat în afara Uniunii.

d. *responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator*. Operatorul şi persoana împuternicită de operator se asigură că responsabilul cu protecția datelor nu primeşte niciun fel de instrucțiuni în ceea ce priveşte îndeplinirea acestor sarcini (responsabilul cu protecția datelor nu este demis sau sancționat de către operator şi nici de persoana împuternicită de operator, pentru îndeplinirea atribuțiilor sale). Aceste prevederi sunt o garanție a faptului că, în toate cazurile (indiferent că este

---

[16] Ghidul recomandă ca, în cazul în care nu se dă curs opiniei responsabilului cu protecția datelor, să se procedeze la precizarea motivelor pentru care decizia nu este conformă avizului acestuia (p. 13).

[17] „Încălcarea securității datelor cu caracter personal" este acea încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea" (art. 4 pct. 12 din Regulamentul nr. 679/2016).

18 *Ghidul privind responsabilul pentru protecția datelor (DPO)*, *op. cit.*, p. 10-11.

unul dintre angajații operatorului sau o persoană din afara organizației), responsabilul cu protecția datelor funcționează independent.

e. *responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce priveşte îndeplinirea sarcinilor sale*, în conformitate cu dreptul Uniunii sau cu dreptul intern. Importanța confidențialității în materia datelor cu caracter personal este lesne de înțeles. Literatura de specialitate menționează concluziile unui studiu efectuat de Microsoft în 12 țări (SUA, Franța, Germania, Japonia, Coreea de Sud, Brazilia, India, Rusia, China, Turcia, Africa de Sud şi Indonezia). La nivelul anului 2014, utilizatorii, într-un procent semnificativ, au declarat că nu sunt suficient informați cu privire la informațiile colectate care îi vizează[19].

f. *responsabilul cu protecția datelor poate îndeplini şi alte sarcini şi atribuții*, cu condiția ca niciuna dintre aceste sarcini şi atribuții să nu genereze conflict de interese.

**Sarcinile responsabilului cu protecția datelor** sunt concepute de manieră a asigura câteva direcții esențiale: informare şi consiliere, monitorizare şi cooperare. Enumerarea legală este enunțiativă, responsabilul cu protecția datelor având posibilitatea să îşi asume şi alte sarcini, cu evitarea conflictelor de interese (art. 38 alin. 6, art. 39). Paleta largă de atribuții conferă responsabilului cu protecția datelor rolul unui veritabil „chef d'orchestre" al conformității, în materie de protecție a datelor personale în cadrul entității respective[20].

*Informarea şi consilierea* sunt destinate responsabilului cu protecția datelor, persoanei împuternicite, angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentului regulament şi al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor. Unul dintre aspectele sensibile priveşte consilierea în raport cu realizarea studiului de impact, aflat în relație directă cu ocrotirea vieții private.

*Monitorizarea* vizează respectarea prevederilor Regulamentului. Exemplificativ, între activitățile specifice pot fi reținute: colectarea informațiilor în vederea identificării operațiunilor de prelucrare; analiza şi verificarea conformității acestor operațiuni; informarea, consilierea, emiterea de recomandări adresate operatorului sau împuternicitului acestuia[21].

*Cooperarea cu autoritatea de supraveghere* decurge din rolul conferit responsabilului cu protecția datelor – acela de a fi punct de contact pentru aspectele legate

[19] A. Lisievici, *Cum sporim confidențialitatea navigării online*, în revista Universul Juridic nr. 2/2015, p. 13.

[20] A se vedea, Commission Nationale Informatique et Liberté, *Règlement européen*, material disponibil la adresa https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes, consultată la data de 3 aprilie 2017.

[21] *Ibidem*, p. 17.

de operațiunile de prelucrare. Cooperarea cu autoritatea de supraveghere trebuie configurată ca o constantă a preocupărilor responsabilului cu protecția datelor şi ca o garanție a respectării drepturilor persoanelor vizate.

Ne oprim la una dintre ipotezele în care Regulamentul nr. 679/2016 impune, în mod explicit, linia de cooperare între responsabilul numit cu protecția datelor şi autoritatea de supraveghere. Potrivit art. 35 alin. 2, la realizarea unei evaluări a impactului asupra protecției datelor, operatorul (responsabil cu prelucrarea datelor) solicită avizul responsabilului cu protecția datelor. Este în discuție situația în care studiul de impact obligatoriu precede operațiunile de prelucrare, datorită naturii sensibile a datelor personale, datorită domeniului de aplicare ori datorită contextului sau scopurilor prelucrării (conform art. 35 alin. 1).

Avizul responsabilului cu protecția datelor este obligatoriu, ținând seama de riscul ridicat pentru drepturile şi libertățile persoanelor, generat de operațiunile de prelucrare. Avizul va fi cerut ori de câte ori sunt prezente următoarele situații: crearea de profiluri, consecutivă evaluării sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată (şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă); prelucrarea pe scară largă a unor categorii speciale de date (cum sunt datele arătate la art. 9 alin. 1 sau a unor date cu caracter personal privind condamnări penale ori infracțiuni; monitorizarea pe scară largă a unei zone accesibile publicului etc.

Atunci când evaluarea impactului asupra protecției datelor speciale indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului, operatorul consultă autoritatea de supraveghere anterior prelucrării. Consultarea autorității de resort este însoțită de furnizarea, de către responsabilul prelucrării, a datelor de contact ale responsabilului cu protecția datelor (art. 36 alin. 1, alin. 3 lit. d).

Recomandarea Grupului 29 este solicitarea obligatorie a avizului, de către responsabilul prelucrării, în legătură cu următoarele aspecte: dacă să efectueze sau nu evaluarea impactului operațiunilor de prelucrare; metodologia care urmează a fi utilizată pentru evaluare; efectuarea unei evaluări interne a impactului/ externalizarea procedurii; garanțiile (inclusiv măsuri tehnice şi organizaționale) reducerea oricăror riscuri la adresa drepturilor şi intereselor persoanelor vizate; corectitudinea efectuării evaluării impactului şi conformitatea concluziilor studiului cu prevederile Regulamentului. Se recomandă ca, în situația în care operatorul nu este de acord cu opinia responsabilului cu protecția datelor, documentația aferentă evaluării impactului operațiunilor de prelucrare să conțină motivația pentru care nu a fost urmat avizul[22].

[22] *Ghidul privind responsabilul pentru protecția datelor (DPO)*, *op. cit.*, p. 17.

**Evaluarea impactului şi consultarea prealabilă**

Noua procedură a evaluării impactului riscului anumitor tipuri de prelucrări a fost inițiată pe fondul constatării lipsei de eficiență a vechii proceduri de notificare, pe care o reglementa Directiva nr. 1995/46/CE. În decursul aplicării Directivei, a funcționat obligația generală de a notifica prelucrarea datelor cu caracter personal autorităților de supraveghere. Totuşi (şi cu toate că obligația respectivă a generat sarcini administrative şi financiare), notificarea nu a contribuit întotdeauna la îmbunătățirea protecției datelor cu caracter personal.

Prin urmare, noul Regulament de protecție a datelor personale a optat pentru un sistem structurat pe proceduri şi mecanisme care să pună accentul pe acele operațiuni de prelucrare susceptibile să genereze un risc ridicat pentru drepturile şi libertățile persoanelor fizice prin factori diverşi (natura datelor, domeniul lor de aplicare ş.a.). Astfel de tipuri de operațiuni de prelucrare pot fi cele care presupun, în special, utilizarea unor noi tehnologii sau care reprezintă un nou tip de operațiuni, pentru care nicio evaluare a impactului asupra protecției datelor nu a fost efectuată anterior de către operator ori care evaluarea devine necesară dată fiind perioada de timp care s-a scurs de la prelucrarea inițială. Pentru astfel de situații, se instituie procedura prealabilă a evaluării impactului asupra protecției datelor, procedură concepută a include, în special, măsurile, garanțiile şi mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecției datelor cu caracter personal şi pentru demonstrarea conformității cu Regulamentul.

Considerentele 89-90 din Regulament indică şi scopul noii proceduri – evaluarea gradului specific de probabilitate a materializării riscului ridicat şi gravitatea acestuia. În concret, în funcție de măsurile, garanțiile şi mecanismele preconizate pentru atenuarea riscului, evaluarea impactului se poate dovedi a fi un proces care implică uneori resurse financiare consistente, pe care operatorul, responsabil al prelucrării, trebuie să le pună în operă.

***Operațiunile supuse evaluării impactului***

Procedura evaluării impactului este determinată de factori cum sunt natura, domeniul de aplicare, contextul şi scopurile prelucrării datelor cu caracter personal – în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile şi libertățile persoanelor fizice.

Aşadar, într-o selecție a operațiunilor pentru care apare necesitatea efectuării studiului de impact, sunt reținute cele care, în raport cu criteriul riscului, trebuie analizate anterior prelucrării. Întocmirea şi publicarea listei tipurilor de operațiuni de prelucrare care fac obiectul cerinței evaluării asupra protecției datelor revine în sarcina autorității de supraveghere din statul membru (se înțelege, autoritatea de supraveghere care joacă rolul de „*one-stop-shop*"). Mai departe, lista se transmite

Comitetului european pentru protecția datelor, organ cu personalitate juridică al Uniunii Europene. Comitetul are, între îndatoririle curente, sarcina monitorizării aplicării corecte a Regulamentului în statele Uniunii – ceea ce presupune ca indispensabilă, evidența operațiunilor de prelucrare supuse evaluării prealabile a impactului asupra protecției datelor. Operațiunile care nu necesită evaluarea impactului intră în componența unei liste pe care autoritatea națională de supraveghere o poate pune la dispoziția publicului (şi pe care o comunică, de asemenea, Comitetului).

Potrivit Regulamentului, evaluarea impactului se impune, mai ales, în cazul: a. *evaluării sistematice şi cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată*, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă.

Profilajul sau **crearea de profiluri** implică utilizarea unei cantități semnificative de date referitoare la persoanele fizice, motiv pentru care această activitate este imperativ a se regăsi pe listele obligatorii de evaluare prealabilă a impactului. În accepțiunea Regulamentului nr. 679/2016, prin „*creare de profiluri*" se înțelege orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia. Crearea profilului pe baza datelor personale presupune colectarea şi prelucrarea unor categorii de date personale ce acoperă nu numai activitatea profesională a persoanei vizate, dar şi aspecte sensibile de viață personală şi chiar de intimitate;

b. *prelucrării pe scară largă a unor categorii speciale de date*, menționată la art. 9 alin. 1 sau a unor date cu caracter personal privind condamnări penale sau infracțiuni, conform art. 10. Un exemplu menționat introductiv în Regulament (considerentul 91) este cel în care operațiunile au ca obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, național sau supranațional, ce ar putea afecta un număr mare de persoane vizate şi care sunt susceptibile de a genera un risc ridicat – de pildă, în cazul în care, în conformitate cu nivelul atins al cunoştințelor tehnologice, se foloseşte la scară largă o tehnologie nouă;

c. *prelucrarea datelor cu caracter personal nu ar trebui considerată a fi la scară largă, în cazul în care prelucrarea se referă la date cu caracter personal de la pacienți sau clienți de către un anumit medic, un alt profesionist în domeniul sănătății sau un avocat*. În aceste cazuri, o evaluare a impactului asupra protecției datelor nu ar trebui să fie obligatorie;

d. *monitorizării sistematice pe scară largă a unei zone accesibile publicului.* Natura sensibilă a datelor şi, respectiv, datele referitoare la condamnări penale/infracțiuni, reclamă evaluarea prealabilă şi obligatorie a impactului asupra protecției datelor. Se oferă exemplul utilizării dispozitivelor optoelectronice sau pentru orice alte operațiuni în cazul în care autoritatea de supraveghere competentă consideră că prelucrarea este susceptibilă de a genera un risc ridicat pentru drepturile şi libertățile persoanelor vizate, deoarece acestea împiedică persoanele vizate să exercite un drept sau să utilizeze un serviciu ori un contract (considerentul 91).

**Nu este necesară evaluarea impactului** asupra protecției datelor personale, pentru acele operațiuni de prelucrare ce sunt incluse pe lista autorității de supraveghere (lista cu operațiunile care nu fac obiectul evaluării, conform art. 35 alin. 5).

Ambele categorii de liste presupun aplicarea mecanismului pentru asigurarea coerenței (mecanism la care face referire art. 63) în cazul în care listele implică activități de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii către persoane vizate sau monitorizarea comportamentului acestora în mai multe state membre ori care pot afecta în mod substanțial libera circulație a datelor cu caracter personal în cadrul Uniunii.

Ghidul privind evaluarea impactului menționează încă două situații în care evaluarea nu este obligatorie[23]:

a. *natura/contextul/finalitatea prelucrării sunt asemănătoare cu cele ale operațiunilor pentru care s-a efectuat deja evaluarea impactului, astfel că se va recurge la rezultatele anterioare ale evaluării*. În ce priveşte această ipoteză, credem că este util să se verifice data la care a fost efectuat studiul anterior de impact. Un interval de timp mai îndelungat sau o perioadă în care au intervenit modificări ale datelor cunoscute la nivel național/internațional, necesită evaluare de impact, pentru a evita atingerea drepturile şi libertățile persoanelor vizate;

b. atunci când prelucrarea în temeiul art. 6 alin. 1 lit. c) sau lit. e) are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar dreptul respectiv reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză şi *deja s-a efectuat o evaluare a impactului asupra protecției datelor,* ca parte a unei evaluări a impactului general în contextul adoptării respectivului temei juridic, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfăşurării activităților de prelucrare (alin. 10, art. 35 din Regulament).

---

[23] O. Guerguinov, T. Léonard, *GDPR: le Groupe 29 (G29) dévoile ses lignes directrices concernant «l'analyse d'impact»*, informații disponibile pe pagina https://www.droit-technologie.org/actualites/gdpr-groupe-29-g29-devoile-lignes-directrices-concernant-lanalyse-dimpact/ (accesată la data de 3 mai 2017).

***Obiectul evaluării impactului***

Minimal, activitatea de evaluare a impactului cuprinde **elementele** ce urmează: descrierea sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, precum şi a interesului legitim urmărit de operator; evaluarea necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri; evaluarea riscurilor pentru drepturile şi libertăţile persoanelor fizice vizate; măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor cu caracter personal şi să demonstreze conformitatea cu dispoziţiile prezentului regulament, luând în considerare drepturile şi interesele legitime ale persoanelor vizate şi ale altor persoane interesate.

***Aspecte privind procesul de evaluare a impactului şi consultarea prealabilă***

*Evaluarea impactului asupra protecţiei datelor*

Procesul de evaluare a impactului asupra protecţiei datelor este reglementat în detaliu în Regulament, iar unele precizări utile se regăsesc în considerentele acestuia.

a. *procesul evaluării impactului precede operaţiunile de prelucrare a datelor cu caracter personal*. Procedura evaluării impactului are scopul de a identifica garanţiile optime pentru a evita lezarea drepturilor şi libertăţilor persoanelor fizice (între care dreptul la respectarea vieţii private ocupă un loc primordial).

b. *evaluarea impactului necesită avizul responsabilului cu protecţia datelor/avizul persoanelor vizate sau al reprezentanţilor acestora.* Firesc şi logic, exprimarea opiniei cu privire la impactul prelucrării este una dintre atribuţiile responsabilul desemnat cu protecţia datelor în cadrul organizaţiei în care se intenţionează prelucrarea. Solicitarea avizului persoanelor vizate se cere să nu aducă atingere protecţiei intereselor comerciale sau publice ori securităţii operaţiunilor de prelucrare. Grupul 29 subliniază necesitatea motivării refuzului de a ţine seama de avizul responsabilului cu protecţia datelor sau, după caz, de avizul celui vizat de prelucrare/reprezentantului acestuia.

c. la evaluarea impactului operaţiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, *se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate* menţionate la articolul 40, în special în vederea unei evaluări a impactului asupra protecţiei datelor.

d. *acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecţiei datelor*, cel puţin atunci când are loc o modificare a riscului reprezentat de operaţiunile de prelucrare.

*Consultarea prealabilă*

Evaluarea impactului este în strânsă relație cu procedura consultării prealabile. Atunci când **evaluarea impactului asupra protecției datelor indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului**, responsabilul prelucrării consultă autoritatea de supraveghere.

În cazul în care o evaluare a impactului asupra protecției datelor arată că prelucrarea ar genera, în absența garanțiilor, măsurilor de securitate şi mecanismelor de atenuare a riscului, un risc ridicat pentru drepturile şi libertățile persoanelor fizice, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile şi al costurilor implementării, autoritatea de supraveghere urmează a fi consultată înainte de începerea activităților de prelucrare. Un astfel de risc ridicat este susceptibil să fie generat de anumite tipuri de prelucrare, precum şi de amploarea sau frecvența prelucrării, care pot duce la cauzarea unor prejudicii ori pot atinge drepturile şi libertățile persoanelor fizice.

În ipotezele menționate, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris responsabilului cu prelucrarea datelor/împuternicitului acestuia, în termen de cel mult opt săptămâni de la primirea cererii de consultare. Termenul poate fi prelungit cu şase săptămâni, ținându-se seama de complexitatea prelucrării preconizate. Autoritatea de supraveghere informează operatorul şi, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii (aceste perioade pot fi suspendate până când autoritatea de supraveghere a obținut informațiile pe care le-a solicitat în scopul consultării).

Cu prilejul consultării prealabile a autorității de supraveghere, responsabilul prelucrării furnizează acesteia toate informațiile care privesc scopul şi mijloacele prelucrării, responsabilitățile persoanelor implicate în operațiuni, datele de contact ale responsabilului cu protecția datelor, măsuri şi garanții prevăzute pentru protecția drepturilor şi libertăților celor vizați de prelucrare, evaluarea impactului, precum şi orice alte informații solicitate de autoritate.

Regulamentul prevede încă două situații în care consultarea prealabilă este obligatorie (art. 36 alin. 4-5). Statele membre consultă autoritatea de supraveghere **în cadrul procesului de pregătire a propunerii unei măsuri legislative care urmează a fi adoptată de un parlament național sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă, care se referă la prelucrarea datelor personale.** Apoi**, dreptul intern poate impune operatorilor să se consulte cu autoritatea de supraveghere şi să obțină în prealabil autorizarea din partea acesteia** în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecția socială şi sănătatea publică.

**Concluzii**

Reglementarea responsabilului pentru protecția datelor este unul dintre „punctele tari" ale Regulamentului (UE) nr. 679/216 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi libera circulație a acestor date. Importanța instituției nou introduse de Regulament poate fi citită şi prin prisma consecințelor omisiunii de a numi un asemenea responsabil, până la data de 25 mai 2018 (în cazurile în care legea obligă la numire). Sancțiunea administrativă constă în amendă de până la 10.000.000 euro sau, în cazul unei întreprinderi, de până la 2% din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare (art. 83 alin. 4 lit. a).

Procedura evaluării impactului, corelată cu consultarea prealabilă, are rolul de a evidenția riscurile prelucrării, în raport cu drepturile şi libertățile persoanelor vizate. În măsura în care activitățile ce reclamă evaluarea riscurilor vor fi riguros identificate (de către autoritățile de supraveghere), iar mecanismul complex al garanțiilor, măsurilor, remediilor de atenuare/anihilare a riscurilor se va dovedi viabil, noua procedură de evaluare a impactului se poate converti într-un instrument util şi eficient pentru toate persoanele implicate în prelucrarea datelor personale.