RESPONSABILUL CU PROTECTIA DATELOR - EXEMPLE DE ORGANIZARE LA NIVEL EUROPEAN

Lucrarea de fata isi propune sa abordeze mai putin aspecte de natura teoretica privind rolul, numirea si atributiile *Responsabilului pentru protectia datelor (“DPO”)*, asa cum sunt acestea definite in art. 37-39 din *Regulamentul General pentru Protecţia Datelor* (“Regulamentul”), ci doreste sa adreseze aspecte de natura practica legate de pozitia Responsabilului pentru protectia datelor in cadrul organizatiei, astfel incat sa fie respectate cerintele legale din Regulament, atunci cand, desigur, operatorul a decis sa nu externalizeze aceasta activitate.

Baza legala privind funcţia Responsabilului pentru protectia datelor in cadrul organizatiei, o reprezinta prevederile art. 38 alin (3) din Regulament care stabilesc cateva conditii, respectiv:

- *„responsabilul cu protecţia datelor nu primeşte niciun fel de instrucţiuni în ceea ce priveşte îndeplinirea sarcinilor sale de la operator sau de la persoana împuternicită de operator si*
- *responsabilul cu protecţia datelor răspunde direct în faţa celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator*.”

La o prima vedere, pare ca Responsabilul pentru protectia datelor nu ar putea indeplini alte sarcini in cadrul organizatiei. Insa, in acest sens, sunt relevante dispozitiile art. 38 (6) din Regulament, unde se arata explicit faptul ca „(6) *Responsabilul cu protecţia datelor poate îndeplini şi alte sarcini şi atribuţii.”* insa *„Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini şi atribuţii nu generează un conflict de interese*.”

Trebuie de asemenea mentionat faptul ca, in raport de prevederile Art. 24 din Regulament, sarcina probei respectarii prelucrarii in conformitate cu prevederile Regulamentului, revine operatorului „*operatorul pune în aplicare măsuri*

tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament."

Totusi, din punct de vedere practic, textul ramane in continuare cu o formulare generala si, datorita diferentelor de legislatie intre Statele Membre, inclusiv in ceea ce priveste definirea unor termeni, este de asteptat ca pozitionarea Responsabilului cu protecţia datelor in cadrul organizatiei in Statele Membre sa fie diferita, desi, de aceasta data, spre deosebire de Directiva 95/46/CE, avem in analiza un text direct aplicabil.

Astfel, revine in sarcina doctrinei, legiuitorului statelor membre, Comisiei si, in final, instantei nationale si CJUE sa clarifice corecta interpretare ulterioara a textului legal.

Insa, pana atunci, putem analiza modelul statelor care au inteles sa creeze institutia "*responsabilului cu protecţia datelor"*, chiar in procesul de transpunere a Directivei 95/46/CE, in considerarea recomandarilor cuprinse in ghiduri, precum Grupul de Lucru Articolul 29.

Analizand dispozitiile noului Ghid privind Responsabilul cu protecția datelor ('*DPOs*') [1], acesta reitereaza, ca si in varianta precedenta, ca „*DPO reprezintă un punct important al responsabilității […] si ar trebui considerat un "dirijor al conformitatii" si un intermediar între părţile interesate relevante (precum autoritățile de supraveghere, persoanele vizate și unitățile de afaceri din cadrul unei organizații)."*

De asemenea, in dezvoltarea prevederilor Regulamentului, analizand "pozitia Responsabilului pentru protectia datelor in organizatie" arata ca:

"*DPO „indiferent dacă este sau nu angajat al operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent". Acest lucru înseamnă că, îndeplinirea sarcinilor ce revin în temeiul art. 39, DPO nu trebuie să fie instruit cum să se ocupe de o problemă, de exemplu, ce rezultat ar*

[1] 16/ROWP 243 rev.01 - Ghid privind Responsabilul cu protecția datelor ('DPOs') Adoptat în data de 13 decembrie 2016 Revizuit și adoptat în data de 5 aprilie 2017

trebui atins, cum să fie investigată o plângere sau dacă să consulte autoritatea de supraveghere. Mai mult, acesta nu trebuie să fie instruit să adopte o anumită perspectivă a problemei legată de legislația privind protecția datelor, de exemplu, o anumită interpretare a legii.

Cu toate acestea, autonomia DPO nu înseamnă că acesta are competențe de luare a deciziilor care se extind dincolo de sarcinile sale, potrivit art. 39. Operatorul sau persoana împuternicită de operator este responsabil pentru respectarea legislației privind protecția datelor și trebuie să poată demonstra conformitatea. Dacă operatorul sau persoana împuternicită de operator ia decizii care sunt incompatibile cu RGPD și cu opinia DPO, DPO ar trebui să aibă posibilitatea de a-și exprima clar opinia sa divergentă la cel mai înalt nivel de management și persoanelor implicate în luarea deciziilor. În acest sens, art. 38(3) prevede că DPO „răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator". O asemenea raportare directă asigură că managementul superior (consiliul de conducere) este conștient de consilierea și recomandările DPO ca parte a misiunii DPO de a informa și a consilia operatorul sau persoana împuternicită de operator. Un alt exemplu de raportare directă este elaborarea unui raport annual al activităților DPO oferit la cel mai înalt nivel de management."

In continuare, *„art. 38(6) permite DPO „să îndeplinească și alte sarcini și atribuții". Cu toate acestea, este nevoie ca organizația să se asigure că „niciuna dintre aceste sarcini și atribuții nu generează un conflict". Absența conflictului de interese este strâns legată de obligația de a acționa în mod independent. Cu toate că îi este permis să aibă și alte funcții, acestuia îi pot fi încredințate alte sarcini și atribuții cu condiția ca acestea să nu dea naștere unor conflicte de interese. Acest lucru presupune, în special, faptul că DPO nu poate deține o poziție în cadrul organizației care ar conduce la posibilitatea ca DPO să stabilească scopurile și mijloacele de prelucrare a datelor cu caracter personale. Acest lucru trebuie luat în considerare de la caz la caz, ținându-se*

cont de structura organizațională specifică fiecărei organizații. Ca regulă generală, funcții din cadrul organizației cu care poate intra în conflict pot include funcții de conducere (cum ar fi director executiv, director operațional, director financiar, șeful departamentului de marketing, șef departamentului de resurse umane sau șeful departamentului IT), dar, în același timp, și alte funcții inferioare dacă acestea conduc la posibilitatea de a stabili scopurile și mijloacelor de prelucrare. În plus, un conflict de interese poate apărea, de asemenea, de exemplu, în situația în care un DPO extern este rugat să reprezinte oporatorul sau persoana împuternicită de operator în instanță, în cazurile care implică probleme de protecție a datelor. În funcție de activitățile, dimensiunea și structura organizației, o bună practică pentru operatori și persoanele împuternicite de operatori ar putea fi:

- *să identifice funcțiile ce ar fi incompatibile cu funcția de DPO*
- *să elaboreze norme interne în acest sens pentru a evita conflictele de interese*
- *să includă o explicație mai generală cu privire la conflictele de interese*
- *să declare că DPO lor nu are niciun conflict de interese în ceea ce privește funcția sa ca și DPO, ca și modalitate de creștere a gradului de conștientizare a acestei cerințe*
- *să includă garanții în normele interne ale organizației și să se asigure că anunțul de post vacant pentru funcția de DPO sau contractul de prestări servicii este suficient de precis și detaliat pentru a evita conflictul de interese. În acest context, trebuie avut în vedere faptul că respectivele conflicte de interese pot lua diverse forme în funcție de faptul dacă DPO este recrutat intern sau extern*."[2]

Revenind la aspectul practic, conform informatiilor furnizate de Comisie, din cele 28 de State Membre, rezulta ca doar in cazul Germaniei si al Croatiei exista obligatia legala a numirii unui Responsabilul pentru protectia datelor in cazul

[2] Sursa: http://www.dataprotection.ro/servlet/ViewDocument?id=1384

entitatilor private, - *cele cu peste 9 si, respectiv peste 20 de salariati* -, iar in cazul Ungariei, pentru anumite tipuri de entitati, printre care si institutiile financiare.
In cazul Ungariei, Responsabilul pentru protectia datelor trebuie sa aiba studii universitare in drept, economie sau IT si raporteaza direct Directorului General.

Un caz interesant este cel al Lituaniei, stat in care desi nu este obligatorie numirea unui Responsabilul pentru protectia datelor, in cazul in care organizatia nu il desemneaza, Directorul General va fi considerat din oficiu persoana responsabila cu respectarea conformitatii cu legea privind protectia datelor si poate raspunde chiar penal.

Unele State Membre precum Franta, Norvegia, Polonia, Suedia, Elvetia nu obliga numirea unui Responsabilul pentru protectia datelor, dar ofera beneficii - *precum scutirea de la obligatia de notificare* in cazul desemnarii unui Responsabilul pentru protectia datelor.

Toate institutiile si organismele UE au desemnat un Responsabilul pentru protectia datelor.

Am ales sa prezint trei exemple de subordonare a Responsabilului pentru protectia datelor, reprezentative dupa pararea mea: organizarea unei entitati private - *ATOS SE* si a doua entitati la nivel european, respectiv *Autoritatea Europeană pentru Protecția Datelor* si *Banca Europeana de Investitii*.
Am ales ca exemplu privat cazul Atos SE pentru ca este unul din cei mai importanti furnizori de servicii digitale, cu venituri anuale de aproximativ €10 miliarde si 86,000 angajati in 66 de tari[3], astfel ca, aceasta entitate este necesar a se conforma cerintelor legale din 66 de state in materia protectiei datelor, un

[3] Sursa: https://atos.net/content/dam/global/documents/investor-financial-reports/atos-2014-registration-document.pdf

subiect extrem de important in activitatea societatii. Dupa cum se poate observa din rapoartele publicate de Atos[3], aceasta entitate a ales ca model de organizare in materie de supraveghere a conformitatii protectiei datelor, numirea unui Responsabil pentru protectia datelor la nivelul fiecarei tari, acesta fiindsustinut in activitatea sa de mai multi ofiteri de protectia datelor. Ca cerinta, Responsabilul pentru protectia datelor este un expert legal, specializat in legislatia privind protectia datelor, iar ofiterii de protectia datelor, sunt experti in zona tehnica, de securitate IT. Responsabilul pentru protectia datelor raporteaza catre „*Group Data Protection Officer*" care raporteaza la randul sau catre „*Group General Counsel"* si catre *„Group Head of Human Resources"*.

Autoritatea Europeană pentru Protecția Datelor, entitate independenta, care are ca scop asigurarea conformitatii cu legislatia privind protectia datelor la nivelul Uniunii, are la randul sau un Responsabil pentru protectia datelor care raporteaza catre "*Directorul"* entitatii.

In cazul Bancii Europene de Investitii, Responsabilul pentru protectia datelor raporteaza Directorului de Conformitate[4].

Asa cum se poate observa, structura corporativa in care isi desfasoara activitatea Responsabilul pentru protectia datelor in entitati este diversa, astfel ca, revine fiecarui operator sau imputernicit al operatorului sarcina de a stabili structura care se potriveste cel mai bine actiivitatii sale, respectand principiul independentei Responsabilului pentru protectia datelor, principiu care insa nu trebuie interpretat ca o cerinta absoluta, a lipsei vreunei subordonari ierarhice si nici ca o interdictie de a indeplini alte activitati in cadrul entitatii, cata vreme sunt respectate pricipiile legale privind evitarea conflictului de interese stabilite de Regulament.

[4] Sursa: http://www.eib.org/about/governance-and-structure/organisation/services/entity/egco/?lang=-en