Responsabilul cu protecţia datelor cu caracter personal

Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul General privind Protecția Datelor) urmează să fie pus direct în aplicare în toate statele membre ale Uniunii Europene începând cu data de 25 mai 2018.

Un element de noutate pe care acest act normativ european îl aduce în peisajul juridic românesc îl reprezintă instituirea obligativității desemnării la nivelul operatorului sau persoanei împuternicite de operator, în anumite cazuri, a unui **responsabil cu protecția datelor**. Pentru asigurarea unei aplicări unitare a Regulamentului General privind Protecția Datelor, Grupul de Lucru Art. 29 de pe lângă Comisia Europeană a emis **Ghidul privind Responsabilul cu protecția datelor (DPO)**, accesibil la secțiunea specială dedicată Regulamentului General privind Protecția Datelor, la adresa http://www.dataprotection.ro/servlet/ViewDocument?id=1384, accesibilă pe site-ul Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal.

I. Cazurile în care este obligatorie desemnarea unui responsabil cu protecția datelor

1. **Când prelucrarea este efectuată de o autoritate publică sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale**
2. **Dacă activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrarea care necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă**
3. **Dacă activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date sau a unor categorii de date cu caracter personal privind condamnări penale și infracțiuni**

Ce înseamnă ”**Activități principale**”?
Pentru a stabili activitatea principală desfășurată de un operator sau împuternicit, aceasta trebuie analizată prin raportare la prelucrările de date cu caracter personal efectuate.

La ce se referă „**Monitorizarea periodică și sistematică**”?
Aceasta presupune toate formele de urmărire și profilare pe Internet, inclusiv în scop de publicitate comportamentală, nefiind însă restrictionată în mediul online.

Sintagma ”periodică și sistematică” presupune o activitate continuă și recurentă, care implică prelucrări de date.

Ce presupune prelucrarea ”**Pe scară largă**”?
Pentru a se stabili dacă o prelucrare este pe scară largă trebuie ținut cont de 4 criterii:

- numărul persoanelor vizate – un număr exact ori un procent din populația relevantă;
- volumul datelor și/sau gama de elemente diferite de date în curs de prelucrare;
- durata sau permanența activității de prelucrare a datelor;
- suprafața geografică a activității de prelucrare.

Ce înseamnă ”**Categorii speciale de date**”?
Categoriile speciale sunt acele date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

Exemple de situații care pot constitui o monitorizare periodică și sistematică a persoanelor vizate:

- gestionarea unei rețele de telecomunicații;
- profilare și scoring în scopul evaluării riscurilor (de exemplu, în scopul acordării unui credit, stabilirea primelor de asigurare, de prevenire a fraudelor, detectarea spălării banilor);
- urmărirea locației, spre exemplu prin aplicații mobile (geolocalizare);
- desfășurarea de programe de loialitate;
- monitorizarea stării de sănătate prin intermediul dispozitivelor portabile;
- televiziune cu circuit închis – CCTV;
- prelucrarea datelor pacienților de către un spital;
- prelucrarea datelor datelor de conținut, locație, trafic de către furnizorii de servicii de internet;

- prelucrarea datelor personale de către companii de asigurări;
- publicitate comportamentală.

Când nu este necesară desemnarea unui responsabil cu protecţia datelor?
– atunci când nu se prelucrează pe scară largă date cu caracter personal.

Spre exemplu:

- prelucrarea datelor pacientului de către un cabinet medical individual;
- prelucrarea datelor personale referitoare la condamnările penale și infracțiuni de către un cabinet individual de avocatură.

De reținut !
Deși în unele cazuri nu este necesară desemnarea unui responsabil cu protecția datelor, Autoritatea de Supraveghere recomandă numirea unei astfel de persoane, întrucât este utilă operatorului pentru respectarea obligațiilor în domeniul protecției datelor cu caracter personal.

II. Cine poate îndeplini funcția de responsabil cu protecția datelor?
Articolul 37 alin. 5 din Regulamentul UE 2016/679 stabileşte ca responsabilul cu protecţia datelor să fie ”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.”

Responsabilul cu protecția datelor
1. **în domeniul public,**
2. **în domeniul privat, raportat la situațiile prevăzute expres de art. 37 RGDP**

Responsabilul cu protecția datelor poate fi angajat al operatorului/persoanei împuternicite de operator sau poate să-și îndeplinească sarcinile pe baza unui contract de prestări servicii.
În domeniul public, poate fi **desemnat pentru mai multe autorități sau instituții publice**, luând în considerare structura organizatorică și dimensiunea acestora

Calități și competențe:
Trebuie să aibă capacitatea de a îndeplini sarcinile. În acest sens sunt necesare anumite calități personale (ex: integritate și etica profesională), cunoștințe, dar și o anumită poziție în cadrul organizației.

Trebuie să aibă anumite calități profesionale, astfel:

- experiență în legislația și practicile de protecție a datelor la nivel național și european, precum și o înțelegere adecvată a RGPD;
- nivelul necesar de cunoștințe în domeniul protecției datelor în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție necesar pentru datele cu caracter personal prelucrate;
- să înțeleagă operațiunile de prelucrare efectuate, precum și sistemele de informații și necesitățile de securitate și protecție a datelor prelucrate de operator;
- în cazul unei autorități sau instituții publice, responsabilul cu protecția datelor trebuie să dețină, de asemenea, cunoștințe privind reglementările legale referitoare la organizarea și funcționarea acestora, precum și a procedurilor interne administrative ce vizează desfășurarea activității.

Principala preocupare a responsabilului cu protecția datelor trebuie să fie respectarea Regulamentului General privind Protecția Datelor și a reglementărilor naționale incidente.

Este **obligat să păstreze secretul sau confidențialitatea** în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.
Operatorul sau persoana împuternicită de operator, în ceea ce privește raporturile cu responsabilul cu protecția datelor, este obligat să:

- publice datele de contact ale responsabilului (adresă poștală, număr de telefon alocat special și/sau o adresă de email alocată special).
- comunice datele de contact ale responsabilului către Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal.

Responsabilului cu protecția datelor îi este permis să aibă și alte funcții.
Acestuia îi pot fi încredințate și alte sarcini și atribuții, **cu condiția** ca acestea să **nu dea naștere unor conflicte de interese** (de ex: nu poate fi director executiv, director operațional, director financiar, șeful serviciului medical, șeful departamentului de marketing, șeful departamentului de resurse umane sau șeful departamentului IT).
Responsabilul pentru protecția datelor nu poate fi demis sau sancționat de operator sau persoana împuternicită de operator pentru **îndeplinirea sarcinilor sale**.
De exemplu, responsabilul nu poate fi demis pentru oferirea unui sfat conform sacinilor sale.

Un responsabil cu protecția datelor **ar putea fi totuși demis**, în mod legal, din alte motive decât cele privind îndeplinirea sarcinilor sale în această calitate.
De exemplu, responsabilul poate fi demis în caz de furt, hărțuire ori o abatere gravă similară.

III. **Sarcinile responsabilului cu protecția datelor**

- **de a informa şi consilia operatorul, sau persoana împuternicită de operator, precum şi angajaţii care se ocupă de prelucrările de date;**
- **de a monitoriza respectarea Regulamentului, a altor dispoziţii de drept al Uniunii sau de drept intern referitoare la protecţia datelor;**
- **de a consilia operatorul în ceea ce priveşte realizarea unei analize de impact asupra protecţiei datelor şi de a monitoriza executarea acesteia;**
- **de a coopera cu Autoritatea de Supraveghere și de a reprezenta punctul de contact cu aceasta;**
- **de a ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, la îndeplinirea sarcinilor sale.**

Pentru mai multe informații recomandăm consultarea **Ghidului privind Responsabilul cu protecția datelor (DPO)**, accesibil în secțiunea specială privind Noul Regulament de pe site-ul Autorității Naționale de Supraveghere a Datelor cu Caracter Personal – www.dataprotection.ro.
Biroul Juridic și Comunicare

ANSPDCP