

# DPO – furnizor extern sau salariat nou/existent? Standardul ocupațional

Unul dintre elementele importante pentru aliniere la Regulamentul (UE) 2016/679 este **înființarea unei noi funcții** în cadrul organizațiilor vizate, un Data Protection Officer (DPO) care oferă consultanță la nivel executiv și care se asigură că toate reglementările Regulamentului sunt respectate. Acest aspect intervine în primul rând pe fondul caracterului tehnic și al dificultății de înțelegere a Regulamentului de către cineva care nu este avizat, existând așadar o nevoie acerbă de îndrumări și ghidaj din partea unui specialist.

Potrivit art. 37 alin. 6 din Regulament: „*Responsabilul cu protecția datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să își îndeplinească sarcinile în baza unui contract de servicii.*”, organizațiile având o marjă de apreciere în privința modalităților prin care înțeleg să angajeze un astfel de specialist, respectiv: contractarea unui consultant extern sau angajarea unui salariat nou sau existent – chestiune ce ridică câteva probleme specifice managementului organizațiilor.

Din punct de vedere organizațional, funcția de DPO ar trebui să se reflecte în organigrama societății, fie prin actualizarea acesteia – crearea unui nou post, fie prin completarea cu atribuțiile specifice a unui post deja existent. De asemenea, funcția de DPO presupune existența unor raporturi contractuale care să îi reglementeze atribuțiile specifice funcției, indiferent că vorbim despre o persoană nou angajată sau o persoană deja existentă în cadrul companiei (contract de prestări servicii, contract de

muncă, act adițional la contractul de muncă).

Din perspectiva evaluării activității unui DPO, considerăm că aceasta s-ar putea desfășura în mod similar cu cea a angajaților. Toate aceste chestiuni impun însă întocmirea unor politici clare care să prevadă și să definească:

- mecanismele de prelucrare a datelor cu caracter personal;
- procesele/măsurile care trebuie respectate și urmărite;
- prevederea clară a sarcinilor și atribuțiilor DPO-ului;
- politici interne, fișe ale postului, contract prin care să se prevadă inclusiv sarcini de raportare către conducerea societății;
- instituirea unui mecanism de control a activității DPO, din partea unor terți sau din partea autorității de supraveghere.

Datorită noutății rolului, responsabilităților și funcționalităților acestui rol al DPO în organigrama unei companii, Autoritatea Națională pentru Calificări a aprobat **standardul ocupațional pentru Responsabil cu protecția datelor cu caracter personal** (COR 242231), prin Decizia nr. 74 din 19 martie 2018, standard care va sta la baza cursurilor de formare profesională viitoare pentru această poziție în România.

Acest standard permite astfel recunoașterea la nivel oficial în România (prin COR) a acestei noi ocupații în România și autorizarea unor cursuri de training DPO, confirmate de o diplomă de calificare oficială în

## ATENȚIE!

**Autoritatea Națională pentru calificări a aprobat standardul ocupațional pentru Responsabil cu protecția datelor cu caracter personal – COR – 242231.**

## ATENȚIE!

**Operatorul de date cu caracter personal trebuie să se asigure că atribuțiile DPO-ului nu intră în conflict cu alte sarcini pe care acesta le îndeplinește.**

cea ce privește protecția datelor cu caracter personal, cât și securitatea informației, organizarea proceselor interne și managementul datelor. În acest fel, pe de o parte, fiecare operator ar fi capabil să se poată conforma prevederilor Regulamentului și a evita riscul unor amenzi care pot fi extrem de costisitoare pentru companii, iar pe de altă parte, această certificare permite celor doritori să își construiască o carieră în domeniul protecției datelor cu caracter personal.

Standardul ocupațional pentru educație și formare profesională are în vedere **competențele și deprinderile** care trebuie să se regăsească în persoana unui DPO, și anume:

1. Informarea organizației și persoanelor vizate cu privire la drepturile și obligațiile lor în baza legislației privind protecția datelor cu caracter personal
2. Monitorizarea modalității în care organizația respectă legislația privind protecția datelor cu caracter personal și standardele specifice la care organizația a aderat
3. Emiterea de recomandări și oferirea asistenței de specialitate organizației cu privire la interpretarea și aplicarea prevederilor legislației privind protecția datelor cu caracter personal
4. Gestionarea relației cu autoritatea de supraveghere în domeniul protecției datelor cu caracter personal
5. Respectarea principiului obiectivității în domeniul protecției datelor cu caracter personal
6. Asigurarea și gestionarea registrului de evidență al prelucrării datelor cu caracter personal
7. Gestionarea și coordonarea resurselor umane, financiare, tehnice necesare

realizării sarcinilor și activităților specifice domeniului protecției datelor cu caracter personal

8. Dezvoltarea profesională continuă în domeniul protecției datelor cu caracter personal
9. Monitorizarea aplicării instrumentelor și metodelor de îmbunătățire a eficacității sistemului de management al securității informației
10. Analizarea și evaluarea riscurilor de prelucrare a datelor cu caracter personal.

### **Cerințe speciale de exercitare a ocupației Responsabilului cu protecția datelor cu caracter personal:**

- vechime în muncă: minimum 1 an;
- studii superioare absolvite cu diplomă de licență și curs de specializare/perfecționare absolvit cu certificat care să ateste competențele formate;
- cunoașterea aprofundată a legislației domeniului;
- abilități de comunicare;
- responsabilitate, seriozitate, punctualitate, empatie, capacitate de analiză-sinteză;
- capacitatea de a asigura confidențialitatea datelor la care are acces.

### **Cerințele privind nivelul minim de calificare și experiență profesională pentru formatori și instructori/preparatori formare:**

- îndeplinește condițiile impuse de legislația în vigoare aplicabilă formatorilor și instructorilor/preparatori formare;
- are o experiență de minimum 3 ani în domeniul protecției datelor cu caracter personal.

### **Cerințe privind nivelul minim de calificare și experiență profesională pentru evaluatori:**

- îndeplinește condițiile impuse de legislația în vigoare aplicate evaluatorilor;

- are o experiență de minimum 5 ani în domeniul protecției datelor cu caracter personal.

Sunt prevăzute de asemenea, informații referitoare la procesul de elaborare, verificare, validare, avizare și aprobare a standardului ocupațional (*inițiatori/autori, specialiștii care se vor ocupa de verificarea profesională/avizare/validare documentație/aprobare*).

Regulamentul nu stabilește foarte precis situațiile în care organizațiile implicate în prelucrarea de date cu caracter personal sunt obligate să desemneze un DPO (*de exemplu, atunci când activitățile principale ale organizației constau în operațiuni de prelucrare care necesită o monitorizare pe scară largă, periodică și sistematică a persoanelor vizate sau a unor categorii speciale de date*).

Un lucru este cert, și anume: desemnarea DPO se poate face nu doar în situațiile în care este obligatorie, potrivit Regulamentului, ci orice operator poate să-și desemneze un DPO, avându-se în vedere în special cantitatea riscurilor la care organizația se expune prin prelucrarea datelor cu caracter personal, atât din perspectiva naturii datelor cu caracter personal pe care le prelucrează, cât și amplitudinii activității sale (*numărul persoanelor vizate, volumul datelor cu caracter personal, durata activității de prelucrare a datelor personale, aria geografică a activității de prelucrare*).

## ȘTIAȚI CĂ?

„Responsabilul” cu protecția datelor cu caracter personal nu este persoana care preia responsabilitatea protecției datelor, ci această responsabilitate rămâne în sarcina operatorului. Responsabilul este denumit așa în virtutea atribuțiilor sale, nu în virtutea obligațiilor sale.

Fie că vorbim despre un DPO – contractant extern sau despre un DPO angajat cu contract de muncă (și/persoană deja existentă în cadrul companiei), în ambele situații, operatorul sau persoana împuternicită trebuie să se asigure că niciuna dintre aceste sarcini și atribuțiile acestuia nu generează un conflict de interese, având în vedere următoarele linii directoare a activității unui DPO:

- responsabilul cu protecția datelor **nu primește niciun fel de instrucțiuni** în ceea ce privește îndeplinirea acestor sarcini din partea operatorului sau a persoanei împuternicite;
- DPO **nu este demis sau sancționat** de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale;
- responsabilul cu protecția datelor **răspunde direct** în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

De aici rezultă și **independența DPO-ului** ce impune excluderea oricăror sarcini suplimentare de natură a da naștere unor presiuni la nivelul companiei, legate de scopurile și mijloacele de prelucrare a datelor.

În esență, deși nu există o listă a surselor ce pot crea un conflict de interese, urmând a fi determinate în fiecare caz în parte, una dintre ele poate fi reprezentată de ocuparea funcției de DPO de persoane cu funcții de execuție (persoane cu putere de decizie cu privire la activitatea societății), *spre exemplu*: administrator/director general, director financiar, director resurse umane, director de marketing etc. Și nu în ultimul rând, conflictul de interese poate apărea și în persoana consilierului juridic, dacă ar ocupa și funcția de DPO – în special atunci când reprezintă compania într-un litigiu în materia legalității prelucrării datelor cu caracter personal sau în persoana celui care se ocupă de calitatea măsurilor de securitate IT în ideea conformării cu prevederile Regulamentului.

## ATENȚIE!

**Conflictul de interese apare în momentul în care DPO-ul are funcție de execuție sau când este juristul firmei.**