

# Procesarea datelor cu caracter personal – societăți comerciale



Cum trebuie să aplice Regulamentul GDPR (Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului) o societate care trimite diferite newslettere informative și desfășoară activitate de consultanță și contabilitate, din 25 mai 2018? Are obligația pregătirii unui DPO?

Dacă da, poate fi directorul economic (5 angajați) DPO? Menționez că societatea contactează persoane juridice dintr-o bază de date cumpărată, în vederea promovării serviciilor sale (prin intermediul a 2 operatori call-center). Ulterior, în urma acceptului PJ respectiv, după o perioadă scurtă de testare (5-10 zile) se încheie un contract de prestări servicii.

Ce alte documente am putea încerca să obținem pentru a fi acoperiți de acest Regulament.

Societatea respectivă are mare nevoie de niște indicații legate de GDPR.

## Răspuns:

Sfera de aplicare a legii este deosebit de amplă deoarece art. 2 din Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date dispune că

este aplicabilă prelucrărilor de date cu caracter personal efectuate de persoane fizice sau juridice, române ori străine, de drept public sau de drept privat, indiferent dacă au loc în sectorul public sau în sectorul privat.

Din perspectiva exemplurilor concrete pot fi enumerați toți angajatorii, pentru unii dintre aceștia existând inclusiv obligații de raportare către Autoritatea de supraveghere. Spre exemplu, instalarea unor sisteme de supraveghere video la locul de muncă determină o astfel de obligație. De asemenea, este subiect al reglementării orice persoană care organizează o evidență a clienților persoane fizice.

În conformitate cu prevederile art. 8 alin. (1) din Legea nr. 677/2001 prelucrarea codului numeric personal sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală poate fi efectuată numai dacă persoana vizată și-a dat în mod expres consimțământul sau prelucrarea este prevăzută în mod expres de o dispoziție legală.

Modificarea legislației din domeniu presupune intrarea în vigoare a Regulamentului (UE) 2016/679 și a Directivei (UE) 2016/680. Noile reglementări sunt destinate sporirii protecției persoanelor fizice impunând pentru cei care obțin date o mai mare rigoare în obținerea și prelucrarea acestora. Răspunderea pentru implementarea dispozițiilor din domeniu revine administratorilor care însă le vor putea pune în apli-

Autoritatea de supraveghere poate stabili și alte cazuri în care se poate efectua prelucrarea acestor date personale însă numai cu condiția instituirii unor garanții adecvate pentru respectarea drepturilor persoanelor vizate.

care prin persoane de specialitate care să se asigure, de exemplu, de legalitatea obținerii consimțământului, sau de compartimentul informatic care să asigure protecția bazelor de date. Începând cu 25 mai 2018 o parte dintre aceste responsabilități sunt stabilite în sarcina responsabilului cu protecția datelor.

Pentru operatorii de date sunt stabilite o serie de noi obligații și noi reguli:

- **One stop shop** - pentru operatorii de date care își desfășoară activitățile în mai multe state membre UE, autoritatea de supraveghere competentă este cea din statul membru în care operatorul respectiv își are stabilit sediul principal.
- **Responsabilizarea operatorilor de date** - accentul este pus pe transparența față de persoana vizată și responsabilitatea operatorului de date față de modul în care sunt prelucrate datele.
- **Studiu de impact** - în cazul prelucrărilor de date care presupun un risc ridicat pentru viața privată a persoanelor, operatorul trebuie să efectueze un Studiu de Impact asupra vieții private. Rezultatul unui astfel de studiu îi va permite să identifice riscuri specifice și să adopte măsuri care să împiedice apariția/producerea acestor situații.
- **Transferul datelor în afara UE** – pentru transferul datelor în afara Uniunii, Regulamentul introduce instrumente noi, pe lângă cele consacrate deja: BCR, clauze contractuale standard și Decizii ale Comisiei Europene privind un nivel adecvat de protecție.
- **Privacy by design & Privacy by default** – două noi principii esențiale pentru operatorii de date Privacy by design – ești dezvoltator de aplicații (care vor prelucra și date personale)? Trebuie să te asiguri, încă din stadiul dezvoltării, că aplicația ta va respecta regulile și principiile stabilite de Regulament.
- **Privacy by default** – în cazul în care se furnizează o aplicație care prelucrează date personale este necesară asigurarea că setările inițiale le vor permite utilizatorilor să își mențină controlul asupra vieții lor private/asupra a ceea ce postează sau împărtășesc cu alți utilizatori
- **DPO** – data protection officer/ responsabilul pentru protecția datelor. Numirea unui DPO la nivelul operatorului de date reprezintă una dintre măsurile prin care se încearcă responsabilizarea operatorilor de date. Acesta oferă operatorului consultanța necesară în vederea respectării tuturor obligațiilor acestuia și asigurării transparenței necesare față de persoanele vizate.

Noile sancțiuni pentru nerespectarea obligațiilor ce revin operatorilor și celorlalte persoane implicate sunt deosebit de aspre în noul Regulament. Față de maximumul existent în prezent de 50.000 lei din Legea nr. 677/2001, se pot aplica 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 exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.

Desemnarea unui responsabil cu protecția datelor este obligatorie din 25 mai 2018, raportat la dispozițiile art. 37 - 39 din **Regulamentul general privind protecția datelor** aprobat prin regulamentul menționat mai sus, în cazul în care operatorul sau persoana împuternicită de operator:

- este o autoritate publică sau un organism public, cu excepția instanțelor în exercitarea funcțiilor lor jurisdicționale;
- desfășoară o activitate principală care conduce la realizarea unei monitorizări constante și sistematice pe scară largă a persoanelor;
- desfășoară o activitate principală care constă în prelucrarea pe scară largă de date sensibile (cum ar fi: date privind originea rasială sau etnică, convingerile religioase, apartenența sindicală, date genetice, biometrice, privind starea de sănătate) sau referitoare la condamnări penale și infracțiuni.

Așadar, considerăm că, pe baza dispozițiilor legale aplicabile la această dată, în cazul prezentat nu este necesară desemnarea unui DPO.

Trebuie subliniat că prevederile cuprinse în noul Regulament sunt incluse la nivel general în legislația internă însă vor fi necesare, până la intrarea în vigoare, reglementări proprii care să stabilească limite în sfera obligațiilor concrete ale operatorilor de date. Până la această dată vor fi aplicabile dispozițiile Legii nr. 677/2001.

**ȘTIAȚI CĂ?**

În cazul în care datele cu caracter personal sunt obținute direct de la persoana vizată, operatorul este obligat să furnizeze persoanei vizate cel puțin următoarele informații, cu excepția cazului în care această persoană posedă deja informațiile respective:

- a) identitatea operatorului (societății) și a reprezentantului acestuia, dacă este cazul;
- b) scopul în care se face prelucrarea datelor;
- c) informații suplimentare, precum:

- destinatarii sau categoriile de destinatari ai datelor;
- dacă furnizarea tuturor datelor cerute este obligatorie și consecințele refuzului de a le furniza;
- existența drepturilor prevăzute prin lege pentru persoana vizată, în special a dreptului de acces, de intervenție asupra datelor și de opoziție;
- condițiile în care pot fi exercitate drepturile de mai sus;

d) orice alte informații a căror furnizare este impusă prin dispoziție a autorității de supraveghere, ținând seama de specificul prelucrării.

# Principii legate de prelucrarea datelor cu caracter personal

Datele cu caracter personal sunt:

- prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);
- colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu articolul 89 alineatul (1) din Regulamentul 679/2016, care dispune: *„Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice are loc cu condiția existenței unor garanții corespunzătoare, în conformitate cu prezentul regulament, pentru drepturile și libertățile persoanelor vizate. Respectivul garanții asigură faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivul măsuri pot include pseudonimizarea, cu condiția ca respectivele scopuri să fie îndeplinite în acest mod. Atunci când respectivele scopuri pot fi îndeplinite printr-o prelucrare ulterioară care nu permite sau*

*nu mai permite identificarea persoanelor vizate, scopurile respective sunt îndeplinite în acest mod.”;*

- adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);
- exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate”);
- păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în Regulament în vederea garantării drepturilor și libertăților persoanei vizate („limitări legate de stocare”);
- prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, in-

Operatorul este responsabil de respectarea tuturor principiilor legate de prelucrarea datelor cu caracter personal și poate demonstra această respectare „responsabilitate”.

clusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate“).

### Condițiile legalității prelucrării

Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

- persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
- prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

- prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
- prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul;
- prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalază interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil. **Excepție:** nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor. ■

### IMPORTANT

### Obligațiile societății în privința prelucrării datelor

Regula este că orice prelucrare de date cu caracter personal poate fi efectuată numai dacă persoana vizată și-a dat consimțământul în mod expres și neechivoc pentru acea prelucrare.

Ca excepție, consimțământul persoanei vizate NU este cerut în următoarele cazuri:

- a) când prelucrarea este necesară în vederea executării unui contract sau antecontract la care persoana vizată este parte ori în vederea luării unor măsuri, la cererea acesteia, înaintea încheierii unui contract sau antecontract;
- b) când prelucrarea este necesară în vederea protejării vieții, integrității fizice sau sănătății persoanei vizate ori a unei alte persoane amenințate;
- c) când prelucrarea este necesară în vederea îndeplinirii unei obligații legale a operatorului;
- d) când prelucrarea este necesară în vederea aducerii la îndeplinire a unor măsuri de interes public sau care vizează exercitarea prerogativelor de autoritate publică cu care este investit operatorul sau terțul căruiia îi sunt dezvăluite datele;
- e) când prelucrarea este necesară în vederea realizării unui interes legitim al operatorului sau al terțului căruiia îi sunt dezvăluite datele, cu condiția ca acest interes să nu prejudicieze interesul sau drepturile și libertățile fundamentale ale persoanei vizate;
- f) când prelucrarea privește date obținute din documente accesibile publicului, conform legii;
- g) când prelucrarea este făcută exclusiv în scopuri statistice, de cercetare istorică sau științifică, iar datele rămân anonime pe toată durata prelucrării.