

# *Principiile RGPD*

## **Ce date pot fi prelucrate și în ce condiții?**

Tipul și cantitatea de date cu caracter personal pe care societatea/organizația are dreptul să le prelucereze depind de motivul pentru care sunt prelucrate (temeiul juridic în cauză) și de scopul în care sunt prelucrate. Societatea/organizația trebuie să respecte mai multe norme-cheie, inclusiv următoarele:

- datele cu caracter personal trebuie prelucrate într-un **mod legal și transparent**, garantând echitatea în ceea ce privește persoanele fizice ale căror date cu caracter personal sunt prelucrate („legalitate, echitate și transparență”);
- trebuie să existe **scopuri specifice** ale prelucrării datelor și societatea/organizația trebuie să informeze persoanele fizice în legătură cu scopurile respective atunci când le colectează date cu caracter personal. Societatea/organizația nu poate colecta pur și simplu date cu caracter personal în scopuri nedefinite („limitări legate de scop”);
- societatea/organizația trebuie să colecteze și să prelucereze **numai acele date cu caracter personal care sunt necesare pentru îndeplinirea scopului respectiv** („reducerea la minimum a datelor”);
- societatea/organizația trebuie să se asigure că datele cu caracter personal sunt exacte și actualizate, având în vedere scopurile pentru care sunt prelucrate, și să fie corectate în caz contrar („exactitate”);
- societatea/organizația nu are dreptul să utilizeze datele cu caracter personal în alte scopuri care nu sunt **compatibile** cu scopul inițial;
- societatea/organizația trebuie să se asigure că datele cu caracter personal **nu sunt stocate mai mult timp decât este necesar** pentru scopurile în care au fost colectate („limitări legate de stocare”);
- societatea/organizația trebuie să prevadă **garanții tehnice și organizaționale** adecvate care să asigure securitatea datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnologice adecvate („integritate și confidențialitate”).

### Exemplu

Societatea/organizația dvs. administrează o agenție de turism. Când obțineți date cu caracter personal ale clienților dvs., ar trebui să le explicați într-un limbaj clar și simplu de ce aveți nevoie de datele respective, cum le veți utiliza și cât timp intenționați să le păstrați. Prelucrarea ar trebui adaptată la principiile-cheie de protecție a datelor.

### Referințe

- Articolul 5 alineatul (1) și considerentul (39) al RGPD
- Avizul 03/2013 al Grupului de lucru al articolului 29 privind limitările legate de scop (WP 203)

# Scopul prelucrării datelor

## Pot fi prelucrate datele în orice scop?

Nu. Scopul în care sunt prelucrate datele cu caracter personal trebuie cunoscut, iar persoanele fizice ale căror date le prelucrați trebuie informate. Nu puteți menționa pur și simplu că se vor colecta și prelucra date cu caracter personal. Acesta este principiul „limitărilor legate de scop”.

### Referințe

- Avizul 03/2013 al Grupului de lucru al articolului 29 privind limitările legate de scop (WP 203)

## Putem folosi date în alt scop?

Da, dar numai în unele cazuri. Dacă societatea/organizația dvs. a colectat date în baza unui **interes legitim**, a unui **contract** sau a unor **interese vitale**, le puteți folosi în alt scop, dar numai după ce vă asigurați că **noul scop este compatibil cu scopul inițial**.

Trebuie luate în considerare următoarele aspecte:

- legătura dintre scopul inițial și scopul nou/viitor;
- contextul în care au fost colectate datele (care este relația dintre societatea/organizația dvs. și persoana fizică în cauză?);
- tipul și natura datelor (sunt acestea sensibile?);
- posibilele consecințe ale prelucrării ulterioare preconizate (cum vor influența acestea persoana fizică în cauză?);
- existența unor garanții adecvate (cum ar fi criptarea sau pseudonimizarea).

Dacă societatea/organizația dvs. dorește să utilizeze datele pentru statistici sau pentru cercetare, nu este obligatoriu să testeze compatibilitatea.

Dacă societatea/organizația dvs. a colectat date în temeiul unui **consimțământ sau al unei cerințe legislative**, nu este posibilă nicio prelucrare ulterioară care depășește domeniile acoperite de consimțământul inițial sau de dispoziția legislativă. Prelucrarea ulterioară ar necesita obținerea unui nou consimțământ sau un nou temei juridic.

### Exemple

#### Este posibilă prelucrarea ulterioară

O bancă are un contract cu un client pentru a-i oferi clientului un cont bancar și un împrumut de nevoi personale. La sfârșitul primului an, banca utilizează datele cu caracter personal ale clientului pentru a verifica dacă acesta este eligibil pentru un tip de împrumut mai avantajos și pentru un sistem de economii. Banca informează clientul. Banca poate prelucra din nou datele clientului, deoarece noile scopuri sunt compatibile cu scopul inițial.

## Nu este posibilă prelucrarea ulterioară

Aceeași bancă dorește să transmită datele clientului unor firme de asigurări, în temeiul aceluiași contract pentru constituirea unui cont bancar și acordarea unui împrumut de nevoi personale. Această prelucrare nu este permisă fără consimțământul explicit al clientului, deoarece scopul nu este compatibil cu scopul inițial în care au fost prelucrate datele.

### Referințe

- Articolul 5 alineatul (1) litera (b), articolul 6 alineatul (4) și articolul 89 alineatul (1); considerentele (39) și (50) ale RGPD
- Avizul 03/2013 al Grupului de lucru al articolului 29 privind limitările legate de scop, 2 aprilie 2013 (WP 203)

## Cât de multe date se pot colecta?

Datele cu caracter personal ar trebui prelucrate numai atunci când nu este posibilă în mod rezonabil efectuarea prelucrării în alt mod. Dacă este posibil, este preferabil să se utilizeze date anonime. În cazul în care sunt necesare date cu caracter personal, acestea ar trebui să fie **adecvate, relevante și limitate la ceea ce este necesar în scopul respectiv („reducerea la minimum a datelor”)**. În calitate de operator, societății/organizației dvs. îi revine responsabilitatea de a evalua ce volum de date este necesar și de a se asigura că nu se colectează date irelevante.

### Exemplu

Societatea/organizația dvs. oferă persoanelor fizice servicii de partajare a autoturismelor. Pentru aceste servicii poate avea nevoie de numele, adresa și numărul cardului de credit al clienților și, poate, chiar de informații privind o eventuală dizabilitate de care suferă persoana în cauză (așadar, date privind sănătatea), dar nu și de originea rasială a clienților.

### Referințe

- Articolul 5 alineatul (1) litera (c) și considerentul (39) al RGPD

## Cât timp pot fi păstrate datele și se impune actualizarea lor?

Trebuie să stocați datele pentru **o perioadă cât mai scurtă posibil**. Perioada ar trebui să țină seama de motivele pentru care societatea/organizația dvs. trebuie să prelucreze datele, precum și de eventuale obligații juridice de a păstra datele o perioadă fixă de timp (de exemplu, legile privind ocuparea forței de muncă, legile fiscale sau legile antifraudă naționale care vă impun păstrarea datelor cu caracter personal despre angajații dvs. pentru o perioadă determinată, durata garanției produselor etc.).

Societatea/organizația dvs. ar trebui să stabilească **termene** pentru **ștergerea sau revizuirea** datelor stocate.

Ca excepție, datele cu caracter personal pot fi păstrate o perioadă mai îndelungată în scopuri de arhivare în interes public ori în scopuri de cercetare științifică sau istorică, cu condiția să fie puse în aplicare măsuri de ordin tehnic și organizatoric adecvate (precum anonimizare, criptare etc.).

De asemenea, societatea/organizația dvs. trebuie să se asigure că datele pe care le deține sunt exacte și să le actualizeze.

## Exemplu

### Date păstrate prea mult timp fără actualizare

Societatea/organizația dvs. administrează un birou de recrutări și, în acest scop, colectează CV-uri ale unor persoane dornice de angajare, care, în schimbul serviciilor dvs. de intermediere, vă plătesc o taxă. Intenționați să păstrați datele timp de 20 de ani și nu aveți măsuri de actualizare a CV-urilor. Perioada de stocare nu pare proporțională cu scopul de a găsi un loc de muncă pentru o persoană pe termen scurt până la mediu. Mai mult, faptul că nu cereți actualizări ale CV-urilor la intervale regulate face ca unele căutări să fie inutile pentru persoana care caută un loc de muncă după o anumită perioadă de timp (de exemplu, pentru că persoana respectivă a dobândit calificări noi).

## Referințe

- Articolul 5 alineatul (1) litera (e) și considerentul (39) al RGPD

# Ce informații trebuie să le oferim persoanelor ale căror date sunt colectate?

În momentul în care colectați datele, persoanele trebuie clar informate cel puțin despre:

- **cine** este societatea/organizația dvs. (datele de contact ale dvs. și ale eventualului RPD al dvs., dacă este cazul);
- **la ce** va folosi societatea/organizația dvs. datele cu caracter personal ale acestora (scopurile);
- categoriile de date cu caracter personal în cauză;
- **justificarea juridică** a prelucrării datelor;
- **cât** timp vor fi păstrate datele;
- **cine altcineva** le-ar putea primi;
- dacă datele cu caracter personal ale acestor oameni vor fi **transferate** către un destinatar din afara UE;
- că aceștia au dreptul la o **copie a datelor** (dreptul de a accesa datele cu caracter personal) și alte **drepturi de bază** în domeniul protecției datelor ([consultați lista completă a drepturilor](#));
- **dreptul de a depune o plângere** în fața unei autorități de protecție a datelor (APD);
- **dreptul de a-și retrage consimțământul** în orice moment;
- eventuala existență a unui **proces decizional automatizat** și logica utilizată, inclusiv consecințele acestui fapt.

Consultați [lista completă](#) a informațiilor care trebuie furnizate (link to Art. 13).

Aceste informații trebuie furnizate **în scris, oral** la solicitarea persoanei vizate, dacă identitatea acesteia a fost dovedită prin alte mijloace, sau prin mijloace electronice atunci când este oportun. Societatea/organizația dvs. trebuie să furnizeze informațiile într-un mod **concis, transparent, inteligibil și ușor accesibil**, într-un **limbaj clar și simplu și în mod gratuit**.

Când datele sunt obținute de la o altă societate/organizație, societatea/organizația dvs. ar trebui să îi furnizeze persoanei informațiile menționate mai sus în termen de o lună de la momentul la care societatea/organizația dvs. a obținut datele cu caracter personal; sau, în cazul în care societatea/organizația dvs. comunică cu persoana fizică, în momentul în care datele sunt utilizate pentru comunicarea cu aceasta; sau, dacă se intenționează divulgarea datelor către o altă societate, la data la care datele cu caracter personal au fost divulgate pentru prima oară.

De asemenea, societatea/organizația dvs. are obligația de a informa persoana fizică în legătură cu categoriile de date și cu sursa din care a obținut datele, inclusiv dacă au fost obținute din surse disponibile public. În anumite situații enumerate la articolul 13 alineatul (4) și la articolul 14 alineatul (5) din RGPD, societatea/organizația dvs. poate fi scutită de obligația de a informa persoana fizică. Vă rugăm să verificați dacă această excepție se aplică societății/organizației dvs.

## Referințe

- Articolul 12 alineatele (1), (5) și (7), articolele 13 și 14 și considerentele (58)-(62) ale RGPD
- Orientările Grupului de lucru al articolului 29 privind transparența