

AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Ghid orientativ de aplicare a Regulamentului General privind Protecția Datelor destinat operatorilor



Ghid referitor la aplicarea Regulamentului General privind Protecția Datelor destinat operatorilor

CONTEXT

Parlamentul European și Consiliul au adoptat, în data de 27 aprilie 2016, **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 - RGPD).**

Regulamentul (UE) 2016/679 a fost publicat în Jurnalul Oficial al Uniunii L119 din 4 mai 2016, iar **prevederile lui vor fi direct aplicabile în toate statele membre ale Uniunii Europene, începând cu data de 25 mai 2018.**

Regulamentul (UE) 2016/679 impune un set unic de reguli în materia protecției datelor cu caracter personal, înlocuind Directiva 95/46/CE și, implicit, prevederile Legii nr. 677/2001.

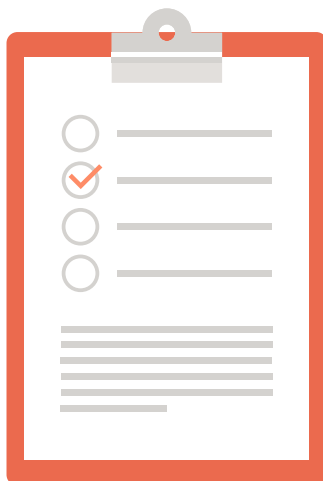
NOUTĂȚI

Regulamentul (UE) 2016/679 pune accent pe transparența față de persoana vizată și responsabilizarea operatorului de date față de modul în care prelucrează datele cu caracter personal.

Regulamentul (UE) 2016/679 stabilește o serie de garanții specifice pentru a proteja cât mai eficient viața privată a minorilor, în special în mediul on-line.

Regulamentul (UE) 2016/679 consolidează drepturile garantate persoanelor vizate și introduce noi drepturi: dreptul de a fi uitat, dreptul la portabilitatea datelor și dreptul la restricționarea prelucrării.

Regulamentul (UE) 2016/679 introduce sancțiuni severe, pâna la 10 – 20 milioane de euro sau între 2% și 4% din cifra de afaceri la nivel internațional, pentru operatorii din sectorul privat.





DOMENIU DE APLICARE

RGPD se aplică:

Prelucrării datelor cu caracter personal în cadrul activităților derulate la sediul unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii.

Prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Uniune de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Uniune, atunci când activitățile de prelucrare sunt legate de:

- oferirea de bunuri sau servicii unor astfel de persoane vizate în Uniune, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată; sau
- monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

Prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Uniune, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internațional public.





PRINCIPALELE OBLIGAȚII PENTRU OPERATORII DE DATE ÎN APLICAREA RGPD

DESEMNAREA UNUI RESPONSABIL CU PROTECȚIA DATELOR

Pentru a îndruma modul în care sunt gestionate datele cu caracter personal în cadrul unui operator sau al unei persoane împuternicite de operator, în anumite situații, este necesară o persoană care să exercite o misiune de informare, de consiliere și de control în plan intern: **responsabilul cu protecția datelor**.

Desemnarea unui responsabil cu protecția datelor este obligatorie din 25 mai 2018, raportat la dispozițiile art. 37 - 39 din Regulamentul General privind Protecția Datelor, în cazul în care operatorul sau persoana împuternicită de operator:

- este o autoritate publică sau un organism public, cu excepția instanțelor în exercitarea funcției 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.

Chiar dacă entitatea nu are obligația expresă de a desemna un responsabil cu protecția datelor, ANSPDCP recomandă numirea acestuia, în considerarea efectului benefic al activității responsabilului în vederea asigurării respectării Regulamentului General de Protecția Datelor de către operatorul respectiv sau persoana împuternicită de operator.

Un **responsabil cu protecția datelor** reprezintă un avantaj major pentru operator în vederea înțelegerii și respectării obligațiilor prevăzute de RGPD, dialogului cu autoritățile pentru protecția datelor și reducerii riscurilor apariției unor litigii.

Rolul responsabilului cu protecția datelor

- **să informeze și să consilieze** operatorul sau persoana împuternicită de operator, precum și angajații acestora cu privire la obligațiile existente în domeniul protecției datelor cu caracter personal;
- **să monitorizeze respectarea RGPD** și a legislației naționale în domeniul protecției datelor;
- **să consilieze operatorul sau persoana împuternicită** în legătură cu realizarea de studii de impact privind protecția datelor și să verifice efectuarea acestora;
- **să coopereze cu autoritatea pentru protecția datelor** și să reprezinte punctul de contact în relația cu aceasta.





CARTOGRAFIEREA PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

Toți operatorii din sistemul public, persoanele împuternicite de operator, precum și operatorii din sistemul privat cu peste 250 de angajați, au obligația cartografierii prelucrărilor de date cu caracter personal efectuate, raportat la prevederile art. 30 din Regulamentul General privind Protecția Datelor.

Chiar și operatorii din sistemul privat cu mai puțin de 250 de angajați au obligația cartografierii prelucrărilor în cazurile în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, în cazul în care prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date ori date cu caracter personal referitoare la condamnări penale și infracțiuni.

În acest sens:

Pentru a evalua în mod eficient impactul RGPD asupra activității entității, este necesară identificarea prelucrărilor de date cu caracter personal efectuate și **păstrarea evidenței** activităților de prelucrare.

Pentru a avea o evidență completă și exactă a prelucrărilor de date cu caracter personal efectuate și pentru a răspunde noilor exigențe, **trebuie identificate**, în prealabil, cu precizie:

- diferitele prelucrări de date cu caracter personal;
- categoriile de date cu caracter personal prelucrate;
- scopurile urmărite prin operațiunile de prelucrare a datelor;
- persoanele care prelucrează aceste date;
- fluxurile de date, indicând originea și destinația datelor, în special pentru a identifica eventualele transferuri de date în afara Uniunii Europene.

Evidența păstrată de operator va cuprinde:

- (a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
- (b) scopurile prelucrării;
- (c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
- (d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țări terțe sau organizații internaționale;
- (e) dacă este cazul, transferurile de date cu caracter personal către o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la articolul 49 alineatul (1) al doilea paragraf din Regulamentul General privind Protecția Datelor, documentația care dovedește existența unor garanții adecvate;
- (f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
- (g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la articolul 32 alineatul (1) din Regulamentul General privind Protecția Datelor.



CARTOGRAFIEREA PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

Ca atare, pentru fiecare prelucrare de date cu caracter personal, este necesar a se avea în vedere următoarele:

CINE?

Se înscriu în evidența numele și coordonatele operatorului (și ale reprezentantului sau legal) și, după caz, ale responsabilului cu protecția datelor;

Se întocmește lista persoanelor împuternicite, după caz.

CE?

Se identifică categoriile de date cu caracter personal prelucrate;

Se identifică datele susceptibile de a prezenta riscuri datorită naturii lor sensibile deosebite (datele privind sănătatea sau infracțiunile)

DE CE?

Se precizează scopul sau scopurile în care sunt colectate sau prelucrate datele cu caracter personal (ex. gestionarea relației comerciale, managementul resurselor umane, geolocalizare, videosupraveghere etc.)

UNDE?

Se stabilește locația sistemului de evidență și, dacă e cazul, destinatarii datelor.

Se stabilesc statele către care sunt, eventual, transferate datele.

PÂNĂ CÂND?

Se precizează, pentru fiecare categorie de date, perioada de stocare.

CUM?

Se precizează măsurile de securitate implementate pentru a reduce la minimum riscurile de acces neautorizat la date și, în consecință, impactul asupra vieții private a persoanelor vizate.





PRIORITIZAREA ACȚIUNILOR DE ÎNTREPRINS

Operatorul și persoana împuternicită de operator **identifică acțiunile** care trebuie întreprinse pentru conformarea la cerințele impuse de RGPD.

Se **prioritizează** aceste acțiuni în funcție de riscurile pe care le prezintă prelucrările efectuate pentru drepturile și libertățile persoanelor vizate.

După identificarea prelucrărilor de date cu caracter personal efectuate în cadrul entității, se stabilesc, pentru fiecare dintre acestea, acțiunile care trebuie întreprinse în vederea respectării obligațiilor impuse de Regulamentul General privind Protecția Datelor.

Indiferent de prelucrările efectuate, se vor avea în vedere, în principal, următoarele aspecte:

- colectarea și prelucrarea **doar a datelor strict necesare** pentru realizarea scopurilor;
- identificarea **temeiului legal** în baza căruia se efectuează prelucrarea raportat la art. 6 din Regulamentul General privind Protecția Datelor (ex. consimțământul persoanelor vizate, contract, obligație legală);
- revizuirea/completarea **informațiilor furnizate persoanelor vizate**, astfel încât să respecte cerințele impuse de Regulamentul General privind Protecția Datelor (articolele 12, 13 și 14);
- asigurarea că **persoanele împuternicite** își cunosc noile obligații și responsabilități;
- verificarea existenței clauzelor contractuale și actualizarea obligațiilor **persoanelor împuternicite** privind securitatea, confidențialitatea și protecția datelor cu caracter personal prelucrate;
- stabilirea modalităților de exercitare a **drepturilor persoanelor vizate** (ex. dreptul de acces, dreptul de rectificare, dreptul la portabilitate, retragerea consimțământului);
- verificarea **măsurilor de securitate** implementate.



Se pot aplica **măsuri speciale**, precum: evaluarea impactului asupra protecției datelor, extinderea dreptului la informare al persoanelor vizate, obținerea consimțământului persoanelor vizate (după caz), obținerea autorizării pentru transferurile de date în state terțe (dacă este cazul), în cazul în care prelucrările de date cu caracter personal efectuate în cadrul operatorului sau persoanei împuternicite de operator îndeplinesc următoarele **caracteristici**:

- Prelucrarea efectuată vizează și categorii de date precum:

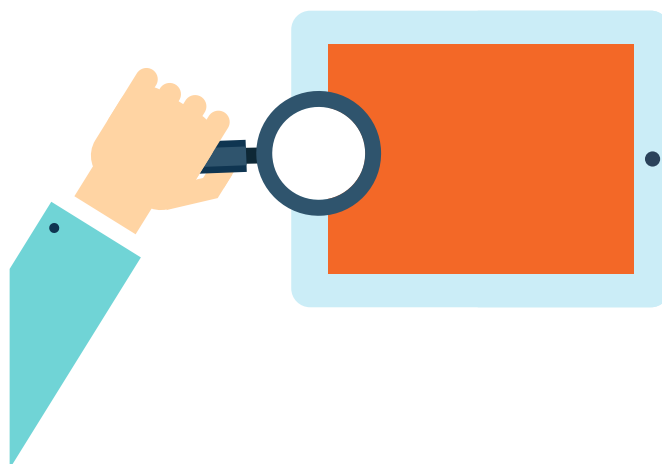
- date care dezvăluie originea rasială sau etnică, opiniile politice, filozofice sau religioase, apartenența sindicală;
- date privind sănătatea sau orientarea sexuală, date genetice sau biometrice;
- date referitoare la infracțiuni sau condamnări penale;
- date referitoare la minori.

- Prelucrarea efectuată are ca scop și ca efect:

- monitorizarea permanentă pe scară largă a unei zone accesibile publicului;
- evaluarea sistematică și aprofundată a unor aspecte personale, inclusiv profilarea, pe baza căreia sunt luate decizii care produc efecte juridice referitoare la o persoană fizică sau care o afectează pe aceasta în mod semnificativ.

- Prelucrarea efectuată implică transferuri de date în afara Uniunii Europene, către state care nu asigură un nivel de protecție adecvat recunoscut de Comisia Europeană.

Se realizează o analiză aprofundată a legislației privind protecția datelor și a cerințelor impuse de Regulamentul General privind Protecția Datelor pentru a stabili măsurile care trebuie aplicate la nivelul fiecărui operator, în funcție de sectorul de activitate și specificul prelucrării/prelucrărilor efectuate.





GESTIONAREA RISCURILOR

În cazul în care au fost identificate prelucrări de date cu caracter personal susceptibile de a prezenta **riscuri ridicate** pentru drepturile și libertățile persoanelor fizice, operatorul va efectua o **evaluare a impactului asupra protecției datelor**, în condițiile art. 35 din Regulamentul General privind Protecția Datelor.

Evaluarea impactului asupra protecției datelor se realizează **anterior colectării** datelor cu caracter personal și efectuării prelucrării.

Se va pune accent pe **estimarea riscurilor asupra protecției datelor din punctul de vedere al persoanelor vizate, luând în considerare natura datelor, domeniul de aplicare, contextul și scopurile prelucrării și utilizarea noilor tehnologii**.

Evaluarea impactului asupra protecției datelor **presupune**:

- o descriere a prelucrării de date efectuate și a scopurilor acestora;
- o evaluare a necesității și a proporționalității prelucrării de date efectuate;
- o estimare a riscurilor asupra drepturilor și libertăților persoanelor vizate;
- măsurile prevăzute pentru a trata riscurile și a asigura conformitatea cu dispozițiile RGPD.

Evaluarea impactului asupra protecției datelor permite:

- realizarea unei prelucrări de date cu caracter personal sau a unui produs care respectă viața privată;
- estimarea impactului asupra vieții private a persoanelor vizate;
- demonstrarea faptului că principiile fundamentale ale Regulamentului General privind Protecția Datelor sunt respectate.

Evaluarea impactului asupra protecției datelor se impune, mai ales, în cazul:

- (a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
- (b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10; sau
- (c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

Când evaluarea de impact indică riscuri ridicate, în absența unor măsuri luate de operator pentru atenuarea acestora, se consultă Autoritatea națională de supraveghere.



ORGANIZAREA PROCEDURILOR INTERNE

Pentru a asigura permanent un nivel ridicat de protecție a datelor cu caracter personal, operatorul trebuie să elaboreze proceduri interne care să garanteze respectarea protecției datelor în orice moment, luând în considerare toate evenimentele care pot apărea pe parcursul efectuării prelucrărilor de date, precum:

- breșe de securitate;
- solicitări privind exercitarea drepturilor persoanelor vizate;
- modificarea datelor cu caracter personal colectate;
- schimbarea prestatorului.

Organizarea procedurilor interne implică, în special:

- **luarea în considerare a protecției datelor cu caracter personal încă de la momentul conceperii (privacy by design)** unei aplicații sau a unei prelucrări: minimizarea colectării datelor în funcție de scop, cookie-uri, perioada de stocare, informațiile furnizate persoanelor vizate, obținerea consimțământului persoanelor vizate, securitatea și confidențialitatea datelor cu caracter personal, garantarea rolului și responsabilității părților implicate în efectuarea prelucrării datelor;
- **aplicarea de măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării (privacy by default)**, având în vedere: volumul de date colectate, gradul de prelucrare a acestora, perioada de stocare și accesibilitatea lor, astfel încât datele cu caracter personal să nu fie accesate, fără intervenția persoanei, de un număr nelimitat de persoane;
- **sensibilizarea și organizarea diseminării informației**, în special prin stabilirea unui plan de pregătire și de comunicare cu persoanele care prelucrează date cu caracter personal;





- **soluționarea plângerilor și cererilor adresate de persoanele vizate în exercitarea drepturilor lor**, stabilind părțile implicate și modalitățile de exercitare a acestora; exercitarea drepturilor trebuie să se poată realiza inclusiv pe cale electronică, în cazul în care datele au fost colectate prin astfel de mijloace;
- **anticiparea unei posibile încălcări a securității datelor** specificând, pentru anumite cazuri, obligativitatea notificării autorității pentru protecția datelor în termen de 72 de ore și a persoanelor vizate în cel mai scurt timp;
- **asigurarea confidențialității și securității prelucrării** prin adoptarea de măsuri tehnice și organizatorice adecvate, incluzând printre altele, după caz:
 - a) pseudonimizarea și criptarea datelor cu caracter personal;
 - b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
 - c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
 - d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.



**AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL**

**BD. G-ral Gheorghe Magheru 28 - 30,
sector 1,
București, cod poștal 010336
Telefon: +40.318.059.211
E-mail: anspdcp@dataprotection.ro**