

RAPORT SPECIAL

17 sfaturi pentru aplicarea în mod corect a modificărilor aduse de Regulamentul privind protecția datelor

Raport special realizat de Rentrop&Straton în colaborare cu Juridice.ro

Manager Produs: Georgiana Istudor

Manager Proiect: Răzvan Tănase

Președinte: George Straton

Director General: Octavian Breban

Director Creație-Producție: Cristina Straton

Lucrare editat de: RENTROP&STRATON Group

Toate drepturile rezervate. Nicio parte din această lucrare nu poate fi reprodusă, arhivată sau transmisă sub nicio formă și prin niciun fel de mijloace, mecanice sau electronice, fotocopiere, înregistrare audio sau video, fără permisiunea în scris din partea editorului. Autorii sau editorii nu

sunt responsabili pentru nicio pierdere provocată vreunei persoane fizice sau juridice care acționează sau se abține de la acțiuni ca urmare a citirii materialelor publicate în această lucrare.

Sursa foto copertă:

Sursă imagini: <https://pixabay.com/>

Serviciul Clienți Tel.: 021.209.45.45; Fax: 021.408.28.99 E-mail: dataprotection@rs.ro

DATA PROTECTION

Regulamentul General privind Protecția Datelor (GDPR)

Pentru cine este important Regulamentul General
privind Protecția Datelor și de ce

[Regulamentul \(UE\) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 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 \(Regulamentul general privind protecția datelor\)](#) se va aplica din 25 mai 2018

1. Ce-i cu acest Regulament?

Ne spune chiar el. Conform art. 1 alin. (1) RGPD, „Prezentul regulament stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, precum și normele referitoare la libera circulație a datelor cu caracter personal.”

Normele stabilite prin Regulament au forță juridică superioară reglementărilor naționale.

p. 2/9

Regulamentul privește exclusiv protecția persoanelor fizice.

Datele cu caracter personal sunt definite de art. 4 pct. 1 din Regulament.

Regulamentul stabilește norme nu doar cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, ci și cu privire la colectarea, stocarea și utilizarea datelor cu caracter personal.

Preliminar extras din „RGPD comentat”.

2. Pentru cine este important Regulamentul?

Pentru toate organizațiile, indiferent de forma de proprietate, care prelucrează date cu caracter personal.

3. Ce înseamnă prelucrarea datelor cu caracter personal?

Din punct de vedere, „prelucrarea” are o definiție chiar în cuprinsul Regulamentului (art. 2 pct. 2 RGPD). În înțelesul Regulamentului, prelucrare înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea. **Adică orice atingere, cât de mic .**

4. Regulamentul se aplică oricărui prelucrări de date cu caracter personal?

Nu chiar, dar aproape tuturor. Art. 2 nu lasă mult loc pentru a evita aplicarea Regulamentului. Iată :

„(1) Prezentul regulament se aplică prelucrării datelor cu caracter personal, efectuat total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât

cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.

(2) Prezentul regulament nu se aplică prelucrării datelor cu caracter personal:

- (a) în cadrul unei activități care nu intră sub incidența dreptului Uniunii;
- (b) de către statele membre atunci când desfășoară activități care intră sub incidența capitolului 2 al titlului V din Tratatul UE; (*politica de securitate și apărare comună*);
- (c) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;
- (d) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmării penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora.”

5. De ce este important Regulamentul?

Din pricina (i) felului în care reglementează tragerea la răspundere și din pricina (ii) sancțiunilor foarte aspre.

6. Cine poate să tragă la răspundere operatorii de date personale?

Oricine, orice persoană fizică. Orice persoană vizată are dreptul de a depune o plângere la autoritatea națională de supraveghere, în special în statul membru în care își are reședința obișnuită, în care se află locul său de muncă sau în care a avut loc presupusa încălcare, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă regulamentul (art. 77 RGPD). Legea nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date reglementează procedura plângerii la Autoritate.

7. Exist sancțiuni penale?

Din fericire, Regulamentul nu instituie sancțiuni penale, și nici nu ar putea, întrucât reglementările europene nu instituie sancțiuni penale. Însă nerespectarea dispozițiilor Regulamentului poate atrage răspunderea penală, de exemplu în cadrul infracțiunii de abuz în serviciu.

8. Dar sancțiuni civile?

Regulamentul nu prevede sancțiuni civile, însă reglementează într-un mod foarte împovăritor modul în care intervine răspunderea civilă în cazul încălcării prevederilor lui. Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a RGPD are dreptul să obțină despăgubiri de la operator (art. 82 alin. 1 RGPD) și, corelativ, orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă RGPD (art. 82 alin. 2 RGPD).

9. Dar sancțiuni administrative (amenzi)?

Da, foarte periculoase. Acesta este de altfel motivul pentru care Regulamentul a devenit celebru și constituie o preocupare importantă în toate țările Uniunii Europene. În concepția RGPD, sancțiunile civile (răspunderea civilă) pot coexista cu cele administrative. Sancțiunile administrative (amenzi) vor fi aplicate de către autoritatea națională și vor fi uriașe, comparativ cu sancțiunile care pot fi aplicate astăzi de către Autoritate. Încălcarile obligațiilor prevăzute la art. 83 alin. 4 RGPD pot atrage amenzi administrative de până la 10 mil. Euro, dar nu mai mult de 2% din cifra de afaceri la nivel mondial, iar încălcările obligațiilor prevăzute la art. 83 alin. 5 pot atrage amenzi administrative de până la 20 mil. Euro, dar nu mai mult de 4% din cifra de afaceri la nivel

mondial. Această din urmă sancțiune este aplicabilă și în cazul încălcării unui ordin emis de autoritatea de supraveghere (art. 83 alin. 6 RGPD).

Ce trebuie să fac operatorii în următoarea perioadă

10. Cine sunt operatorii? Cui și se aplică Regulamentul?

Operator înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal [art. 4 pct. (7) RGPD].

Cu alte cuvinte, operator este cel pentru care se realizează prelucrarea datelor, chiar dacă operatorul nu realizează el însuși nicio prelucrare.

11. Cine poate să apeleze la un “responsabil cu protecția datelor”? Cine trebuie să apeleze la un “responsabil cu protecția datelor”?

Oricine poate să apeleze la un responsabil cu protecția datelor personale.

Operatorii **trebuie** să desemneze un responsabil cu protecția datelor atunci când printre altele, activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă (art. 37 alin. 1 lit. b) RGPD).

Pe larg, cf. art. 37 alin. (1), operatorul desemnează un responsabil cu protecția datelor ori de câte ori:

- (a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;
- (b) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă; sau
- (c) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, menționată la articolul 9, sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10.

12. Cine este responsabilul cu protecția datelor personale?

Responsabilul cu protecția datelor trebuie să fie desemnat (art. 37 alin. 5 RGPD) pe baza calificărilor profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor. Responsabilul cu protecția datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să îndeplinească sarcinile în baza unui contract de servicii (art. 37 alin. 6).

13. Cine trebuie să țină evidența prelucrărilor de date cu caracter personal?

Fiecare operator trebuie să păstreze evidența activităților de prelucrare desfășurate sub responsabilitatea lui și în numele lui, evidențe care trebuie să cuprindă informațiile prevăzute de art. 30 alin. (1) lit. (a)-(g) și, respectiv, alin. (2) lit. (a)-(d) RGPD.

Această evidență este necesară întrucât autoritatea de supraveghere poate să ceară oricând acces la ea (art. 30 alin. 4 RGPD).

14. Cum stăm?

Având în vedere sancțiunile prevăzute de Regulament în timpul scurt rămas până când se va aplica, operatorii trebuie să realizeze un DATAPROTECTION AUDIT, prin care conducerea să obțină o imagine clară cu privire la fluxurile de date personale.

15. Ce-i de făcut?

Pe fond, operatorii au de făcut 3 lucruri importante:

1. să se adapteze procedurile de lucru, pentru ca accesul la date să fie cât mai limitat și cât mai securizat;
2. să securizeze informatic datele personale;
3. să încheie acorduri cu operatorii asociați.

Procedural, operatorii trebuie:

- să își aleagă un responsabil pentru protecția datelor personale;
- să țină evidența prelucrărilor de date personale.

Aprecieri finale

Întreaga activitate a operatorului ar trebui să fie atent procedurată, cu integrare atent în procedurile de lucru existente deja. O structură arborescentă de proceduri ar fi binevenită în domeniul protecției datelor cu caracter personal, dar sunt conștient că asta nu se poate face decât prin corelarea cu procedurile existente deja, astfel încât noile proceduri trebuie să fie sincronizate cu procedurile existente. Ceea ce de bun seamă este un proces de durată care necesită colaborare între toate departamentele și cu implicarea activă a responsabilului pentru protecția datelor personale.

16. Ce activități de consultanță sunt necesare?

- Realizarea efectiv , pe teren, i redactarea DATAPROTETION AUDIT
- Redactarea/avizarea procedurilor de lucru cu datele personale
- Redactarea/avizarea procedurilor de transfer (de la cum este acum la cum ar trebui s fie)
- Instruirea personalului operatorului
- Redactarea/avizarea inform rilor care trebuie comunicate persoanelor vizate
- Redactarea/avizarea acordurilor cu operatorii asociați și împuterniciții