



Noul Regulament General privind Protecția Datelor



2018



**Regulamentul nr. 679/2016 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)**

Comisia Europeană a semnalat, în anul 2012, necesitatea actualizării cadrului normativ european aplicabil în domeniul protecției datelor și a propus noi reguli utilizând ca instrument normativ regulamentul.

Regulamentul (UE) 2016/679 a intrat în vigoare pe 25 mai 2016, iar prevederile lui vor fi aplicabile începând cu data de 25 mai 2018.

Deși principiile și obiectivele principale stabilite de Directiva 95/46/CE rămân valabile, scopul principal al Regulamentului este acela de a adapta și actualiza aceste principii în acord cu evoluția tehnologiei.

Regulamentul stabilește un set unic de reguli, direct aplicabile în toate statele membre ale Uniunii, destinat protejării mai eficiente a vieții private a persoanelor fizice de pe teritoriul Uniunii Europene.

Principiile și regulile stabilite de Regulament privesc un drept fundamental al persoanei – dreptul la protecția datelor personale, garantat de art. 8 al Cartei Drepturilor Fundamentale a UE și art. 16 al Tratatului UE.

Regulamentul accentuează responsabilitatea operatorilor care prelucrează date personale, simplificând, în același timp, formalitățile administrative pe care aceștia trebuie să le parcurgă.

Prevederile Regulamentului consolidează drepturile garantate persoanelor vizate (persoanele ale căror date sunt prelucrate).

Astfel, dreptul la informare este extins, în sensul că persoanele vizate pot obține de la operatorul de date informații mai clare și cuprinzătoare cu privire la scopul și temeiul legal în care se prelucrează datele personale, perioada de stocare a acestora și drepturile de care beneficiază.

Dreptul de a fi uitat cu aplicabilitate în mediul on-line este consacrat expres.

Regulamentul mai prevede și un drept nou, cel la portabilitatea datelor - mai exact posibilitatea persoanelor vizate de a cere transferarea datelor la un alt operator de date.



Minorii beneficiază de mai multă atenție întrucât regulamentul stabilește o serie de garanții specifice pentru a proteja cât mai eficient viața privată a acestora, în special, în mediul on-line.

Regulile stabilite de Regulament vor fi aplicabile tuturor operatorilor de date, indiferent de locul unde sunt stabiliți aceștia, în anumite condiții.

Astfel, în măsura în care bunurile sau serviciile oferite de o companie aflată în afara UE, care presupun prelucrarea datelor personale, sunt adresate în mod vădit și cetățenilor Uniunii Europene, regulile stabilite de Regulament îi vor fi aplicabile și acestei companii.



Domeniul de aplicare:

- este direct aplicabil în toate statele membre UE
- protejează drepturile tuturor persoanelor fizice aflate pe teritoriul UE, indiferent de situarea geografică a operatorului de date
- extinde sfera de aplicare și asupra operatorilor de date stabiliți în afara UE, în măsura în care bunurile și/sau serviciile acestora sunt adresate (și) persoanelor aflate pe teritoriul UE

Scopul Regulamentului este să contribuie la asigurarea unei zone de libertate, securitate și justiție pe teritoriul Uniunii Europene, o zonă în care este asigurat atât progresul economic și social, cât și binele individual.

Regulile și principiile stabilite de Regulament protejează viața privată a tuturor persoanelor aflate pe teritoriul Uniunii Europene, ale căror date personale sunt prelucrate de companii

/persoane fizice/instituții/orice alte entități de drept public sau privat.

Aceste reguli și principii sunt aplicabile tuturor persoanelor, indiferent de cetățenia acestora sau de reședință (în interiorul UE).

Operatorilor de date le este oferită posibilitatea de a interacționa cu o singură autoritate de supraveghere, respectiv cea din statul membru în care este stabilit sediul principal al operatorului de date.



Regulamentul privește atât companiile aflate pe teritoriul Uniunii Europene, cât și cele din afara acestui spațiu care prelucrează, însă, date personale pentru a oferi bunuri și servicii persoanelor aflate pe teritoriul Uniunii Europene, indiferent dacă bunurile și serviciile respective sunt condiționate sau nu de efectuarea unei plăți.

Importantă este intenția companiei de a oferi în mod efectiv bunuri și/sau servicii persoanelor aflate pe teritoriul UE.

Pentru a identifica intenția de a oferi bunuri sau servicii pe teritoriul Uniunii Europene sunt analizați mai mulți factori, cum ar fi: utilizarea limbii oficiale a unuia dintre statele membre, posibilitatea de a plăti în euro sau altă monedă oficială a statelor membre ori de a livra produsele comandate pe teritoriul UE sau orice alte asemenea indicii.

De asemenea, Regulamentul va fi aplicabil și companiilor aflate în afara Uniunii Europene în măsura în care prelucrarea de date efectuată presupune monitorizarea comportamentului persoanelor aflate pe teritoriul UE.

O astfel de monitorizare presupune, spre exemplu, urmărirea comportamentului în mediul on-line, inclusiv folosirea unor tehnici ulterioare de prelucrare a datelor cum ar fi crearea de profiluri. Astfel de tehnici sunt folosite pentru a stabili preferințele persoanelor, comportamentele și atitudinile acestora.

Excepții:

- prevederile Regulamentului nu vor fi aplicabile prelucrărilor efectuate în scopul prevenirii, cercetării și urmăririi penale a infractorului sau executarea sancțiunii penale. În cazul acestora vor fi aplicabile prevederile unei reglementări naționale în aplicabilitatea Directivei (UE) 2016/680, (care face parte din același „pachet legislativ” cu Regulamentul UE 2016/679).

- Regulamentul nu va fi aplicabil activităților aflate în afara dreptului Uniunii – aici se încadrează și prelucrările de date referitoare la securitatea națională a statelor membre și relațiile externe.

- Regulamentul nu va fi aplicabil prelucrărilor de date efectuate de o persoană fizică în cadrul unei activități exclusiv personale.



• Activitățile cuprinse în ultima excepție sunt unele strict personale și exclud orice legătură cu profesia sau cu orice activitate comercială. Sunt incluse

în această excepție, spre exemplu, corespondența personală prin e-mail, socializarea în mediul on-line și orice altă asemenea activitate.



Pentru persoanele vizate:

Sunt consolidate drepturile garantate persoanelor și sunt introduse drepturi noi:

• **dreptul de a fi uitat** - persoanele fizice pot cere ștergerea datelor personale dacă acestea au fost prelucrate ilegal, fără consimțământul acestora sau dacă datele nu mai sunt necesare scopului în care au fost prelucrate inițial.

În cazul dreptului de a fi uitat, a fost avută în vedere în special prelucrarea datelor în mediul on-line.

• Dreptul de a fi uitat nu este unul absolut – vor fi analizate întotdeauna circumstanțele specifice fiecărui caz în parte. Regulamentul permite păstrarea în continuare a datelor cu

caracter personal în cazul în care aceasta este necesară pentru respectarea libertății de exprimare și a dreptului la informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, din motive de interes public în domeniul sănătății publice, în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanță.



- **dreptul la portabilitatea datelor**

- oferă posibilitatea persoanei fizice de a cere să se transmită datele la un alt operator sau de a primi datele personale care o privesc și pe care le-a furnizat operatorului.

Operatorul de date trebuie să ofere datele într-un format structurat, utilizat în mod curent, prelucrabil automat și interoperabil, tocmai pentru ca și un alt operator de date să le poată prelucra ulterior.

Dreptul la portabilitatea datelor este aplicabil în măsura în care persoana vizată a oferit operatorului datele personale, iar acesta le prelucerează în baza consimțământului sau în executarea unui contract.

Nu se va putea exercita dreptul la portabilitatea datelor în cazul operatorilor de date care prelucerează datele persoanelor fizice în cadrul exercitării funcțiilor lor publice, în cazul în care prelucrarea este necesară în vederea respectării unei obligații legale căreia îi este supus operatorul ori în cazul îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea unei autorități publice cu care este investit operatorul de date.

În exercitarea dreptului la portabilitatea datelor, nu trebuie aduse atingeri drepturilor și

libertăților altor persoane – spre exemplu cazul unui set de date care privește mai multe persoane sau dreptul altei persoane de a obține ștergerea datelor care o privesc.

Atunci când se exercită dreptul la portabilitatea datelor, operatorul de date poate transmite datele personale direct altui operator de date ales de persoana vizată.



Aspecte diverse:

Regulamentul stabilește obligația operatorului de a demonstra obținerea consimțământului persoanei pentru prelucrările de date personale. Persoana vizată are dreptul să își retragă în orice moment consimțământul, în situația în care acesta constituie temei de prelucrare a datelor.



Absența unei manifestări clare de acord nu poate fi privită ca o formă de exprimare a consimțământului. Spre exemplu, în cazul căsuțelor bifate (prin care este prestabilit acordul) nu poate fi prezumat un consimțământ exprimat în cunoștință de cauză.

În cazul în care datele sunt prelucrate în mai multe scopuri, este important ca operatorul de date să poată demonstra că a obținut acordul persoanei pentru a-i prelucra datele în toate acele scopuri.

Regulamentul stabilește obligația operatorului de date de a asigura un anumit nivel de transparență față de persoanele vizate. Acestea trebuie să știe cine este operatorul de date, scopul în care le vor fi prelucrate datele, ce date sunt utilizate, ce drepturi le sunt garantate, cum își pot exercita aceste drepturi și cine sunt/vor fi terții cărora operatorul le va dezvălui datele, dacă este cazul.

În cazul în care sunt prelucrate date personale ale minorilor, operatorul de date trebuie să ofere informațiile respective utilizând un limbaj cât mai simplu și clar, astfel încât copilul/minorul să poată înțelege cu ușurință scopul și modul în care îi vor fi prelucrate datele personale.

Proximitatea față de persoana vizată - autoritatea de supraveghere din statul membru în care se află persoana vizată acționează ca interlocutor/punct de contact atunci când operatorul de date este stabilit într-un alt stat.

În cazul prelucrărilor de date care vizează persoane din mai multe state membre, fiecare persoană are posibilitatea de a se adresa (după caz, de a depune plângere) autorității de supraveghere din statul (membru UE) în care își are domiciliul/reședința. În acest fel, este asigurată implicarea autorității de supraveghere din statul membru în care se află persoana în procedura de adoptare a unei decizii în cazul unui operator de date stabilit într-un alt stat membru.

Cooperare consolidată între autoritățile de supraveghere - în cazul prelucrărilor de date transnaționale (cele care privesc persoane din mai multe state membre UE), autorității de supraveghere din statul respectiv îi sunt oferite competențe pentru a se asigura, alături de autoritățile din celelalte state implicate, că datele sunt prelucrate conform regulilor și principiilor stabilite de Regulament.



Pentru operatorii de date:

One stop shop - formalități reduse pentru operatorii de date (interlocutor unic la nivel UE).

Operatorii de date care își desfășoară activitățile în mai multe state membre UE își pot alege un singur interlocutor - autoritatea de supraveghere din statul membru în care își au stabilit sediul principal.

R e s p o n s a b i l i z a r e a operatorilor de date - accentul este pus pe transparența față de persoana vizată și responsabilitatea operatorului de date față de modul în care prelucrează datele.

În cazul prelucrărilor de date care pot presupune 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. Prelucrarea categoriilor de „date sensibile” poate presupune, de cele mai multe ori, apariția unor riscuri specifice referitoare la viața privată a persoanelor.

O asemenea evaluare va începe întotdeauna cu inventarierea datelor/categoriilor de date personale pe care operatorul intenționează să le prelucreze.

Acestea vor fi supuse unei analize de necesitate pentru a verifica dacă sunt, într-adevăr, necesare toate acele date/categorii de date pentru a atinge scopul urmărit de operator, în vederea respectării principiului minimizării datelor.

Ulterior pot fi identificate și riscurile presupuse de prelucrarea acelor date, spre exemplu dezvăluirea neautorizată/accidentală/ilicită a datelor și atingerile pe care producerea unui astfel de risc le pot aduce dreptului persoanei la viață privată.



În funcție de riscurile identificate, operatorul de date își va stabili și măsuri tehnice și organizatorice (proceduri interne) pentru a preveni producerea acestora.

Privacy by design & Privacy by default - două principii esențiale pentru operatorii de date.

Privacy by design - ești dezvoltator de aplicații prin care se 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 - furnizezi o aplicație care prelucrează date personale? Trebuie să te asiguri că setările inițiale le vor permite utilizatorilor să își mențină controlul asupra vieții lor private/ceea ce postează sau împărtășesc cu alți utilizatori. Utilizatorul poate alege să dezvăluie mai multe informații/date personale, însă trebuie să o facă în cunoștință de cauză, nu implicit (datorită setărilor inițiale).

Transferul datelor în afara UE - atunci când datele personale sunt transferate în afara Uniunii Europene,

acestea vor beneficia în continuare de nivelul de protecție asigurat de regulile și principiile stabilite de Regulament.

Operatorul de date utilizează unul dintre instrumentele prevăzute de Regulament:

- BCR - reguli corporatiste obligatorii
- clauze contractuale standard
- Decizii privind caracterul adecvat al nivelului de protecție emise de către Comisia Europeană.

Pentru a se asigura nivelul de protecție a datelor persoanelor fizice, transferul datelor cu caracter personal într-un stat terț sau către o organizație internațională se poate realiza doar cu respectarea unor condiții de către operator și persoana împuternicită de operator, inclusiv în ceea ce privește transferurile ulterioare de date din statul terț către un alt stat terț sau către o altă organizație internațională.





Transferul datelor cu caracter personal către un stat terț, un teritoriu sau un sector specificat dintr-un stat terț sau o organizație internațională nu necesită autorizare atunci când Comisia Europeană a decis că statul terț, teritoriul, sectorul specificat sau organizația internațională oferă un nivel de protecție adecvat.

În absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită trebuie să adopte măsuri care să compenseze lipsa protecției datelor într-un stat terț prin adoptarea unor garanții eficiente pentru persoanele vizate, cum ar fi:

- un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice (acorduri administrative);
- reguli corporatiste obligatorii/ BCR (binding corporate rules);
- clauzele standard de protecție a

datelor adoptate de Comisia Europeană;

- clauzele standard de protecție a datelor adoptate de autoritatea de supraveghere;
- un cod de conduită aprobat;
- un mecanism de certificare aprobat;
- clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor din statul terț sau organizația internațională;
- dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate (autorizația autorității competente ar trebui obținută când garanțiile sunt oferite prin acorduri administrative fără caracter juridic obligatoriu).



Un transfer către un stat terț sau o organizație internațională mai poate avea loc, în absența unei decizii privind caracterul adecvat al nivelului de protecție sau a unor garanții adecvate, în una din următoarele condiții:

- persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus;
- transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;
- transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;
- transferul este necesar din considerente importante de interes public;
- transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;
- transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul;
- transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau dreptului intern, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în condițiile în care sunt îndeplinite condițiile cu privire la consultare prevăzute de dreptul Uniunii Europene sau de dreptul intern în acel caz specific.





Responsabilul pentru protecția datelor - DPO

Numirea unui responsabil pentru protecția datelor la nivelul operatorului de date reprezintă una dintre măsurile prin care se încearcă responsabilizarea operatorilor de date.

Responsabilul pentru protecția datelor oferă consultanța necesară în vederea respectării tuturor obligațiilor operatorului de date și asigurării transparenței necesare față de persoanele vizate.

Responsabilul pentru protecția datelor poate oferi operatorului de date consultanța necesară în vederea efectuării studiului de impact asupra vieții private.

Operatorul de date trebuie să își desemneze un responsabil pentru protecția datelor în următoarele situații:

- atunci când operatorul de date este o autoritate publică (cu excepția instanțelor sau a autorităților judiciare);

- în cazul în care activitatea principală a operatorului de date constă în operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate pe scară largă;
- în cazul în care activitatea principală a operatorului de date (sau a împuternicitului acestuia) constă în prelucrarea pe scară largă de categorii speciale de date cu caracter personal și de date privind condamnările penale și infracțiunile.

Este recomandată numirea unui responsabil pentru protecția datelor la nivelul operatorului de date și în afara cazurilor de mai sus, întrucât în acest fel poate fi asigurată respectarea prevederilor Regulamentului în cadrul prelucrării de date efectuată de către operatorul de date / împuternicitul acestuia.





Sanțiuni severe - până la 10 – 20 milioane de euro sau între 2% și 4% din cifra de afaceri la nivel internațional, pentru operatorii din sectorul privat.

Regulamentul stabilește criterii clare de individualizare a sancțiuni – vor fi avute în vedere în mod corespunzător natura, gravitatea și durata încălcării, caracterul deliberat al încălcării, acțiunile întreprinse pentru a reduce prejudiciul cauzat, gradul de răspundere sau orice încălcări anterioare relevante, modul în care

încălcarea a fost adusă la cunoștința autorității de supraveghere, conformitatea cu măsurile adoptate împotriva operatorului sau a persoanei împuternicite de operator, aderarea la un cod de conduită și orice alt factor agravant sau atenuant.

Fiecare stat membru poate prevedea norme prin care să se stabilească dacă și în ce măsură pot fi impuse amenzi autorităților publice.





Bulevardul G-ral Gheorghe Magheru 28-30, sector 1

București, cod poștal 010336

Telefon : 031.805.9211

Fax : 031.805.9602

E-mail : anspdcp@dataprotection.ro

Web : www.dataprotection.ro

