Noul Regulament General privind Protecţia Datelor

2017

ANS
PDCP

Regulamentul nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)

Comisia Europeană a semnalat, în anul 2012, necesitatea actualizării cadrului normativ european aplicabil în domeniul protecţiei datelor şi 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.

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

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

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

Regulamentul accentuează responsabilitatea operatorilor care prelucrează date personale, simplificând, în acelaşi timp, formalităţile administrative pe care aceştia 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 obţine de la operatorul de date informaţii mai clare şi cuprinzătoare cu privire la scopul şi temeiul legal în care se prelucrează datele personale, perioada de stocare a acestora şi drepturile de care beneficiază.

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

Regulamentul mai prevede şi 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 atenţie întrucât regulamentul stabileşte o serie de garanţii specifice pentru a proteja cât mai eficient viaţa 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 stabiliţi aceştia, în anumite condiţii.

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 şi cetăţenilor Uniunii Europene, regulile stabilite de Regulament îi vor fi aplicabile şi 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 şi asupra operatorilor de date stabiliţi în afara UE, în măsura în care bunurile şi/sau serviciile acestora sunt adresate (şi) persoanelor aflate pe teritoriul UE

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

Regulile şi principiile stabilite de Regulament protejează viaţa privată a tuturor persoanelor aflate pe teritoriul Uniunii Europene, ale căror date personale sunt prelucrate de companii /persoane fizice/instituţii/orice alte entităţi de drept public sau privat.

Aceste reguli şi principii sunt aplicabile tuturor persoanelor, indiferent de cetăţenia acestora sau de reşedinţă (în interiorul UE).

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

Regulamentul priveşte atât companiile aflate pe teritoriul Uniunii Europene, cât şi cele din afara acestui spaţiu care prelucrează, însă, date personale pentru a oferi bunuri şi servicii persoanelor aflate pe teritoriul Uniunii Europene, indiferent dacă bunurile şi serviciile respective sunt condiţionate sau nu de efectuarea unei plăţi.

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

Pentru a identifica intenţia de a oferi bunuri sau servicii pe teritoriul Uniunii Europene sunt analizaţi mai mulţi 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 şi 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 preferinţele persoanelor, comportamentele şi atitudinile acestora.

Excepţii:

• prevederile Regulamentului nu vor fi aplicabile prelucrărilor efectuate în scopul prevenirii, cercetării şi urmăririi penale a infractorului sau executarea sancţiunii penale. În cazul acestora vor fi aplicabile prevederile unei reglementări naţionale în aplicabilitatea Directivei (UE) 2016/680, (care face parte din acelaşi „pachet legislativ" cu Regulamentul UE 2016/679).

• Regulamentul nu va fi aplicabil activităţilor aflate în afara dreptului Uniunii – aici se încadrează şi prelucrările de date referitoare la securitatea naţională a statelor membre şi relaţiile externe.

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

• Activităţile cuprinse în ultima excepţie sunt unele strict personale şi exclud orice legătură cu profesia sau cu orice activitate comercială. Sunt incluse în această excepţie, spre exemplu, corespondenţa personală prin e-mail, socializarea în mediul on-line şi orice altă asemenea activitate.

Pentru persoanele vizate:

Sunt consolidate drepturile garantate persoanelor şi sunt introduse drepturi noi:

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

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 circumstanţele specifice fiecărui caz în parte. Regulamentul permite păstrarea în continuare a datelor cu caracter personal în cazul în care aceasta este necesară pentru respectarea libertăţii de exprimare şi a dreptului la informare, pentru respectarea unei obligaţii legale, pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul, din motive de interes public în domeniul sănătăţii publice, în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanţă.

- **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 şi pe care le-a furnizat operatorului.

Operatorul de date trebuie să ofere datele într-un format structurat, utilizat în mod curent, prelucrabil automat şi interoperabil, tocmai pentru ca şi 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 prelucrează în baza consimţământului sau în executarea unui contract.

Nu se va putea exercita dreptul la portabilitatea datelor în cazul operatorilor de date care prelucrează datele persoanelor fizice în cadrul exercitării funcţiilor lor publice, în cazul în care prelucrarea este necesară în vederea respectării unei obligaţii legale căreia îi este supus operatorul ori în cazul îndeplinirii unei sarcini care serveşte unui interes public sau care rezultă din exercitarea unei autorităţi publice cu care este învestit operatorul de date.

În exercitarea dreptului la portabilitatea datelor, nu trebuie aduse atingeri drepturilor şi libertăţilor altor persoane – spre exemplu cazul unui set de date care priveşte mai multe persoane sau dreptul altei persoane de a obţine ştergerea 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 stabileşte obligaţia operatorului de a demonstra obţinerea consimţământului persoanei pentru prelucrările de date personale. Persoana vizată are dreptul să îşi retragă în orice moment consimţământul, în situaţia în care acesta constituie temei de prelucrare a datelor.

Absenţa unei manifestări clare de acord nu poate fi privită ca o formă de exprimare a consimţământului. Spre exemplu, în cazul căsuţelor bifate (prin care este prestabilit acordul) nu poate fi prezumat un consimţământ exprimat în cunoştinţă de cauză.

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

Regulamentul stabileşte obligaţia operatorului de date de a asigura un anumit nivel de transparenţă faţă de persoanele vizate. Acestea trebuie să ştie cine este operatorul de date, scopul în care le vor fi prelucrate datele, ce date sunt utilizate, ce drepturi le sunt garantate, cum îşi pot exercita aceste drepturi şi cine sunt/vor fi terţii 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 informaţiile respective utilizând un limbaj cât mai simplu şi clar, astfel încât copilul/minorul să poată înţelege cu uşurinţă scopul şi modul în care îi vor fi prelucrate datele personale.

Proximitatea faţă de persoana vizată - autoritatea de supraveghere din statul membru în care se află persoana vizată acţionează 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) autorităţii de supraveghere din statul (membru UE) în care îşi are domiciliul/reşedinţa. În acest fel, este asigurată implicarea autorităţii 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 autorităţile de supraveghere - în cazul prelucrărilor de date transnaţionale (cele care privesc persoane din mai multe state membre UE), autorităţii de supraveghere din statul respectiv îi sunt oferite competenţe pentru a se asigura, alături de autorităţile din celelalte state implicate, că datele sunt prelucrate conform regulilor şi principiilor stabilite de Regulament.

Pentru operatorii de date:

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

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

Responsabilizarea operatorilor de date - accentul este pus pe transparenţa faţă de persoana vizată şi responsabilitatea operatorului de date faţă de modul în care prelucrează datele.

În cazul prelucrărilor de date care pot presupune un risc ridicat pentru viaţa privată a persoanelor, operatorul trebuie să efectueze un studiu de impact asupra vieţii private.

Rezultatul unui astfel de studiu îi va permite să identifice riscuri specifice şi să adopte măsuri care să împiedice apariţia / producerea acestor situaţii. Prelucrarea categoriilor de „date sensibile" poate presupune, de cele mai multe ori, apariţia unor riscuri specifice referitoare la viaţa privată a persoanelor.

O asemenea evaluare va începe întotdeauna cu inventarierea datelor/categoriilor de date personale pe care operatorul intenţionează 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 şi riscurile presupuse de prelucrarea acelor date, spre exemplu dezvăluirea neautorizată/accidentală/ilicită a datelor şi atingerile pe care producerea unui astfel de risc le pot aduce dreptului persoanei la viaţă privată.

În funcţie de riscurile identificate, operatorul de date îşi va stabili şi măsuri tehnice şi organizatorice (proceduri interne) pentru a preveni producerea acestora.

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

Privacy by design - eşti dezvoltator de aplicaţii prin care se vor prelucra şi date personale? Trebuie să te asiguri, încă din stadiul dezvoltării, că aplicaţia ta va respecta regulile şi principiile stabilite de Regulament.

Privacy by default - furnizezi o aplicaţie care prelucrează date personale? Trebuie să te asiguri că setările iniţiale le vor permite utilizatorilor să îşi menţină controlul asupra vieţii lor private/ceea ce postează sau împărtăşesc cu alţi utilizatori. Utilizatorul poate alege să dezvăluie mai multe informaţii/date personale, însă trebuie să o facă în cunoştinţă de cauză, nu implicit (datorită setărilor iniţiale).

Transferul datelor în afara UE - atunci când datele personale sunt transferate în afara Uniunii Europene, acestea vor beneficia în continuare de nivelul de protecţie asigurat de regulile şi 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 protecţie emise de către Comisia Europeană.

Pentru a se asigura nivelul de protecţie a datelor persoanelor fizice, transferul datelor cu caracter personal într-un stat terţ sau către o organizaţie internaţională se poate realiza doar cu respectarea unor condiţii de către operator şi persoana împuternicită de operator, inclusiv în ceea ce priveşte transferurile ulterioare de date din statul terţ către un alt stat terţ sau către o altă organizaţie internaţională.

Transferul datelor cu caracter personal către un stat terţ, un teritoriu sau un sector specificat dintr-un stat terţ sau o organizaţie internaţională nu necesită autorizare atunci când Comisia Europeană a decis că statul terţ, teritoriul, sectorul specificat sau organizaţia internaţională oferă un nivel de protecţie adecvat.

În absenţa unei decizii privind caracterul adecvat al nivelului de protecţie, operatorul sau persoana împuternicită trebuie să adopte măsuri care să compenseze lipsa protecţiei datelor într-un stat terţ prin adoptarea unor garanţii eficiente pentru persoanele vizate, cum ar fi:

- un instrument obligatoriu din punct de vedere juridic şi executoriu între autorităţile sau organismele publice (acorduri administrative);
- reguli corporatiste obligatorii/ BCR (binding corporate rules);
- clauzele standard de protecţie a datelor adoptate de Comisia Europeană;
- clauzele standard de protecţie 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 şi operatorul,persoana împuternicită de operator sau destinatarul datelor din statul terţ sau organizaţia internaţională;
- dispoziţii care urmează să fie incluse în acordurile administrative dintre autorităţile sau organismele publice, care includ drepturi opozabile şi efective pentru persoanele vizate (autorizaţia autorităţii competente ar trebui obţinută când garanţiile sunt oferite prin acorduri administrative fără caracter juridic obligatoriu).

Un transfer către un stat terţ sau o organizaţie internaţională mai poate avea loc, în absenţa unei decizii privind caracterul adecvat al nivelului de protecţie sau a unor garanţii adecvate, în una din următoarele condiţii:

- persoana vizată şi-a exprimat în mod explicit acordul cu privire la transferul propus;
- transferul este necesar pentru executarea unui contract între persoana vizată şi 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 şi 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 instanţă;
- 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-şi exprima acordul;
- transferul se realizează dintr-un registru care, potrivit dreptului Uniunii sau dreptului intern, are scopul de a furniza informaţii publicului şi care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în condiţiile în care sunt îndeplinite condiţiile cu privire la consultare prevăzute de dreptul Uniunii Europene sau de dreptul intern în acel caz specific.

Responsabilul pentru protecţia 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 protecţia datelor oferă consultanţa necesară în vederea respectării tuturor obligaţiilor operatorului de date şi asigurării transparenţei necesare faţă de persoanele vizate.

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

Operatorul de date trebuie să îşi desemneze un responsabil pentru protecția datelor în următoarele situaţii:

- atunci când operatorul de date este o autoritate publică (cu excepţia instanţelor sau a a autorităţilor judiciare);
- în cazul în care activitatea principală a operatorului de date constă în operaţiuni de prelucrare care necesită o monitorizare regulată şi 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 şi de date privind condamnările penale şi infracţiunile.

Este recomandată numirea unui responsabil pentru protecția datelor la nivelul operatorului de date şi 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.

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

Regulamentul stabileşte criterii clare de individualizare a sancţiuni – vor fi avute în vedere în mod corespunzător natura, gravitatea şi durata încălcării, caracterul deliberat al încălcării, acţiunile întreprinse pentru a reduce prejudiciul cauzat, gradul de răspundere sau orice încălcări anterioare relevante, modul în care încălcarea a fost adusă la cunoştinţa autorităţii de supraveghere, conformitatea cu măsurile adoptate împotriva operatorului sau a persoanei împuternicite de operator, aderarea la un cod de conduită şi 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
Bucureşti, cod poştal 010336
Telefon : 031.805.9211
Fax : 031.805.9602
E-mail : anspdcp@dataprotection.ro
Web : www.dataprotection.ro