Comisia Europeană

RGPD: noi oportunități, noi obligații

Ce trebuie să știe orice firmă despre Regulamentul general al UE privind protecția datelor

Justiție și Consumatori

Luxemburg: Oficiul pentru Publicații al Uniunii Europene, 2018

Print	ISBN 978-92-79-79415-5	doi:10.2838/124172	DS-01-18-082-RO-C
PDF	ISBN 978-92-79-79435-3	doi:10.2838/576916	DS-01-18-082-RO-N

CUPRINS

CAPITOLUL 1

O OPORTUNITATE DE AFACERI 2

CAPITOLUL 2

EXPLICAȚII PRIVIND RGPD 4

CAPITOLUL 3

OBLIGAȚIILE DUMNEAVOASTRĂ CONFORM RGPD. 8

CAPITOLUL 4

SUNTEȚI GATA SĂ VĂ CONFORMAȚI? 18

CAPITOLUL 1

O OPORTUNITATE DE AFACERI

Regulamentul general al UE privind protecția datelor (RGPD) reglementează modul în care societățile prelucrează și gestionează datele cu caracter personal. Urmând a intra în vigoare la 25 mai 2018, regulamentul se aplică tuturor societăților și organizațiilor (de exemplu, spitale, administrații publice etc.) și reprezintă cea mai mare schimbare adusă normelor UE privind protecția datelor în ultimii peste 20 de ani.

RGPD nu numai că le oferă cetățenilor mai mult control asupra modului în care le sunt folosite datele cu caracter personal, ci și simplifică semnificativ mediul de reglementare pentru societăți. În acest scop, regulamentul stabilește un cadru uniform pentru legislația privind protecția datelor la nivelul întregii UE. Cu alte cuvinte, în loc ca fiecare țară să aibă legi proprii privind protecția datelor, se aplică acum un regulament unic la nivelul întregii UE. Astfel, o societate care își desfășoară activitatea în țări diferite nu mai trebuie să se conformeze mai multor regulamente – adesea diferite. Tot ce trebuie să facă este să se conformeze RGPD pentru a-și oferi serviciile oriunde în UE.

Ce beneficii poate aduce RGPD societății dumneavoastră

- **O singură Uniune, o singură lege:** având un set unic de norme, societățile își pot desfășura activitatea în UE mai simplu și mai ieftin.
- **Ghișeu unic:** în majoritatea cazurilor, societățile trebuie să interacționeze cu o singură autoritate de protecție a datelor (APD).
- **Norme europene pe teritoriul european:** societățile cu sediul în afara UE trebuie să aplice aceleași norme ca și societățile europene când oferă bunuri sau servicii persoanelor fizice din UE.
- **Abordare bazată pe riscuri:** RGPD evită crearea unei obligații universale împovărătoare, adaptând obligațiile la riscurile în cauză.
- **Norme potrivite pentru inovare:** RGPD este neutru din punctul de vedere al tehnologiei.

Este vorba despre încredere

Protecția datelor cu caracter personal este o sursă de îngrijorare importantă a oamenilor. Din acest motiv, încrederea lor în mediile digitale rămâne scăzută. Potrivit unui sondaj Eurobarometru:

- opt din 10 persoane consideră că nu dețin pe deplin controlul asupra propriilor date cu caracter personal;
- șase din 10 afirmă că nu au încredere în firmele online;
- peste 90 % dintre europeni spun că doresc ca drepturile privind protecția datelor să fie aceleași în toate țările UE.

RGPD reprezintă o oportunitate nouă pentru societatea dumneavoastră de a spori încrederea consumatorilor prin gestionarea bazată pe riscuri a datelor cu caracter personal.

„Societățile care nu protejează în mod adecvat datele cu caracter personal ale oamenilor riscă să piardă încrederea consumatorilor, care este esențială pentru a încuraja oamenii să folosească produse și servicii noi.”

CAPITOLUL 2

EXPLICAȚII PRIVIND RGPD

Mi se aplică și mie RGPD?

Pe scurt, RGPD se aplică ***oricărei*** societăți care:

prelucrează date cu caracter personal prin mijloace **automate** sau **manuale** (cu condiția ca datele să fie organizate conform criteriilor).

Chiar dacă firma dumneavoastră prelucrează date numai în numele altor societăți, tot trebuie să respectați normele.

RGPD se aplică dacă:

- societatea dumneavoastră prelucrează date cu caracter personal și are sediul în UE, indiferent unde are loc prelucrarea propriu-zisă a datelor; sau
- societatea dumneavoastră are sediul în afara UE, dar oferă bunuri sau servicii sau monitorizează comportamentul unor persoane fizice din UE.

Ce sunt datele cu caracter personal?

Datele cu caracter personal reprezintă orice informații care se referă la o persoană fizică identificată sau identificabilă. Printre acestea se pot număra:

- numele;
- adresa și numărul de telefon;
- locația;
- evidențele privind sănătatea;
- venitul și datele bancare;
- preferințele de ordin cultural;
- ... și altele.

Datele cu caracter personal care au fost anonimizate sau pseudonimizate, dar pot fi utilizate în continuare pentru reidentificarea unei persoane, sunt vizate și ele de RGPD. Cu toate acestea, datele cu caracter personal care au fost anonimizate în mod ireversibil, astfel încât persoana fizică respectivă să nu mai fie identificabilă, nu sunt considerate a fi date cu caracter personal și deci nu fac obiectul RGPD.

RGPD este și neutru din punctul de vedere al tehnologiei, ceea ce înseamnă că protejează datele cu caracter personal indiferent de tehnologia utilizată sau de modul în care sunt stocate aceste date. Indiferent dacă societatea dumneavoastră prelucrează și stochează date cu caracter personal folosind un sistem de IT complex sau evidențe pe hârtie, RGPD vi se aplică și dumneavoastră.

„Indiferent dacă societatea dumneavoastră prelucrează și stochează date cu caracter personal folosind un sistem de IT complex sau evidențe pe hârtie, RGPD vi se aplică și dumneavoastră.”

Aveți mare grijă la categoriile speciale (sensibile) de date cu caracter personal

Dacă printre datele cu caracter personal pe care le colectați se numără informații privind sănătatea, rasa, orientarea sexuală, religia, convingerile politice sau apartenența unei persoane fizice la un sindicat, datele respective sunt considerate sensibile. Societatea dumneavoastră poate prelucra aceste date numai în anumite condiții speciale și puteți avea obligația de a aplica garanții suplimentare, precum criptarea.

Ce constituie prelucrare de date cu caracter personal?

Potrivit RGPD, acțiunile precum colectarea, utilizarea și ștergerea datelor cu caracter personal se înscriu toate în definiția prelucrării de date cu caracter personal.

Vă monitorizați incinta printr-un sistem de televiziune cu circuit închis? Consultați o bază de date care conține date cu caracter personal în scop de afaceri? Trimiteți e-mailuri promoționale? Ștergeți evidențe (digitale) despre angajați sau distrugeți documente? Sau postați o fotografie a unei persoane pe site-ul dumneavoastră sau pe canalul dumneavoastră de rețele sociale?

Dacă ați răspuns afirmativ la oricare dintre cele de mai sus, atunci societatea dumneavoastră prelucrează cu siguranță date cu caracter personal.

Cum contribuie RGPD la reducerea costurilor?

RGPD ia în considerare nevoile firmelor. De exemplu, regulamentul urmărește înlăturarea cerințelor administrative, pentru a reduce costurile și a minimiza povara administrativă:

- **eliminarea notificărilor prealabile:** reforma elimină majoritatea notificărilor prealabile către autoritățile de supraveghere, precum și costurile asociate acestora;
- **responsabilii cu protecția datelor (RPD):** societățile trebuie să numească un RPD mai ales dacă activitățile lor principale implică prelucrarea de date sensibile la scară largă sau monitorizarea periodică, sistematică și la scară largă a persoanelor fizice. Administrațiile publice au obligația de a numi un RPD;
- **evaluările impactului asupra protecției datelor:** societățile sunt obligate să efectueze o evaluare a impactului asupra protecției datelor numai dacă o activitate propusă de prelucrare a datelor implică un risc ridicat la adresa drepturilor și libertăților persoanelor fizice;
- **păstrarea evidențelor:** societățile cu mai puțin de 250 de angajați nu au obligația de a păstra evidențe decât dacă prelucrarea datelor nu este ocazională sau dacă implică informații sensibile.

„Regulamentul urmărește înlăturarea cerințelor administrative, pentru a reduce costurile și a minimiza povara administrativă.”

CAPITOLUL 3

OBLIGAȚIILE DUMNEAVOASTRĂ CONFORM RGPD

RGPD impune societăților obligații directe privind prelucrarea datelor la nivelul întregii UE. Potrivit RGPD, o societate poate prelucra date cu caracter personal numai în anumite condiții. De exemplu, prelucrarea trebuie să fie echitabilă și transparentă, să fie efectuată cu un scop specific și legitim și să se limiteze la datele necesare pentru îndeplinirea scopului respectiv. De asemenea, prelucrarea trebuie să se bazeze pe unul dintre următoarele temeiuri juridice:

- **consimțământul** persoanei în cauză;
- o **obligație contractuală** între dumneavoastră și persoana în cauză;
- în vederea respectării unei **obligații legale**;
- pentru a proteja **interesele vitale** ale persoanei fizice respective;
- pentru a executa o **sarcină în interes public**;
- în scopul **intereselor legitime** ale societății dumneavoastră, dar numai după ce v-ați asigurat că acest lucru nu are un impact grav asupra drepturilor și libertăților fundamentale ale persoanei fizice ale cărei date le prelucrați. Dacă drepturile persoanei respective prevalează în raport cu interesele dumneavoastră, nu puteți prelucra datele.

În atenție: obținerea consimțământului privind utilizarea datelor

RGPD aplică norme stricte pentru prelucrarea datelor pe bază de consimțământ. Obiectivul acestor norme este de a asigura faptul că persoana fizică înțelege pentru ce își dă consimțământul. Cu alte cuvinte, consimțământul trebuie să fie **liber exprimat**, **specific**, **în cunoștință de cauză** și **clar**, în urma unei cereri formulate într-un limbaj clar și simplu. Mai mult, consimțământul trebuie acordat printr-o **acțiune fără echivoc**, cum ar fi bifarea unei căsuțe online sau semnarea unui formular.

Dacă prelucrați date cu caracter personal referitoare la un **copil** pe baza consimțământului, este necesar consimțământul părinților. Se recomandă să consultați însă legislația națională, deoarece pragul de vârstă variază între 13 și 16 ani de la o țară la alta.

Rețineți! În cazul în care cineva își dă consimțământul privind prelucrarea datelor sale cu caracter personal, puteți prelucra datele numai în scopurile pentru care a fost dat consimțământul. Mai mult, trebuie să îi oferiți posibilitatea de a-și retrage consimțământul.

Stabiliți-vă rolul și responsabilitatea

Odată ce ați stabilit că RGPD se aplică în cazul societății dumneavoastră și că are loc o prelucrare de date cu caracter personal, următorul pas este să vă stabiliți rolul.

Normele privind protecția datelor fac distincție între operatorul de date și persoana împuternicită de operator, fiecăruia aplicându-i-se obligații diferite. În timp ce operatorul de date stabilește scopul și mijloacele de prelucrare a datelor cu caracter personal, persoana împuternicită de operator doar prelucrează datele în numele operatorului de date. Acest lucru nu înseamnă însă că persoana împuternicită de operator se poate ascunde pur și simplu în spatele acestuia din urmă.

RGPD impune obligația ca operatorul de date să angajeze numai o persoană împuternicită care oferă garanții suficiente. Aceste garanții ar trebui incluse într-un contract scris între operatorul de date și persoana împuternicită de operator. Contractul trebuie să conțină, de asemenea, mai multe clauze obligatorii, inclusiv, de exemplu, o clauză care să prevadă că persoana împuternicită de operator va prelucra datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului.

Obligații care protejează drepturile persoanelor fizice

RGPD include mai multe obligații menite să protejeze dreptul persoanelor fizice de a deține controlul asupra propriilor date cu caracter personal.

Obligația dumneavoastră: furnizarea de informații transparente

Societățile trebuie să le ofere persoanelor fizice informații privind cine, ce și de ce prelucrează. Aceste informații trebuie să arate clar cel puțin:

- cine sunteți;
- de ce prelucrați datele;
- care este temeiul juridic;
- cine va primi datele (dacă este cazul).

În unele cazuri, informațiile trebuie să cuprindă și:

- datele de contact ale RPD;
- interesul legitim (dacă interesul legitim reprezintă temeiul juridic al prelucrării);
- baza pentru transferarea datelor într-o țară din afara UE;
- cât timp vor fi stocate datele;
- drepturile persoanei fizice în ceea ce privește protecția datelor (adică dreptul de acces, dreptul la corectare, ștergere, restricționare, opoziție, portabilitate etc.);
- cum se poate retrage consimțământul (în cazul în care consimțământul reprezintă temeiul juridic al prelucrării);
- dacă există o obligație legală sau contractuală de furnizare a datelor;
- în cazul proceselor decizionale automatizate, informații privind logica, importanța și consecințele deciziei.

„Societățile trebuie să le ofere persoanelor fizice informații privind cine, ce și de ce prelucrează.”

Obligația dumneavoastră: dreptul de acces și dreptul la portabilitatea datelor

Persoanele fizice au dreptul de a solicita acces la datele lor cu caracter personal, gratuit și într-un format accesibil. Dacă primiți o astfel de solicitare, trebuie:

- să îi spuneți persoanei fizice respective dacă prelucrați datele sale cu caracter personal;
- să informați persoana în legătură cu prelucrarea (cum ar fi scopurile prelucrării, categoriile de date cu caracter personal în cauză, destinatarii datelor sale etc.);
- să îi furnizați persoanei o copie a datelor cu caracter personal care se prelucrează.

În plus, când prelucrarea este bazată pe consimțământ sau pe un contract, persoana fizică poate solicita returnarea datelor sale cu caracter personal sau transmiterea acestora către o altă societate. Acest drept se numește dreptul la portabilitatea datelor. Datele ar trebui furnizate într-un format utilizat în mod curent și prelucrabil automat.

Deși aceste două drepturi sunt strâns legate unul de celălalt, ele sunt totuși două drepturi distincte. Astfel, trebuie să vă asigurați că nu există confuzie între cele două drepturi și să informați persoana fizică în mod corespunzător.

Obligația dumneavoastră: dreptul la ștergerea datelor („dreptul de a fi uitat”)

În unele situații, o persoană poate cere ca operatorul de date să îi șteargă datele cu caracter personal, cum ar fi atunci când datele nu mai sunt necesare pentru realizarea scopului prelucrării. Societatea dumneavoastră nu este însă obligată să dea curs cererii unei persoane fizice dacă:

- prelucrarea este necesară în vederea respectării libertății de exprimare și de informare;
- aveți obligația de a păstra datele cu caracter personal pentru a respecta o obligație legală;
- există alte motive de interes public pentru păstrarea datelor cu caracter personal, cum ar fi sănătatea publică sau scopuri de cercetare științifică și istorică;
- aveți nevoie să păstrați datele cu caracter personal în vederea stabilirii unui drept în instanță.

Obligația dumneavoastră: dreptul la corectarea datelor și dreptul la opoziție

Dacă o persoană fizică consideră că datele sale cu caracter personal sunt incorecte, incomplete sau inexacte, aceasta are dreptul de a cere rectificarea sau completarea acestora fără întârzieri nejustificate.

De asemenea, o persoană fizică are dreptul de a se opune în orice moment prelucrării propriilor date cu caracter personal într-un anumit scop în cazul în care societatea dumneavoastră prelucrează datele în baza interesului dumneavoastră legitim sau pentru îndeplinirea unei sarcini în interes public. Cu excepția cazului în care aveți un interes legitim care prevalează în raport cu interesul persoanei fizice, trebuie să încetați a mai prelucra datele cu caracter personal ale acesteia. Tot astfel, o persoană poate solicita restricționarea prelucrării propriilor date cu caracter personal în timp ce se verifică dacă interesul dumneavoastră legitim prevalează sau nu în raport cu interesul său. Cu toate acestea, în cazul marketingului direct, aveți întotdeauna obligația de a înceta prelucrarea datelor cu caracter personal la cererea persoanei fizice.

O atenționare privind procesele decizionale automate și crearea de profiluri

Persoanele fizice au dreptul de a nu fi supuse la o decizie bazată exclusiv pe prelucrarea automată. Există însă unele excepții de la această regulă, cum ar fi în cazul în care persoana fizică și-a dat consimțământul explicit în ceea ce privește decizia automatizată. Cu excepția cazului în care decizia automatizată este bazată pe o lege, societatea dumneavoastră trebuie:

- să informeze persoana fizică respectivă în legătură cu procesul decizional automatizat;
- să îi acorde persoanei fizice dreptul de a solicita analizarea deciziei automatizate de către o persoană;
- să îi ofere persoanei fizice posibilitatea de a contesta decizia automatizată.

De exemplu, dacă o bancă își automatizează decizia de a acorda sau de a nu acorda un împrumut unei anumite persoane fizice, persoana respectivă ar trebui informată cu privire la decizia automatizată și ar trebui să i se dea posibilitatea de a contesta decizia și de a solicita intervenția umană.

Obligații bazate pe risc

Pe lângă obligațiile menite să protejeze drepturile persoanelor fizice, RGPD conține și obligații a căror aplicare depinde de risc.

Obligația dumneavoastră: numirea unui responsabil cu protecția datelor

Un RPD este responsabil cu monitorizarea conformării dumneavoastră la RGPD. Una dintre atribuțiile de bază ale RPD este de a informa și consilia angajații care efectuează prelucrarea propriu-zisă a datelor cu caracter personal în legătură cu obligațiile care le revin. De asemenea, RPD cooperează cu APD, îndeplinind rolul de punct de contact cu APD și cu persoanele fizice.

Societatea dumneavoastră are obligația de a numi un RPD dacă:

- monitorizați persoane fizice în mod periodic sau sistematic sau prelucrați categorii speciale de date;
- această prelucrare este o activitate principală a societății; și
- faceți acest lucru la scară largă.

De exemplu, dacă prelucrați date cu caracter personal pentru direcționarea de mesaje publicitare prin intermediul motoarelor de căutare pe baza comportamentului online al oamenilor, RGPD vă impune să aveți un RPD. Dacă însă le trimiteți clienților dumneavoastră materiale promoționale numai o dată pe an, nu aveți nevoie de un RPD. Tot astfel, dacă sunteți medic și colectați date privind sănătatea pacienților, probabil că nu este necesar un RPD. Dacă însă prelucrați date cu caracter personal privind genetica și sănătatea pentru un spital, este necesar un RPD.

Obligația dumneavoastră: asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

RGPD introduce două principii noi: asigurarea protecției datelor începând cu momentul conceperii și în mod implicit.

Asigurarea protecției datelor începând cu momentul conceperii contribuie la asigurarea faptului că o societate ține cont de protecția datelor încă din etapele inițiale ale planificării unei modalități noi de prelucrare a datelor cu caracter personal. În conformitate cu acest principiu, un operator de date trebuie să ia toate măsurile tehnice și organizatorice pentru a pune în aplicare principiile privind protecția datelor și a proteja drepturile persoanelor fizice. Printre aceste măsuri s-ar putea include, de exemplu, utilizarea pseudonimizării.

Asigurarea protecției datelor începând cu momentul conceperii reduce la minimum riscurile la adresa vieții private și sporește încrederea. Punând pe primul plan protecția datelor în cadrul dezvoltării de noi bunuri sau servicii, orice eventuale probleme privind protecția datelor pot fi evitate dintr-o etapă timpurie. Mai mult, această practică ajută la conștientizarea privind protecția datelor în toate departamentele și la toate nivelurile unei societăți.

Protecția datelor în mod implicit presupune ca firma dumneavoastră să stabilească drept implicit scenariul care protejează cel mai bine viața privată. De exemplu, dacă sunt posibile două scenarii referitoare la viața privată, iar unul dintre ele previne accesarea de către alte persoane a datelor cu caracter personal, acesta ar trebui utilizat drept scenariu implicit.

„Asigurarea protecției datelor începând cu momentul conceperii reduce la minimum riscurile la adresa vieții private și sporește încrederea.”

„Protecția datelor în mod implicit presupune ca firma dumneavoastră să stabilească drept implicit scenariul care protejează cel mai bine viața privată.”

Obligația dumneavoastră: notificarea corespunzătoare în cazul unei încălcări a securității datelor

Se produce o încălcare a securității datelor atunci când datele cu caracter personal de care răspundeți sunt dezvăluite, fie accidental, fie în mod ilegal, unor destinatari neautorizați sau sunt făcute temporar indisponibile sau modificate.

Este vital ca firmele să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a evita încălcările securității datelor. Dacă se produce însă o încălcare a securității datelor, iar respectiva încălcare reprezintă un risc la adresa drepturilor și libertăților persoanelor fizice, trebuie să notificați APD în termen de 72 de ore din momentul în care aflați despre încălcare.

Dacă încălcarea securității datelor reprezintă un risc *ridicat* la adresa celor afectați, firma poate avea și obligația de a informa toate persoanele fizice afectate de încălcarea securității datelor..

Transferați date cu caracter personal în afara UE?

RGPD se aplică în Spațiul Economic European (SEE), care include toate țările UE, precum și Islanda, Liechtenstein și Norvegia. Când se transferă datele cu caracter personal în afara SEE, protecția oferită de RGPD trebuie să le însoțească. Acest lucru înseamnă că, pentru a exporta date în străinătate, societățile trebuie să se asigure că există anumite garanții.

RGPD oferă un set diversificat de mecanisme pentru transferarea datelor în țări terțe. Potrivit RGPD, asemenea transferuri sunt permise dacă:

1. măsurile de protecție ale țării respective sunt considerate de UE ca fiind adecvate; sau
2. societatea dumneavoastră ia, de exemplu, măsurile necesare pentru a asigura garanții adecvate, cum ar fi includerea anumitor clauze în contractul încheiat cu importatorul din afara Europei al datelor cu caracter personal; sau
3. societatea dumneavoastră, de exemplu, se bazează pe anumite temeiuri pentru transfer (numite „derogări”), cum ar fi consimțământul persoanei fizice.

Pentru mai multe informații privind normele aplicabile transferurilor internaționale de date, consultați Comunicarea Comisiei Europene privind schimbul de date cu caracter personal și protecția acestora într-o lume globalizată: http://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52017DC0007&from=RO

Trebuie să efectuați o evaluare a impactului asupra protecției datelor (EIPD)?

Efectuarea unei EIPD este obligatorie ori de câte ori prelucrarea avută în vedere ar genera un risc ridicat pentru drepturile și libertățile persoanelor fizice. Așa se poate întâmpla, de exemplu, când se utilizează tehnologii noi.

Potrivit RGPD, există cel puțin un asemenea risc ridicat atunci când:

- se folosesc mecanisme de prelucrare automatizată și de creare de profiluri pentru a evalua persoanele fizice în mod sistematic și cuprinzător;
- o zonă accesibilă publicului este monitorizată sistematic la scară largă (de exemplu, printr-un sistem de televiziune cu circuit închis);
- se prelucrează la scară largă date sensibile (de exemplu, date referitoare la sănătate).

Obiectivul EIPD este de a identifica riscurile potențiale la adresa drepturilor și libertăților persoanelor fizice înainte de a începe prelucrarea datelor cu caracter personal și înainte de a se materializa riscul. Atenuând riscul în mod anticipat, se pot evita prejudiciile și se pot reduce la minimum costurile.

Dacă măsurile indicate în EIPD nu reușesc să elimine toate riscurile ridicate identificate, trebuie consultată APD înainte de a se efectua prelucrarea avută în vedere a datelor.

„Efectuarea unei EIPD este obligatorie ori de câte ori prelucrarea avută în vedere ar genera un risc ridicat pentru drepturile și libertățile persoanelor fizice.”

Ce aveți de făcut

Răspunsul la solicitări

Dacă societatea dumneavoastră primește o solicitare de la o persoană care dorește să își exercite drepturile, trebuie să răspundeți acestei solicitări fără întârzieri nejustificate și, în orice caz, în termen de o lună de la primirea solicitării. Acest termen de răspuns se poate prelungi însă cu două luni, în cazul solicitărilor complexe sau multiple, cu condiția ca persoana în cauză să fie informată în privința prelungirii. În plus, solicitările trebuie tratate **gratuit**. În caz de respingere a solicitării, trebuie să informați persoana în cauză cu privire la motivele respingerii și la dreptul său de a depune o plângere la APD.

Demonstrați conformitatea și păstrați evidențe!

Unul dintre principiile esențiale de la baza RGPD este asigurarea posibilității societăților de a-și demonstra conformitatea. Acest lucru înseamnă că trebuie să puteți dovedi că societatea dumneavoastră acționează în conformitate cu RGPD și îndeplinește toate obligațiile aplicabile – în special ca urmare a unei cereri sau inspecții a APD.

Un mod de a face acest lucru este păstrarea de evidențe detaliate privind aspecte precum:

- numele și datele de contact ale societății dumneavoastră implicate în prelucrarea datelor;
- motivul (motivele) prelucrării datelor cu caracter personal;
- descrierea categoriilor de persoane care furnizează date cu caracter personal;
- categoriile de organizații care primesc datele cu caracter personal;
- transferul datelor cu caracter personal către o altă țară sau organizație;
- perioada de stocare a datelor cu caracter personal;
- descrierea măsurilor de securitate folosite pe parcursul prelucrării datelor cu caracter personal.

În plus, societatea dumneavoastră ar trebui să mențină – și să actualizeze periodic – proceduri și orientări scrise și să le aducă la cunoștința angajaților proprii.

CAPITOLUL 4

SUNTEȚI GATA SĂ VĂ CONFORMAȚI?

În ceea ce privește prelucrarea datelor cu caracter personal, RGPD așează mingea în terenul dumneavoastră. Primul pas este să vă cartografiați activitățile actuale de prelucrare a datelor și să vă reevaluați procesele interne de afaceri. În special, trebuie:

- să identificați ce date dețineți, în ce scop și pe ce temei juridic le dețineți;
- să evaluați toate contractele existente, în special cele dintre operatori și persoanele împuternicite de operatori;
- să evaluați toate căile disponibile pentru transferurile internaționale; și
- să analizați guvernanța societății dumneavoastră în ansamblu (adică ce măsuri de IT și de natură organizatorică aveți puse în aplicare), inclusiv eventuala obligație sau dorință a dumneavoastră de a numi un responsabil cu protecția datelor.

Un element esențial în acest proces este să vă asigurați că în aceste evaluări se implică nivelul cel mai înalt de management al societății dumneavoastră, că acesta contribuie la evaluări și că este informat și consultat periodic cu privire la modificările aduse politicii privind datele.

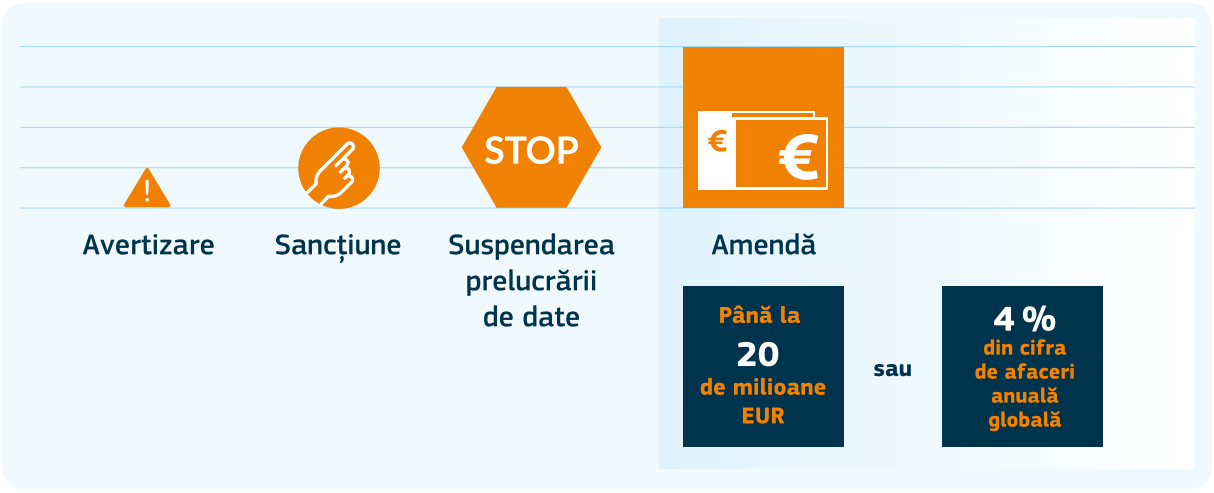
Prelucrați date în mai multe țări?

Pentru prelucrarea transfrontalieră, este posibil ca autoritatea competentă să fie o autoritate de supraveghere din altă țară, nu APD din țara dumneavoastră. De obicei, competența revine APD din țara UE în care se află sediul principal al societății dumneavoastră (unde se iau deciziile despre mijloacele și scopurile prelucrării).

Riscurile neconformării

Neconformarea la RGPD poate duce la amenzi considerabile – de până la 20 de milioane EUR sau 4 % din cifra de afaceri globală a societății dumneavoastră pentru anumite încălcări. APD poate impune și măsuri corective suplimentare, cum ar fi ordonarea sistării prelucrării datelor cu caracter personal. De asemenea, ar trebui să țineți cont de prejudiciul pe care neconformitatea l-ar putea aduce renumelui dumneavoastră.

Fără îndoială, costurile neconformării la RGPD depășesc cu mult orice investiție făcută în scopul conformării.



Întrebări? Neclarități? Consultați APD din țara dumneavoastră.

Găsiți online autoritatea dumneavoastră națională de protecție a datelor

http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm

ANUNȚ IMPORTANT

Informațiile și îndrumările din această broșură sunt menite să contribuie la o mai bună înțelegere a normelor UE privind protecția datelor.

Instrumentul acesta are un rol pur orientativ – numai textul Regulamentului general privind protecția datelor (RGPD) are efect juridic. În consecință, numai RGPD poate crea drepturi și obligații pentru persoanele fizice. Acest ghid nu creează niciun drept și nicio așteptare care să se poată pune în aplicare.

Competența privind interpretarea cu caracter obligatoriu a legislației UE îi revine exclusiv Curții de Justiție a Uniunii Europene. Opiniile exprimate în acest ghid nu aduc atingere poziției pe care ar putea-o adopta Comisia în fața Curții de Justiție.

Nici Comisia Europeană, nici vreo persoană care acționează în numele Comisiei Europene nu este responsabilă pentru posibila utilizare a informațiilor din broșură.

Această broșură reflectă situația actuală la momentul redactării; ea trebuie privită ca „document viu”, deschis la perfecționare, iar conținutul său poate fi modificat fără nicio notificare.

Găsiți informații despre UE

Online

Informații despre Uniunea Europeană în toate limbile oficiale ale UE sunt disponibile pe site-ul Europa, la: https://europa.eu/european-union/index_ro

Publicații ale UE

Puteți descărca sau comanda publicații ale UE gratuite și contra cost pe site-ul EU Bookshop, la: https://publications.europa.eu/bookshop. Mai multe exemplare ale publicațiilor gratuite pot fi obținute contactând Europe Direct sau centrul dumneavoastră local de informare (a se vedea https://europa.eu/european-union/contact_ro).

Dreptul UE și documente conexe

Pentru accesul la informații juridice din UE, inclusiv la ansamblul legislației UE începând din 1952 în toate versiunile lingvistice oficiale, accesați site-ul EUR-Lex, la: http://eur-lex.europa.eu

Datele deschise ale UE

Portalul de date deschise al UE (http://data.europa.eu/euodp/ro) oferă acces la seturi de date din UE. Datele pot fi descărcate și reutilizate gratuit, atât în scopuri comerciale, cât și necomerciale.

DS-01-18-082-RO-N

Regulamentul general privind protecția datelor (RGPD) reglementează modul în care societățile prelucrează și gestionează datele cu caracter personal. Având o lege europeană unică pentru protecția datelor cu caracter personal, societatea dumneavoastră trebuie acum să se conformeze în principal la o singură lege privind protecția datelor, indiferent unde pe teritoriul UE oferă bunuri și servicii.

Simplificând mediul de reglementare pentru întreprinderi, RGPD reprezintă o nouă oportunitate pentru societatea dumneavoastră de a îmbunătăți gestionarea datelor cu caracter personal și de a câștiga astfel mai multă încredere din partea consumatorilor.

Această broșură subliniază obligațiile care îi revin societății dumneavoastră în temeiul RGPD.

europa.eu/dataprotection/ro

Oficiul pentru Publicații