

I. Protecţia datelor la nivel european

În data de 4 mai 2016, a fost publicat în Jurnalul Oficial al Uniunii Europene pachetul legislativ privind protecţia datelor la nivelul Uniunii Europene, respectiv:

– **Regulamentul (UE) 2016/679** 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), care va avea **directă aplicabilitate în toate statele membre, inclusiv în România, începând cu data de 25 mai 2018**
și

– **Directiva (UE) 2016/680** referitoare la protecţia datelor personale în cadrul activităţilor specifice desfăşurate de autorităţile de aplicare a legii.

Regulamentul UE 2016/679 circumstanțiază și detaliază multe condiții deja existente în legislația europeană (Directiva privind protecția datelor cu caracter personal 95/46/EC, care își va înceta aplicabilitatea).

II. Regulamentul General privind Protecția Datelor

PREVEDERI PRINCIPALE

Regulamentul General privind Protecția Datelor 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.**

Din punct de vedere al **domeniului de aplicare material,** Regulamentul se aplică prelucrării datelor cu caracter personal, efectuată 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.

Din punct de vedere al **domeniului de aplicare teritorial**, Regulamentul se aplică prelucrării datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Uniunii, indiferent dacă prelucrarea are loc sau nu pe teritoriul Uniunii. Regulament se aplică 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
- monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Uniunii.

Cu privire la **tipul de date colectate,** Regulamentul UE 2016/679 **lărgește spectrul** de date incluse sub sigla ”personale”, fiind din această perspectivă cea mai strictă reglementare

europeană de până acum.

Regulamentul definește datele personale ca orice fel de informație despre o persoană fizică care poate duce, direct sau indirect, la identificarea acestei persoane. În această categorie sunt incluse **numele, numerele de identificare, date despre locație** dar și orice alt tip de **identificator online**
care este specific din punct de vedere
fizic, psihologic, genetic, mental, economic, cultural sau social
unei anumite persoane fizice. Spre deosebire de Directiva 95/46/EC,
informațiile despre locație sau identificatorii online vor fi considerate date personale
. Regulamentul UE 2016/679 vizează și identificatorii online oferiți de device-uri, de aplicații sau de protocoale, markeri de tipul adrese internet protocol,
chiar și cookies
sau tag-uri de radio frecvență.

Principiile de prelucrarea datelor cu caracter personal– datele cu caracter personal trebuie să fie:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri;

(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);

(d) exacte și, în cazul în care este necesar, să fie actualizate;

(e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele;

(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal.

Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele **condiții:**

(a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

(b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

(d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

(e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Persoana vizată are dreptul de a obține din partea operatorului o **confirmare că se prelucrează sau nu date cu caracter personal**

care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:

(a) scopurile prelucrării;

(b) categoriile de date cu caracter personal vizate;

(c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;

(d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;

(f) dreptul de a depune o plângere în fața unei autorități de supraveghere;

(g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;

(h) existența unui proces decizional automatizat incluzând crearea de profiluri.

Cu privire la **responsabilitatea operatorului,** ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare **măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să**

demonstreze că prelucrarea se efectuează în conformitate cu prezentul regulament. Respectivele măsuri se revizuiesc
și se actualizează dacă este necesar.

Obligațiile de păstrare a evidenței **nu se aplică unei întreprinderi sau organizații cu mai puțin de 250 de angajați** , cu **excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc**
pentru drepturile și libertățile persoanelor vizate, prelucrarea
nu este ocazională sau prelucrarea include categorii speciale de date
, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10.

La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.

Operatorul și persoana împuternicită de operator **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.

Un grup de întreprinderi poate numi un responsabil cu protecția datelor unic, cu condiția ca responsabilul cu protecția datelor să fie ușor accesibil din fiecare întreprindere.

Nerespectarea Regulamentului General privind Protecția Datelor poate atrage mai multe tipuri de **sancțiuni/despăgubiri**, inclusiv **amenzi foarte mari de până la 20 de milioane de euro sau 4% din cifra de afaceri globală** .

III. Proces complex de implementare și costuri ridicate

Cheltuielile vor fi **diferite în funcție de sectorul de activitate și de complexitatea activităților desfășurate** , fiind vizate aducerea site-ului și a sistemelor interne în conformitate cu Regulamentul, prelucrarea datelor angajaților, a datelor clienților în scopuri de marketing, a datelor sensibile ale unor clienți (date de sănătate, cazier fiscal/judiciar etc.), vânzarile on-line, etc.

Potrivit studiului *"The Economic Costs of the European Union's Cookie Notification Policy"* din 2014 politica de notificare a vizitatorilor asupra folosirii cookie-urilor (cea pe care Regulamentul General privind Protecția Datelor vine să o înlocuiască) genera o cheltuială anuală de peste 2 miliarde de euro în cadrul Uniunii Europene. Costul investit în aducerea site-ului și a sistemelor interne în conformitate cu reglementările în vigoare fusese atunci
estimat la
900€/site
,
sum
ă ce poate fi un reper și pentru cerintele Regulamentului General privind Protecția Datelor.

IV. CNIPMMR SOLICITĂ MĂSURI DE SUSȚINERE A IMM-URILOR

Deși, de regulă, obligațiile de păstrare a evidenței nu se aplică IMM-urilor, **întreprinderile sau organizațiile cu mai puțin de 250 de angajați au**
obligații de păstrare a evidenței
în
cazul în care prelucrarea este susceptibilă să genereze un risc
pentru drepturile și libertățile persoanelor vizate, dacă prelucrarea
nu este ocazională sau prelucrarea include categorii speciale de date
,
foarte multe întreprinderi încadrându-se în aceste situații
.

Nu există **măsuri/programe de consiliere și susținere a IMM-urilor** din România pentru implementarea Regulamentului General privind Protecția Datelor, în conditiile în care mai sunt **3 luni**
până la data aplicării Regulamentului (25 mai 2018).

CNIPMMR solicită autorităților competente adoptarea următoarelor măsuri urgente:

- **asigurarea unui serviciu de consiliere gratuită pentru IMM-uri** operațional înainte cu minim 2 luni de data aplicării Regulamentului General privind Protecția Datelor;

- realizarea unui **ghid aplicativ concret și complet pentru IMM-uri**, cu pași de urmat, proceduri operaționale, instituții, termene, formulare, etc. disponibil on-line;

- realizarea unei **ample campanii de informare** adaptate specificului IMM-urilor;
- punerea în aplicare a art. 3 alin. (1) din **Legea prevenirii nr. 270/2017**, potrivit cu care: *"Toate autoritățile/instituțiile publice cu atribuții de control, constatare și sancționare a contravenților au obligația, corespunzător domeniilor aflate în responsabilitatea acestora, ca, în termen de 3 luni de la data intrării în vigoare a prezentei legi,*
să elaboreze și să difuzeze materiale documentare și ghiduri și să aloce pe pagina de internet secțiuni special dedicate informării publice";

- punerea în aplicare a art. 3 alin. (3) din Legea prevenirii nr. 270/2017, potrivit cu care: autoritățile/instituțiile publice cu atribuții de control au obligația **să elaboreze proceduri** de îndrumare și control, să afișeze pe site-urile proprii spețele cu frecvență ridicată și soluțiile de îndrumare emise, să exercite activ rolul de îndrumare, oferind, conform procedurilor, indicațiile și orientările necesare pentru evitarea pe viitor a încălcării prevederilor legale;

- punerea în aplicare a art. 3 alin. (4) din Legea prevenirii nr. 270/2017, potrivit cu care: *„Autoritatea administrației publice centrale cu atribuții de coordonare la nivel național a domeniului mediul de afaceri*
(Ministerul pentru Mediul de Afaceri, Comerț și Antreprenoriat)
are obligația ca, în termen de 6 luni de la data intrării în vigoare a prezentei legi, de a dezvolta și opera un portal dedicat
oferirii în
mod centralizat de servicii online și resurse în vederea informării
în ceea ce privește aspectele prevăzute la alin. (1)".

** *sursa--* CNIPMMR