Ce este GDPR?

Regulamentul general privind protecția datelor (GDPR - General Data Protection Regulation) este noua lege privind protecția datelor din Uniunea Europeană. El înlocuiește Directiva privind protecția datelor, aflată în vigoare încă din 1995. Deși GDPR păstrează multe dintre principiile stabilite în Directivă, este o lege mult mai ambițioasă. Printre modificările notabile se numără faptul că GDPR oferă oamenilor mai mult control asupra datelor lor cu caracter personal, impunând noi obligații organizațiilor care colectează, manipulează sau analizează date cu caracter personal. De asemenea, GDPR acordă autorităților naționale de reglementare noi puteri, astfel încât acestea să poată aplica amenzi importante organizațiilor ce încalcă legea.

GDPR intră în vigoare pe 25 mai 2018

Care sunt principalele cerințe ale GDPR?

GDPR impune o gamă largă de cerințe organizațiilor care colectează sau prelucrează date cu caracter personal, inclusiv obligația de a respecta șase principii cheie:

- Transparență, corectitudine și legalitate în manipularea și utilizarea datelor cu caracter personal;
- Limitarea prelucrării datelor cu caracter personal la scopurile explicite și legitime;
- Restrângerea colectării și a păstrării la cantitatea minimă de date cu caracter personal necesară pentru un anumit scop;
- Asigurarea corectitudinii datelor, inclusiv a posibilității de a le șterge și edita;
- Limitarea păstrării datelor cu caracter personal;
- Asigurarea securității, a integrității și a confidențialității datelor cu caracter personal.

Modificări cheie în GDPR
Confidențialitatea personala
Persoanele au dreptul:

- Să își acceseze și să își exporte datele cu caracter personal;
- Să își șteargă datele cu caracter personal;
- Să corecteze greșelile din datele lor cu caracter personal;
- Să se opună prelucrării datelor lor cu caracter personal.

Măsuri de control și notificări
Companiile și organizațiile trebuie:

- Să protejeze datele cu caracter personal prin măsuri de securitate adecvate;
- Să notifice autoritățile despre încălcări privind datele cu caracter personal;
- Să obțină consimțământul pentru colectarea și prelucrarea datelor cu caracter personal;
- Să țină evidențe detaliate despre activitățile de prelucrare a datelor.

Transparență
Companiile și organizațiile trebuie să aibă politici care:

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.294, E-mail: oana.velcota@e-uvt.ro

- Să comunice clar colectarea datelor;
- Să precizeze de ce și când se prelucrează datele cu caracter personal;
- Să stabilească politici de păstrare și ștergere a datelor.

IT și instruire
Companiile și organizațiile vor fi obligate:

- Să își instruiască angajații despre bune practici de confidențialitate și securitate;
- Să auditeze și actualizeze politicile privind datele;
- Să angajeze, dacă este cazul, un responsabil de protecția datelor;
- Să redacteze și gestioneze contracte conforme cu furnizorii.

4 pași cheie ce pot fi urmați chiar azi privind conformitatea cu GDPR

- **Descoperă –** identifică datele cu caracter personal și unde se află ele. Auditează-ți datele și procesele, pentru a evalua măsura în care GDPR se aplică și organizației tale.
- **Gestionează –** controlează cum se utilizează datele cu caracter personal. Creează politici transparente, care arată clar în ce fel, când și cum colectează și prelucrează organizația ta date cu caracter personal.
- **Protejează** – stabilește măsuri de securitate pentru a-ți proteja datele. Este responsabilitatea ta să protejezi datele cu caracter personal. Creează un plan de gestiune a riscurilor și utilizează infrastructura sigură
- **Raportează** – dă curs solicitărilor de date și documente obligatorii

GDPR stabilește noi standarde privind transparența, răspunderea și păstrarea evidențelor.
Care sunt termenii cheie din GDPR pe care trebuie să îi cunosc
Articolul 4 din GDPR include o listă de termeni cu definiții, utilizați în cadrul regulamentului. Iată termenii cheie pe care trebuie să îi înțelegi:

• **Operator.** 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.

• **Persoana împuternicită de operator**. Persoana împuternicită de operator înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele unui operator.

• **Date cu caracter personal.** Înseamnă orice informații privind o persoană fizică identificată sau identificabilă, cunoscută și sub denumirea de „persoană vizată”. O persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.

• **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. Printre operațiuni se numără colectarea, înregistrarea, organizarea, structurarea, stocarea și altele.

• **Pseudonimizare.** Înseamnă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat.
Alte intrebari frecvente:
Organizația mea prelucrează anumite date. De unde știu dacă sunt acoperite de GDPR?

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.294, E-mail: oana.velcota@e-uvt.ro

GDPR reglementează colectarea, păstrarea, utilizarea și partajarea „datelor cu caracter personal”. Datele cu caracter personal sunt definite de GDPR, în mare, ca fiind orice date referitoare la o persoană fizică identificată sau identificabilă. Ele pot include informații ca adrese IP, baze de date de vânzări, date aferente serviciilor pentru clienți, formulare de feedback și altele.

Ce înseamnă „confidențialitate din faza de proiectare” și „confidențialitate implicită”?

Conform GDPR, este obligatoriu ca produsele și serviciile tale să încorporeze caracteristici și funcționalități pentru confidențialitate încă din faza de proiectare a acestora. La dezvoltarea caracteristicilor, trebuie să ții cont de factori precum natura prelucrării și riscurile la adresa confidențialității pe care le implică, nevoia de securitate și costurile de implementare. De asemenea, trebuie să implementezi măsuri prin care să garantezi implicit că nu se prelucrează mai multe date decât este necesar.

Ce se întâmplă dacă nu respectăm GDPR?

Amenda maximă pentru încălcări grave va depăși 20 de milioane de euro sau patru procente (in cazul Romaniei s-a stabilit prin decizie guvernamentala ca se limiteaza la 200.000 EURO) din veniturile globale anuale ale unei organizații, aplicându-se suma cea mai mare dintre cele două. În plus, GDPR acordă consumatorilor (și organizațiilor care acționează în numele lor) dreptul de a intenta acțiuni civile în instanță împotriva organizațiilor care încalcă GDPR.

Ce este important la securitatea prevăzută de GDPR?

Conform GDPR, organizația ta are obligația să ia măsuri pentru a păstra în siguranță datele cu caracter personal. Printre măsuri se numără „măsurile organizatorice”, de exemplu, limitarea numărului de persoane din cadrul organizației care au acces la datele cu caracter personal, și „măsurile tehnice”, cum ar fi criptarea.

GDPR nu specifică și nu impune exact măsurile de securitate pe care trebuie să le ia organizațiile. În schimb, acesta cere să stabilești singur ce măsuri de securitate trebuie să iei, ținând cont de factori ca natura datelor cu caracter personal pe care le colectezi, cât de sensibile sunt acestea și riscurile implicate în prelucrare.

Există numeroase riscuri care trebuie luate în considerare. Printre riscurile frecvente se numără intruziunea fizică, angajații rău-intenționați, pierderea accidentală sau atacurile hackerilor. Dezvoltarea unui plan de gestiune a riscurilor și luarea unor măsuri de reducere a riscurilor, cum ar fi protejarea prin parolă, jurnalele de audit și implementarea sistemelor de criptare, te pot ajuta să asiguri conformitatea.

Ce prevede GDPR în caz de încălcare a securității datelor cu caracter personal?

GDPR definește „încălcarea securității datelor cu caracter personal” ca „o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea”.

În cazul unei astfel de încălcări, ai obligația să notifici autoritățile de reglementare în termen de 72 de ore de la luarea la cunoștință. De asemenea, este posibil să fie obligatorie notificarea clienților (sau a „persoanelor vizate”), dacă există un risc semnificativ de vătămare a acestora din cauza încălcării respective.

Organizațiile trebuie să fie „transparente”. Ce înseamnă acest lucru?

Înseamnă că trebuie să explici sincer și clar de ce și în ce fel prelucrezi datele oamenilor. GDPR include informații detaliate despre ceea ce trebuie să le comunici oamenilor cu privire la prelucrarea datelor cu caracter personal; printre altele, informații despre:

- De ce prelucrezi datele cu caracter personal;
- Cât timp vei păstra datele (sau criteriile prin care stabilești cât timp ai nevoie să păstrezi datele);
- Cui vei împărtăși datele cu caracter personal și

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.294, E-mail: oana.velcota@e-uvt.ro

- Dacă datele cu caracter personal vor fi transferate în afara Spațiului Economic European.

Trebuie să prezinți aceste informații într-o manieră clară și accesibilă. De aceea, este o idee bună să treci în revistă cu atenție informațiile publicate de tine, în raport cu cerințele GDPR.

B-dul Vasile Pârvan, Nr. 4, 300223 Timişoara, România
Tel.: +4 0256-592.294, E-mail: oana.velcota@e-uvt.ro