GDPR: cinci ani de provocări și numărătoarea continuă

Autor: Anca Atanasiu, Avocat, Senior Managing Associate, Băncilă, Diaconu şi Asociaţii

Conformitatea cu GDPR implică asumarea de către operatori a unui angajament permanent de a proteja în mod eficient datele cu caracter personal și de a respecta drepturile persoanelor vizate. Acest angajament este însoțit însă de multiple provocări pe care companiile le întâmpină în mod frecvent în activitatea de zi cu zi. Revizuirea constantă a politicilor de prelucrare a datelor, punerea în aplicare a măsurilor de securitate din ce în ce mai stricte și instruirea corespunzătoare a personalului sunt doar câteva dintre activitățile esențiale pe care orice operator de date cu caracter personal trebuie să le aibă în vedere.

În cei cinci ani de la apariția GDPR, s-a putut observa o creștere a gradului de complexitate a mediului economic și social, mai ales în contextul digitalizării și adoptării tehnologiilor avansate, astfel că se impune o atenție sporită în ceea ce privește măsurile și practicile ce trebuie adoptate de către organizații, pentru a evita sancțiunile și riscul reputațional.

Cadrul de reglementare

Una dintre provocările în această materie rezultă din însuși cadrul de reglementare. De la stabilirea bazelor legale pentru prelucrarea datelor, până la implementarea principiilor privacy by design și privacy by default, companiile au nevoie de o înțelegere profundă a legislației. În multe situații, GDPR folosește termeni vagi sau nedefiniți, cum ar fi „întârziere nejustificată”, „risc pentru drepturi și libertăți” și „efort disproporționat”.

În mod similar, GDPR nu oferă nicio definiție a ceea ce constituie un nivel „rezonabil” de protecție a datelor cu caracter personal, oferind autorităților de reglementare o oarecare libertate în evaluarea nivelului de conformitate.

Astfel, se conturează din ce în ce mai mult nevoia de revizuire a cadrului de reglementare actual sau emiterea de îndrumări din partea autorităților de supraveghere pentru mai multă claritate.

Controale interne și monitorizare

În ultimii ani, am putut observa un progres notabil din partea organizațiilor, în special a multinaționalelor care lucrează cu volume mari de date, în aria de monitorizare a activităților de prelucrare și introducere de controale interne și mecanisme de verificare a conformității cu principiile GDPR.

Companiile trebuie să efectueze audituri, evaluări și revizuiri periodice pentru a monitoriza și demonstra conformitatea lor. Totodată, trebuie să fie pregătite să gestioneze solicitările persoanelor vizate, cum ar fi dreptul de acces, rectificare sau ștergere, prin stabilirea unor proceduri interne și fluxuri de soluționare cât mai rapide și eficiente.

Gestionarea unui volum mare de cereri și menținerea unui sistem centralizat pentru a putea urmări și răspunde acestor solicitări reprezintă o provocare suplimentară pentru organizații.

Multe companii și-au format echipe interne sau externe de experți în domeniul protecției datelor care au pus la punct procesele de prelucrare și au ajutat la conștientizarea colectivă privind necesitatea conformării cu regulile GDPR. Echipele interne, prin rolul lor de a monitoriza, actualiza și îmbunătăți în mod constant procesele interne, contribuie semnificativ la o creștere a calității practicilor GDPR în

Romania.

Costuri ridicate de conformitate

Pentru a putea asigura conformitatea și menține un nivel adecvat de monitorizare și control, organizațiile sunt nevoite să ia în considerare și costurile generate de aceste activități și să aloce bugete importante în acest sens.

Companiile trebuie să investească în sisteme performante de management al datelor, să implementeze măsuri tehnice și organizatorice de securitate eficiente împotriva atacurilor cibernetice, să folosească instrumente de monitorizare a duratei de stocare a datelor și mecanisme de ștergere a acestora și, nu în ultimul rând, să asigure instruirea periodică a personalului.

Obținerea consimțământului valabil

O altă provocare are în vedere obținerea din partea persoanelor vizate a consimțământului privind prelucrarea datelor personale în anumite scopuri, într-un mod transparent și complet informat, anterior colectării și prelucrării datelor lor.

Organizațiile trebuie să se asigure că, acolo unde prelucrarea datelor personale are loc pe baza consimțământului persoanelor vizate, acestea l-au exprimat în mod liber, specific, informat și lipsit de ambiguitate.

Astfel, companiile trebuie să instituie mecanisme de colectare și management al consimțământului, asigurându-se că acesta este colectat și exprimat în mod valabil, precum și păstrat și utilizat în baza unor evidențe clare și complete.

GDPR și AI

Inteligența Artificială (AI) prezintă noi provocări pentru respectarea GDPR. Sistemele de AI pot implica procese automate de luare a deciziilor care pot încălca drepturile și

libertățile fundamentale ale persoanei vizate, în cazul în care aceste tehnologii nu sunt utilizate în mod corespunzător.

Conform GDPR, persoanele vizate au dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă. În situațiile de excepție, atunci când luarea acestor decizii este permisă, persoanele vizate au dreptul de a obține intervenție umană, de a-și exprima punctul de vedere și de a contesta decizia.

Acest lucru ridică provocări, deoarece funcționarea unor modele de AI poate fi opacă. Sistemele de AI pot lua decizii pe care chiar și creatorii lor nu le înțeleg complet, încălcând astfel principiul transparenței GDPR. De asemenea, conceptul de minimizare a datelor stabilit de GDPR și nevoia AI pentru volume mari de date sunt aparent contradictorii.

Organizațiile care intenționează să folosească AI vor trebui să găsească un echilibru între utilizarea datelor pentru a instrui sistemele lor de AI și respectarea cerințelor GDPR pentru a proteja drepturile și libertățile fundamentale ale persoanelor vizate.