

GDPR bate la ușă: Cum să ne pregătim pentru noua Lege privind protecția datelor

Parlamentul Republicii Moldova a adoptat recent Legea privind protecția datelor cu caracter personal, publicată în Monitorul Oficial nr. 367-369 art. 574. Aceasta urmează să intre în vigoare la 23 august 2026. Noua lege, aliniată la Regulamentul General privind Protecția Datelor (GDPR) al Uniunii Europene, va aduce schimbări majore în modul în care companiile gestionează datele. În special, legea introduce reglementări mai stricte privind colectarea datelor, obligând companiile să demonstreze în mod activ că respectă aceste prevederi.

Eugen KANSKI



Sergiu BOZIANU,
Director, Data Protection Law Firm

Companiile vor trebui să își asume o responsabilitate mai mare în ceea ce privește modul în care colectează și utilizează datele cu caracter personal, deoarece persoanele fizice vor avea mai multe drepturi de a controla modul în care datele lor sunt prelucrate și pot depune plângeri cu privire la orice potențiale încălcări. Este important de menționat că sancțiunile în conformitate cu noua lege vor crește semnificativ, ajungând până la două milioane de lei sau 2% din cifra de afaceri totală a companiei din anul precedent, oricare dintre acestea este mai mare. În plus, ar putea exista și alte sancțiuni, cum ar fi suspendarea, ștergerea sau distrugerea datelor. Așadar, cu cât compania este mai mare și implică mai multe procese, cu atât responsabilitățile și sancțiunile potențiale vor fi mai mari.

Este esențial ca antreprenorii să înțeleagă că timpul este limitat și orice neglijență în implementarea noilor reglementări va fi taxată dur. Anume pentru a oferi posibilitatea de a implementa noul cadru legal, care este unul deosebit de complex, a și fost acordat acest termen de doi ani până va intra în vigoare. Deci, după doi ani, nu vor mai exista scuze.

Primul pas recomandat pentru companii este angajarea sau contractarea unui responsabil cu protecția datelor (Data Protection Officer, DPO) calificat, care să inițieze neîntârziat conformarea la noile cerințe legale. Acest lucru implică o analiză detaliată a proceselor interne, identifi-

carea eventualelor deficiențe și elaborarea unui plan pentru remedierea acestora. De asemenea, este esențial să se actualizeze politicile de protecție a datelor și să se asigure că toată documentația este la zi. În cele din urmă, companiile trebuie să implementeze măsurile organizatorice și tehnice adecvate pentru a garanta un nivel corespunzător de protecție a datelor.

Principalele provocări cu care companiile se pot confrunta includ diminuarea importanței respectării cerințelor legale, complexitatea noilor reglementări și, cel mai important, reticența de a investi resursele administrative și financiare necesare pentru implementarea noilor cerințe. Pentru a ajuta companiile să se pregătească, Centrul Național pentru Protecția Datelor cu Caracter Personal, precum și alte instituții implicate, vor dezvolta ghiduri și cursuri de instruire. În plus, companiile de consultanță, cele care oferă servicii de DPO externalizat și asociațiile publice specializate vor juca un rol activ în ajustarea cadrului legal și asigurarea implementării sale corecte.

Primul pas recomandat este angajarea sau contractarea unui responsabil cu protecția datelor, care să inițieze neîntârziat conformarea la noile cerințe legale.

Daniela OZEROV,
Șefă departament conformitate,
ASTERRA GRUP



CA „ASTERRA GRUP” SA salută orice act normativ ce vine întru realizarea angajamentelor asumate de Republica Moldova prin Acordul de Asociere RM-UE. Trebuie să percepem această nouă Lege privind protecția datelor cu caracter personal nu doar prin prisma unor angajamente asumate la nivel de țară, ci ca pe un mod de a proteja drepturile cetățenilor. Odată ce noile reglementări vor intra în vigoare, cetățenii moldoveni vor beneficia de un nivel înalt de protecție a datelor cu caracter personal. Legea se va alinia standardelor Uniunii Europene. Chiar și astăzi, în cadrul legislației actuale, CA „ASTERRA GRUP” SA, în calitate de operator al prelucrării datelor cu caracter personal, pune în aplicare, pe lângă prevederile legislative și normative, și un cadru intern propriu pentru protecția datelor.

Orice noi reglementări pun presiune pe business, iar în acest moment, cea mai mare problemă pe care o observăm ține de personalul calificat, fie că este vorba de domeniul asigurărilor, fie că este vorba de calitatea de operator de prelucrare a datelor cu caracter personal. Companiile trebuie să întreprindă un șir de măsuri ce vizează demonstrarea conformității în ceea ce privește identificarea riscului legat de prelucrare, evaluarea acestuia din punctul de vedere al originii, naturii, al probabilității de a se materializa și al gravității. În plus, entitățile trebuie să elaboreze și să pună în aplicare coduri de conduită, care efectiv vor prelua cele mai bune practici în domeniul de referință.

Autoritatea responsabilă pentru monitorizarea aplicării legislației în domeniul protecției datelor cu caracter personal, implicit și a noii Legi nr. 195/2024 – Centrul Național pentru Protecția Datelor cu Caracter Personal, trebuie să vină cu un șir de instruiți și materiale didactice în domeniul de referință. Noi, cei din lumea afacerilor, trebuie nu doar să punem bifa că suntem conformi, că dispunem de coduri de conduită sau că am aderat la reguli corporatiste obligatorii, dar trebuie să ne păstrăm de responsabilitate atunci când aplicăm cerințele ce vizează prelucrarea datelor cu caracter personal.

Sunt ambigue prevederile care presupun că fiecare operator va fi obligat individual să demonstreze existența unor garanții adecvate pentru prelucrarea datelor cu caracter personal. Sperăm că odată cu elaborarea cadrului normativ subsecvent se va oferi răspuns la șirul de întrebări care derivă din noua lege și nu doar de pe poziția de operator, dar de pe poziția de persoană fizică ale cărui date cu caracter personal sunt prelucrate.

Entitățile trebuie să elaboreze și să pună în aplicare coduri de conduită, care efectiv vor prelua cele mai bune practici în domeniul de referință.

Victor BACIU,
Policy Manager, AmCham Moldova



Noua lege impune, în general, cerințe mai stricte privind protecția datelor. Acest lucru va forța companiile să-și adapteze politicile și practicile interne, să investească în soluții tehnice, să implementeze sisteme de gestionare a incidentelor de securitate și să ia măsuri proactive pentru a evita penalități semnificativ mai mari decât cele prevăzute de vechea lege. Cu toate acestea, cadrul legal armonizat în beneficiul unei piețe unice este o noutate binevenită pentru companiile moldovenești care, în unele cazuri, au trebuit să se confrunte cu legislația națională din Republica Moldova și cu cerințe diferite la nivelul UE, fapt care genera sarcini administrative inutile.

Principalele dificultăți cu care se pot confrunta companiile includ lipsa expertizei tehnice, costul implementării, complexitatea soluțiilor de securitate și protecție, amplexarea procesului de conformare, potențialul de interpretare greșită a legii, necesitatea de a angaja specialiști și timpul necesar pentru a face toate ajustările necesare.

Pentru a asigura conformitatea, companiile pot elabora și implementa politici interne adecvate pentru a se conforma cu principiile de protecție a datelor. Acestea mai pot efectua analize interne pentru a aprecia eficacitatea măsurilor tehnice și organizatorice de care dispun pentru a garanta securitatea prelucrării datelor. Totodată, și formarea personalului va fi importantă pentru a asigura aplicarea corectă a măsurilor de protecție a datelor.

Companiile se pot baza pe consultanți și experți în protecția datelor pentru asistență practică în implementarea măsurilor necesare. La o anumită etapă, și asociațiile de business se vor angaja în facilitarea schimbului de experiențe, iar unele pot alege să elaboreze Coduri de conduită privind buna practică de aplicare a legii. Sper, de asemenea, că autoritățile publice vor oferi sprijin, cum ar fi ghiduri de conformitate și seminarii de instruire pentru întreprinderi. În cele din urmă, Comitetul European pentru protecția datelor oferă resurse scrise foarte utile, având îndrumări și bune practici pentru implementarea GDPR, care a și fost transpus prin noua Lege privind protecția datelor cu caracter personal.

Formarea personalului va fi importantă pentru a asigura aplicarea corectă a măsurilor de protecție a datelor.



Eugen COZMULICI,
Manager Politici și Advocacy,
EBA Moldova

Noua legislație, în dezvoltare încă din 2017 cu o contribuție semnificativă din partea EBA Moldova, va aduce standarde mai stricte pentru colectarea, stocarea și prelucrarea datelor. Companiile vor trebui să obțină consimțământul explicit al utilizatorilor, să asigure transparență în modul în care sunt utilizate datele și să protejeze drepturile persoanelor, inclusiv dreptul de a accesa, corecta sau șterge datele proprii. În plus, companiile trebuie să raporteze prompt orice breșe de securitate și ar putea fi obligate să efectueze evaluări ale impactului asupra protecției datelor (DPIA) atunci când lucrează cu date cu risc ridicat. Pentru unele companii, numirea unui DPO va fi, de asemenea, obligatorie.

Printre dificultățile majore cu care companiile s-ar putea confrunta în procesul de adaptare la noua lege se numără costurile ridicate de implementare, în special pentru IMM-uri, care trebuie să investească în soluții tehnologice avansate, precum criptarea și monitorizarea securității IT. Multe companii nu dispun de expertiză internă, ceea ce face ca efectuarea DPIA și raportarea încălcărilor să fie una dificilă. În plus, organizațiile care gestionează volume mari de date personale sau sensibile, cum ar fi companiile telecom, bănci sau furnizorii de servicii medicale, se confruntă cu sarcina impunătoare de a actualiza procedurile interne, de a revizui mecanismele de consimțământ și de a gestiona un val de solicitări de acces la date și de ștergere a acestora.

Pentru a se conforma noilor reguli privind protecția datelor, companiile ar trebui să înceapă prin a efectua un audit detaliat al datelor pe care le dețin, pentru a înțelege ce tipuri de date cu caracter personal ges-

tionează și cum sunt acestea procesate. Ulterior, ar trebui să-și revizuiască politicile de confidențialitate ca să asigure transparența și claritatea pentru utilizatori. Datele nu ar trebui procesate fără un consimțământ explicit din partea utilizatorilor.

De asemenea, este esențial să existe proceduri clare pentru gestionarea eventualelor breșe de securitate, iar personalul calificat ar trebui să supravegheze respectarea reglementărilor. Prin luarea acestor măsuri, companiile pot asigura o tranziție lină către conformitate și pot evita potențialele repercusiuni legale.

Companiile ar trebui să înceapă prin a efectua un audit detaliat al datelor pe care le dețin.

