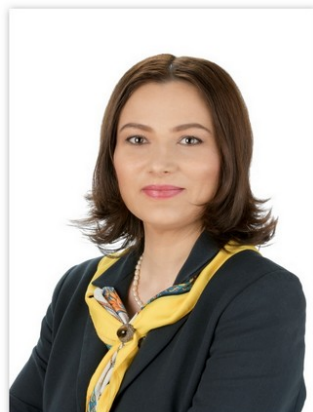


GDPR – A trecut un an. Dar viitorul este înainte!



Cel puțin teoretic, Regulamentul General pentru Protecția Datelor (GDPR sau „Regulamentul”) a reprezentat *Anul2k* în domeniul protecției datelor, nu numai în Europa, ci și la nivel mondial. Desigur, organizațiile din întreaga lume s-au grabit să se conformeze acestuia, temându-se de consecințe foarte oneroase în caz de neconformitate. Dar GDPR este adesea vag redactat și nu oferă soluții unice sau suficient de clare, astfel încât respectarea pune în multe cazuri semne de întrebare. Deci, un an mai târziu, unde ne aflăm? S-au mai limpezit lucrurile astfel încât să avem acum o anumită claritate?

2018 – Intrarea în vigoare a GDPR și adaptarea legislației naționale

La scurt timp după intrarea în vigoare a GDPR, legislația națională a primit noi reglementări pentru adaptarea GDPR la contextul local. Astfel, Legea nr. 190/2018 a adus câteva cerințe speciale pentru prelucrarea anumitor categorii de date cu caracter personal, precum și câteva derogări de la prelucrarea datelor cu caracter personal în anumite situații (de exemplu, în scopuri jurnalistice). Autoritatea Română pentru Protecția Datelor s-a dovedit și ea activă emițând legislație secundară care reglementează situații în care evaluările de impact privind protecția datelor sunt obligatorii sau procedura de primire și soluționare a plângerilor sau de efectuare a investigațiilor de către autoritate.

Încalcare GDPR constatate și primele sancțiuni aferente

Au apărut și primele sancțiuni emise de autoritățile de protecție a datelor din întreaga UE pentru încălcări ale GDPR. Iată câteva exemple:

- Compania Facebook a fost amendată cu 500.000 GBP pentru colectarea datelor cu caracter personal despre prietenii de pe Facebook ai utilizatorilor, fără ca acești prieteni să fie informați că datele lor au fost colectate și fără să li se ceară acordul.
- Autoritatea pentru protecția datelor din Polonia (UODO) a aplicat prima amendă în baza GDPR unui broker de date pentru nerespectarea obligației de informare prevăzută la art. 14 alin (1) și (2) din Regulament. Amendă aplicată este în cuantum de 220.000 Euro.
- Compania Uber a fost amendată cu 385.000 GBP pentru aranjamentele de securitate necorespunzătoare care au dat posibilitatea ca hackerii să descarce o cantitate mare de date cu caracter personal despre șoferi și clienți.

Unele sancțiuni se încadrează în limitele permise de legislația privind protecția datelor înainte de GDPR și ați putea crede ca nu s-au schimbat multe în această privință. Cu toate acestea, CNIL (Autoritatea Franceza de Protecție a Datelor) a aplicat împotriva Google o amendă de 50 de milioane EUR, o valoare semnificativ mai mare decât cele prevăzute în legislația anterioară. CNIL a declarat ca prelucrările Google în ceea ce privește personalizarea reclamelor sale nu erau transparente, conțineau informații inadecvate și nu aveau consimțământul valabil acordat.

Ce urmează?

Ce este, deci, la orizont în ceea ce privește GDPR? Trebuie să ne așteptăm ca, în domeniul protecției datelor și comunicațiilor electronice, să înceapă să se aplice reglementări suplimentare, inclusiv Regulamentul privind confidențialitatea în mediul electronic *E-Privacy*. Vom vedea o intensificare a aplicării GDPR și un impact crescut al acestuia în activitățile obișnuite, inclusiv aplicarea unor amenzi și a altor sancțiuni semnificative. De asemenea, ne putem aștepta ca Brexit-ul să aibă impact asupra obligațiilor de protecția datelor pentru anumite companii. Alte preocupări viitoare includ pe cele legate de inteligența artificială (AI) și responsabilitatea roboților.

Ne așteptăm, prin urmare, ca activitatea legată de conformarea la GDPR să crească mai degrabă decât să scadă în acest al doilea an. Adeverata protecție a confidențialității și respectarea totală a GDPR și a regulamentului *E-Privacy* vor necesita mai mult efort și mai multe investiții decât s-ar fi putut anticipa anterior.

Ce puteți face dacă nu v-ați conformat la GDPR în cursul anului 2018? Sau dacă nu sunteți sigur că ați implementat corect GDPR?

Iată o listă de conformitate (non-exhaustivă) pe care orice companie ar trebui să o verifice:

Conștientizarea la nivelul companiei. Stabilirea unui cadru de responsabilitate și guvernanta corporativă	Informați-vă angajații asupra aplicării GDPR și oferiți-le training asupra elementelor esențiale ale noii reglementari. Conformarea la GDPR presupune efectiv la nivelul board-ului companiei dar este, în egală măsură, un efort de angajați. Faceți recomandări board-ului privind riscurile și oportunitățile GDPR. Încluderți proiectul GDPR. Încorporați riscul de protecție a datelor în cadrul managementului corporativ și al controlului intern.
Efectuarea unui inventar de date și a unui flux de date	Efectuați o investigație internă pentru a cartografia activitățile operaționale și prelucrări de date personale, determinați care sunt acele date, care sunt odată date și dacă le transferați în afara companiei. Pregătiți registrul activității. Evaluați temeiul juridic al prelucrărilor de date din companie.
Efectuarea unei analize detaliate a decalajelor (gap analysis)	Întocmiți o analiză de tip audit al situației actuale de conformitate cu cerințele GDPR și lista pașilor de urmat pentru conformare. Asigurați o atenție deosebită în ceea ce privește munca.
Elaborarea politicilor, procedurilor și proceselor operaționale	Pregătiți documente-suport ale acestor politici pentru a putea asigura implementarea lor stabilite.
Asigurarea securității datelor personale prin măsuri procedurale și tehnice	Puneți în aplicare "măsuri tehnice și organizatorice adecvate" conform principiilor de care o adoptați. Aveți permanent în vedere principiile Privacy by design.
Conformarea mijloacelor de comunicații electronice la GDPR;	Verificați și conformați la GDPR mijloacele de comunicații electronice utilizate de companie (de ex: email, internet, CCTV, aplicații de tip GPS).

Conformarea site-ului companiei la GDPR

Site-ul este cartea de vizita a companiei dvs. dar și un mod important de a interacționa cu potențialii clienți sau simpli vizitatori. Asigurați-va ca interacțiunea cu a site-ului dvs. să fie în conformanță cu GDPR.

Monitorizarea continua și verificarea conformității la GDPR.

Instituiți reguli corporative de monitorizare permanenta a nivelului de conformanță la GDPR. Trebuie să includa cel puțin audituri interne periodice, actualizarea procesurilor interne, a procedurilor personale, a registrelor interne de prelucrari, instruirea periodica a angajaților și a securitate IT.

Pentru companiile care au depus eforturi interne pentru a se conforma la GDPR, este recomandată utilizarea unui consultant extern GDPR pentru a verifica nivelul de conformanță și a remedia eventualele lipsuri.