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 sa se conformeze acestuia, temându-se de consecințe foarte oneroase în caz de neconformitate. Dar GDPR este adesea vag redactat și nu ofera soluții unice sau suficient de clare, astfel încât respectarea pune în multe cazuri semne de întrebare. Deci, un an mai târziu, unde ne aflam? S-au mai limpezit lucrurile astfel încât sa avem acum o anumita claritate?

2018 – Intrarea în efectivitate a GDPR și adaptarea legislației naționale

La scurt timp dupa intrarea în vigoare a GDPR, legislația națională a primit noi reglementari 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 derogari 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 activa emițând legislație secundara care reglementeaza situații în care evaluarile de impact privind protecția datelor sunt obligatorii sau procedura de primire și soluționare a plângerilor sau de efectuare a investigațiilor de catre autoritate.

Încalcari GDPR constatate și primele sancțiuni aferente

Au aparut si primele sancțiuni emise de autoritațile de protecție a datelor din întreaga UE pentru încalcari ale GDPR. Iata câteva exemple:

→ Compania Facebook a fost amendata cu 500.000 GBP pentru colectarea datelor cu caracter personal despre prietenii de pe Facebook ai utilizatorilor, fara ca acești prieteni sa fie informați ca datele lor au fost colectate și fara sa li se ceara acordul.
→ Autoritatea pentru protecția datelor din Polonia (UODO) a aplicat prima amenda în baza GDPR unui broker de date pentru nerespectarea obligației de informare prevazuta la art. 14 alin (1) și (2) din Regulament. Amenda aplicata este în cuantum de 220.000 Euro.
→ Compania Uber a fost amendata cu 385.000 GBP pentru aranjamentele de securitate necorespunzatoare care au dat posibilitatea ca hackerii sa descarce o cantitate mare de date cu caracter personal despre șoferi și clienți.

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

Ce urmeaza?

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

Ne așteptam, prin urmare, ca activitatea legata de conformarea la GDPR sa creasca mai degraba decât sa scada în acest al doilea an. Adevarata protecție a confidențialitații și respectarea totala 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 daca nu v-ați conformat la GDPR în cursul anului 2018? Sau daca nu sunteți sigur ca ați implementat corect GDPR?

Iata o lista de conformitate (non-exhaustiva) pe care orice companie ar trebui sa o verifice:

Conștientizarea la nivelul companiei. Stabilirea unui cadru de responsabilitate și guvernanța corporativa	Informați-va angajații asupra aplicarii GDPR și oferiți-le training asupra elementelor esențiale ale noii reglementari. Conformarea la GDPR presu efectiv la nivelul board-ului companiei dar este, in egala masura, un efor Faceți recomandari board-ului privind riscurile și oportunitațile GDPR. I proiect GDPR. Încorporați riscul de protecție a datelor în cadrul manage corporative și al controlului intern.
Efectuarea unui inventar de date și a unui flux de date	Efectuați o investigație interna pentru a cartografia activitațile operațional prelucrari de date personale, determinați care sunt acele date, care sunt c datelor și daca le transferați în afara companiei. Pregatiți registrul activit Evaluați temeiul juridic al prelucrarilor de date din companie.
Efectuarea unei analize detaliate a decalajelor (gap analysis)	Întocmiți o analiza de tip audit al situației actuale de conformitate cu cer lista pașilor de urmat pentru conformare. Asigurați o atenție deosebita in de munca.
Elaborarea politicilor, procedurilor și proceselor operaționale	Pregatiți documente-suport ale acestor politici pentru a putea asigura imp stabilite.
Asigurarea securitații datelor personale prin masuri procedurale și tehnice	Puneți în aplicare "masuri tehnice și organizatorice adecvate" conform p care o adoptați. Aveți permanent în vedere principiile Privacy by design
Conformarea mijloacelor de comunicații electronice la GDP;	Verificați și conformați la GDPR mijloacele de comunicații electronice u 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 potențialii clienți sau simpli vizitatori. Asigurați-va ca interacțiunea cu a GDPR.
Monitorizarea continua și verificarea conformității la GDPR.	Instituiți reguli corporative de monitorizare permanenta a nivelului de co trebui sa includa cel puțin audituri interne periodice, actualizarea proces personale, a registrelor interne de prelucrari, instruirea periodica a angaj de securitate IT. Pentru companiile care au depus eforturi interne pentru a se conforma G recomandata utilizarea unui consultant extern GDPR pentru a verifica ni și a remedia eventualele lipsuri.