Neconformarea costă scump! Cum să protejezi finanțele companiei de cheltuieli cu amenzi pentru nerespectarea regulilor GDPR?

Autor: Alex Milcev, Liderul departamentului de Asistenţă fiscală şi juridică, EY România

O simplă căutare pe Google după *General Data Protection Regulation* (GDPR) arată, în mai puțin de 50 de secunde, aproape 700 de milioane de rezultate (a se citi „pagini”), ceea ce este un bun indiciu nu doar despre complexitatea subiectului, ci și despre gradul de interes al jucătorilor din piață, fie companii, fie persoane fizice. Pentru că este vorba, pe de o parte, de protejarea datelor și a informațiilor din și despre companie, într-o piață puternic concurențială, iar, pe de altă parte, despre siguranța datelor personale, oferite și utilizate în diferite circumstanțe.

Lucrurile dobândesc o și mai mare anvergură când vine vorba despre fluxurile financiare ale companiilor – intrări și ieșiri de active – bănești, digitale și materiale, bazate pe contracte comerciale. Totul înseamnă **date**, iar tot ceea ce înseamnă **date** în timpurile actuale și, mai ales **big data** presupune obligatoriu măsuri de siguranță, confidențialitate, protecție.

Am putea aprecia, fără nicio exagerare, că, din punct de vedere financiar, implementarea normelor GDPR scutește compania de potențiale neplăceri de pe urma nerespectării acestora, fie din neștiință, fie din rea-voință. Iar înainte de amenzi și penalizări, sunt procesele costisitoare în

instanță, pe care le pot deschide terți (persoane fizice sau juridice) pentru a-și apăra integritatea datelor folosite abuziv sau fără acordul lor precis exprimat.

Regulile generale de protecție a datelor au fost adoptate și, ca urmare, impuse în Uniunea Europeană, în anul 2016. Potrivit programului gradual de implementare, România a trebuit să se conformeze regulamentului european începând cu anul 2018.

Vorbim despre o istorie scurtă, chiar la nivelul UE, dar plină de evenimente neplăcute, care s-au concretizat în amenzi absolut amețitoare, inclusiv în România. Și, pentru că cei mai la îndemână pentru autorități – în cazul României vorbim despre Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) – de a fi subiectul unui control sunt întotdeauna marii jucători, amenzile au mers către companii importante din piață, inclusiv către bănci. Mai mult, într-un clasament anual al țărilor în care s-au aplicat amenzi pentru încălcarea Regulamentului, România figura, în anul 2021, pe locul trei, după Italia și Ungaria.

Este foarte posibil ca mediul economic local, mai ales companiile românești mici și mijlocii, să nu fi luat încă foarte în serios ideea că adoptarea unei politici interne coerente de aplicare și conformare pe regulile europene GDPR este absolut obligatorie și depășește cadrul strict al unei cheltuieli prevăzute în bugetul companiei, fie cu o soluție GDPR, fie cu un angajat care să fie format și să se ocupe exclusiv de acest aspect în cadrul companiei (*data protection officer* – DPO).

Exemplele amenzilor pentru nerespectarea regulilor de protecție a datelor – fie că este vorba despre date interne (financiare sau ale angajaților) sau externe (ale clienților/partenerilor/acționarilor) – ar trebui să dea de gândit oricărui coordonator de business, fiind de preferat o investiție în *pachetul* de protejare a datelor prelucrate de companie, în locul unei penalizări drastice pentru

neconformare.

Implementarea prevederilor GDPR este, de fapt, o investiţie care poate să ducă la creșterea profitabilității, astfel cum reiese dintr-un studiu al companiei CISCO dat publicității: peste 40% din organizațiile intervievate au beneficii de cel puțin două ori mai mari, decât cheltuielile lor realizate cu implementarea conformităţii GDPR.

Cel puțin la fel de important ca însăși adoptarea uneia sau alteia dintre cele două variante rămâne premisa de la care orice top manager sau owner al unei companii trebuie să pornească: oricine, oricând poate face obiectul unui control al autorității. Cu alte cuvinte, să nu se bazeze nimeni pe ideea că autoritatea NU va ajunge să controleze respectarea normelor GDPR.

Tocmai de aceea, sunt de avut în vedere trei mari aspecte din această perspectivă: **analiza cost *versus* beneficii a implementării și respectării regulilor GDPR în companie; analiza consecințelor pe termen lung a nerespectării regulamentului GDPR, din punct de vedere al notorietății, imaginii și al relațiilor de business în domeniul de activitate al companiei; poziționarea ca lider și impunerea conduitei de conformare în respectarea regulilor GDPR în sectorul de activitate al fiecăruia.**

La primul punct, este vorba despre decizia de a implementa regulile, a le monitoriza și a face update-urile de conformitate pe parcursul anului, astfel încât la evaluarea anuală să existe cât mai puține puncte de neconformare. Dacă, într-un anumit interval, stabilit de echipa de control, compania nu rezolvă aspectele constatate ca fiind în neregulă, urmează sancțiunile.

Vorbim aici despre creșterea eficienței activității, a vânzărilor și a veniturilor companiei – ceea înseamnă amortizarea cheltuielilor cu implementarea unei formule de

GDPR, indiferent care ar fi aceasta: externalizată ori printr-un DPO intern.

Prin urmare, atenție la: monitorizarea periodică și actualizarea proceselor de business din companie, astfel încât să respecte normele GDPR, concomitent cu monitorizarea noutăților în standardele GDPR, tocmai pentru ca fluxurile interne de lucru și relația cu terții să fie conforme cu acestea.

Nu mai puțin importantă este educarea personalului prin traininguri în domeniul protecţiei datelor, astfel încât echipa să înţeleagă și să aplice întocmai regulile în acest domeniu, pentru a evita incidente nedorite, care duc la amenzi și penalizări.

_____

Notă: Conform datelor din sondajul companiei CISCO, în perioada 2018 – 2021, în Uniunea Europeană amenzile aplicate pentru nerespectarea regulilor GDPR, au crescut constant, de la 436.000 euro, pentru anul 2018, la 72 milioane euro pentru anul 2019, 171 milioane euro pentru anul 2020, după care anul trecut s-a ajuns la 1 miliard euro, record absolut.