Ce au de facut bancile pentru a proteja datele personale ale clienților și a se conforma regulamentului GDPR

Confidențialitatea și securitatea datelor personale devin elemente primordiale în relația bancilor cu potențiali clienți. Ce reguli trebuie sa respecte acestea pentru a evita expunerea datelor clienților, dar și sancțiunile care le pot afecta reputația ?

Doua dintre cele mai importante instituții financiare din România, aflate în topul celor mai mari 10 banci dupa active, au fost amendate recent, de catre Autoritatea Națională de Supraveghere a Prelucrarii Datelor cu Caracter Personal (ANSPDCP), pentru nerespectarea normelor de protecție a datelor personale. Nu atât sumele ca atare sunt importante, modice comparativ cu veniturile sau activele bancilor, cât mai ales motivele care au generat aceste amenzi. Ce a stat la baza deciziei autorității, în fiecare dintre cele doua cazuri și la ce trebuie sa fie atenți chiar clienții în relația cu instituțiile financiare, tocmai pentru a se asigura de o dubla protecție a datelor pe care le ofera spre prelucrare?

Autoritatea Națională de Supraveghere a Prelucrarii Datelor a invocat multipe încalcari are prevederilor Regulamentului 679/2016 - G.D.P.R., în esența fiind vorba despre faptul ca au fost prelucrate date ale clienților, în scopul creditarii, fara consimțamântul acestora sau chiar fara sa fi solicitat un credit, fiind încalcate astfel normele privind prelucrarea datelor cu caracter personal. Pentru neregulile constatate, prima banca sancționata a primit doua avertismente și trei amenzi.

În cazul celei de-a doua banci, a fost vorba, potrivit precizarilor autorității, despre faptul ca aceasta nu a implementat masuri tehnice și organizatorice adecvate în vederea asigurarii unui nivel de securitate corespunzator riscului prezentat de prelucrare, generat în special, în mod accidental sau ilegal, de divulgarea neautorizata și accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod. Ceea ce, pe cale de consecința, a condus la divulgarea neautorizata și accesul neautorizat la datele cu caracter personal ale acelor clienți.

Detaliul important aici este acela ca instituțiile financiare au obligația de a obține consimțamântul clientului pentru a putea efectua operațiunile premergatoare creditarii. Entitațile financiar-bancare, pe lânga respectarea prevederilor privind protecția datelor din regulamentul menționat mai sus, trebuie sa țina cont de asemenea de normele de reglementare specifice industriei, cum ar fi secretul profesional reglementat de prevederile O. U. G. nr. 99/2006, regulamentele Bancii Naționale a României (BNR), precum și de cadrul legal privind cunoașterea clientelei și evitarea potențialelor tentative de spalare a banilor murdari.

Toate aceste acte normative reglementeaza în mod specific activitaţile desfaşurate de catre instituţiile financiar-bancare, completând cadrul general creat de regulamentul GDPR.

Plecând de la sancţiunile aplicate de ANSPDCP celor doua banci, se evidenţiaza trei tipuri de acţiuni ce pot ajuta instituţiile financiar-bancare în a se asigura ca programul de conformitate ramâne la un nivel adecvat.

În primul rând, este vorba despre instruirea periodica a angajaţilor, astfel încât aceştia sa înţeleaga perfect care sunt regulile de prelucrare a datelor, ce anume trebuie sa respecte pentru fiecare operaţiune de prelucrare de date în parte pe care o fac şi, de asemenea, care sunt limitele prelucrarii acestor date.

În al doilea rând, devine absolut obligatorie reevaluarea periodica a fluxurilor de date din companie şi actualizarea planului de masuri de mitigare (reducere a riscurilor), precum şi a planului de conformare, în acord cu inadvertenţele evidenţiate în urma procesului de reevaluare.

În al treilea rând, apare necesitatea evaluarii şi a analizei în detaliu a fluxurilor de date cu risc ridicat pentru drepturile fundamentale al persoanelor fizice, cum ar fi dreptul la libera exprimare, ale caror date sunt prelucrate. De exemplu, odata prelucrata cartea de identitatea a unei persoane, se pot face discriminari privind vârsta acelei persoane, sexul, vârsta sau zona unde s-a nascut. Entitaţile financiare au de respectat foarte multe reglementari bancare şi naţionale, şi europene.

Într-adevar, entitaţile financiar-bancare, instituţiile financiare non bancare, precum şi companiile de tip fintech au de respectat o multitudine de reguli si in ceea ce priveste cunoasterea clientelei si potentialele tentative de spalare a banilor murdari, iar aceste actiuni de verificare presupun prelucrarea unui volum mare de date cu caracter personal, dar si prelucrarea unor categorii de date speciale, cum ar fi cele privind apartenenţa politica.

Fintech-urile – adica noile entitaţi financiare, de tip aplicaţii de servicii financiare online - înca nu au legislaţie aplicabila specific, ci se conformeaza (sau nu) anumitor reguli mai degraba în funcţie de tipul de activitate pe care îl desfaşoara. Cu alte cuvinte, depinde de gradul în care s-au aliniat şi cum anume, pe ce linii de business, legislaţiei aplicabile instituţiilor financiar-bancare cum ar fi emiterea de moneda electronica, plaţi electronice, alte servicii de tip neobanking şi administrare de active digitale. Pentru toate aceste operaţiuni, fintech-urile trebuie sa obţina licenţe şi autorizari, care vin la pachet cu necesitatea conformarii regulamentelor în vigoare de pastrare a confidenţialitaţii şi securitaţii datelor prelucrate ale clienţilor.

La fel de importanta ramâne zona de cybersecurity în sectorul financiar-bancar, fie el clasic, fie de tip nou. Din perspectiva securitaţii cibernetice, instituţiile financiare trebuie sa se asigure ca masurile tehnice de securizare a datelor pe care le-a implementat respecta întru totul prevederile articolului 32 din Regulamentul GDPR. Reamintim aici ca cea mai mare a amenzilor aplicate în acest an de catre ANSPDCP au fost pentru lipsa unor masuri tehnice şi organizatorice, la nivel de companie, suficient de acoperitoare, care sa asigure şi protecţie cibernetica.

Pe de alta parte, instituţiile financiar-bancare, de asigurari ori de intermediere a serviciilor din zona financiara şi de creditare, trebuie sa ţina cont şi de reglementarile din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice (directiva NIS), precum şi obligaţiile de comunicare a anumitor incidente de securitate catre Directoratul Naţional de Securitate Cibernetica (DNSC), prin responsabilul NIS.

În final, dar nu mai puţin important aspect, este acela al necesitaţii ca, la nivelul unor asemenea instituţii, cum sunt cele bancare, pentru faptul ca acestea lucreaza cu un volum imens de date personale, atât ale clienţilor existenţi, cât mai ales cu ale celor care intenţioneaza sa devina clienţi, este obligatoriu constituirea unei echipe dedicate conformitaţii în domeniul protectiei datelor condusa de Responsabilul cu protectia Datelor (D.P.O).

În ultimii trei ani, ANSPDCP a aplicat amenzi de peste 400 milioane euro în domeniul financiar-bancar, punctând astfel importanța pe care toate companiile ce prelucreaza date trebuie sa o acorde programului de conformare cu prevederile GDPR.