Creșterea bunastarii în domeniul Fintech prin securitate și reziliența cibernetica

Pe masura ce sectorul financiar devine din ce în ce mai digitalizat, Uniunea Europeana introduce cadre de reglementare solide pentru a proteja reziliența operațională și securitatea cibernetica în cadrul sectorului. Introducerea Regulamentului UE nr. 2022/2554 privind reziliența operațională digitala („DORA") și a Directivei UE nr. 2022/2555 privind masuri pentru un nivel comun ridicat de securitate cibernetica în Uniune („Directiva NIS 2") în cadrul de reglementare al Uniunii Europene reprezinta un pas decisiv catre consolidarea sistemului de aparare al sectorului financiar împotriva amenințarilor digitale și de securitate cibernetica. Aceste reglementari, care vizeaza consolidarea securității cibernetice și a rezilienței operaționale, au implicații profunde care depașesc sfera conformității, influențând în mod direct stabilitatea și succesul organizațiilor fintech.

1. Intrarea în vigoare

DORA a intrat în vigoare la data de 17 ianuarie 2025, aplicându-se direct la nivelul UE, fara a fi necesara transpunerea în legislațiile naționale. Aceasta aplicabilitate uniforma asigura o punere în aplicare consecventa în toate statele membre. În schimb, Directiva NIS2 a intrat în vigoare la 16 ianuarie 2023 și a necesitat transpunerea în legislația naționala de catre statele membre, ceea ce a condus la unele variații în aplicarea sa. În România, legea de transpunere a intrat în vigoare la 31 decembrie 2024.

2. Domeniul de aplicare al DORA și NIS 2

O diferența esențiala între cele doua acte legislative ale UE consta în domeniul lor de aplicare. Pe de o parte, Directiva NIS 2 se aplica unui **spectru larg de sectoare**, inclusiv sectorul bancar, energia, asistența medicala, transporturile și infrastructura digitala. Aceasta vizeaza atât entitațile esențiale, deosebit de importante pentru stabilitatea unor funcții cheie în cadrul societații, cât și entitațile importante care opereaza în domenii semnificative din punct de vedere economic. Obiectivul Directivei NIS 2 este de a spori securitatea cibernetica în diverse sectoare, afectând zeci de mii de întreprinderi.

DORA, în schimb, **vizeaza exclusiv sectorul financiar**, concentrându-se pe asigurarea rezilienței operaționale digitale a entitaților financiare și a **furnizorilor lor terți de servicii IT&C**. În ceea ce privește entitațile financiare care intra în domeniul de aplicare al DORA, aceasta categorie include atât instituțiile de credit tradiționale, cât și anumite societați fintech, cum ar fi instituțiile de plata, prestatorii de servicii de informare cu privire la conturi, instituțiile emitente de moneda electronica, prestatorii de servicii de criptoactive sau platformele de crowdfunding.

Faptul ca furnizorii terți, inclusiv companiile de servicii cloud și de gazduire, care lucreaza cu instituțiile financiare

sunt, de asemenea, incluși în DORA, reflecta abordarea cuprinzatoare a acestui regulament în ceea ce privește întarirea securitații cibernetice a ecosistemului financiar. Cu toate acestea, trebuie menționat faptul ca furnizorii terți neesențiali sunt supuși unei supravegheri indirecte, în principal printr-un conținut minim obligatoriu al acordurilor pe care le încheie cu entitațile financiare (incluzând clauze privind dreptul de audit al entitații financiare, raportarea incidentelor și clauze privind continuitatea operaționala în cazul unor întreruperi), în timp ce furnizorii terți esențiali sunt supravegheați direct. Aceștia din urma vor fi identificați și supravegheați la nivelul UE pe baza criteriilor de importanța strategica pentru funcționarea sistemului financiar. Dupa desemnarea ca furnizori esențiali, aceștia vor avea obligația de a se conforma cerințelor stricte, precum implementarea de masuri avansate de securitate, raportarea incidentelor în timp real și participarea la evaluari periodice de rezilienta cibernetica. Mai mult, aceștia vor trebui sa înființeze o filiala în UE în termen de 12 luni de la desemnarea ca atare.

Pe de alta parte, instituțiile financiare nebancare, care reprezinta o categorie raspândita de fintech-uri în România, nu intra însa în domeniul de aplicare al DORA.

3. Ce se întâmpla daca o entitate intra atât în domeniul de aplicare al DORA, cât și al Directivei NIS 2?

Atunci când o entitate intra atât sub incidența DORA, cât și a Directivei NIS 2, este important sa înțeleaga cum sa navigheze printre cerințele care se suprapun pentru a asigura conformitatea deplina cu cadrul legislativ în domeniu.

În considerentele DORA, se prevede ca DORA este considerat un regulament cu caracter de lege speciala pentru entitațile din sectorul financiar, ceea ce înseamna ca are întâietate asupra regulamentelor generale precum Directiva NIS2 în domeniile în care dispozițiile acestora se suprapun. Acest principiu garanteaza faptul ca entitațile financiare adera în primul rând la cerințele specifice ale DORA adaptate sectorului lor, ținând seama, de asemenea, de dispozițiile generale ale Directivei NIS 2, în special în domeniile care nu sunt acoperite în mod explicit de DORA.

4. Implicații asupra sectorului Fintech

4.1. Implicații operaționale

Atât DORA, cât și NIS 2 sunt concepute pentru a se asigura ca societațile fintech care intra sub incidența DORA, printre alte tipuri de instituții care intra sub incidența lor, pot rezista și se pot recupera în urma incidentelor cibernetice. Pentru societațile fintech, acest lucru înseamna, din perspectiva operaționala:

•€€€€€€€€ **atenuarea riscurilor**, având în vedere ca DORA impune entitaților financiare sa dispuna de un cadru solid de guvernanța IT&C, de politici și proceduri de gestionare continua a riscurilor și de testare avansata prin teste de penetrare bazate pe amenințari (TLPT), ambele ajutând societațile fintech sa anticipeze și sa neutralizeze amenințarile, reducând timpii morți și asigurând funcționarea neîntrerupta a serviciilor lor.

•€€€€€€€€ **raportarea sistematica a incidentelor și raspunsul sistematic la astfel de incidente**: Atât DORA, cât și Directiva NIS 2 pun accentul pe raportarea și raspunsul la incidente pentru a se asigura ca fintech-urile sunt pregatite sa gestioneze rapid evenimentele de securitate cibernetica, minimizând potențialele daune.

În cazul DORA, în **cazul unui incident major legat de IT&C**, entitațile financiare trebuie sa raporteze incidentul respectiv autoritații competente relevante. Procesul de raportare presupune transmiterea unei notificari inițiale (**cât mai curând posibil în primele 4 ore** de la clasificarea incidentului ca fiind major, dar nu mai târziu de 24 de ore de la descoperirea acestuia), urmata de rapoarte intermediare pe masura ce situația evolueaza și de un raport final dupa finalizarea unei analize a cauzelor principale. Aceste rapoarte ar trebui sa furnizeze suficiente informații

pentru ca autoritatile sa poata evalua importanța incidentului și orice impact transfrontalier potențial. În plus, entitațile financiare pot notifica în mod voluntar autoritațile cu privire la amenințarile cibernetice semnificative considerate relevante pentru sistemul financiar sau pentru clienții lor. În cazul în care un incident afecteaza interesele financiare ale clienților, entitațile sunt obligate sa îi informeze cu promptitudine cu privire la incident și la orice masuri luate pentru a atenua efectele negative.

În mod similar, Directiva NIS 2 impune organizațiilor din sectoarele critice sa raporteze **incidentele semnificative de securitate cibernetica** autoritaților naționale sau echipelor de raspuns la incidentele de securitate informatica (CSIRT) fara întârzieri nejustificate și cel târziu în termen de 24 de ore de la detectare. În cazul entitaților care intra sub incidența ambelor reglementari, incidentele vor fi raportate conform cerințelor DORA catre autoritatea competenta (de exemplu, în România, Banca Națională a României în cazul entitaților care sunt supravegheate de aceasta), care se va asigura apoi ca incidentul este raportat catre autoritatea competenta în temeiul Directivei NIS 2 (de exemplu, în România, Directoratul Național de Securitate Cibernetica).

În plus, daca incidentul IT&C sau de securitate cibernetica implica și o încalcare a securitații datelor cu caracter personal, notificarea în temeiul Regulamentului GDPR ramâne aplicabila.

4.2. Implicații financiare

În ceea ce privește costurile și alte aspecte financiare, conformitatea cu aceste reglementari necesita investiții inițiale în infrastructura de securitate cibernetica și în personal. Cu toate acestea, aceste costuri sunt compensate de **reducerea riscurilor cibernetice**, deoarece masurile solide de securitate cibernetica reduc șansele unor viitoare încalcari ale securitații datelor și atacuri.

În plus, conformarea timpurie poate fi benefica din punct de vedere financiar prin **evitarea amenzilor, printre alte sancțiuni** asociate nerespectarii DORA și a Directivei NIS 2.

4.3. Impactul reputațional asupra clienților și investitorilor

Aderarea la DORA și la Directiva NIS 2 demonstreaza un angajament ferm fața de securitate și reziliența, ceea ce este esențial pentru **consolidarea încrederii clienților**. Clienții și partenerii de afaceri sunt mai predispuși sa aiba încredere în societațile fintech care implementeaza masuri solide de securitate cibernetica. În plus, o societate fintech sigura din punct de vedere cibernetic și conforma **atrage investitori** care percep riscuri mai mici în investițiile lor.

4.4. Implicații organizaționale și în legatura cuangajații

Eforturile inițiale de conformare pot crește volumul de munca, în special pentru **rolurile IT, juridice și cele de conformitate** sau chiar pot necesita angajarea de personal suplimentar în scopul asigurarii conformitații cu DORA. Cu toate acestea, în același timp, conformitatea favorizeaza dezvoltarea competențelor, încurajând învațarea continua pe masura ce angajații ramân la curent cu evoluția practicilor și tehnologiilor de securitate cibernetica.

4.5. Implicații la nivelul ecosistemului

Atât DORA, cât și Directiva NIS 2 încurajeaza societațile fintech sa participe la eforturile mai ample ale industriei de a spori securitatea cibernetica.

De exemplu, ambele acte legislative includ dispoziții privind **schimbul de informații** între entitațile care intra sub incidența lor. Acestea pot partaja în mod voluntar informații privind securitatea cibernetica, cum ar fi amenințarile,

vulnerabilitățile și strategiile de raspuns, pentru a consolida securitatea cibernetica colectiva. Acest schimb vizeaza prevenirea sau atenuarea incidentelor cibernetice și sporirea gradului de conștientizare și a capacităților defensive. Cu toate acestea, acest schimb de informații trebuie sa aiba loc în cadrul comunităților de încredere și trebuie sa se bazeze, de asemenea, pe acorduri de schimb de informații care sa asigure conformitatea cu cerințele de reglementare privind secretele comerciale, concurența și protecția datelor.

În plus, atât DORA, cât și NIS 2 includ dispoziții care încurajeaza cooperarea cu autoritățile competente, în scopul creșterii rezilienței generale a ecosistemului digital.

În concluzie, punerea în aplicare a DORA și a Directivei NIS 2 ofera societăților fintech care intra sub incidența acestora o oportunitate unica de a-și consolida reziliența operațională și securitatea cibernetica. Prin aderarea la aceste cadre, fintech-urile pot minimiza riscurile, își pot proteja sanatatea financiara și își pot construi o reputație de organizații sigure și de încredere. În cele din urma, aceste reglementari servesc drept catalizator pentru inovare și îmbunatățire continua, permițând societăților fintech sa prospere într-o lume digitala tot mai complexa și interconectata.