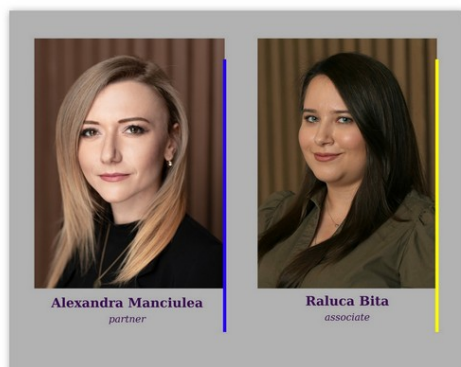


Creșterea bunăstării în domeniul Fintech prin securitate și reziliența cibernetică



Pe măsura ce sectorul financiar devine din ce în ce mai digitalizat, Uniunea Europeană introduce cadre de reglementare solide pentru a proteja reziliența operațională și securitatea cibernetică în cadrul sectorului. Introducerea Regulamentului UE nr. 2022/2554 privind reziliența operațională digitală („DORA”) și a Directivei UE nr. 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune („Directiva NIS 2”) în cadrul de reglementare al Uniunii Europene reprezintă un pas decisiv către consolidarea sistemului de apărare al sectorului financiar împotriva amenințărilor digitale și de securitate cibernetică. Aceste reglementări, care vizează consolidarea securității cibernetică și a rezilienței operaționale, au implicații profunde care depășesc 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, fără a fi necesară transpunerea în legislațiile naționale. Această aplicabilitate uniformă asigură o punere în aplicare consecventă în toate statele membre. În schimb, Directiva NIS2 a intrat în vigoare la 16 ianuarie 2023 și a necesitat transpunerea în legislația națională de către 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 diferență esențială între cele două acte legislative ale UE constă în domeniul lor de aplicare. Pe de o parte, Directiva NIS 2 se aplică unui **spectru larg de sectoare**, inclusiv sectorul bancar, energia, asistența medicală, transporturile și infrastructura digitală. Aceasta vizează atât entitățile esențiale, deosebit de importante pentru stabilitatea unor funcții cheie în cadrul societății, cât și entitățile importante care operează în domenii semnificative din punct de vedere economic. Obiectivul Directivei NIS 2 este de a spori securitatea cibernetică în diverse sectoare, afectând zeci de mii de întreprinderi.

DORA, în schimb, **vizează exclusiv sectorul financiar**, concentrându-se pe asigurarea rezilienței operaționale digitale a entităților financiare și a **furnizorilor lor terți de servicii IT&C**. În ceea ce privește entitățile financiare care intra în domeniul de aplicare al DORA, această categorie include atât instituțiile de credit tradiționale, cât și anumite societăți fintech, cum ar fi instituțiile de plată, prestatorii de servicii de informare cu privire la conturi, instituțiile emitente de monedă electronică, prestatorii de servicii de criptoactive sau platformele de crowdfunding.

Faptul că furnizorii terți, inclusiv companiile de servicii cloud și de gazduire, care lucrează cu instituțiile financiare

sunt, de asemenea, incluși în DORA, reflecta abordarea cuprinzătoare a acestui regulament în ceea ce privește întărirea securității 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 entitățile financiare (incluzând clauze privind dreptul de audit al entităților financiare, raportarea incidentelor și clauze privind continuitatea operațională 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 importanță strategică pentru funcționarea sistemului financiar. După desemnarea ca furnizori esențiali, aceștia vor avea obligația de a se conforma cerințelor stricte, precum implementarea de măsuri avansate de securitate, raportarea incidentelor în timp real și participarea la evaluări periodice de reziliență cibernetică. Mai mult, aceștia vor trebui să înființeze o filială în UE în termen de 12 luni de la desemnarea ca atare.

Pe de alta parte, instituțiile financiare nebankare, care reprezintă o categorie răspândită de fintech-uri în România, nu intra însă în domeniul de aplicare al DORA.

3. Ce se întâmplă dacă 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 să înțeleagă cum să navigheze printre cerințele care se suprapun pentru a asigura conformitatea deplină cu cadrul legislativ în domeniu.

În considerentele DORA, se prevede ca DORA este considerat un regulament cu caracter de lege specială pentru entitățile din sectorul financiar, ceea ce înseamnă că are întâietate asupra regulamentelor generale precum Directiva NIS2 în domeniile în care dispozițiile acestora se suprapun. Acest principiu garantează faptul că entitățile 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 că societățile 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 societățile fintech, acest lucru înseamnă, din perspectiva operațională:

- **atenuarea riscurilor**, având în vedere că DORA impune entităților financiare să dispună de un cadru solid de guvernanta IT&C, de politici și proceduri de gestionare continuă a riscurilor și de testare avansată prin teste de penetrare bazate pe amenințări (TLPT), ambele ajutând societățile fintech să anticipeze și să neutralizeze amenințările, reducând timpii morți și asigurând funcționarea neîntreruptă a serviciilor lor.

- **raportarea sistematică a incidentelor și răspunsul sistematic la astfel de incidente**: Atât DORA, cât și Directiva NIS 2 pun accentul pe raportarea și răspunsul la incidente pentru a se asigura că fintech-urile sunt pregătite să gestioneze rapid evenimentele de securitate cibernetică, minimizând potențialele daune.

În cazul DORA, în **cazul unui incident major legat de IT&C**, entitățile financiare trebuie să raporteze incidentul respectiv autorității competente relevante. Procesul de raportare presupune transmiterea unei notificări 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), urmată de rapoarte intermediare pe măsura ce situația evoluează și de un raport final după finalizarea unei analize a cauzelor principale. Aceste rapoarte ar trebui să furnizeze suficiente informații

pentru ca autoritațile sa poata evalua importanța incidentului și orice impact transfrontalier potențial. În plus, entitațile financiare pot notifica în mod voluntar autoritațile cu privire la amenințările cibernetice semnificative considerate relevante pentru sistemul financiar sau pentru clienții lor. În cazul în care un incident afectează 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 Naționala 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 încălcare a securității 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 încălcari ale securității datelor și atacuri.

În plus, conformarea timpurie poate fi benefica din punct de vedere financiar prin **evitarea amenzilor, printre alte sancțiuni** asociate nerespectării 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 față de securitate și reziliența, ceea ce este esențial pentru **consolidarea încrederii clienților**. Clienții și partenerii de afaceri sunt mai predispuși sa aiba încredere în societățile 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 cu angajații*

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 asigurării conformității cu DORA. Cu toate acestea, în același timp, conformitatea favorizeaza dezvoltarea competențelor, încurajând învățarea 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 societățile 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 amenințările,

vulnerabilitățile și strategiile de răspuns, pentru a consolida securitatea cibernetică colectivă. Acest schimb vizează prevenirea sau atenuarea incidentelor cibernetică și sporirea gradului de conștientizare și a capacităților defensive. Cu toate acestea, acest schimb de informații trebuie să aibă loc în cadrul comunităților de încredere și trebuie să se bazeze, de asemenea, pe acorduri de schimb de informații care să asigure conformitatea cu cerințele de reglementare privind secretele comerciale, concurența și protecția datelor.

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

În concluzie, punerea în aplicare a DORA și a Directivei NIS 2 oferă societăților fintech care intra sub incidența acestora o oportunitate unică de a-și consolida reziliența operațională și securitatea cibernetică. Prin aderarea la aceste cadre, fintech-urile pot minimiza riscurile, își pot proteja sănătatea financiară și își pot construi o reputație de organizații sigure și de încredere. În cele din urmă, aceste reglementări servesc drept catalizator pentru inovare și îmbunătățire continuă, permițând societăților fintech să prospere într-o lume digitală tot mai complexă și interconectată.