

Securitate cibernetică: România transpune Directiva NIS2. Ce urmează?



Directiva (UE) 2022/2555 (NIS2) are scopul de a întări reziliența cibernetică a Uniunii Europene, solicitând entităților din diverse sectoare să își consolideze măsurile de securitate cibernetică. NIS2 înlocuiește fosta Directiva NIS1 (UE) 2016/1148, extinde gama de entități reglementate și introduce cerințe mai stricte pentru acestea.

Pe 31 decembrie 2024, Guvernul României a adoptat Ordonanța de Urgență nr. 155/2024 (OUG 155/2024) pentru transpunerea NIS2 în legislația națională.

Cine este vizat?

NIS2 și OUG 155/2024 se aplică entităților din diverse sectoare economice, împărțindu-le în entități esențiale și entități importante. Entitățile din următoarele domenii trebuie să verifice dacă aceste reglementări li se aplică:

□ Entități esențiale: energie (electricitate, încălzire centralizată, petrol, gaze, hidrogen); transport (aerian, feroviar, naval, rutier); bancar; infrastructuri ale pieței financiare; sănătate; apă potabilă; apă uzată; administrație publică și spațiu. Infrastructura digitală și serviciile de gestionare a TIC au obligații și mai stricte.

□ Entități importante: servicii poștale și de curierat; gestionarea deșeurilor; fabricarea, producția și distribuția de produse chimice; producția, procesarea și distribuția alimentelor; fabricarea de dispozitive medicale; produse informatice, electronice și optice; echipamente electrice; mașini și echipamente; autovehicule, remorci și semiremorci, alte echipamente de transport; furnizori digitali de piețe online, motoare de căutare și rețele sociale.

Chiar dacă există praguri de dimensiune (NIS2 și OUG 155/2024 se aplică în principal întreprinderilor mijlocii și mari), o entitate mai mică poate fi totuși supusă acestor reguli dacă are un rol critic într-un sector specific. De asemenea, unele obligații se extind și la furnizorii acestor entități, întrucât NIS2 vizează și creșterea nivelului de securitate cibernetică în lanțurile de aprovizionare.

Ce trebuie făcut?

Dacă o entitate constată că intră sub incidența NIS2 și OUG 155/2024, aceasta trebuie să respecte toate obligațiile prevăzute pentru categoria sa. Printre măsurile impuse de OUG 155/2024 se numără:

- Implementarea unor masuri tehnice, operaționale și organizatorice adecvate și proporționale pentru gestionarea riscurilor de securitate și reducerea impactului incidentelor asupra sistemelor informatice, respectând cerințele specifice fiecarui sector.
- Înregistrarea la Directoratul Național de Securitate Cibernetică (DNSC), autoritatea responsabilă cu aplicarea prevederilor OUG 155/2024.
- Efectuarea de audituri periodice și comunicarea rezultatelor acestora către DNSC.
- Instruirea conducerii în domeniul securității cibernetice și asigurarea faptului că persoana responsabilă cu deciziile privind securitatea cibernetică este independentă de șeful operațional IT.
- Raportarea incidentelor cibernetice autorităților în termen de 6-24 ore, iar, în funcție de caz, informarea persoanelor afectate sau a partenerilor contractuali.

Sanctiuni

OUG 155/2024 stabilește un regim sever de sancțiuni pentru fiecare încălcare a obligațiilor impuse:

→ Firmele esențiale: amenzi de până la 10 milioane EUR sau 2% din cifra de afaceri globală anuală (se aplică valoarea mai mare).

→ Firmele importante: amenzi de până la 7 milioane EUR sau 1,4% din cifra de afaceri globală anuală (se aplică valoarea mai mare).

În plus, NIS2 și OUG 155/2024 introduc răspunderea personală a membrilor conducerii pentru nerespectarea obligațiilor.

Ce urmeaza?

OUG 155/2024 a stabilit un termen-limită pentru înregistrarea la DNSC care a expirat pe 30 ianuarie 2025. Totuși, în prezent, DNSC nu a emis încă normele de aplicare necesare pentru efectuarea înregistrării.

Conform unui comunicat de presă de pe site-ul DNSC, înregistrările se vor efectua pe baza normelor de aplicare pe care DNSC s-a angajat să le publice în primul trimestru al anului 2025. După publicarea acestora, entitățile vizate vor trebui să se înregistreze conform cerințelor și termenelor stabilite.

Neîndeplinirea obligațiilor de securitate cibernetică poate atrage nu doar amenzi pentru companie și conducere, ci și cereri de despăgubire din partea partenerilor contractuali, dacă aceștia suferă pierderi din cauza unui incident ce putea fi prevenit prin măsuri corespunzătoare.

Entitățile vizate ar trebui să ia măsuri cât mai curând posibil pentru a respecta aceste cerințe legale.