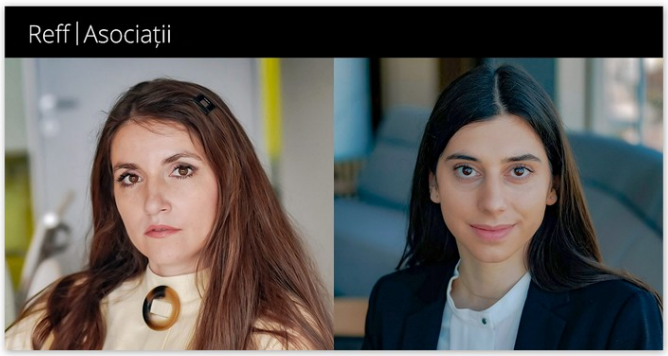
Directiva NIS 2: criterii pentru evaluarea conformitații companiilor și obligațiile legale din urmatoarea perioada



La data de 31 decembrie 2024, a intrat în vigoare Ordonanța de Urgența nr. 155/2024 (OUG 155/2024), care stabilește cadrul legislativ pentru securitatea cibernetica a rețelelor și sistemelor informatice din România. Actul normativ transpune Directiva (UE) 2022/2555, cunoscuta sub numele de Directiva NIS (*Network and Information Security Directive*) 2, și impune cerințe de conformitate pentru entitațile care opereaza în sectoare considerate critice sau importante pentru funcționarea societații și economiei. Autoritatea competenta pentru aplicarea și monitorizarea prevederilor ordonanței este Directoratul Național de Securitate Cibernetica (DNSC).

Trei criterii pentru evaluarea conformitații unei companii cu OUG 155/2024

Primul pas pe care trebuie sa îl aiba în vedere companiile în vederea asigurarii conformarii cu cerințele OUG 155/2024 este sa efectueze o analiza preliminara pentru a vedea în ce masura cadrul legislativ în materia securitații cibernetice le este aplicabil. Pentru a stabili daca intra sub incidența ordonanței, fiecare entitate trebuie sa efectueze o analiza interna bazata pe trei criterii.

Aplicabilitatea ordonanței se stabilește, în primul rând, prin **identificarea sectorului de activitate**, lucru realizat prin verificarea codurilor CAEN autorizate conform Registrului Comerțului și care trebuie sa corespunda celor listate în anexele 1 și 2 ale OUG 155/2024. Doar activitațile autorizate la Registrul Comerțului pot genera obligații de înregistrare. În lipsa unor coduri CAEN relevante sau autorizate, entitatea nu este supusa cerințelor ordonanței.

De asemenea, este important de determinat **dimensiunea companiei**. Aceasta este stabilita conform Legii nr. 346/2004 privind stimularea înființarii și dezvoltarii întreprinderilor mici și mijlocii, în funcție de o serie de aspecte, precum numarul mediu de angajați, cifra de afaceri sau totalul activelor principale ale societații. Aceasta clasificare presupune un demers de analiza complex și esențial pentru diferențierea între entitațile esențiale și cele importante, în scopul aplicarii proporționale a obligațiilor relevante din perspectiva prevederilor OUG 155/2024.

Al treilea criteriu de luat în considerare este **profilul entității**. O companie poate fi considerata importanta sau esențiala chiar și în lipsa îndeplinirii primelor doua criterii, daca are un impact sistemic sau strategic asupra sanatații publice, economiei, siguranței cetațenilor sau securitații naționale. Acest criteriu este reglementat în articolele 9 și 10 din OUG 155/2024.

Recent, pe 30 aprilie, DNSC a publicat în transparența decizionala un nou proiect de ordin pentru aprobarea

criteriilor şi pragurilor de determinare a gradului de perturbare a unui serviciu şi a metodologiei de evaluare a nivelului de risc al entităţilor. Proiectul referitor la evaluarea nivelului de risc detaliaza criteriile şi pragurile de determinare a gradului de perturbare a unui serviciu, precum şi modalitatea prin care entităţile îşi calculeaza scorul în acest sens, pornind de la valorile de baza aferente sectorului din care fac parte, prevazute în cadrul uneia dintre anexele proiectului de ordin, precum şi în conformitate cu dimensiunea acestora.

În fiecare vineri, la sediul DNSC sunt organizate consultari publice dedicate implementarii OUG 155/2024, la care pot participa reprezentanţi ai entităţilor vizate, consultanţi şi alţi actori relevanţi pentru sectorul securităţii cibernetice. Aceste sesiuni de lucru reprezinta o oportunitate importanta de a adresa întrebari directe şi de a contribui la modelarea detaliilor procedurale.

Care sunt obligaţiile şi termenele pe care companiile trebuie sa le aiba în vedere?

Companiile care se încadreaza în prevederile OUG 155/2024 trebuie sa ţina cont de anumite aspecte, precum înregistrarea în Registrul Entităţilor esenţiale gestionat de DNSC, desemnarea unei persoane de contact pentru gestionarea relaţiei cu autoritatea, implementarea unor masuri tehnice şi organizaţionale pentru protejarea sistemelor informatice şi notificarea incidentele de securitate în termenul prevazut de lege.

Termenul de înregistrare în registru este de **30 de zile de la data intrarii în vigoare a OUG 155/2024** sau de la momentul la care condiţiile devin aplicabile pentru o entitate. Totuşi, cerinţele legislative vor deveni aplicabile doar la momentul la care vor exista instrumentele tehnice puse la dispoziţie de catre DNSC şi care vor operaţionaliza Registrul Entităţilor şi procedura de notificare. DNSC a emis un proiect de ordin la finalul lunii aprilie, care are ca obiect procedura de notificare şi modul de transmitere a informaţiilor în Registrul Entităţilor, astfel încât obligaţia va deveni aplicabila pentru companii începând cu publicarea acestuia în Monitorul Oficial.

Instrumente de suport

Conform proiectului de ordin referitor la procedura de notificare emis de DNSC, autoritatea ofera sprijin prin platforma NIS2@RO atât pentru autoevaluare şi informare, cât şi pentru depunerea documentelor de înregistrare şi notificare. Aceasta platforma este înca în faza de **dezvoltare tehnica**, nefiind operaţionala pentru moment.

O alta opţiune pentru realizarea unei analize la nivelul organizaţiei în vederea verificarii încadrarii în categoria de entitaţi din domeniul de aplicare a OUG 155/2024 pot fi şi instrumentele de autoevaluare.

Aşteptarile pentru perioada urmatoare

Dupa publicarea celor doua proiecte de ordin ale DNSC în Monitorul Oficial, entităţile vizate de OUG 155/2024 vor avea la dispoziţie toate clarificarile necesare legate de documentaţia ce va trebui depusa la autoritatea competenta, platforma de transmitere a notificarilor şi etapele de verificare procedurala.

În contextul actual, este esenţial ca entităţile vizate sa acorde o atenţie sporita în ceea ce priveşte intrarea sau nu sub sfera de aplicare a OUG 155/2024 şi, ulterior publicarii proiectelor de ordin în Monitorul Oficial, **sa se concentreze pe înregistrarea în Registrul Entităţilor.**