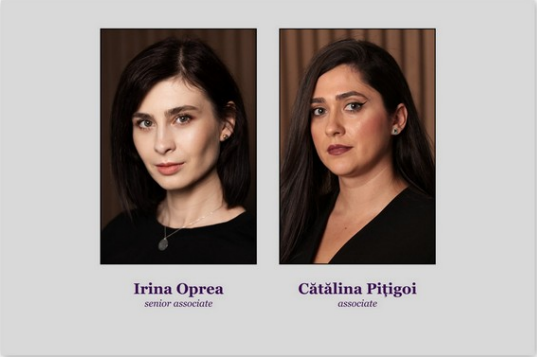
NIS 2 în România. Cum îți pregatești compania pentru noua era a securitații cibernetice



Sfârșitul anului 2024 a adus in prim-plan un nou cadru legislativ în domeniul securitații cibernetice, Romania adoptând Ordonanța de Urgența nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetica a rețelelor și sistemelor informatice din spațiul cibernetic național civil (OUG 155/2024) pentru transpunerea Directivei NIS 2. Aceasta reglementare vine sa întareasca masurile de securitate aplicabile rețelelor și sistemelor informatice în contextul creșterii amenințarilor cibernetice. Companiile care opereaza în sectoare considerate critice sau importante trebuie sa se pregateasca pentru un set complex de obligații menite sa asigure un nivel crescut de reziliența cibernetica.

Principalele schimbari introduse de OUG 155/2024

Transpunerea Directivei NIS 2 în legislația națională extinde semnificativ sfera de aplicare, vizând doua categorii de entitați: entitațile esențiale și entitațile importante. Entitațile esențiale sunt cele care activeaza în sectoare critice, precum energie, transport, sanatate sau infrastructuri digitale, având un impact semnificativ asupra societații și economiei. În schimb, entitațile importante sunt cele care, deși nu se încadreaza în criteriile stricte pentru a fi considerate esențiale, desfașoara activitați în sectoare relevante și pot avea o influența majora asupra continuitații economice.

Companiile trebuie sa efectueze o autoevaluare riguroasa pentru a determina daca intra sub incidența noii reglementari. Daca rezultatul acestei evaluari indica faptul ca se încadreaza în definițiile stabilite de lege, acestea au obligația sa se înregistreze la Directoratul Național pentru Securitate Cibernetica (DNSC) în termen de 30 de zile de la intrarea în vigoare a OUG sau de la data la care prevederile acesteia le sunt aplicabile.

Pentru a standardiza procesul de notificare, DNSC a emis un proiect de ordin care reglementeaza cerințele privind procesul de înregistrare și metodele de transmitere a informațiilor. Ordinul prevede utilizarea a doua instrumente digitale esențiale: Platforma ATHENA și Instrumentul NIS2@RO. Acestea faciliteaza procesul de evaluare și notificare, oferind o structura standardizata pentru completarea și transmiterea formularului de notificare.

Platforma ATHENA permite înregistrarea online, gestionarea notificarilor şi facilitarea comunicarii cu DNSC, iar în caz de indisponibilitate a platformei, entitaţile pot utiliza local Instrumentul NIS2@RO. Formularul de notificare include secţiuni clare cu privire la identitatea entitaţii, dimensiunea şi serviciile furnizate, persoana responsabila de securitate cibernetica şi datele referitoare la reţelele informatice. Formularul trebuie semnat electronic şi transmis catre DNSC, iar în cazul în care se identifica neconcordanţe, DNSC poate solicita informaţii suplimentare.

Este de remarcat ca proiectul de ordin accentueaza importanţa autoevaluarii şi a documentarii adecvate a masurilor de securitate, impunând obligativitatea transmiterii documentelor justificative care atesta respectarea cerinţelor legale. Aflat în prezent în stadiul de proiect, documentul este deschis consultarii publice, nefiind înca adoptat.

În ceea ce privește obligațiile esențiale impuse de OUG 155/2024, acestea includ implementarea unor masuri tehnice și organizatorice adaptate pentru gestionarea riscurilor de securitate cibernetica. Aceste masuri trebuie sa asigure trasabilitatea activitaților în cadrul sistemelor informatice, sa prevada politici clare de evaluare a riscurilor, precum și adoptarea de soluții pentru protecția lanțului de aprovizionare și utilizarea metodelor avansate de autentificare. Mai mult, entitațile trebuie sa se supuna auditului periodic de securitate cibernetica, cu frecvența și condițiile stabilite prin ordin emis de DNSC, iar în cazuri excepționale, pot fi solicitate de catre DNSC și audituri ad-hoc.

Un aspect de neratat este legat de raportarea incidentelor de securitate cibernetica. Companiile sunt obligate sa transmita o avertizare timpurie în termen de 24 de ore de la identificarea unui incident semnificativ, urmata de un raport detaliat în termen de 72 de ore si un raport final, în termen de cel mult o luna de la transmiterea notificarii incidentului. În funcție de complexitatea incidentului, pot fi solicitate și rapoarte intermediare. Raportarile se vor face exclusiv prin intermediul Platformei Naționale pentru Raportarea Incidentelor de Securitate Cibernetica (PNRISC).

În ceea ce privește sancțiunile, regimul introdus de OUG 155/2024 este strict, amenzile putând ajunge pâna la 10 milioane EUR sau 2% din cifra de afaceri neta pentru entitațile esențiale și pâna la 7 milioane EUR sau 1,4% din cifra de afaceri neta pentru cele importante. În plus, în cazul entitaților esențiale, este prevazuta ca masura suplimentara posibilitatea DNSC de a solicita autoritaților competente sa suspende temporar certificarea sau autorizarea acordata entitații respective pentru anumite servicii sau activitați relevante sau sa impuna o interdicție temporara de a ocupa funcții de conducere.

Pentru a detalia cerințele procedurale și tehnice, DNSC va publica un ordin care stabilește metodologia pentru efectuarea auditului de securitate cibernetica și evaluarea nivelului de maturitate. Ordinul va trebui sa stabileasca criterii clare pentru determinarea periodicitații auditului, în funcție de dimensiunea, sectorul și istoricul incidentelor înregistrate de fiecare entitate. De asemenea, este necesar sa fie prevazute reguli detaliate privind conținutul rapoartelor de audit, inclusiv cerințe privind descrierea sistemelor auditate, identificarea

vulnerabilitaților și recomandarile de remediere. Ordinul va trebui sa adreseze și aspectele privind colaborarea între entitați și DNSC, în vederea stabilirii unui schimb eficient de informații pentru prevenirea și gestionarea incidentelor cibernetice.

Legatura dintre NIS2 si GDPR

Noul cadru legislativ are implicații directe și asupra protecției datelor cu caracter personal, reglementata de GDPR. În primul rând, incidentele de securitate cibernetica care implica date personale trebuie raportate și catre Autoritatea Națională de Supraveghere a Prelucrarii Datelor cu Caracter Personal (ANSPDCP), în termen de 72 de ore. În plus, implementarea masurilor de securitate trebuie sa respecte principiul "*privacy by design*", iar în cazul prelucrarii datelor sensibile sau a introducerii unor noi sisteme informatice, companiile au obligația de a efectua evaluari de impact în conformitate cu articolul 35 din GDPR. Astfel, integrarea cerințelor NIS 2 în cadrul politicilor de conformitate GDPR este esențiala pentru evitarea riscurilor legale și reputaționale.

Concluzii

Conformarea cu noua reglementare reprezinta un demers important pentru întarirea rezilienței cibernetice și protecția datelor. Deși cerințele impuse sunt complexe, acestea constituie o oportunitate pentru companii de a-și consolida structurile de securitate și a evita riscurile financiare și reputaționale. Integrarea cerințelor de audit, gestionarea atenta a incidentelor si colaborarea strânsa cu DNSC sunt pași ce trebuie avuți în vedere pentru asigurarea conformității.