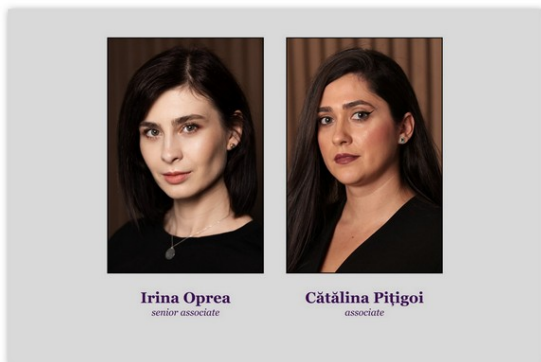


NIS 2 în România. Cum îți pregatești compania pentru noua era a securității cibernetice



Sfârșitul anului 2024 a adus în prim-plan un nou cadru legislativ în domeniul securității cibernetice, România adoptând Ordonanța de Urgență nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil (OUG 155/2024) pentru transpunerea Directivei NIS 2. Aceasta reglementare vine să întărească măsurile de securitate aplicabile rețelelor și sistemelor informatice în contextul creșterii amenințărilor cibernetice. Companiile care operează în sectoare considerate critice sau importante trebuie să se pregătească pentru un set complex de obligații menite să asigure un nivel crescut de reziliență cibernetică.

Principalele schimbări introduse de OUG 155/2024

Transpunerea Directivei NIS 2 în legislația națională extinde semnificativ sfera de aplicare, vizând două categorii de entități: entitățile esențiale și entitățile importante. Entitățile esențiale sunt cele care activează în sectoare critice, precum energie, transport, sănătate sau infrastructuri digitale, având un impact semnificativ asupra societății și economiei. În schimb, entitățile importante sunt cele care, deși nu se încadrează în criteriile stricte pentru a fi considerate esențiale, desfășoară activități în sectoare relevante și pot avea o influență majoră asupra continuității economice.

Companiile trebuie să efectueze o autoevaluare riguroasă pentru a determina dacă intra sub incidența noii reglementări. Dacă rezultatul acestei evaluări indică faptul că se încadrează în definițiile stabilite de lege, acestea au obligația să se înregistreze la Directoratul Național pentru Securitate Cibernetică (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 reglementează cerințele privind procesul de înregistrare și metodele de transmitere a informațiilor. Ordinul prevede utilizarea a două instrumente digitale esențiale: Platforma ATHENA și Instrumentul NIS2@RO. Acestea facilitează procesul de evaluare și notificare, oferind o structură standardizată pentru completarea și transmiterea formularului de notificare.

Platforma ATHENA permite înregistrarea online, gestionarea notificărilor și facilitarea comunicării cu DNSC, iar în caz de indisponibilitate a platformei, entitățile pot utiliza local Instrumentul NIS2@RO. Formularul de notificare include secțiuni clare cu privire la identitatea entității, dimensiunea și serviciile furnizate, persoana responsabilă de securitate cibernetică și datele referitoare la rețelele informatice. Formularul trebuie semnat electronic și transmis către DNSC, iar în cazul în care se identifică neconcordanțe, DNSC poate solicita informații suplimentare.

Este de remarcat ca proiectul de ordin accentuează importanța autoevaluării și a documentării adecvate a măsurilor de securitate, impunând obligativitatea transmiterii documentelor justificative care atestă respectarea cerințelor legale. Aflat în prezent în stadiul de proiect, documentul este deschis consultării publice, nefiind încă adoptat.

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

Un aspect de neratat este legat de raportarea incidentelor de securitate cibernetică. Companiile sunt obligate să transmită o avertizare timpurie în termen de 24 de ore de la identificarea unui incident semnificativ, urmată de un raport detaliat în termen de 72 de ore și un raport final, în termen de cel mult o lună de la transmiterea notificării incidentului. În funcție de complexitatea incidentului, pot fi solicitate și rapoarte intermediare. Raportările se vor face exclusiv prin intermediul Platformei Naționale pentru Raportarea Incidentelor de Securitate Cibernetică (PNRISC).

În ceea ce privește sancțiunile, regimul introdus de OUG 155/2024 este strict, amenzile putând ajunge până la 10 milioane EUR sau 2% din cifra de afaceri netă pentru entitățile esențiale și până la 7 milioane EUR sau 1,4% din cifra de afaceri netă pentru cele importante. În plus, în cazul entităților esențiale, este prevăzută ca măsură suplimentară posibilitatea DNSC de a solicita autorităților competente să suspende temporar certificarea sau autorizarea acordată entității respective pentru anumite servicii sau activități relevante sau să impună o interdicție temporară 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 cibernetică și evaluarea nivelului de maturitate. Ordinul va trebui să stabilească criterii clare pentru determinarea periodicității auditului, în funcție de dimensiunea, sectorul și istoricul incidentelor înregistrate de fiecare entitate. De asemenea, este necesar să fie prevăzute reguli detaliate privind conținutul rapoartelor de audit, inclusiv cerințe privind descrierea sistemelor auditate, identificarea

vulnerabilităților și recomandările de remediere. Ordinul va trebui să adreseze și aspectele privind colaborarea între entități și DNSC, în vederea stabilirii unui schimb eficient de informații pentru prevenirea și gestionarea incidentelor cibernetice.

Legătura dintre NIS2 și GDPR

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

Concluzii

Conformarea cu noua reglementare reprezintă un demers important pentru întărirea 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 atentă a incidentelor și colaborarea strânsă cu DNSC sunt pași ce trebuie avuți în vedere pentru asigurarea conformității.