



DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Nr. 9176 / DRP
DATA 31-07-2026

1440 a

SG. 3688/06.08

Către Secretariatul General al Guvernului
Departamentul pentru Relația cu Parlamentul
În atenția Domnului Nini SĂPUNARU, Secretar de stat
Referitor la Adresa nr. 8885/2026 din 23.07.2026 referitoare la întrebarea doamnei senator Niculina STELEA

21.07

Nr. D1391 din 30 iulie 2026

NECLASIFICAT

Ex. nr. 1/2

Stimate domnule Secretar de stat,

Urmare a solicitării dumneavoastră nr. 8885/2026 din 23.07.2026 privind formularea unui răspuns la întrebarea doamnei senator Niculina STELEA, cu obiectul *"Respectarea prevederilor OUG nr. 155/2024 privind securitatea cibernetică (transpunerea Directivei NIS2) în contextul incidentelor cibernetice care au afectat infrastructuri digitale esențiale ale statului"* înregistrată la DNSC cu nr. D1367 din 23.07.2026, vă rugăm să primiți următoarele:

Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, aprobată cu modificări și completări prin Legea nr. 124/2025, cu modificările și completările ulterioare, prevede o serie de obligații în sarcina entităților esențiale și importante. În acest sens, o entitate trebuie să fie încadrată drept entitate esențială sau entitate importantă conform prevederilor legii ante-menționate, adică trebuie să dobândească o anumită calitate juridică, astfel încât prevederile legii să îi fie aplicabile.

Amintim în acest sens dispozițiile art. 18 alin. (2) din același act normativ: *"Entitățile care desfășoară activitate în sectoarele din anexa nr. 1 sau anexa nr. 2 notifică DNSC în vederea înregistrării în cel mult 30 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență sau în termen de cel mult 30 de zile de la data la care prevederile prezentei ordonanțe de urgență le sunt aplicabile, atunci când, conform art. 5 și 6, se încadrează ca entități esențiale sau entități importante."*

Astfel, cu privire la identificarea și încadrarea entităților în discuție drept entități esențiale (având în vedere apartenența lor la *sectorul 10. Administrație publică*) și înregistrarea lor în Registrul entităților, vă comunicăm faptul că acestea, la data producerii incidentelor referite de dumneavoastră, nu se notificaseră în vederea înregistrării la Directorat. În acest context, prevederile din Ordonanța de urgență a Guvernului nr. 155/2024 referitoare la obligațiile ce revin entităților esențiale nu erau exigibile.

Având în vedere cele de mai sus, precizăm faptul că Directoratul nu poate desfășura toate activitățile de supraveghere, verificare și/sau control conform prevederilor Ordonanței de urgență a Guvernului nr. 155/2024 asupra unor entități care nu au dobândit calitatea de entitate esențială sau entitate importantă deoarece acestea nu fac obiectul legii.

De asemenea, precizăm faptul că, având în vedere că aplicarea legii ține de dobândirea unei anumite calități prin procesul de înregistrare la Directorat, proces ce presupune o amplă analiză a situației de fapt și de drept a entității notificate, iar nu numai un simplu act de luare la cunoștință a acestei calități în urma notificării de către entitate, celelalte obligații nu pot fi îndeplinite anterior de către entitățile neînregistrate. Amintim aici o serie de obligații relevante, ulterioare înregistrării entității, care determină chiar aplicarea nivelului de măsuri de gestionare a riscurilor de securitate cibernetică corespunzător

nivelului de risc al entității: evaluarea nivelului de risc a entității, autoevaluare a nivelului de maturitate a măsurilor de gestionare a riscurilor de securitate cibernetică, plan de măsuri pentru remedierea deficiențelor identificate urmare a realizării autoevaluării ș.a..

Cu privire la raportarea incidentului de la nivelul Agenției Naționale de Cadastru și Publicitate Imobiliară (ANCPPI), precum și incidentului de la nivelul Ministerului Investițiilor și Proiectelor Europene (MIPE), vă comunicăm faptul că Directoratul a fost notificat atât de către ANCPPI cu privire la un incident de securitate cibernetică ce afecta serviciile agenției, cât și de către MIPE cu privire la un incident de securitate cibernetică ce afecta una dintre platformele administrate de acesta, amândouă prin intermediul Platformei naționale pentru raportarea incidentelor de securitate cibernetică (PNRISC). Echipa DNSC s-a aflat în contact permanent cu aceștia și le-a acordat sprijin de specialitate pentru gestionarea incidentului și limitarea impactului asupra serviciilor. Cu toate acestea, având în vedere că au fost puse în mișcare acțiuni penale în vederea tragerii la răspundere a persoanelor care au săvârșit faptele, nu pot fi furnizate informații suplimentare celor comunicate deja public.

În legătură cu îndeplinirea atribuțiilor care îi revin, precum și pentru asigurarea respectării dispozițiilor Ordonanței de urgență a Guvernului nr. 155/2024 de către entități, DNSC poate aplica fie avertisment, fie amendă. De asemenea, DNSC poate dispune, după caz: a) adoptarea unor măsuri atunci când acestea sunt necesare pentru a preveni sau remedia un incident, precum și termene- limită pentru punerea în aplicare a acestor măsuri, inclusiv a unui audit ad-hoc; b) remedierea deficiențelor identificate în aplicarea lit. a); c) încetarea conduitei entităților prin care încalcă dispozițiile prezentei ordonanțe de urgență; d) punerea în aplicare a recomandărilor formulate ca urmare a unui audit de securitate; e) desemnarea unei persoane din cadrul personalului de control cu sarcini bine definite pe o perioadă de timp determinată, responsabilă cu supravegherea respectării de către entitatea esențială în cauză a dispozițiilor referitoare la măsurile de gestionare a riscurilor de securitate cibernetică; f) respectarea măsurilor de gestionare a riscurilor în materie de securitate cibernetică și a obligațiilor de raportare, într-o anumită modalitate și într-un interval de timp; g) ca încălcările dispozițiilor să fie făcute publice de către entitatea responsabilă.

Referitor la exercitarea atribuțiilor de supraveghere, verificare și control de către Directorat, vă transmitem faptul că în prezent, având în vedere stadiul implementării Ordonanței de urgență a Guvernului nr. 155/2024 - DNSC analizează datele și informațiile transmise de către entități în cadrul procesului de înregistrare și le încadrează, conform rezultatului evaluării realizate, drept entități esențiale, importante sau în afara legii, după caz, obligațiile a căror îndeplinire poate fi supravegheată conform pașilor cronologici în aplicarea legii, sunt cele de notificare în vederea înregistrării și de transmitere a evaluării nivelului de risc (în situația entităților înregistrate).

Astfel, până în prezent a fost înregistrat un număr de 1.218 entități în Registrul entităților, în timp ce în lucru se află un număr de aprox. 2.500 de notificări în vederea înregistrării.

Având în vedere cele precizate anterior, subliniem faptul că, în prezent, Directoratul este insuficient încadrat cu personal (la un nivel de aprox. 20% din capacitatea prevăzută de organigramă) raportat la nivelul de responsabilități și de activitate prevăzute de legislația în domeniu, precum și conexas.

Astfel, pentru exemplificare, menționăm că începând cu septembrie 2025 și până în prezent, Serviciul de Evidență și Sprijin, ce desfășoară activitățile de înregistrare a entităților care fac obiectul Directivei NIS 2, își desfășoară activitatea numai cu 6 persoane, gestionând până în prezent peste 3.500 de entități (înregistrarea presupunând și păstrarea unei corespondențe, uneori aceasta având ca obiect realizarea de analize și schimb de puncte de vedere complexe purtate cu entitatea în cauză). Cu toate că Direcția de Verificare și Control își desfășoară activitatea cu 3 persoane (dintre care o persoană inițial încadrată cu studii medii - student, în format part-time), a identificat și analizat până în prezent peste 2.500 de entități, activitățile finalizându-se prin transmiterea unui număr de 832 de notificări în vederea aducerii la cunoștință a obligației de înregistrare entităților care intră sub incidența Ordonanței de urgență a Guvernului nr. 155/2024.

De asemenea, în ciuda faptului că activitatea de reglementare se desfășoară cu numai 3 persoane (dintre care o persoană fiind încadrată cu studii medii - student), pe lângă actele normative deja emise, în transparență decizională se află proiectul de act normativ referitor la măsurile de gestionare a riscurilor de securitate cibernetică aferente rețelelor și sistemelor informatice utilizate de entitățile esențiale și importante și a metodologiei de auto-evaluare a maturității măsurilor (document care are aproximativ 670 de pagini), precum și cel privitor la standardul de pregătire a membrilor organelor de conducere ale entităților esențiale și importante și a listei de certificări de securitate cibernetică.

În plus, precizăm că inclusiv capacitatea de reacție a Directoratului la atacurile cibernetice derulate în spațiul cibernetic național civil este direct dependentă de numărul și specializarea experților angrenați cu expertiză tehnică. Intervențiile pentru remedierea incidentelor, conservarea probelor colectate, documentarea modalității de atac, dimensionarea măsurilor de limitare a pagubelor nu pot fi realizate decât printr-un nivel înalt de expertiză profesională, rolurile tehnice fiind foarte clar delimitate. Cu toate acestea, nivelul de salarizare din DNSC este depășit de cel din mediul privat, în ciuda faptului că domeniul de expertiză este caracterizat de competitivitate ridicată (generată de evoluția accelerată a noilor tehnologii).

Această subdimensionare a nivelului curent de personal de specialitate implică riscuri majore de întârziere în implementarea angajamentelor naționale și europene în materie de securitate cibernetică și poate afecta capacitatea de reacție la amenințări, motiv pentru care considerăm că, în vederea consolidării capacității instituționale, se impun măsuri care privesc, spre exemplu, posibilitatea de derulare a concursurilor de angajare, actualizarea nivelului de salarizare în vederea întâmpinării obstacolelor în angajare generate de competitivitatea ridicată din domeniu.

Cu privire la creșterea rezilienței în fața amenințărilor cibernetice, precizăm că aceasta se realizează în primul rând prin implementarea măsurilor și mecanismelor pentru asigurarea unui nivel comun ridicat de securitate cibernetică la nivel național prevăzute de Ordonanța de urgență a Guvernului nr. 155/2024 care a transpus în legislația română Directiva NIS 2 - aceasta contribuind la consolidarea capacității naționale de a reacționa în mod eficient în fața evoluțiilor regionale și globale din domeniul securității cibernetice. În acest sens, subliniem faptul că prevederile actului normativ nu presupun numai rezultate de natură a fi obținute într-un termen foarte scurt, ci acestea presupun maturizarea coerentă și susținută a entităților, astfel încât nivelul securității cibernetice a rețelelor și sistemelor informatice ale acestora, îndeosebi a celor din sectoare corespunzătoare serviciilor esențiale pentru societate, precum și a celor cu valențe critice pentru securitatea națională, să fie suficient pentru a menține în parametri optimi disponibilitatea, continuitatea, integritatea și reziliența acestora în vederea susținerii în condiții optime a domeniilor aferente vieții economice și sociale.

Cu deosebită considerație,

Dan Cîmpean

Directorul Directoratului Național de Securitate Cibernetică (DNSC)

prin împuternicit,

Gabriel-Cătălin Dinu,

Adjunct al Directorului DNSC

Gabriel-
Catalin Dinu

Digitally signed by
Gabriel-Catalin Dinu
Date: 2026.07.30
16:21:00 +03'00'