CONSILIUL ECONOMIC ŞI SOCIAL
Str. Dimitrie D. Gerota nr. 7-9, sector 2, Bucureşti, cod poştal: 020027
Telefoane: 021.310.23.56, 021.316.31.34 Fax: 021.316.31.31
021.310.23.57, 021.316.31.33
Cod fiscal: 10464660 E-mail: ces@ces.ro www.ces.ro

Nr. 1036/11.02.2026

AVIZ
referitor la propunerea legislativă privind înființarea şi operaționalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, precum şi pentru modificarea şi completarea unor acte normative (plx2/2.02.2026)

În temeiul art. 2 alin. (1) din Legea nr. 248/2013 privind organizarea și funcționarea Consiliului Economic și Social, republicată, cu modificările și completările ulterioare, și art. 11 lit. a) din Regulamentul de organizare și funcționare, Consiliul Economic și Social a fost sesizat cu privire la avizarea *propunerii legislative privind înființarea şi operaționalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, precum şi pentru modificarea şi completarea unor acte normative (plx2/2.02.2026).*

CONSILIUL ECONOMIC ŞI SOCIAL

În temeiul art. 5 lit. a) din Legea nr. 248/2013 privind organizarea și funcționarea Consiliului Economic și Social, republicată, cu modificările și completările ulterioare, în ședința din data de 11.02.2026, desfășurată online, conform prevederilor Hotărârii Plenului nr.86/17.05.2022, avizează **FAVORABIL** prezentul proiect de act normativ, cu **propunerile de modificare** prevăzute în anexă și cu următoarele **observații:**

- se impune o mai bună corelare cu prevederile legislației UE (NIS2 / NCCS):
  - periodicitatea testelor de reziliență trebuie corelată cu Regulamentul delegat (UE) 2024/1366, nu fixată la 4 ani;
  - Legea CRISCE (Centrul de Răspuns la Incidente de Securitate Cibernetică în Energie) trebuie să facă trimitere expresă la actul de transpunere Directivei

europeane NIS2 (nr. 2555/2022). Este necesară evitarea unor contradicții între obligațiile CRISCE și cele directe ale operatorilor;

- accesul CRISCE la OT/ICS (Tehnologia Operațională și Sistemele de Control Industrial) trebuie limitat și proporțional:
  - *„Accesul continuu”* la rețelele operatorilor este excesiv și riscant. Accesul trebuie să fie strict necesar scopului, securizat, fără perturbarea funcționării sistemelor, conform principiului need-to-know;
- CRISCE nu trebuie să devină furnizor monopolist de servicii SOC (Security Operations Center):
  - operatorii care au SOC/CSIRT (Cyber Security Incident Response Team) propriu, certificat NIS2, nu trebuie obligați să achiziționeze servicii de la CRISCE;
  - se respectă principiul subsidiarității și libertatea de organizare prevăzută de NIS2;
- serviciile CRISCE trebuie adresate doar persoanelor juridice:
  - Eliminarea referirii la „persoane fizice” – nu au infrastructuri energetice sau OT/ICS (Tehnologia Operațională și Sistemele de Control Industrial);
- este necesară clarificarea rolului CRISCE în raport cu prevederile GDPR - Protecția datelor cu caracter personal:
  - operatorii din energie rămân operatori de date;
  - CRISCE acționează ca persoană împuternicită, nu operator independent;
- costurile impuse operatorilor de distribuție trebuie recunoscute integral în tarife:
  - obligațiile introduse de lege generează costuri inevitabile;
  - operatorii reglementați nu le pot recupera decât prin tarife aprobate;
  - se aplică principiul neutralității financiare din legislația UE;
- **referitor la art. 8, după alin. (5), considerăm că este necesară introducerea unui nou alineat, alin. (6),** cu următorul cuprins: *„(6) Operatorii de distribuție a energiei electrice și a gazelor naturale care dețin SOC/CSIRT propriu certificat conform cerințelor NIS2 și auditat periodic, nu sunt obligați să achiziționeze servicii comerciale de la CRISCE”.* Prin introducerea alin. (6) se recunoaște principiul subsidiarității: CRISCE oferă servicii operatorilor fără capacități proprii, dar nu creează monopol forțat. Astfel se evită conflictul cu art. 21 din NIS2 (care lasă operatorului libertatea să-și organizeze SOC intern) și cu regulile de concurență UE;
- **referitor la art. 10, după alin. (2), apreciem ca fiind necesară introducerea unui nou alineat, alin. (3),** cu următorul cuprins: *„(3) Distincția între regimul juridic aplicabil datelor se face astfel: a) datele cu caracter personal se supun exclusiv*

Regulamentului (UE) 2016/679 și legislației naționale de punere în aplicare; b) datele privind persoane juridice, inclusiv informațiile comerciale sensibile, sunt protejate prin legislația națională aplicabilă în materie de concurență neloială și protecția secretelor comerciale." În textul actual, toate datele sunt tratate generic („date și informații"), fără a face diferența între date personale (supuse GDPR) și date comerciale (supuse legislației concurenței/secrete comerciale). GDPR (art. 4) se aplică strict datelor personale, nu este corect juridic să extindem protecția GDPR asupra datelor privind persoane juridice. Această delimitare clară elimină riscul de confuzie juridică și asigură aplicarea corectă a cadrului legal.

Președinte,
Sterică FUDULEA

Anexă

Propuneri de modificare aferente

propunerii legislative privind înființarea şi operaţionalizarea Centrului de Răspuns la Incidente de Securitate Cibernetică în Energie, precum şi pentru modificarea şi completarea unor acte normative (plx2/2.02.2026)

Nr. crt.	***Text inițial***	***Text propus***	***Motivare***
1.	*Art. 4* (11) Pentru personalul CIRSCE care a obținut Ia evaluarea performanțelor profesionale nota finală mai mică de 2,50 inclusiv CISO, comisia de evaluare propune ministrului energiei încetarea contractului individual de muncă.	(11) Pentru personalul CRISCE care a obținut la evaluarea performanțelor profesionale nota finală mai mică de 2,50 inclusiv CISO, comisia de evaluare propune ministrului energiei încetarea contractului individual de muncă, **cu respectarea prevederilor Codului muncii privind concedierea pentru necorespundere profesională.**	În lipsa acestei completări, dispoziția analizată riscă să instituie o nouă formă de concediere de drept, automată, bazată exclusiv pe rezultatul unei evaluări profesionale realizate de angajator. Or, Codul muncii reglementează exhaustiv cazurile și procedura concedierii pentru necorespundere profesională, ca garanție a protecției salariatului și a respectării dreptului la apărare. Evaluarea profesională poate fundamenta propunerea de concediere a comisiei, însă nu poate produce, în sine, încetarea raportului de muncă fără parcurgerea procedurii legale. Respectarea dreptului comun este necesară pentru a evita riscuri de neconstituționalitate și litigii de muncă, precum și pentru a asigura un just echilibru între exigențele ridicate de performanță ale CRISCE și protecția juridică a personalului încadrat.

2.	*Art. 5.* (1) În exercitarea funcției de centru operațional de securitate cibernetică la nivel sectorial în domeniul energetic și resurselor energetice, atribuțiile principale ale CRISCE sunt următoarele: (...) d) organizarea, monitorizarea și finalizarea, **cel puțin o dată la 4 ani,** a unui test de reziliență cibernetică **împreună cu toți administratorii infrastructurilor critice din sectorul energetic;** cadrul de testare, normele, regulamentul și condițiile de desfășurare a testelor vor fi aprobate prin ordin comun al ministrului energiei și al directorului DNSC; e) asigurarea **accesului continuu și integrat la datele și telemetria** operatorilor economici din sectorul energetic, **inclusiv la rețelele de tip tehnologie operațională/sisteme de control industrial, denumite în continuare rețele de tip OT/ICS, în scopul monitorizării eficiente și proactive a securității cibernetice.**	d) organizarea, monitorizarea și finalizarea unui test de reziliență cibernetică în conformitate **cu periodicitatea prevăzută de Regulamentul delegat (UE) 2024/1366 (NCCS) – inclusiv testarea anuală a procedurilor de răspuns și testarea planurilor de continuitate/criză se efectuează la intervale de maximum 3 ani;** cadrul de testare, normele, regulamentul și condițiile de desfășurare a testelor vor fi aprobate prin ordin comun al ministrului energiei și al directorului DNSC. e) asigurarea **posibilității de interconectare securizată cu sistemele de monitorizare ale** operatorilor economici din sectorul energetic, **pentru transmiterea către CRISCE a datelor relevante și strict necesare privind securitatea cibernetică, inclusiv în ceea ce privește rețelele de tip OT/ICS, fără a perturba buna funcționare a sistemelor și asigurând confidențialitatea, integritatea și disponibilitatea datelor.**	NCCS stabilește obligații mai stricte și mai recurente: evaluări periodice de risc și reziliență, audituri și teste recurente, în unele cazuri la interval de 3 ani (nu 4 ani), cerințe suplimentare în situații de modificări majore. Dacă România fixează în proiectul de lege un termen minim de 4 ani, iar NCCS cere uneori 3 ani sau chiar mai des, există riscul ca legislația națională să fie percepută ca sub-nivel UE. „Acces continuu” al unei entități externe poate încălca principiul need-to-know, poate crea risc operațional. Accesul CRISCE la datele din infrastructurile OT/ICS ale distribuitorului DEGR ar trebui să se limitează la un minim set de date necesar indeplinirii scopului/ misiunii CRISCE.
3.	*Art. 8.* (1) Ministerul Energiei, prin CRISCE, poate realiza venituri din prestații de servicii de securitate cibernetică, în limitele atribuțiilor și activităților prevăzute la art.	(1) Ministerul Energiei, prin CRISCE, poate realiza venituri din prestații de servicii de securitate cibernetică, în limitele atribuțiilor și activităților prevăzute la art.	Eliminarea „persoanelor fizice” (alin. 1) - în realitate, persoanele fizice nu au rețele sau infrastructuri OT/ICS care să necesite servicii de SOC. Formularea actuală generează confuzie și risc de interpretare

	5, **persoanelor fizice și juridice** de drept public sau privat din sectorul energetic. (2) Serviciile și tarifele prevăzute la alin. (1) se stabilesc în baza unei metodologii de calcul realizată în baza unor standarde de cost stabilite prin ordin al ministrului energiei, cu avizul prealabil și conform al DNSC și al Consiliului Concurenței, care se publică în Monitorul Oficial al României, Partea I. **(3) Tarifele reglementate din sectorul energetic aferente costurilor cu auditul de securitate cibernetică, pentru serviciile prestate de CRISCE către operatorii economici se recuperează prin tarife de rețea sau alte mecanisme similare stabilite de prevederile legale aplicabile, potrivit Regulamentului delegat (UE) 2024/1366.**	5, **către persoanele juridice** de drept public sau privat din sectorul energetic. (2) Serviciile și tarifele prevăzute la alin. (1) se stabilesc în baza unei metodologii de calcul realizată în baza unor standarde de cost stabilite prin ordin al ministrului energiei, cu avizul prealabil și conform al DNSC, al Consiliului Concurenței **și ANRE,** care se publică în Monitorul Oficial al României, Partea I. **(3) Costurile înregistrate de către operatorii economici din sectorul energetic, aferente implementării și aplicării prevederilor prezentului proiect de Lege, vor fi recunoscute integral de către autoritatea de reglementare în tarifele de distribuție energie electrică și gaze naturale.**	(de ex. prestări către persoane fizice – contrar rolului CRISCE). ANRE este autoritatea de reglementare a tarifelor de rețea și are competența exclusivă să stabilească ce costuri sunt recunoscute ca fiind justificate. Dacă serviciile CRISCE sunt obligatorii sau recuperabile prin tarife, ANRE trebuie să confirme metodologia (altfel risc de dublă reglementare și litigii). Prevederile proiectului de Lege introduc obligații suplimentare pentru operatorii economici din sectorul energetic (ex. audituri de securitate cibernetică, interconectare cu CRISCE, teste de reziliență). Aceste obligații generează costuri noi, inevitabile și independente de voința operatorilor. Întrucât operatorii de distribuție energie electrică și gaze naturale sunt entități reglementate, aceștia nu își pot recupera aceste cheltuieli prin mecanisme comerciale proprii, ci exclusiv prin tarife aprobate de autoritatea națională de reglementare. Conform principiului neutralității financiare și al recunoașterii costurilor justificate și eficiente, prevăzut de legislația europeană (Regulamentul (UE) 2019/943, Regulamentul delegat (UE) 2024/1366 – NCCS), costurile aferente aplicării prezentului proiect de Lege trebuie recunoscute integral în tarifele de distribuție de către ANRE. Această prevedere este necesară pentru:

			- a asigura predictibilitate și securitate juridică pentru operatori, - a evita riscul de subfinanțare a măsurilor de securitate cibernetică, - a garanta că implementarea CRISCE nu se transformă într-o povară financiară neacoperită.
4.	*Art. 10.* (1) Ministerul Energiei, prin CRISCE, **în situația în care solicită şi primește date şi informaţii de la orice persoană fizică şi juridică în temeiul prezentei legi ia măsuri adecvate pentru a proteja interesele de securitate şi comerciale ale acestora, ale persoanelor care furnizează datele şi informaţiile respective, precum şi ale persoanelor la care se referă datele şi informaţiile respective.**	(1) Ministerul Energiei, prin CRISCE, **atunci când solicită şi primește date şi informaţii de la persoane fizice sau juridice în temeiul prezentei legi, aplică măsuri tehnice și organizatorice adecvate, cel puțin la nivelul standardelor naționale și europene în materie de securitate a informațiilor și protecția datelor (inclusiv Regulamentul (UE) 2016/679, Legea nr. 124/2025 și standardele ISO/IEC 27001 sau echivalente), pentru a proteja:** **a) drepturile fundamentale și confidențialitatea persoanelor fizice vizate ale căror date sunt prelucrate;** **b) interesele legitime și secretele comerciale ale persoanelor juridice care furnizează datele și informaţiile respective și ale persoanelor la care se referă datele şi informaţiile respective;**	Textul actual al proiectului de Lege se limitează la „măsuri adecvate”, care este o formulare prea vagă și susceptibilă de interpretări. Conform art. 32 GDPR, operatorii sunt obligați să aplice „măsuri tehnice și organizatorice corespunzătoare” în funcție de riscuri. Legea 124/2025 impune operatorilor esențiali din energie obligații explicite de a implementa standarde tehnice, raportare incidente și audit periodic. Astfel, textul va fi aliniat la GDPR + NIS2 (Legea 124/2025) și la bune practici recunoscute internațional. Referirea la ISO/IEC 27001 (sau echivalente) este aliniată practicilor internaționale și cerințelor de audit aplicate în majoritatea SOC-urilor din energie. Această precizare reduce riscul ca Ministerul/CRISCE să aplice măsuri insuficiente sau arbitrare.
	(2) Transmiterea de date şi informaţii obţinute **potrivit** prezentei Legi de la orice persoană fizică şi juridică de drept public sau privat **poate fi efectuată numai pentru îndeplinirea atribuţiilor legale ale CRISCE care obţine aceste date şi**	(2) Transmiterea de date şi informaţii obţinute de la orice persoană fizică şi juridică de drept public sau privat, **în temeiul** prezentei legi, **către alte autorități publice sau terți, la nivel național sau internațional, se efectuează**	Conform art. 5 GDPR – principiul minimizării, orice prelucrare de date trebuie să fie „adecvată, relevantă și limitată la ceea ce este necesar”. Transmiterea internațională de date se supune art. 44-49 GDPR și necesită

	informaţii, cu garantarea păstrării confidenţialităţii datelor cu caracter personal şi a protecţiei intereselor şi secretelor de serviciu și comerciale ale persoanelor fizice şi juridice de drept public și privat.	**exclusiv în măsura în care este strict necesară și proporțională pentru îndeplinirea atribuţiilor legale ale CRISCE.** **În toate cazurile se asigură:** **a) garantarea păstrării confidenţialităţii datelor cu caracter personal prin aplicarea principiilor prevăzute de Regulamentul (UE) 2016/679 și legislația conexă;** **b) protejarea secretelor de serviciu și comerciale prin acorduri de confidențialitate și prin măsuri tehnice, inclusiv criptare, segregarea mediilor de stocare și controlul accesului pe bază de roluri;** **c) trasabilitatea completă a prelucrărilor de date, prin înregistrarea și auditarea accesărilor, stocărilor și transmiterilor.**	garanții suplimentare (clauze contractuale standard, acorduri de confidențialitate). Pentru secrete comerciale → Directiva (UE) 2016/943 privind protecția know-how-ului și a informațiilor comerciale nedivulgate obligă statele membre să asigure măsuri eficiente de protecție. Lipsa acestor limitări ar putea genera riscuri de acces excesiv la date, transferuri arbitrare și posibile litigii între operatori și stat. Propunerea aliniază textul la GDPR + directiva privind secretele comerciale și evită conflictul cu legislația UE. Trasabilitatea este cerută de ISO 27001 și de NIS2 (art. 21 privind măsuri de management al riscului). Este esențială pentru demonstrarea conformității, investigarea incidentelor și răspunderea juridică în caz de scurgeri de informații. În lipsa trasabilității, nu există niciun control real asupra modului în care sunt folosite datele primite de CRISCE. Măsura e o garanție atât pentru persoanele vizate, cât și pentru operatorii economici.
5.	*Art. 11* (1) Prelucrările de date cu caracter personal ce intră sub incidenţa prezentei legi se efectuează cu respectarea **reglementărilor legale** privind protecţia persoanelor fizice **și juridice în ceea ce privește prelucrarea datelor cu caracter personal.**	(1) Prelucrările de date cu caracter personal ce intră sub incidenţa prezentei legi se efectuează cu respectarea **Regulamentului (UE) 2016/679 și a legislației naționale de punere în aplicare legale** privind protecţia persoanelor fizice. **Referința la persoane juridice privește exclusiv protecția**	Art. 1 și 4 GDPR stabilesc explicit că regulamentul se aplică doar persoanelor fizice. Extinderea formală la persoane juridice ar fi contrară dreptului UE și ar crea confuzie juridică. Protecția persoanelor juridice se face prin alte instrumente legale.

		confidențialității și secretului comercial, fără a extinde aplicabilitatea GDPR.	
	(2) Notificările realizate în temeiul prezentei legi nu afectează obligaţiile operatorilor de date cu caracter personal stabilite potrivit art. 33 şi 34 din Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).	(2) Notificările realizate în temeiul prezentei legi nu afectează obligaţiile operatorilor de date cu caracter personal stabilite potrivit art. 33 şi 34 din Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor). **În relaţia dintre operatorii din sectorul energetic şi CRISCE, aceştia rămân operatori de date, iar CRISCE acţionează în calitate de persoană împuternicită, conform art. 28 GDPR, pentru prelucrările efectuate în numele operatorilor.**	Conform art. 4 pct. 7–8 GDPR, operatorul este cel care stabilește scopurile și mijloacele prelucrării, iar persoana împuternicită acționează doar în numele operatorului. Operatorii decid ce date transmit și în ce scop (incident, conformitate), CRISCE doar procesează și transmite date pentru aceleași scopuri – rol de împuternicit. Această clarificare evită riscul ca ME/CRISCE să fie tratat ca „operator independent”, ceea ce ar duce la confuzie privind responsabilitățile și obligațiile de informare/notificare.
	(3) În scopul îndeplinirii atribuţiilor ori furnizării serviciilor prevăzute de prezenta lege, precum şi în scopul prevenirii şi răspunsului la incidentele de securitate cibernetică ori al cooperării la nivel naţional, comunitar şi internaţional în prevenirea şi răspunsul la incidentele de securitate cibernetică, Ministerul Energiei, prin CRISCE, primește, prelucrează şi transmite date şi informaţii ce pot constitui sau pot conţine date cu caracter personal, în limitele legislaţiei aplicabile, cu asigurarea respectării prevederilor alin. (2).	(3) În scopul îndeplinirii atribuţiilor prevăzute de prezenta lege, **Ministerul Energiei, prin CRISCE, poate primi, prelucra și transmite exclusiv datele cu caracter personal strict necesare și proporționale pentru prevenirea și răspunsul la incidentele de securitate cibernetică, cu respectarea principiilor de minimizare, confidențialitate și securitate prevăzute de Regulamentul (UE) 2016/679. Transmiterea acestor date către terți la nivel național, comunitar sau internațional se face numai în baza unui temei legal și cu garanții adecvate de protecție.**	Textul proiectului de Lege este unul generic, nu menționează limite sau garanții suplimentare și poate legitima prelucrări excesive, disproporționate sau lipsite de trasabilitate. CRISCE poate prelucra doar datele strict necesare, cu respectarea principiilor GDPR (art. 5: legalitate, minimizare, proporționalitate, confidențialitate). Transmiterea se face numai pe temei legal și cu garanții adecvate.

6.	*Art. 12.* Prezenta lege se completează **cu prevederile corespunzătoare** din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, **precum și pentru modificarea și completarea unor acte normative, cu modificările și completările ulterioare,** Ordonanţa de urgenţă nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil, precum și cu Ordonanța de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, cu modificările și completările ulterioare.	Prezenta lege se completează cu prevederile corespunzătoare **din Legea nr. 124/2025 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și de transpunere a Directivei (UE) 2022/2555 (Directiva NIS2), cu prevederile** Legii nr. 58/2023 privind securitatea și apărarea cibernetică a României, cu Ordonanţa de urgenţă nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil, precum și cu Ordonanța de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, cu modificările și completările ulterioare.	Textul art. 12 face trimitere la trei acte, fără a menţiona Legea 124/2025. Dacă art. 12 nu o menționează, poate apărea o contradicție între CRISCE și obligațiile directe ale operatorilor prevăzute în Legea 124/2025.