APARATUL PREȘEDINTELUI REPUBLICII MOLDOVA

Bd. Ștefan cel Mare și Sfânt, nr. 154, MD-2073 Chișinău
www.presedinte.md

03 martie 2023 Nr.2/1-05-277

Ministerului Dezvoltării Economice și Digitalizării

Ca urmare a examinării repetate a proiectului de *hotărâre a Guvernului privind aprobarea proiectului de lege privind securitatea cibernetică* (număr unic 41/ME/2023), Aparatul Președintelui Republicii Moldova informează despre lipsa obiecțiilor și propunerilor adiționale.

Andrei SPÎNU,
Secretar general

Digitally signed by Spînu Andrei
Date: 2023.03.06 15:30:22 EET
Reason: MoldSign Signature
Location: Moldova

CANCELARIA DE STAT A REPUBLICII MOLDOVA

Chişinău

Nr. 29 - 69 - 2272 2 martie 2023

Ministerul Economiei

Urmare a examinării repetate a proiectului de lege privind securitatea cibernetică *(num. unic: 41/ME/2023)*, în limita competenţelor funcţionale, comunicăm lipsa obiecţiilor şi propunerilor.

Secretar general al Guvernului **Artur MIJA**

CANCELARIA DE STAT A REPUBLICII MOLDOVA
DIRECŢIA MANAGEMENTUL DOCUMENTELOR
3

Ex. I. Prisăcaru
tel. 250-483

Casa Guvernului,
MD-2012, Chişinău,
Republica Moldova
Telefon:
+ 373 22 250 104
Fax:
+ 373 22 242 696
E-mail:
cancelaria@gov.md

AGENȚIA DE GUVERNARE ELECTRONICĂ

E-GOVERNANCE AGENCY

Republic of Moldova, Chișinău, MD-2012, 134, Ștefan cel Mare și Sfânt Ave.
Phone: +373 22 820 026, email: office@egov.md, web: http://www.egov.md

Nr. 3007 – 36 din 28.02.2023
La nr. 07-519 din 27.02.2023

Ministerul Economiei

Instituția publică „Agenția de Guvernare Electronică" a examinat ***proiectul hotărârii Guvernului privind aprobarea proiectului de lege privind securitatea cibernetică*** **(număr unic 41/ME/2023), autor - Ministerul Economiei,** remis spre avizare repetată.

Analizând argumentarea autorului proiectului de neacceptare a unor propuneri din avizul Agenției nr.3007-19 din 31.01.2023, expuse în sinteză la proiect, susținem, în principiu, argumentele invocate. În acest context, vă comunicăm că, în limitele competențelor instituției, avizăm favorabil versiunea definitivată a proiectului de lege și nu avem obiecții sau propuneri.

Directoare Digitally signed by Tumuruc Olga
Date: 2023.02.28 16:07:13 EET
Reason: MoldSign Signature
Location: Moldova

Olga TUMURUC

Ex.: Eduard Fricațel,
e-mail: eduard.fricatel@egov.md,
tel.: 0794 38 138

AGENȚIA NAȚIONALĂ PENTRU REGLEMENTARE ÎN COMUNICAȚII ELECTRONICE ȘI TEHNOLOGIA INFORMAȚIEI A REPUBLICII MOLDOVA

НАЦИОНАЛЬНОЕ АГЕНТСТВО ПО РЕГУЛИРОВАНИЮ В ОБЛАСТИ ЭЛЕКТРОННЫХ КОММУНИКАЦИЙ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ РЕСПУБЛИКИ МОЛДОВА

Nr. 02 DRAS/308 01 martie 2023
la Nr. din

Ministerul Economiei al Republicii Moldova

Cu referință la scrisoarea nr. 07-519 din 27.02.2023, Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației vă informează că a examinat proiectul de hotărâre privind aprobarea proiectului de lege privind securitatea cibernetică (număr unic 41/ME/2023) și comunică despre lipsa obiecțiilor suplimentare celor incluse în Sinteza obiecțiilor și propunerilor/recomandărilor la proiect.

Cu respect,

Director adjunct

Digitally signed by Bojoga Silvia
Date: 2023.03.01 17:18:11 EET
Reason: MoldSign Signature
Location: Moldova

Silvia BOJOGA

Ex.V.Vozian,
tel: 0 22 251 337

bd. Ștefan cel Mare,134, MD-2012, Chișinau
Telefon: +373-22-25-13-17
Fax: +373-22-22-28-85
E-mail:office@anrceti.md
www.anrceti.md

Republica Moldova

Agenția Națională pentru Reglementare în Energetică
ANRE

str. Alexandr Pușkin, nr. 52/A, MD-2005 Chișinău, Tel: 022 823 955, anre@anre.md, http://www.anre.md

Nr. 06-01/830 din 01.03.2023
La nr. 07-519 din 27.02.2023

Ministerul Economiei
secretariat@me.gov.md
sergiu.florea@me.gov.md

Cu referire la proiectul de hotărâre privind aprobarea proiectului de Lege privind securitatea cibernetică, remis repetat spre avizare în regim de urgență de către Ministerul Economiei (**număr unic 41/ME/2023**), Agenția Națională pentru Reglementare în Energetică comunică despre lipsa obiecțiilor și propunerilor pe marginea proiectului definitivat.

Veaceslav UNTILA
Director General

MINISTERUL ECONOMIEI AL REPUBLICII MOLDOVA
SECRETARIAT

Ex. D. Hîncu
Tel. 067604196

CANCELARIA DE STAT A REPUBLICII MOLDOVA

CENTRUL DE ARMONIZARE A LEGISLAȚIEI

Nr. 31/02-69-2228 Chișinău 2 martie 2023

Ministerul Dezvoltării Economice și Digitalizării
secretariat@me.gov.md

Copie: Cancelaria de Stat

cancelaria@.gov.md

Ref.: scrisoarea nr. 07-519 din 27 februarie 2023/ ***număr unic 41/ME/2023***

Prin prezenta, Centrul de armonizare a legislației, în baza expertizei repetate a **proiectului de lege privind securitatea cibernetică**, promovat în scopul realizării Acțiunii 2.2 din Planul de acțiuni al Guvernului pentru anul 2023, aprobat prin HG nr. 90/2023 și a pct. 5.2. din Planul de acțiuni pentru implementarea măsurilor propuse de către Comisia Europeană în Avizul său privind cererea de aderare a Republicii Moldova la Uniunea Europeană, comunică următoarele.

Proiectul național are drept obiectiv principal transpunerea primară și parțială în legislația națională a Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2). Astfel, proiectul național instituie norme cadru privind competențele autorităților și instituțiilor publice în materie de securitate cibernetică, reglementează cadrul național general de gestionare a crizelor în domeniul securității cibernetice, stabilește cerințele, măsurile și mecanismele pentru asigurarea securității rețelelor și a sistemelor informatice

Casa Guvernului,
MD-2033, Chișinău,
Republica Moldova
Telefon:
+ 373 22 250 229

care sunt esențiale pentru funcționarea societății, precum și reflectă modul de gestionare a incidentelor cibernetice.

Ca urmare a expertizei de compatibilitate a versiunii inițiale a proiectului (Declarația de compatibilitate nr. 31/02-126-1118 din 2 februarie 2023), Centrul de armonizare a legislației a constatat că proiectul în cauză asigură transpunerea parțială a Directivei 2022/2555/UE. Totodată, au fost înaintate o serie de obiecții privind compatibilitatea cu actul UE și referitoare la Tabelul de concordanță, instrument principal al procesului de armonizare legislativă.

Versiunea actuală a proiectului este una îmbunătățită, fiind preluate obiecțiile referitoare la transpunerea art. 2 (1) din actul UE (aplicabilitatea normelor deopotrivă asupra entităților publice sau private, care desfășoară activități în sectoare de o importanță critică ridicată, precum și în alte sectoare de importanță critică), au fost excluse prevederile referitoare la dreptul autorității competente de a restricționa utilizarea sau accesul la un sistem informatic pentru un furnizor, care erau contrare art. 31 (5) din actul UE.

Totodată, **reiterăm** o serie de obiecții, care nu au fost reținute de proiectul național, dar care vor fi transpuse prin acte normative de implementare a Legii și **care nu constituie impedimente pentru promovarea proiectului**, după cum urmează:

- Art. 4, alin. (2) din proiect stabilește că lista sectoarelor, sub sectoarelor, precum și a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și sub sectoare va fi aprobată ulterior de Guvern, ori actul UE, prin art. 3 și Anexa I și II, stabilește norme minime referitoare la entitățile esențiale și cele importante, precum și identifică (la nivel exemplificativ, cu drept de extindere a listei) sectoarele cu o importanță critică ridicată (Anexa I) și alte sectoare de importanță critică (Anexa II);
- Art. 6, alin. (3) din proiectul național a preluat doar la nivel de concept prevederile UE referitoare la Strategia națională de securitate cibernetică din art. 7 al Directivei UE, în speță, în ceea ce privește necesitatea existenței unui atare document de politici în RM și aprobarea acesteia de Parlamentul RM. Nu au fost transpuse prevederile UE aferente elementelor constitutive obligatorii ale Strategiei din art. 7 (1) al actului UE, spectrul de politici care sunt adoptate prin Strategie din art. 7 (2) al actului UE, precum și normele referitoare la actualizarea Strategiilor la intervale de 5 ani din art. 7 (4) al Directivei;
- Art. 18 și 19 din proiectul național, care se referă la supravegherea și controlul de stat asupra furnizorilor de servicii, a transpus doar normele cadru referitoare la supravegherea și controlul exercitat de autoritatea competentă din art. 31 - 33 din actul UE, urmând ca modul detaliat de exercitare a supravegherii și controlului să fie stabilit de către Guvern;

- Art. 6 și 7 din proiectul național stabilesc generic, fără o nominalizare, autoritățile naționale cu competență în domeniul securității cibernetice – autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice și autoritatea competentă la nivel național în domeniul securității cibernetice. Acest fapt denotă o implementare parțială a art. 8 din Directiva UE, care impune statelor membre desemnarea sau instituirea autorităților competente, inclusiv, prin identificarea lor nominală.

Cu referire la instrumentele procesului de armonizare, se constată că în procesul de definitivare al proiectului, nu a fost ajustat Tabelul de concordanță, conform recomandărilor si sugestiilor Centrului. În același timp, având în vedere importanța proiectului care rezultă din Planul de acțiuni pentru implementarea măsurilor propuse de către Comisia Europeană în Avizul său privind cererea de aderare a Republicii Moldova la Uniunea Europeană, solicităm ca Tabelul de concordanță să fie remis în regim de lucru pentru evaluare calitativă în termen rezonabil. Menționăm că, proiectul de Lege însoțit de tot setul de acte, inclusiv Tabelul de concordanță, urmează a fi prezentat Parlamentului pentru examinare și adoptare ulterioară.

Facem mențiunea că analiza Centrului de armonizare a legislației nu are în vedere elementele de oportunitate ale soluțiilor juridice incluse în proiectul de act normativ, ci se referă strict la conformitatea acestora cu Dreptul UE aplicabil și obligațiile juridice asumate în lumina Acordului de Asociere RM – UE.

/semnat electronic/

Șef Centru

Natalia SUCEVEANU

Digitally signed by Suceveanu Natalia
Date: 2023.03.02 11:34:30 EET
Reason: MoldSign Signature
Location: Moldova

Ex. A. Bulat-Rotaru
250354

SERVICIUL TEHNOLOGIA INFORMAȚIEI
ȘI SECURITATE CIBERNETICĂ

MD-2012 mun. Chișinău, Piața Marii Adunări Naționale, 1 IDNO 1003600096694
tel.: + 373 22 820 900, fax: + 373 22 250 522 e-mail: stisc@stisc.gov.md, itsec@itsec.gov.md

01.03.2023 1.4/362/23
La nr. 07-519 din 27.02.2023

Domnului Viorel GARAZ,
Secretar de stat al Ministerului Economiei

Stimate domnule Secretar de Stat,

Prin prezenta, în ordinea examinării repetate a proiectului definitivat de hotărâre *privind aprobarea proiectului de lege privind securitatea cibernetică* **(număr unic 41/ME/2023),** I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică", în limitele competenței funcționale, reiterează obiecțiile prezentate prin avizul cu nr. 1.4/228/23 din 02.02.2023, neacceptate de către autor.

De asemenea, obiectăm repetat asupra faptului că legea privind securitatea cibernetică trebuie să instituie cerințele, măsurile și mecanismele pentru asigurarea securității cibernetice, **inclusiv a sistemelor informaționale.**

Cu respect,

Digitally signed by Ursu Alina
Date: 2023.03.01 15:09:41 EET
Director Reason: MoldSign Signature
Location: Moldova

Gheorghe PANTAZ

Ex.: Oaserele Ana
Tel: 022 828 133

SERVICIUL DE INFORMAȚII ȘI SECURITATE
AL REPUBLICII MOLDOVA

MD-2004, mun. Chișinău, bd. Ștefan cel Mare și Sfînt, 166 tel. 022-239-625, fax 022-234-068, e-mail: sis@sis.md

„06" martie 2023 Nr. E/2334

La nr. 07-519 din 27.02.2023

Ministerul Dezvoltării Economice și Digitalizării

Serviciul de Informații și Securitate al Republicii Moldova (*în continuare - Serviciul*) a examinat repetat proiectul hotărârii de Guvern *„privind aprobarea proiectului de Lege privind securitatea cibernetică"* (**număr unic 41/ME/2023**) (*în continuare – proiect*) și a sintezei obiecțiilor și propunerilor/recomandărilor instituțiilor abilitate la avizare la proiectul nominalizat și comunică următoarele.

1. La obiecția Serviciului privind alin. (3) al art. 3 al proiectului, deși autorul indică că aceasta a fost acceptată, totuși nu a exclus alin. (3) al art. 3, ci l-a expus în redacție nouă, care nu poate fi acceptată. Or, art. 2 alin. (7) din Directiva (UE) 2022/2555 a Parlamentului european și a Consiliului din 14 decembrie 2022, privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), pe care proiectul o transpune, specifică că aceasta **nu se aplică entităților** administrației publice care își desfășoară activitățile în domeniile securității naționale, siguranței publice, apărării sau aplicării legii, inclusiv prevenirii, investigării, depistării și urmăririi penale a infracțiunilor.

Totodată, potrivit art. 5 alin. (5) a Legii nr. 245/2008 cu privire la secretul de stat, elaborarea și realizarea măsurilor de protecție a secretului de stat în cadrul autorităților publice și altor persoane juridice, precum și efectuarea controlului asupra asigurării protecției secretului de stat constituie atribuții ale autorității publice în domeniul protecției secretului de stat care este Serviciul de Informații și Securitate. Prin urmare, exceptată de la aplicarea prevederilor proiectului este anume instituția și nu doar o parte din activitatea acestuia (în speță **doar activitatea de mentenanță** a rețelelor și sistemelor informatice care sunt destinate prelucrării informațiilor atribuite la secret de stat).

2. Potrivit art. 1 alin. (1) al Legii nr. 753/1999 privind Serviciul de Informații și Securitate al Republicii Moldova, Serviciul **este organul de stat specializat în domeniul asigurării** securității **naționale prin exercitarea tuturor măsurilor adecvate de informații** și contrainformații, **de culegere, prelucrare, verificare și valorificare a informațiilor** necesare cunoașterii, prevenirii și contracarării oricăror acțiuni care constituie, potrivit legii, amenințare internă sau externă pentru independența, suveranitatea, unitatea, integritatea teritorială, ordinea constituțională, dezvoltarea democratică, securitatea internă a statului, societății și cetățenilor, statalitatea Republicii Moldova, funcționarea stabilă a ramurilor economiei naționale de importanță vitală, atît pe teritoriul Republicii Moldova, cît și peste hotare.

Astfel, în vederea realizării misiunii de asigurare a securității statului și de contracarare efectivă a amenințărilor hibride, considerăm absolut argumentată și necesară completarea proiectului cu un articol nou, care va avea următorul conținut: *„Autoritatea competentă informează imediat Serviciul de Informații și Securitate al Republicii Moldova, dar nu mai târziu de 24 de ore din momentul în care a luat cunoștință despre un incident cibernetic care poate avea impact asupra securității statului.”.*

În același timp, considerăm nejustificat argumentul autorului precum că completarea propusă ar dubla prevederile art. 7 (fără a indica la care alineat sau literă se referă), or, acesta din urmă stabilește atribuția autorității competente de **a asigura interacțiunea** în domeniul securității cibernetice cu autoritățile și instituțiile publice naționale și cu furnizorii de servicii, și nicidecum nu stabilește obligația acesteia de **raportare** către autorități competente **a incidentelor cibernetice specifice** (în speță – care pot avea impact asupra securității statului).

Mai mult ca atât, alin. (10) al art. 23 din Directiva NIS2 stabilește obligația echipelor CSIRT, după caz, autorităților competente de a furniza autorităților competente în temeiul Directive 2022/2557[1] informații privind incidentele semnificative și amenințările cibernetice din infrastructura entităților critice.

Respectiv, menționăm că în conformitate cu prevederile Regulamentului privind protecția antiteroristă a infrastructurii critice, Serviciul de Informații și Securitate al Republicii Moldova este desemnat în calitate de organ responsabil de coordonarea la nivel național a activității de asigurare a protecției antiteroriste a infrastructurii critice.

Din aceleași considerente este oportună completarea proiectului cu un articol nou care va stabili obligația autorității competente de a remite trimestrial în adresa Serviciului de Informații și Securitate al Republicii Moldova, a rapoartelor de sinteză privind incidentele de securitate cibernetică și amenințările identificate.

---

[1] Directiva (UE) 2022/2557 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului

3. Considerăm necesară completarea art. 18 alin. (2) din proiectul, după cuvântul „*terța*" cu textul „*din contul furnizorului de servicii responsabil, cu excepția persoanelor juridice de drept public.*".

În acest sens, menționăm că reieșind din prevederile alin (1) al aceluiași articol din proiect, furnizorii de servicii au obligația de respectare a prevederilor legale în domeniul securității cibernetice, iar autoritatea competentă exercită funcția de supraveghere a respectării acestora.

Astfel, refuzul autorului de a completa pct. 18 conform propunerii Serviciului expuse în avizul anterior, va rezulta în imposibilitatea punerii efective în aplicare a prevederilor legale. Or, furnizorul de servicii nu va fi interesat în realizarea măsurilor de asigurare a securității cibernetice din cont propriu, odată ce legea oferă posibilitatea de a nu întreprinde nici o acțiune din cont propriu și apelarea la autoritatea competentă, care la necesitate va contracta din bani publici și asistență terță. Considerăm că varianta agreată de autor pe lângă faptul că va crea condiții prielnice apariției manifestărilor de corupție, aceasta nu va duce la realizarea obiectivelor principale ale proiectului.

4. Urmând aceeași logică, dar și conducându-ne de prevederile pct. 5 al Măsurilor necesare pentru asigurarea securității cibernetice la nivel guvernamental, aprobate prin Hotărârea Guvernului nr. 482/2020, considerăm imperativă completarea art. 18 al proiectului cu un alineat nou cu următorul conținut: „*În cazul persoanelor juridice de drept public, asigurarea aplicării măsurilor necesare pentru soluționarea incidentului cibernetic care nu au putut fi soluționate în timp util de către acestea, este realizată prin solicitarea asistenței Centrului guvernamental de reacție la incidente de securitate cibernetică (CERT Gov).*". Or, în lipsa reglementării propuse, persoanelor juridice de drept public li se va aplica norma stabilită la alin. (2) al art. 18[2], care prevede atragerea asistenței terțelor părți la gestionarea incidentelor cibernetice, fapt ce presupune **inclusiv atragerea companiilor private, contra plată**, scenariu care comportă pericole de apariție a manifestărilor de corupție și care nu trebuie să existe, odată ce actualmente este instituit Centrul guvernamental de reacție la incidente de securitate cibernetică (CERT Gov), misiunea căruia constă, inclusiv, în asigurarea răspunsului la incidente de securitate cibernetică la nivel guvernamental.

Totodată, menționăm că argumentul autorului precum că, în cazul completării proiectul cu astfel de prevederi ar putea apărea percepția a două CSIRT naționale nu rezistă criticilor, or, chiar proiectul face referire la Centrul guvernamental de reacție la incidente de securitate cibernetică în art. 8.

Mai mult ca atât, alin. (3) al art. 8 din proiect, stabilește că Centrul guvernamental este responsabil de asigurarea securității rețelelor și sistemelor

[2] În cazul conflictului de norme a unei legi organice și unei hotărâri de Guvern, se va aplica prevederile legii, or, hotărârile Guvernului sunt adoptate în scopul organizării executării legii și nu poate contravine acesteia.

informatice ale căror proprietar este statul şi de facilitarea realizării de către furnizorii de servicii – persoane juridice de drept public a obligaţiilor de asigurare a securităţii cibernetice prevăzute de prezenta lege.

Prin urmare, completarea art. 18 conform propunerii expuse supra, constituie o continuare logică şi necesară în stabilirea atribuţiilor actorilor implicaţi în asigurarea securităţii cibernetice şi mecanismelor de punere în aplicare a legii.

5. Având în vedere climatul de securitate din regiune şi posibilitatea intensificării ameninţărilor hibride asupra obiectelor de infrastructură critică, inclusiv prin atacuri cibernetice, considerăm necesară completarea proiectului cu un articol nou, care ar prevedea obligaţia echipelor CERT/CSIRT/CIRT/SOC ce prestează servicii de răspuns la incidente pentru operatorii de infrastructură critică, de a obţine de la autoritatea competentă, autorizare pentru prestarea acestor servicii.

Suplimentar, în articolul dat urmează a fi prevăzută obligativitatea că, la emiterea autorizaţiei, autoritatea competentă va solicita opinia organului ce coordonează la nivel naţional activităţile de asigurare a protecţiei antiteroriste a infrastructurii critice. Or, lipsa unor astfel de reglementări va crea condiţii prielnice pentru centre subversive de a obţine (de ex. prin companii intermediare care ar propune condiţii de preţ avantajoase) acces la obiectele de infrastructură critică, fapt care va pune în pericol securitatea statului. În acest sens, considerăm argumentată necesitatea acordării unui control deosebit asigurării securităţii cibernetice a obiectivelor de infrastructură critică.

6. Serviciul atenţionează asupra faptului, că obiecţia comună expusă de marea majoritate a autorităţilor care au participat la procesul de avizare a proiectului, constă în necesitatea stabilirii exprese a autorităţii competente. Or, desemnarea organului competent prin act al Guvernului, este iraţională şi incorectă din momentul în care atribuţiile organului competent sunt stabilite în proiect, iar Directiva NIS2 stabileşte obligaţia statelor de desemnare a acesteia.

Menţionăm că, nu poate fi acceptat argumentul autorului precum că desemnarea organului competent de către Guvern, se încadrează în împuternicirile Guvernului stabilite în art. 6 lit. b), d) şi e) din Legea nr. 136/2017 cu privire la Guvern şi considerăm că desemnarea organului unic naţional, prin act a Guvernului depăşeşte competenţele acestuia. Or, potrivit art. 7 lit. b) a Legii nr. 136/2017, Guvernul stabileşte modul de organizare şi funcţionare, domeniile de activitate, structura şi efectivul-limită ale ministerelor, ale altor autorităţi administrative centrale **subordonate Guvernului** şi ale structurilor organizaţionale din sfera lor de competenţă, coordonează şi controlează activitatea acestora.

Potrivit art. 7 lit. d) a Legii nr. 136/2017, Guvernul înfiinţează **în subordinea sa,** alte autorităţi administrative centrale pentru realizarea politicii statului într-un domeniu de activitate care nu intră în competenţa nemijlocită a

ministerelor, precum și în domenii de activitate în care competențele ministerelor se intersectează, precum și le reorganizează și dizolvă.

Potrivit art. 7 lit. e) a Legii nr. 136/2017, Guvernul decide asupra constituirii, reorganizării și dizolvării structurilor organizaționale **din sfera de competentă a ministerelor și altor autorități administrative subordonate** Guvernului.

Prin urmare, având în vedere importanța, statutul și atribuțiile organului național în domeniul securității cibernetice, care urmează să acopere toate domeniile și actorii implicați la nivel național, considerăm imperativ necesară desemnarea acestuia prin lege.

7. O altă obiecție comună, exprimată de către majoritatea autorităților care au participat la procesul de avizare a proiectului, este necesitatea stabilirii sectoarelor/subsectoarelor menționate în Directiva NIS2.

În acest sens, deși autorul proiectului indică corect că statele membre sau cele care transpun această Directivă, cum e cazul Republicii Moldova, pot să stabilească prevederi care asigură un nivel mai ridicat de securitate cibernetică, inclusiv să stabilească și alte sectoare sau subsectoare decât cele menționate în anexe la Directiva NIS2, acesta ajunge la concluzia greșită precum că statele membre sau candidate pot să nu stabilească sectoarele în general, sau să stabilească doar o parte din ele. Or, alin. (1) al art. 10 din Directiva NIS2 stabilește că CSIRT-urile naționale acoperă **cel puțin** sectoarele, subsectoarele și tipurile de entități menționate în anexele I și II.

Astfel, sectoarele indicate în anexe se desemnează în mod obligatoriu, statele membre sau candidate **având opțiunea de a le completa** pe acestea.

Totodată, nu este argumentată opinia autorului precum că, preluarea listei sectoarelor/subsectoarelor comportă riscul neacoperirii unor sectoare esențiale pentru Republica Moldova, or, acesta nu a prezentat nici un studiu care ar demonstra acest lucru.

Astfel, în cazul existenței unui astfel de studiu realizat de către autor, considerăm necesară includerea rezultatelor acestuia în notă informativă și analiza de impact, în caz contrar, constatăm că lista sectoarelor și subsectoarelor stabilite în Directiva NIS este una amplă, universală și urmează a fi transpusă în legislația națională prin lege.

8. Serviciul consideră necesară completarea proiectului cu norme de transpunere a prevederilor art. 20 al Directivei NIS 2. Art.20 alin (1) al Directivei menționate, stabilește posibilitatea de tragere la răspundere a organelor de conducere a entităților esențiale și entităților importante, dacă acestea nu respectă măsurile de gestionare a riscurilor în materie de securitate cibernetică.

Totodată, art. 20 alin. (2) al aceleiași Directive, obligă membrii organelor de conducere a entităților esențiale și entităților importante să urmeze o formare

pentru a dobândi suficiente cunoştinţe şi competenţe pentru a putea identifica riscurile şi a evalua practicile de gestionare a riscurilor în materie de securitate cibernetică.

Astfel, deşi în clauza de adoptare a proiectului se indică faptul că acesta transpune prevederile art. 20 al Directivei NIS 2, proiectul nu conţine astfel de reglementări. Transpunerea acestor norme va asigura punerea în aplicare a legii în mod calitativ şi nu declarativ/formal.

9. Totodată, considerăm oportună completarea proiectului cu norme de transpunere a art. 28 al Directivei NIS 2, care prevede că, pentru consolidarea securităţii cibernetice, registrele de nume TLD şi entităţile care prestează servicii de înregistrare a numelor de domenii sunt obligate să colecteze şi să menţină date exacte şi complete privind înregistrarea numelor de domenii într-o bază de date, iar baza de date să conţină informaţiile necesare pentru identificarea şi contactarea titularilor numelor de domenii.

Respectiv, entităţile care prestează servicii de înregistrare a numelor de domenii se obligă să implementeze politici şi proceduri, inclusiv de verificare, care să asigure că baza de date conţine informaţii exacte şi complete.

Suplimentar, Serviciul consideră imperativ de a transpune în proiect, prevederile articolului menţionat, din considerentul că aceasta va permite identificarea actorilor ce au o activitate malițioasă sau identificarea posesorilor de resurse din Internet ale căror pagini web au fost compromise şi reprezintă o ameninţare de securitate.

Alexandru MUSTEAŢA
Director

Digitally signed by Musteaţa Alexandru
Date: 2023.03.06 12:50:21 EET
Reason: MoldSign Signature
Location: Moldova

Banca Națională a Moldovei

Nr. 31-002/20/703 03.03.2023

Ministerul Economiei al Republicii Moldova
Piața Marii Adunări Naționale, nr. 1
MD-2012, mun. Chișinău

Cu referire la proiectul de hotărâre privind aprobarea proiectului de lege privind securitatea cibernetică *(număr unic 41/ME/2023)*, remis spre avizare repetată prin scrisoarea Ministerului Economiei al Republicii Moldova nr. 07-519 din 27.02.2023, Banca Națională a Moldovei, în limitele competenței sale, reiterează îngrijorările și propunerile enunțate în scrisoarea nr. 31-002/12/431 din 08.02.2023.

În special, atenționăm că, în cazul în care autoritățile publice autonome, responsabile față de Parlament, vor fi incluse în lista de subiecți ai proiectului de lege, acestora nu urmează a le fi aplicabile dispozițiile proiectului de lege cu privire la, cel puțin, supravegherea continuă prin efectuare de controale pe teren, răspunderea furnizorilor de servicii conform capitolului V, inclusiv, sancționarea contravențională a acestora de către autoritate competentă, aplicarea actelor cu caracter obligatoriu emise de către autoritatea competentă, implicarea directă a acesteia în soluționarea incidentelor cibernetice și alte prevederi care ar conduce la imixtiuni în activitatea acestora.

Astfel, înțelegem că proiectul de lege nu se va aplica Băncii Naționale a Moldovei, care dispune de autonomie (care urmează a fi menținută și consolidată, inclusiv în virtutea angajamentelor asumate de Republica Moldova prin Acordul de Asociere RM-UE), inclusiv cu referire la gestionarea crizelor în domeniul securității cibernetice, stabilirea mecanismelor proprii de asigurare a securității cibernetice - mecanisme, care sunt aplicate și în prezent. Pentru a evita orice echivoc, propunem completarea proiectului de lege cu o prevedere care exceptează expres Banca Națională a Moldovei de la dispozițiile proiectului de lege.

Cu respect,

Digitally signed by Armaşu Octavian
Date: 2023.03.03 19:14:04 EET
Reason: MoldSign Signature
Location: Moldova

Octavian ARMAȘU
Guvernator

Adresa: Bulevardul Grigore Vieru nr. 1,MD-2005, Chișinău, Republica Moldova
Tel: (+373) 22 822 606, Fax: (+373) 22 220 591, email: official@bnm.md, web: www.bnm.md