Secţiunea 1:
Titlul proiectului de act normativ

HOTĂRÂRE

pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative

Secţiunea a 2-a:
Motivul emiterii actului normativ

2.1 Sursa proiectului de act normativ

Proiectul de hotărâre a Guvernului a fost iniţiat în temeiul prevederilor art. 25 alin. (1) şi ale art. 52 alin. (5) din *Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative.*

Ministerul Cercetării Inovării şi Digitalizării, denumit în continare MCID, a iniţiat *Legea nr. 58/2023*, în calitate de coordonator de reformă pe Componenta C7 - Transformare digitală, din Programul Naţional de Redresare şi Reziliență, prevederilor Anexei la *Ordonanţa de Urgenţă a Guvernului nr. 124/2021 privind stabilirea cadrului instituţional şi financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare şi reziliență, precum şi pentru modificarea şi completarea Ordonanţei de urgenţă a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului naţional de redresare şi reziliență necesar României pentru accesarea de fonduri externe rambursabile şi nerambursabile în cadrul Mecanismului de redresare şi reziliență, cu modificările şi completările ulterioare*coroborat cu Acordul de finanţare dintre Ministerul Investiţiilor şi Proiectelor Europene şi MCID: Reforma 3 privind Asigurarea securităţii cibernetice a entităţilor publice şi private care deţin infrastructuri cu valenţe critice, Jalonul 151 privind intrarea în vigoare a Legii privind apărarea şi securitatea cibernetică a României.

De asemenea, proiectul de hotărâre a Guvernului este iniţiat de Ministerul Cercetării Inovării şi Digitalizării, în calitatea sa de autoritate de stat în domeniul securităţii cibernetice, conform prevederilor art. 1 alin. (3) şi ale art. 4 alin. (1) din *Hotărârea Guvernului nr. 371/2021 privind organizarea şi funcţionarea Ministerului Cercetării, Inovării şi Digitalizării*, cu modificările şi completările ulterioare.

2.2 Descrierea situaţiei actuale

Securitatea cibernetică reprezintă o provocare globală în creştere, iar ameninţările, riscurile sau vulnerabilităţile la adresa reţelelor şi sistemelor informatice constituie o problemă serioasă, cu un impact major asupra securităţii naţionale şi a activităţilor economice.

Legea nr. 58/2023 a reprezentat un pas important în reglementarea acestui domeniu, stabilind cadrul juridic de funcţionare a furnizorilor de servicii tehnice de securitate cibernetică şi obligaţiile acestora de a furniza date şi informaţii privind incidentele cibernetice, ameninţările, riscurile sau vulnerabilităţile la adresa reţelelor şi sistemelor informatice.

Astfel, art. 25 din *Legea nr. 58/2023* prevede următoarele: *„(1) Furnizorii de servicii tehnice de securitate cibernetică au obligația de a pune la dispoziția autorităților prevăzute la art. 10, la cererea motivată a acestora, în termen de maximum 48 de ore de la data primirii solicitării, date și informații privind incidente, respectiv, în maximum 5 zile de la data primirii solicitării, cu privire la amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau un sistem informatic dintre cele prevăzute la art. 3 alin. (1), precum și interconectarea acestora cu terții și cu utilizatorii finali. (2) Datele și informațiile prevăzute la alin. (1) nu vizează, prin scopul solicitării, date cu caracter personal și date de conținut. (3) Datele și informațiile prevăzute la alin. (1) se transmit în scris, prin mijloace electronice sau prin orice altă modalitate stabilită de comun acord, în formatul și structura conforme raportării de incidente cibernetice în PNRISC, prevăzute la art. 22."*

De asemenea, art. 52 alin. (5) din Legea nr. 58/2023 prevede următoarele: *„(5)Normele metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) se stabilesc prin hotărâre a Guvernului, inițiată de MCID, adoptată în maximum 90 de zile de la data intrării în vigoare a prezentei legi."*

Curtea Constituțională a României, în Decizia nr. 70/2023 referitoare la respingerea obiecțiilor de neconstituționalitate a dispozițiilor art. 3 alin. (1) lit. c), art. 21 alin. (1), art. 22, art. 25, art. 41, art. 48 și art. 50 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, a stabilit următoarele repere jurisprudențiale în ceea ce privește aprobarea normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023, astfel:

- paragr. 84: *„Mai mult, analizând dispozițiile legale mai sus invocate, Curtea reține că sistemele de notificare prevăzute la art. 21, art. 22, respectiv la art. 25 din legea criticată nu presupun colectarea de date de conținut și nici extragerea unilaterală și fără autorizare de date și informații de pe un sistem informatic, iar autoritățile care gestionează incidentele de securitate cibernetică semnalate sunt atât operatori de date cu caracter personal (prin efectul legislației privind datele cu caracter personal), cât și autorități cu atribuții expres prevăzute în domeniul securității cibernetice (atribuțiile acestora neputând fi confundate sau suprapuse cu cele ale organelor judiciare care realizează perchezițiile informatice, conform art. 168 din Codul de procedură penală). Prin urmare, obligațiile care revin subiectelor de drept prevăzute la art. 3 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative nu se referă nici la stocarea de date cu caracter personal ale cetățenilor, nici la accesul, în lipsa unui mandat judecătoresc, într-un sistem informatic și nici la alte proceduri intruzive în viața privată a cetățeanului*";
- paragr. 92: *„dispozițiile legale mai sus invocate trebuie interpretate în coroborare cu prevederile art. 27 lit. b) din Legea nr. 362/2018, care prevăd în sarcina operatorilor de servicii esențiale (OSE) și a furnizorilor de servicii digitale (FSD) obligația de a furniza informații suplimentare cu privire la incidentele de securitate cibernetică, Directoratul Național de Securitate Cibernetică putând solicita informații suplimentare operatorului sau furnizorului autor al notificării, în vederea îndeplinirii obligațiilor ce îi revin, cu menționarea termenului în care informațiile solicitate trebuie furnizate, dar și cu dispozițiile secțiunii 2 "Notificarea incidentelor de securitate" a capitolului IV "Asigurarea securității rețelelor și sistemelor informatice" al aceleiași legi, care prevăd la art. 26 alin. (3) și (4) că notificarea incidentelor conține, în mod obligatoriu, următoarele informații: elementele de identificare ale infrastructurii și operatorului sau furnizorului în cauză; descrierea incidentului; perioada de desfășurare a incidentului; impactul estimat al incidentului; măsuri preliminare adoptate; lista de autorități ale statului afectate de incident; întinderea geografică potențială a incidentului; date despre*

efecte potențial transfrontaliere ale incidentului și, de asemenea, că notificarea prevăzută la alin. (1) și (2) ale art. 26 nu va conține informații clasificate și date care pot aduce atingere drepturilor și libertăților cetățenești ori intereselor legitime ale unor terțe entități implicate în incident, în condițiile legii.";

- paragr. 93: „*obligațiile reglementate prin art. 25 alin. (1) (...) au ca obiect operațiuni strict tehnice de natură a asigura prestarea serviciilor la care fac referire dispozițiile art. 3 din legea criticată, într-un climat de securitate cibernetică. Mai mult, alin. (2) al art. 25 din legea criticată prevede că datele și informațiile mai sus analizate nu vizează, prin scopul solicitării, date cu caracter personal și date de conținut. Totodată, obligațiile prevăzute la art. 25 alin. (1) din legea criticată vor fi îndeplinite cu respectarea prevederilor capitolului IX al aceleiași legi, referitoare la confidențialitatea și protecția securității datelor și informațiilor persoanelor fizice și juridice analizate anterior*";
- paragr. 94: „*stabilește în sarcina furnizorilor de servicii tehnice de securitate cibernetică doar obligații cu caracter tehnic, menite să asigure descoperirea și sancționarea în timp util a incidentelor, amenințărilor, riscurilor sau vulnerabilităților de securitate cibernetică, obligații care exclud furnizarea către autoritățile prevăzute la art. 10 din legea criticată a unor date cu caracter personal sau a unor date de conținut*";
- paragr. 96:„*Curtea constată că art. 25 din legea supusă controlului de constituționalitate reglementează obligații ce au ca finalitate descoperirea unor faptele de natură ilicită, lato sensu. Aceste aspecte nu exclud însă obligația furnizorilor de servicii tehnice de securitate cibernetică de a sesiza organele de urmărire penală, în ipoteza în care constată comiterea unor fapte prevăzute de legea penală, precum cele incriminate în cuprinsul capitolului VI, intitulat "Infracțiuni contra siguranței și integrității sistemelor și datelor informatice" al titlului VII "Infracțiuni contra siguranței publice" din Partea specială a Codului penal, obligație ce rezultă din prevederile art. 267 din Codul penal ce reglementează omisiunea sesizării.*";
- paragr. 112: „*Cu privire la elementul constitutiv al contravenției prevăzute la art. 48 alin. (1) lit. c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, acesta constă în faptele de nerespectare de către furnizorii de servicii de securitate cibernetică a obligației de a pune la dispoziția autorităților prevăzute la art. 10 din aceeași lege a datelor și informațiilor privind incidente, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau un sistem informatic al deținătorului sau al unor terți, în condițiile prevăzute de lege și cu respectarea termenului reglementat la art. 25 alin. (1) din actul normativ criticat. Referitor la contravenția anterior menționată, Curtea constată că actul de punere la dispoziție a datelor și informațiilor prevăzute în ipoteza normei ce reglementează această contravenție se realizează, pe de o parte, în condițiile art. 25 alin. (1) din legea criticată - în ceea ce privește termenele de notificare a incidentelor și, respectiv, de comunicare a amenințărilor, a riscurilor și a vulnerabilităților - iar, pe de altă parte, în condițiile art. 52 alin. (5) din aceeași lege - dispoziție ce face trimitere la hotărârea Guvernului care urmează să prevadă normele metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din legea criticată. Așadar, conduita sancționată prin dispozițiile art. 48 alin. (1) lit. c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative constă în necomunicarea, respectiv nepunerea la dispoziția autorităților prevăzute la art. 10 din legea criticată a incidentelor și, respectiv, a amenințărilor, riscurilor și vulnerabilităților, în termenele prevăzute la art. 25 alin. (1) din legea analizată, în condițiile ce vor fi prevăzute prin hotărâre a Guvernului*";

Totodată, 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) nr. 910/2014 şi a Directivei (UE) 2018/1972 şi de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), care va fi transpusă în legislaţia naţională şi de România, până la 17 octombrie 2024, scoate în evidenţă necesitatea şi obligativitatea schimbului de informaţii tehnice necesare în tratarea riscurilor care decurg din ameninţările cibernetice, astfel:

> *"(85) Abordarea riscurilor care decurg din lanţul de aprovizionare al unei entităţi şi din relaţia acesteia cu furnizorii săi, cum ar fi furnizorii de servicii de stocare şi de prelucrare de date sau furnizorii de servicii de securitate gestionate şi editorii de software, este deosebit de importantă, având în vedere prevalenţa incidentelor în care entităţile au fost victime ale atacurilor cibernetice şi în care actori răuvoitori au fost în măsură să compromită securitatea reţelelor şi a sistemelor informatice ale unei entităţi prin exploatarea vulnerabilităţilor care afectează produsele şi serviciile unei părţi terţe.*
>
> *(119) Ameninţările cibernetice devenind tot mai complexe şi mai sofisticate, eficacitatea măsurilor de detectare a unor astfel de ameninţări şi prevenirea lor depinde în mare măsură de schimbul regulat de informaţii privind ameninţările şi vulnerabilităţile care are loc între entităţi. Schimbul de informaţii contribuie la creşterea gradului de sensibilizare cu privire la ameninţările cibernetice, ceea ce, la rândul său, consolidează capacitatea entităţilor de a preveni materializarea unor astfel de ameninţări în incidente şi le permite entităţilor să controleze mai bine efectele incidentelor şi să se redreseze mai eficient."*

Cu toate acestea, există o lacună în ceea ce priveşte reglementarea specifică a procedurilor de solicitare şi comunicare a acestor date şi informaţii. În prezent, nu există un mecanism clar şi uniform pentru solicitarea şi comunicarea acestor date şi informaţii, ceea ce poate duce la întârzieri în aplicarea legii, ineficienţe şi riscuri de securitate.

În plus, protecţia datelor cu caracter personal şi respectarea drepturilor fundamentale, precum dreptul la viaţă privată, secretul corespondenţei şi libertatea de exprimare, constituie un aspect central în cadrul oricărei activităţi de procesare a datelor şi informaţiilor.

Lipsa de claritate şi uniformitate în ceea ce priveşte procedurile de solicitare şi comunicare a datelor şi informaţiilor, precum şi de garanţii specifice privind respectarea drepturilor fundamentale, pot duce la incertitudini, posibile încălcări ale legii şi riscuri de securitate.

Experienţa altor state membre ale Uniunii Europene arată că reglementarea clară şi uniformă a acestor proceduri, precum şi stabilirea unor garanţii specifice privind respectarea drepturilor fundamentale, pot contribui semnificativ la eficienţa şi securitatea activităţilor de securitate cibernetică.

Prin urmare, se impune reglementarea unei proceduri clare şi uniforme de solicitare şi comunicare a datelor şi informaţiilor prevăzute la art. 25 alin. (1) din *Legea nr. 58/2023*, precum şi stabilirea unor garanţii specifice privind respectarea drepturilor fundamentale.

Această reglementare va contribui la creşterea eficienţei şi securităţii activităţilor de securitate cibernetică, la asigurarea respectării drepturilor fundamentale şi la consolidarea cadrului juridic de funcţionare a furnizorilor de servicii tehnice de securitate cibernetică. Prin urmare, adoptarea prezentului proiect de hotărâre a Guvernului este necesară şi oportună pentru a aborda aceste probleme, pentru a asigura un cadru clar, uniform şi eficient pentru solicitarea şi comunicarea

datelor şi informaţiilor în domeniul securităţii cibernetice, precum şi pentru a proteja drepturile fundamentale ale persoanelor fizice şi juridice.

2.3 Schimbări preconizate

În contextul evoluţiei tehnologice şi a amplificării ameninţărilor la adresa securităţii cibernetice, este evident că procedurile existente în prezent sunt insuficiente pentru a face faţă provocărilor curente. Prin urmare, este esenţială reglementarea clară şi uniformă a solicitării şi comunicării datelor şi informaţiilor între autorităţile menţionate la art. 10 din *Legea nr. 58/2023* şi furnizorii de servicii tehnice de securitate cibernetică.

Proiectul de hotărâre stabileşte normele metodologice pentru solicitarea şi comunicarea datelor şi informaţiilor relevante pentru securitatea cibernetică şi reprezintă un important pas înainte în implementarea efectivă a *Legii nr. 58/2023*. Prin intermediul acestui proiect, se clarifică procesul de solicitare şi comunicare a datelor şi informaţiilor, se stabilesc criteriile pentru evaluarea gravităţii incidentelor de securitate cibernetică şi se formalizează procesul de notificare a acestora.

Proiectul de hotărâre prevede faptul că solicitarea datelor şi informaţiilor relevante pentru securitatea cibernetică se va realiza de către autorităţile enumerate la art. 10 din *Legea nr. 58/2023*, iar furnizorii de servicii de securitate cibernetică vor avea obligaţia de a răspunde acestor solicitări. Este important de menţionat că solicitarea nu vizează date cu caracter personal sau date de conţinut, ci informaţii strict necesare pentru asigurarea securităţii cibernetice.

Proiectul de hotărâre introduce criterii clare pentru evaluarea gravităţii incidentelor de securitate cibernetică, în funcţie de impactul acestora asupra funcţionării normale a reţelelor şi sistemelor informatice. Acest lucru va permite o abordare mai eficientă şi mai obiectivă în gestionarea incidentelor.

Proiectul de hotărâre formalizează procesul de notificare a incidentelor de securitate cibernetică, stabilind termenele în care acestea trebuie raportate către autorităţile competente. De asemenea, se oferă un cadru clar cu privire la tipul de informaţii care trebuie să fie incluse în aceste notificări.

Punerea în aplicare a acestor norme metodologice va aduce mai multă claritate şi va eficientiza procesul de gestionare a securităţii cibernetice în România. Aceasta va asigura un nivel mai ridicat de protecţie pentru reţelele şi sistemele informatice, va îmbunătăţi capacitatea de răspuns în cazul incidentelor de securitate cibernetică şi va contribui la dezvoltarea unui mediu cibernetic mai sigur pentru toţi utilizatorii.

Proiectul introduce un sistem mai riguros de notificare a incidentelor de securitate, cu termene bine definite şi proceduri clare. Autorităţile vor putea astfel să ia măsuri prompte şi eficiente pentru a contracara ameninţările la securitatea cibernetică, limitând potenţialul daunelor.

Proiectul prevede reguli stricte privind protecţia datelor cu caracter personal şi a secretului corespondenţei. În acest sens, prevederile proiectului vizează asigurarea unui echilibru între nevoia de securitate cibernetică şi respectarea drepturilor fundamentale ale individului. Proiectul reglementează modul de colaborare între autorităţi şi furnizorii de servicii tehnice de securitate cibernetică, bazat pe transparenţă, responsabilitate şi cooperare activă. Astfel, se urmăreşte

crearea unui mediu propice pentru îmbunătățirea constantă a securității cibernetice, promovând un dialog deschis și un schimb de informații rapid și eficient.

În lumina jurisprudenței Curții Constituționale a României, normele metodologice propuse prin proiectul de hotărâre a Guvernului respectă cu strictețe principiile reținute în Decizia nr. 70/2023, corespunzând cu preocuparea pentru protecția datelor personale și respectarea vieții private, conform exigențelor constituționale. Prezentul argument se bazează pe următoarele puncte de vedere:

a) **Colectarea și accesul la date:** În concordanță cu paragr. 84 din cuprinsul Deciziei, normele metodologice clarifică faptul că scopul sistemelor de notificare nu constă în colectarea datelor de conținut, nici în extragerea unilaterală și fără autorizare de date și informații de pe un sistem informatic. Aceste sisteme de notificare se bazează pe comunicarea unor date strict necesare gestionării și contracarării incidentelor de securitate cibernetică, fără a aduce atingere drepturilor și libertăților fundamentale ale cetățenilor.
b) **Respectarea sarcinilor operatorilor:** În concordanță cu paragr. 92 din cuprinsul Deciziei, normele metodologice respectă și întăresc obligațiile care revin operatorilor de servicii esențiale (OSE) și furnizorilor de servicii digitale (FSD) în privința furnizării de informații suplimentare cu privire la incidentele de securitate cibernetică. Acestea subliniază necesitatea furnizării de informații detaliate, dar fără a include date clasificate sau care ar putea aduce atingere drepturilor și libertăților cetățenești ori intereselor legitime ale unor terțe entități.
c) **Operațiuni strict tehnice:** În concordanță cu paragr. 93 din cuprinsul Deciziei, normele metodologice respectă principiul potrivit căruia obligațiile furnizorilor de servicii tehnice de securitate cibernetică sunt strict tehnice și nu au drept scop colectarea datelor cu caracter personal. Aceste obligații sunt menite să asigure un climat de securitate cibernetică, conform prevederilor capitolului IX din *Legea nr. 58/2023*, referitoare la confidențialitatea și protecția securității datelor și informațiilor persoanelor fizice și juridice.
d) **Respectarea legii penale:** În concordanță cu paragr. 96 din cuprinsul Deciziei, normele metodologice confirmă faptul că furnizorii de servicii tehnice de securitate cibernetică au obligația de a sesiza organele de urmărire penală, în cazul în care constată comiterea unor fapte prevăzute de legea penală.
e) **Sancțiuni pentru neconformitate**: În concordanță cu paragr. 112 din cuprinsul Deciziei, normele metodologice clarifică și stabilesc obligațiile furnizorilor de servicii de securitate cibernetică și consecințele juridice ale nerespectării acestor obligații. Mai exact, acestea evidențiază faptul că nerespectarea obligațiilor prevăzute la art. 25 alin. (1) din *Legea nr. 58/2023*, de către furnizorii de servicii de securitate cibernetică, poate duce la sancțiuni. Aceste obligații presupun comunicarea în timp util a datelor și informațiilor relevante privind incidente, amenințări, riscuri sau vulnerabilități care pot afecta o rețea sau un sistem informatic.
f) **Respectarea termenelor și a condițiilor legale:** În concordanță cu paragr. 112, normele metodologice precizează că furnizorii de servicii de securitate cibernetică trebuie să respecte termenele de notificare și comunicare stabilite prin lege, precum și condițiile ce vor fi stabilite prin hotărârea de guvern, pentru a evita sancțiunile. Acest lucru subliniază respectul pentru reglementările legale și înțelegerea importanței securității cibernetice în societatea contemporană.

2.4 Alte informații *)

Nu este cazul

Secțiunea a 3-a:
Impactul socioeconomic **)

3.1 Descrierea generală a beneficiilor și costurilor estimate ca urmare a intrării în vigoare a actului normativ

O implementare corectă și eficientă a noilor norme va conduce la o protecție sporită a sistemelor cibernetice, diminuând riscul de incidente de securitate. Acest lucru va aduce beneficii la nivelul societății, prin protejarea datelor și informațiilor cetățenilor, și la nivelul economiei, prin protejarea infrastructurilor critice. Normele metodologice aduc claritate în procesul de solicitare și comunicare a datelor și informațiilor relevante pentru securitatea cibernetică, făcându-l mai previzibil pentru toți actorii implicați. Prin stabilirea unui proces clar de notificare a incidentelor de securitate cibernetică, autoritățile vor fi capabile să răspundă mai rapid și mai eficient în cazul unor astfel de incidente.

Implementarea noilor norme va implica costuri administrative, deoarece furnizorii de servicii de securitate cibernetică vor trebui să se adapteze la noile reguli, să pregătească proceduri interne și să instruiască personalul. Autoritățile vor trebui, de asemenea, să își ajusteze procedurile de gestionare a incidentelor de securitate cibernetică. Furnizorii de servicii de securitate cibernetică vor trebui să îndeplinească obligațiile prevăzute de noile norme, ceea ce ar putea implica investiții în infrastructura tehnologică sau în resurse umane.

În concluzie, deși există costuri asociate cu implementarea acestui act normativ, beneficiile în ceea ce privește protecția sporită a securității cibernetice, claritatea procedurilor și reacția eficientă în fața incidentelor de securitate cibernetică par să justifice aceste costuri. În plus, pe termen lung, acest act normativ ar putea conduce la economii, prin prevenirea unor incidente costisitoare de securitate cibernetică.

3.2 Impactul social

În evaluarea impactului social pozitiv al proiectului de hotărâre a Guvernului, trebuie luat în considerare faptul că securitatea cibernetică este relevantă atât pentru mediul de afaceri și instituțiile guvernamentale, cât și pentru viața de zi cu zi a cetățenilor.

Apropierea neîntreruptă de digitalizare a societății face ca oamenii să devină tot mai dependenți de tehnologie pentru efectuarea sarcinilor de bază, cum ar fi cumpărăturile, plata facturilor, lucrul de la distanță sau interacțiunea cu administrația publică. Prin urmare, siguranța mediului cibernetic este crucială pentru a asigura o funcționare normală a vieții de zi cu zi. Implementare proiectului de hotărâre a Guvernului va contribui la crearea unui mediu cibernetic mai sigur, reducând riscul de incidente care ar putea perturba aceste activități.

Pe de altă parte, proiectul de hotărâre a Guvernului ar putea avea un impact pozitiv asupra protecției datelor personale ale cetățenilor. În era digitală, protecția datelor a devenit o preocupare majoră pentru societate, în contextul în care incidentele de securitate cibernetică pot duce la scurgeri de date personale cu consecințe grave. Prin crearea unui mediu mai sigur și prin instituirea unui proces clar de notificare a incidentelor, proiectul de hotărâre va contribui la protecția datelor personale ale cetățenilor, sporind încrederea acestora în mediul digital.

În plus, proiectul de hotărâre a Guvernului conduce la creșterea gradului de conștientizare cu privire la importanța securității cibernetice în societate. Prin instituirea unor reguli clare și a unui

proces de notificare a incidentelor, acest proiect de hotărâre poate contribui la educarea publicului larg despre riscurile securității cibernetice și despre modalitățile de a le preveni.

În concluzie, proiectul de hotărâre a Guvernului are un impact social pozitiv semnificativ, prin contribuția sa la crearea unui mediu cibernetic mai sigur, la protecția datelor personale și la creșterea gradului de conștientizare cu privire la importanța securității cibernetice.

3.3 Impactul asupra drepturilor și libertăților fundamentale ale omului

Proiectul de hotărâre a Guvernului privind securitatea cibernetică și raportarea incidentelor cibernetice are o serie de implicații potențiale asupra drepturilor și libertăților fundamentale ale omului. Analiza acestei teme necesită un echilibru delicat între nevoia de securitate în spațiul digital și protejarea libertăților fundamentale, cum ar fi dreptul la viață privată și la protecția datelor personale.

Pentru a înțelege acest echilibru, este util să ne referim la jurisprudența națională și internațională existentă, precum și la doctrinele juridice relevante. În cadrul Uniunii Europene, de exemplu, Curtea de Justiție a Uniunii Europene (CJUE) a abordat în mod constant aceste probleme în deciziile sale. În decizia **Digital Rights Ireland din 2014,** CJUE a invalidat Directiva privind retenția datelor din 2006, pe motiv că aceasta încălca drepturile la respectarea vieții private și la protecția datelor personale. Acest caz a pus în evidență necesitatea ca orice măsură de securitate cibernetică să fie proporțională și necesară și să respecte principiul minimizării datelor.

În mod similar, în jurisprudența Curții Europene a Drepturilor Omului (CEDO), se constată o atenție constantă față de aceste probleme. În cazul *Big Brother Watch și alții vs. Regatul Unit,* CEDO a statuat că practicile de supraveghere în masă ale guvernului britanic încălcaseră articolele 8 (dreptul la respectarea vieții private și familiale) și 10 (libertatea de exprimare) din Convenția Europeană a Drepturilor Omului. Aceste hotărâri subliniază că orice reglementare în domeniul securității cibernetice trebuie să se desfășoare într-un cadru care respectă drepturile și libertățile fundamentale.

Evaluarea impactului asupra drepturilor și libertăților fundamentale în contextul securității cibernetice poate fi susținută de precedentele stabilite atât de Curtea Europeană a Drepturilor Omului (CEDO) cât și de Curtea de Justiție a Uniunii Europene (CJUE).

CEDO - Klass și alții împotriva Germaniei, 1978: În acest caz, Curtea a stabilit că interceptarea comunicațiilor nu este în sine incompatibilă cu Convenția Europeană a Drepturilor Omului, atât timp cât există garanții legale adecvate împotriva abuzului. Aceasta a recunoscut necesitatea unui echilibru între dreptul la respectarea vieții private și necesitatea de a proteja securitatea națională.

CEDO - S. și Marper împotriva Regatului Unit, 2008: Aceasta a fost o cauză emblematică privind reținerea datelor. Curtea a decis că reținerea indefinită a datelor biometrice (ADN și amprente) ale persoanelor nevinovate constituie o violare a dreptului la respectarea vieții private. Acest precedent evidențiază necesitatea de a avea reglementări clare și limitări stricte cu privire la reținerea și utilizarea datelor, chiar și în contextul securității naționale.

CJUE - Cauza Digital Rights Ireland, 2014: Aceasta a fost o decizie crucială în care Curtea a invalidat Directiva privind reținerea datelor (2006/24/CE) a Uniunii Europene. Curtea a considerat că directiva a încălcat drepturile la respectarea vieții private și la protecția datelor

personale, deoarece a permis reținerea largă și nediferențiată a datelor. Acest caz subliniază necesitatea de a avea o abordare proporțională și necesară în reglementările de securitate cibernetică.

Toate aceste cazuri indică faptul că securitatea cibernetică și protecția datelor sunt importante, însă măsurile luate în scopul asigurării acestora nu trebuie să încalce drepturile fundamentale. Prin urmare, proiectul de hotărâre a Guvernului încorporează aceste principii și oferă garanții adecvate pentru protejarea drepturilor individuale.

Prin reglementările propuse, proiectul de hotărâre a Guvernului va asigura respectarea acestor principii juridice recunoscute. Acesta prevede măsuri care vizează îmbunătățirea securității cibernetice, dar în același timp respectă drepturile fundamentale ale indivizilor. Procesul de raportare a incidentelor cibernetice este proiectat să fie transparent și responsabil, într-o manieră care respectă dreptul la viață privată și protecția datelor personale. Astfel, proiectul de hotărâre a Guvernului încearcă să echilibreze securitatea cibernetică cu protecția drepturilor fundamentale ale omului, reflectând în mod corespunzător tendințele actuale în jurisprudența națională și internațională.

În plus, pe măsura implementării proiectului, va fi important să se asigure o comunicare deschisă și transparentă cu publicul și cu toate părțile interesate, inclusiv cu industria IT, cu organizațiile din domeniul drepturilor omului și cu societatea civilă, în general. Aceasta va contribui la menținerea încrederii în sistem, iar toți cei implicați vor înțelege scopul și modul de funcționare al acestuia.

În concluzie, proiectul de hotărâre a Guvernului reprezintă un pas important în creșterea securității cibernetice și a conștientizării publicului asupra importanței acesteia. În același timp, se respectă necesitatea unei abordări proporționale și necesare, asigurându-se că sunt luate în considerare drepturile și libertățile fundamentale ale omului.

3.4 Impactul macroeconomic

Într-o eră în care economiile lumii sunt tot mai digitalizate și interconectate, securitatea cibernetică a devenit o componentă crucială a stabilității macroeconomice. Proiectul de hotărâre a Guvernului, prin instituirea unui cadrul normativ riguros pentru protejarea datelor și a informațiilor, are potențialul de a exercita un impact macroeconomic semnificativ.

În primul rând, măsurile de securitate cibernetică cresc încrederea actorilor economici în mediul digital, ceea ce poate stimula investițiile și activitatea economică. Conform unui studiu realizat de Deloitte în 2020, firmele care investesc în securitate cibernetică pot experimenta o creștere a valorii lor de piață cu până la 7%. Această creștere se datorează în mare parte percepției mai bune a investitorilor și a consumatorilor cu privire la securitatea datelor și a informațiilor. Prin urmare, un cadrul normativ solid în domeniul securității cibernetice poate contribui la creșterea generală a economiei.

În al doilea rând, securitatea cibernetică joacă un rol vital în prevenirea și gestionarea riscurilor financiare. Un atac cibernetic poate costa companiile milioane de dolari în pierderi directe și poate avea efecte dăunătoare asupra reputației unei companii. De exemplu, conform raportului Costul unui Atac Cibernetic realizat de Institutul Ponemon, costul mediu al unui atac cibernetic se ridica la 4 milioane de dolari în 2019. Proiectul de hotărâre a Guvernului, prin promovarea

unui ecosistem cibernetic mai sigur, poate contribui la atenuarea acestor riscuri, contribuind astfel la stabilitatea macroeconomică.

În al treilea rând, prin crearea unui cadru normativ pentru securitatea cibernetică, Guvernul poate stimula inovarea și creșterea în sectoarele tehnologiei informației și comunicațiilor. Investițiile în securitatea cibernetică pot duce la crearea de locuri de muncă și la creșterea productivității în sectoarele legate de tehnologia digitală.

În concluzie, securitatea cibernetică nu este doar o chestiune de securitate națională, ci și o componentă vitală a prosperității economice. Proiectul de hotărâre a Guvernului, prin îmbunătățirea securității cibernetice, poate avea un impact pozitiv semnificativ asupra economiei naționale.

3.4.1 Impactul asupra economiei și asupra principalilor indicatori macroeconomici

Securitatea cibernetică și economia digitală sunt împletite într-un mod atât de strâns încât este dificil să discutăm despre una fără cealaltă. Impactul reglementărilor privind securitatea cibernetică asupra economiei și a principalilor indicatori macroeconomici poate fi vizualizat prin intermediul a trei categorii principale: productivitatea economică, creșterea ocupării forței de muncă și stabilitatea financiară.

În ceea ce privește productivitatea, adoptarea măsurilor de securitate cibernetică prin proiectul de hotărâre a Guvernului poate avea un impact semnificativ asupra eficienței economice. În România, contribuția tehnologiei informației și a comunicațiilor (TIC) la PIB a fost de aproximativ 6% în 2022, potrivit Institutului Național de Statistică. Într-un mediu digital sigur, companiile pot explora în continuare tehnologia digitală pentru a-și crește eficiența operațională, ceea ce poate duce la o creștere a productivității generale a economiei.

În plus, securitatea cibernetică poate duce la crearea de noi locuri de muncă. În prezent, sectorul IT din România este unul dintre cele mai dinamice sectoare ale economiei, cu o creștere anuală a ocupării forței de muncă de aproximativ 10%. Implementarea unui cadru legislativ solid în acest domeniu poate încuraja companiile să investească și mai mult în securitatea cibernetică, creând astfel noi oportunități de angajare și contribuind la reducerea ratei șomajului.

De asemenea, în ceea ce privește stabilitatea financiară, securitatea cibernetică este esențială pentru menținerea încrederii în sistemul financiar. Potrivit Băncii Naționale a României, atacurile cibernetice reprezintă una dintre cele mai mari amenințări la adresa stabilității financiare. Prin implementarea reglementărilor propuse de proiectul de hotărâre a Guvernului, se poate reduce riscul de pierderi financiare majore datorate atacurilor cibernetice, protejând astfel stabilitatea financiară și îmbunătățind încrederea în economie.

Concluzionând, prin prisma principalilor indicatori macroeconomici, proiectul de hotărâre a Guvernului va avea un impact pozitiv asupra economiei românești, prin îmbunătățirea productivității, crearea de locuri de muncă și protejarea stabilității financiare.

3.4.2 Impactul asupra mediului concurențial si domeniul ajutoarelor de stat

Nu este cazul.

3.5. Impactul asupra mediului de afaceri

Impactul asupra mediului de afaceri al proiectului de hotărâre a Guvernului care reglementează securitatea cibernetică poate fi considerabil și divers, implicând atât companiile de tehnologie informatică, cât și organizațiile din alte industrii care se bazează pe tehnologia digitală pentru operarea lor de zi cu zi.

În primul rând, securitatea cibernetică este un aspect fundamental al mediului de afaceri modern. Companiile operează într-un peisaj digital tot mai complex, cu o dependență tot mai mare de tehnologie, date și servicii în cloud. În acest context, securitatea cibernetică nu este doar o problemă tehnică, ci și una strategică. Un cadru legislativ robust, așa cum este cel propus de Guvernul României, poate ajuta organizațiile să înțeleagă mai bine riscurile la care se expun și cum să le gestioneze eficient.

Proiectul de hotărâre a Guvernului poate contribui, de asemenea, la crearea unui mediu de afaceri mai sigur pentru companii, ceea ce este esențial pentru încrederea clienților și partenerilor de afaceri. Astfel, se va crea un climat de afaceri mai atractiv pentru investitori, având în vedere importanța crescândă pe care o acordă securitatea cibernetică în deciziile lor de investiții.

În plus, reglementările privind securitatea cibernetică conduc la apariția de noi oportunități de afaceri. Pentru furnizorii de soluții de securitate cibernetică, aceasta vor însemna o creștere a cererii de servicii, deoarece mai multe organizații se străduiesc să respecte noile reglementări. Pentru companiile din alte industrii, aceasta ar putea oferi oportunități pentru a îmbunătăți operațiunile existente sau pentru a crea noi servicii care să profite de avantajele oferite de un mediu digital mai sigur.

În concluzie, proiectul de hotărâre a Guvernului va avea un impact pozitiv asupra mediului de afaceri prin crearea unui climat mai sigur și mai atractiv pentru investitori, îmbunătățirea gestionării riscurilor cibernetice și stimularea apariției de noi oportunități de afaceri.

3.6 Impactul asupra mediului înconjurător

Nu este cazul.

3.7 Evaluarea costurilor și beneficiilor din perspectiva inovării și digitalizării

Implementarea unui cadrul de reglementare robust pentru securitatea cibernetică, așa cum este propus prin proiectul de hotărâre a Guvernului, va avea un impact major asupra inovării și digitalizării în România. Acest impact se poate manifesta într-o serie de moduri, fie că vorbim despre îmbunătățirea încrederii consumatorilor în tehnologie, încurajarea investițiilor în sectorul IT, sau stimularea dezvoltării de noi produse și servicii în domeniul digital.

În privința costurilor, este de așteptat ca implementarea acestui cadru să implice cheltuieli pentru organizații și instituții, în vederea conformării cu noile reguli. Aceste cheltuieli pot consta în costuri pentru achiziția de noi tehnologii de securitate cibernetică, investiții în formarea și pregătirea personalului, sau costuri asociate cu evaluarea și actualizarea constantă a practicilor de securitate cibernetică.

Pe de altă parte, beneficiile propuse de proiect sunt considerabile. Un mediu digital sigur va stimula încrederea consumatorilor și a întreprinderilor de a utiliza și de a investi în tehnologii digitale. Un studiu realizat de Comisia Europeană în 2020 a constatat că încrederea în economia digitală poate avea un impact semnificativ asupra creșterii economice. În plus, măsurile de

securitate cibernetică mai stricte vor încuraja dezvoltarea și adoptarea de noi tehnologii și servicii de securitate, stimulând astfel inovarea în sectorul IT.

Mai mult, în contextul în care digitalizarea este o prioritate la nivel global, acest proiect de hotărâre ar putea plasa România în poziția de lider în materie de securitate cibernetică în regiune. Într-un raport al Băncii Mondiale din 2021, se subliniază că digitalizarea poate stimula productivitatea, creșterea economică și crearea de locuri de muncă.

Crescând nivelul de securitate cibernetică, acest proiect asigură cadrul de reglementare necesar pentru a atrage mai multe investiții în tehnologiile digitale din România, permițând astfel creșterea competitivității și inovației în acest domeniu. Un raport al Organizației pentru Cooperare și Dezvoltare Economică (OCDE) din 2022 a evidențiat că securitatea cibernetică poate influența semnificativ inovația, întrucât aceasta este o condiție prealabilă pentru dezvoltarea și adoptarea de noi tehnologii.

În ceea ce privește costurile, acestea pot fi privite ca o investiție necesară pentru a crea un mediu digital sigur și încrezător, care la rândul său poate genera beneficii economice pe termen lung. Deși costurile inițiale pot fi semnificative, pot fi compensate de beneficiile pe termen lung, inclusiv creșterea încrederii în economia digitală, stimularea investițiilor în sectorul IT și creșterea competitivității economiei românești. În acest sens, un studiu din 2022 al McKinsey Global Institute a arătat că țările care investesc în securitatea cibernetică pot beneficia de un avantaj competitiv semnificativ în economia digitală globală. Acest avantaj poate contribui la creșterea productivității, crearea de noi locuri de muncă și dezvoltarea de noi industrii și servicii în domeniul digital.

Așadar, evaluând costurile și beneficiile din perspectiva inovării și digitalizării, se poate concluziona că acest proiect de hotărâre poate avea un impact pozitiv semnificativ asupra economiei digitale din România. Prin consolidarea securității cibernetice, proiectul poate contribui la stimularea inovării și la creșterea competitivității economiei românești în era digitală.

3.8 Evaluarea costurilor și beneficiilor din perspectiva dezvoltării durabile

Ca aspect al dezvoltării durabile, securitatea cibernetică a devenit un subiect de discuție la nivel global. Într-o lume în care tot mai multe activități se desfășoară în mediul digital, asigurarea unui spațiu cibernetic sigur este esențială pentru atingerea obiectivelor de dezvoltare durabilă. Prin urmare, proiectul de hotărâre poate fi considerat o contribuție semnificativă la dezvoltarea durabilă a României.

În ceea ce privește costurile, acestea pot fi privite ca investiții necesare pentru dezvoltarea durabilă. Asigurarea unui spațiu cibernetic sigur poate necesita resurse semnificative în termen de capital, personal și tehnologie. Cu toate acestea, aceste costuri pot fi considerate o investiție necesară pentru a construi o infrastructură cibernetică robustă care poate rezista la atacuri și perturbări, contribuind astfel la reziliența economică și socială pe termen lung.

Pe de altă parte, beneficiile unui spațiu cibernetic mai sigur sunt multiple și se extind dincolo de sfera economică. În primul rând, securitatea cibernetică poate contribui la protejarea drepturilor și libertăților fundamentale în era digitală, inclusiv dreptul la viață privată și la protecția datelor. În al doilea rând, securitatea cibernetică poate promova incluziunea digitală prin creșterea încrederii utilizatorilor în serviciile digitale. În al treilea rând, un spațiu cibernetic sigur poate

stimula inovarea şi competitivitatea în economia digitală, contribuind astfel la creşterea economică durabilă.

Un studiu publicat în 2022 de World Economic Forum a arătat că ţările care investesc în securitatea cibernetică pot beneficia de o creştere economică mai durabilă, datorită îmbunătăţirii încrederii în serviciile digitale şi a stimulării inovării în economia digitală. Studiul a evidenţiat, de asemenea, că o abordare integrată a securităţii cibernetice, care include participarea tuturor părţilor interesate, poate contribui la crearea unui mediu digital inclusiv şi sigur.

În concluzie, proiectul de hotărâre contribuie semnificativ la dezvoltarea durabilă a României prin consolidarea securităţii cibernetice. În ciuda costurilor iniţiale, beneficiile pe termen lung ale unui spaţiu cibernetic sigur pot fi semnificative şi pot contribui la atingerea obiectivelor de dezvoltare durabilă ale României.

3.9 Alte informaţii

Nu este cazul.

Secţiunea a 4-a

Impactul financiar asupra bugetului general consolidat atât pe termen scurt, pentru anul curent, cât şi pe termen lung (pe 5 ani), inclusiv informaţii cu privire la cheltuieli şi venituri.*)**

- în mii lei (RON) -

Indicatori	Anul curent	Următorii patru ani				Media pe cinci ani
1	2	3	4	5	6	7
4.1 Modificări ale veniturilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta: i. impozit pe profit ii. impozit pe venit						
b) bugete locale i. impozit pe profit						
c) bugetul asigurărilor sociale de stat: i. contribuţii de asigurări						
d) alte tipuri de venituri (se va menţiona natura acestora)						
4.2 Modificări ale cheltuielilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta: i. cheltuieli de personal bunuri şi servicii						
b) bugete locale: i. cheltuieli de personal ii. bunuri şi servicii						

c) bugetul asigurărilor sociale de stat: i. cheltuieli de personal bunuri şi servicii						
d) alte tipuri de cheltuieli (se va menţiona natura acestora)						
4.3 Impact financiar, plus/minus, din care: a) buget de stat						
4.3 Impact financiar, plus/minus, din care: a) buget de stat						
b) bugete locale						
4.4 Propuneri pentru acoperirea creşterii cheltuielilor bugetare						
4.5 Propuneri pentru a compensa reducerea veniturilor bugetare						
4.6 Calcule detaliate privind fundamentarea modificărilor veniturilor şi/sau cheltuielilor bugetare						
4.7 Prezentarea, în cazul proiectelor de acte normative a căror adoptare atrage majorarea cheltuielilor bugetare, a următoarelor documente: a) fişa financiară prevăzută la art.15 din *Legea nr. 500/2002 privind finanţele publice*, cu modificările şi completările ulterioare, însoţită de ipotezele şi metodologia de calcul utilizată; b) declaraţie conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele şi priorităţile strategice specificate în strategia fiscal-bugetară, cu legea bugetară anuală şi cu plafoanele de cheltuieli prezentate în strategia fiscal-bugetară.						
4.8 Alte informaţii						
Secţiunea a 5-a: **Efectele proiectului de act normativ asupra legislaţiei în vigoare**						
5.1 Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ Nu este cazul.						
5.2 Impactul asupra legislaţiei in domeniul achiziţiilor publice Nu este cazul.						
5.3 Conformitatea proiectului de act normativ cu legislaţia UE (în cazul proiectelor ce transpun sau asigură aplicarea unor prevederi de drept UE). Nu este cazul.						
5.3.1 Măsuri normative necesare transpunerii directivelor UE						

Nu este cazul.
5.3.2 Măsuri normative necesare aplicării actelor legislative UE Nu este cazul.
5.4 Hotărâri ale Curții de Justiție a Uniunii Europene Nu este cazul.
5.5 Alte acte normative și/sau documente internaționale din care decurg angajamente asumate Nu este cazul.
5.6. Alte informații Nu este cazul.
Secțiunea a 6-a: **Consultările efectuate în vederea elaborării proiectului de act normativ**
6.1 Informații privind neaplicarea procedurii de participare la elaborarea actelor normative Nu este cazul.
6.2 Informații privind procesul de consultare cu organizații neguvernamentale, institute de cercetare și alte organisme implicate. Nu este cazul.
6.3 Informații despre consultările organizate cu autoritățile administrației publice locale Nu este cazul.
6.4 Informații privind puncte de vedere/opinii emise de organisme consultative constituite prin acte normative Nu este cazul.
6.5 Informații privind avizarea de către: **a)Consiliul Legislativ-** Se solicită avizul Consiliului Legislativ **b)Consiliul Suprem de Apărare a Țării** - Se solicită avizul Consiliului Suprem de Apărare a Țării **c)Consiliul Economic și Social** - Se solicită avizul Consiliului Economic și Social **d)Consiliul Concurenței** **e)Curtea de Conturi**
6.6 Alte informații

Nu este cazul.

Secţiunea a 7-a:
Activităţi de informare publică privind elaborarea şi implementarea proiectului de act normativ

7.1 Informarea societăţii civile cu privire la elaborarea proiectului de act normativ

Pentru proiectul de act normativ a fost îndeplinită procedura stabilită prin dispoziţiile *Legii nr. 52/2003 privind transparenţa decizională în administraţia publică*, republicată.

Necesitatea unui termen de consultare publică mai scurt în cadrul proiectului de hotărâre de guvern în materie de securitate cibernetică se impune, în principal, din cauza situaţiei actuale în domeniul securităţii cibernetice, atât în România, cât şi la nivel global.

În primul rând, trebuie subliniat faptul că ameninţările cibernetice au devenit tot mai prezente şi sofisticate în ultimii ani. Atacurile cibernetice împotriva instituţiilor guvernamentale, companiilor private şi persoanelor cresc în număr şi în intensitate, punând în pericol securitatea naţională, economia şi drepturile şi libertăţile individuale ale cetăţenilor. Acest fapt este bine documentat de numeroase rapoarte naţionale şi internaţionale, inclusiv de către Directoratul Naţional pentru Securitate Cibernetică şi de către Europol.

În al doilea rând, situaţia actuală în materie de securitate cibernetică în România impune adoptarea de soluţii imediate. În prezent, există lacune semnificative în cadrul legislativ şi în capacitatea instituţiilor responsabile de a face faţă ameninţărilor cibernetice. Aceste lacune pot duce la o vulnerabilitate crescută în faţa atacurilor cibernetice, ceea ce poate avea consecinţe grave asupra interesului public.

În acest context, proiectul de hotărâre a Guvernului este menit să răspundă acestor provocări prin stabilirea unui cadru mai solid şi mai eficient pentru gestionarea securităţii cibernetice. Cu toate acestea, având în vedere gravitatea situaţiei şi nevoia urgentă de a răspunde la aceste ameninţări, este necesară adoptarea proiectului într-un termen mai scurt decât cel obişnuit.

Prin urmare, având în vedere situaţia urgentă şi excepţională în materie de securitate cibernetică şi necesitatea adoptării de soluţii imediate pentru a evita o gravă atingere adusă interesului public, proiectul de hotărâre a Guvernului respectă criteriile de excepţie prevăzute la art. 7 alin. (13) Legea nr. 52/2003 şi, în consecinţă, poate fi supus adoptării şi anterior expirării termenului prevăzut de alin. (2).

Prezentul proiect este supus consultării publice potrivit prevederilor art. 7 alin. (13) din Legea nr. 52/2003, termenul de punere în procedura de consultare publică fiind de 10 zile lucrătoare.

7.2 Informarea societăţii civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum şi efectele asupra sănătăţii şi securităţii cetăţenilor sau diversităţii biologice.
Nu este cazul.

Secţiunea a 8-a:
Măsuri privind implementarea, monitorizarea şi evaluarea proiectului de act normativ

8.1 Măsurile de punere în aplicare a proiectului de act normativ

Nu este cazul.
8.2 Alte informaţii Nu este cazul.

Faţă de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Față de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU:
MARIAN NEACȘU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAȚII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAȚII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECȚIE ȘI PAZĂ
LUCIAN-SILVAN PAHONȚU

DIRECTORUL
SERVICIULUI DE INFORMAȚII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAȚIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU ADMINISTRARE ȘI REGLEMENTARE ÎN COMUNICAȚII
VALERIU ȘTEFAN ZGONEA

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANȚELOR
MARCEL-IOAN BOLOȘ

MINISTRUL AFACERILOR EXTERNE
LUMINIȚA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAȚIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIȚIEI
ALINA-ȘTEFANIA GORGHIU

Nu este cazul.
8.2 Alte informaţii Nu este cazul.

Faţă de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Față de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACȘU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAȚII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAȚII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECȚIE ȘI PAZĂ
LUCIAN-SILVAN PAHONȚU

DIRECTORUL
SERVICIULUI DE INFORMAȚII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAȚIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU ADMINISTRARE ȘI REGLEMENTARE ÎN COMUNICAȚII
VALERIU ȘTEFAN ZGONEA

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANȚELOR
MARCEL-IOAN BOLOȘ

MINISTRUL AFACERILOR EXTERNE
LUMINIȚA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAȚIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIȚIEI
ALINA-ȘTEFANIA GORGHIU

Nu este cazul.
8.2 Alte informaţii Nu este cazul.

Faţă de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACŞU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAŢII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAŢII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ
LUCIAN-SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREŞEDINTELE AUTORITĂŢII NAŢIONALE PENTRU ADMINISTRARE ŞI REGLEMENTARE ÎN COMUNICAŢII
VALERIU ŞTEFAN ZGONEA

MINISTRUL INVESTIŢIILOR ŞI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANŢELOR
MARCEL-IOAN BOLOŞ

MINISTRUL AFACERILOR EXTERNE
LUMINIŢA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAŢIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIŢIEI
ALINA-ŞTEFANIA GORGHIU

Nu este cazul.
8.2 Alte informații Nu este cazul.

Față de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Față de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACȘU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAȚII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAȚII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECȚIE ȘI PAZĂ
LUCIAN-SILVAN PAHONȚU

DIRECTORUL
SERVICIULUI DE INFORMAȚII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAȚIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU ADMINISTRARE ȘI REGLEMENTARE ÎN COMUNICAȚII
VALERIU ȘTEFAN ZGONEA

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANȚELOR
MARCEL-IOAN BOLOȘ

MINISTRUL AFACERILOR EXTERNE
LUMINIȚA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAȚIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIȚIEI
ALINA-ȘTEFANIA GORGHIU

Nu este cazul.
8.2 Alte informaţii Nu este cazul.

Faţă de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Față de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACȘU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAȚII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAȚII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECȚIE ȘI PAZĂ
LUCIAN-SILVAN PAȚONȚU

DIRECTORUL
SERVICIULUI DE INFORMAȚII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAȚIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU ADMINISTRARE ȘI REGLEMENTARE ÎN COMUNICAȚII
VALERIU ȘTEFAN ZGONEA

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANȚELOR
MARCEL-IOAN BOLOȘ

MINISTRUL AFACERILOR EXTERNE
LUMINIȚA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAȚIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIȚIEI
ALINA-ȘTEFANIA GORGHIU

Nu este cazul.
8.2 Alte informaţii Nu este cazul.

Faţă de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Față de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACȘU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAȚII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAȚII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECȚIE ȘI PAZĂ
LUCIAN-SILVAN PAHONȚU

DIRECTORUL
SERVICIULUI DE INFORMAȚII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAȚIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU ADMINISTRARE ȘI REGLEMENTARE ÎN COMUNICAȚII
VALERIU ȘTEFAN ZGONEA

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANȚELOR
MARCEL-IOAN BOLOȘ

MINISTRUL AFACERILOR EXTERNE
LUMINIȚA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAȚIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIȚIEI
ALINA-ȘTEFANIA GORGHIU

Nu este cazul.
8.2 Alte informaţii Nu este cazul.

Faţă de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACŞU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAŢII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAŢII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ
LUCIAN-SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREŞEDINTELE AUTORITĂŢII NAŢIONALE PENTRU ADMINISTRARE ŞI REGLEMENTARE ÎN COMUNICAŢII
VALERIU ŞTEFAN ZGONEA

MINISTRUL INVESTIŢIILOR ŞI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANŢELOR
MARCEL-IOAN BOLOŞ

MINISTRUL AFACERILOR EXTERNE
LUMINIŢA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAŢIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIŢIEI
ALINA-ŞTEFANIA GORGHIU

Nu este cazul.
8.2 Alte informații Nu este cazul.

Față de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACŞU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAŢII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAŢII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ
LUCIAN-SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREŞEDINTELE AUTORITĂŢII NAŢIONALE PENTRU ADMINISTRARE ŞI REGLEMENTARE ÎN COMUNICAŢII
VALERIU ŞTEFAN ZGONEA

MINISTRUL INVESTIŢIILOR ŞI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANŢELOR
MARCEL-IOAN BOLOŞ

MINISTRUL AFACERILOR EXTERNE
LUMINIŢA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAŢIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIŢIEI
ALINA-ŞTEFANIA GORGHIU

Nu este cazul.
8.2 Alte informații Nu este cazul.

Față de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

BOGDAN-CRUIA IVAN

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACŞU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAŢII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAŢII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ
LUCIAN-SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREŞEDINTELE AUTORITĂŢII NAŢIONALE PENTRU ADMINISTRARE ŞI REGLEMENTARE ÎN COMUNICAŢII
VALERIU ŞTEFAN ZGONEA

MINISTRUL INVESTIŢIILOR ŞI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANŢELOR
MARCEL-IOAN BOLOŞ

MINISTRUL AFACERILOR EXTERNE
LUMINIŢA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAŢIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIŢIEI
ALINA-ŞTEFANIA GORGHIU

Nu este cazul.
8.2 Alte informații Nu este cazul.

Față de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACŞU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAŢII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAŢII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ
LUCIAN-SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREŞEDINTELE AUTORITĂŢII NAŢIONALE PENTRU ADMINISTRARE ŞI REGLEMENTARE ÎN COMUNICAŢII
VALERIU ŞTEFAN ZGONEA

MINISTRUL INVESTIŢIILOR ŞI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANŢELOR
MARCEL-IOAN BOLOŞ

MINISTRUL AFACERILOR EXTERNE
LUMINIŢA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAŢIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIŢIEI
ALINA-ŞTEFANIA GORGHIU

Nu este cazul.
8.2 Alte informaţii Nu este cazul.

Faţă de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACŞU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAŢII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAŢII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ
LUCIAN-SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREŞEDINTELE AUTORITĂŢII NAŢIONALE PENTRU ADMINISTRARE ŞI REGLEMENTARE ÎN COMUNICAŢII
VALERIU ŞTEFAN ZGONEA

MINISTRUL INVESTIŢIILOR ŞI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANŢELOR
MARCEL-IOAN BOLOŞ

MINISTRUL AFACERILOR EXTERNE
LUMINIŢA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAŢIONALE
ANGEL TÎLVAR

MINISTRUL JUSTIŢIEI
ALINA-ŞTEFANIA GORGHIU

Față de cele prezentate mai sus, a fost elaborat proiectul de Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

VICEPRIM-MINISTRU
MARIAN NEACȘU

VICEPRIM-MINISTRU,
MINISTRUL AFACERILOR INTERNE
MARIAN-CĂTĂLIN PREDOIU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAȚII SPECIALE
IONEL SORIN BĂLAN

p. DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAȚII
RĂZVAN IONESCU

DIRECTORUL
SERVICIULUI DE PROTECȚIE ȘI PAZĂ
LUCIAN-SILVAN PAHONȚU

DIRECTORUL
SERVICIULUI DE INFORMAȚII EXTERNE
GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAȚIONAL AL INFORMAȚIILOR SECRETE DE STAT
MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAȚIONAL DE SECURITATE CIBERNETICĂ
DAN CÎMPEAN

PREȘEDINTELE AUTORITĂȚII NAȚIONALE PENTRU ADMINISTRARE ȘI REGLEMENTARE ÎN COMUNICAȚII
VALERIU ȘTEFAN ZGONEA

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE
ADRIAN CÂCIU

MINISTRUL FINANȚELOR
MARCEL-IOAN BOLOȘ

MINISTRUL AFACERILOR EXTERNE
LUMINIȚA-TEODORA ODOBESCU

MINISTRUL APĂRĂRII NAȚIONALE
ANGEL TÎLVĂR

MINISTRUL JUSTIȚIEI
ALINA-ȘTEFANIA GORGHIU

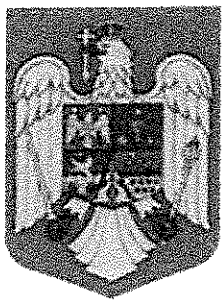
Nu este cazul.
8.2 Alte informaţii Nu este cazul.

Faţă de cele prezentate mai sus, a fost elaborat proiectul de *Hotărâre a Guvernului pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative*, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

BOGDAN-GRUIA IVAN

GUVERNUL ROMÂNIEI



HOTĂRÂRE

pentru aprobarea Normelor metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative

În temeiul art. 108 din Constituţia României, republicată, precum şi al art. 25 alin. (1) şi al art. 52 alin. (5) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative,

Guvernul României adoptă prezenta hotărâre.

Articol unic –Se aprobă Normele metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, prevăzute în anexa care face parte integrantă din prezenta hotărâre.

PRIM-MINISTRU
ION-MARCEL CIOLACU

ANEXĂ

NORME METODOLOGICE

privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative

Art. 1. - Prezentele Norme metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023 privind securitatea şi apărarea cibernetică a României, precum şi pentru modificarea şi completarea unor acte normative, denumite în continuare Norme metodologice, au ca obiect stabilirea modului de îndeplinire a obligaţiilor ce le revin autorităţilor prevăzute la art. 10 din Legea nr. 58/2023 şi furnizorilor de servicii tehnice de securitate cibernetică în procesul de solicitare şi comunicare de date şi informaţii privind incidente, respectiv privind ameninţări, riscuri sau vulnerabilităţi a căror manifestare poate afecta o reţea sau un sistem informatic dintre cele prevăzute la art. 3 alin. (1) din Legea nr. 58/2023, precum şi interconectarea acestora cu terţii şi cu utilizatorii finali.

Art. 2. – **(1)** În vederea asigurării rezilienţei şi protecţiei reţelelor şi sistemelor informatice ce susţin funcţiile de apărare, securitate naţională, ordine publică şi guvernare, precum şi pentru asigurarea unei reacţii rapide şi eficiente la ameninţările provenite din spaţiul cibernetic naţional, autorităţile competente stabilite la art. 10 alin. (1) din Legea nr. 58/2023, în îndeplinirea responsabilităţilor acestora în domeniile securităţii şi apărării cibernetice, pot solicita furnizorilor de servicii tehnice de securitate cibernetică, prin cerere motivată, date şi informaţii privind incidente de securitate cibernetică, ameninţări, riscuri sau vulnerabilităţi, a căror manifestare poate afecta cel puţin o reţea sau un sistem informatic dintre cele prevăzute la art. 3 alin. (1), precum şi interconectarea acestora cu terţii şi cu utilizatorii finali.

(2) Cererea prevăzută la alin. (1) este transmisă prin oricare dintre următoarele mijloace de comunicare la distanţă, dacă asigură primirea acesteia de către destinatar, astfel:

a) prin poştă, cu scrisoare recomandată, cu confirmare de primire, în plic închis, la care se ataşează dovada de primire/procesul-verbal;

b) prin afişare la domiciliul sau la sediul furnizorului de servicii tehnice de securitate cibernetică, activitate care se consemnează într-un proces-verbal, semnat de cel puţin un martor;

c) prin telefon mobil, telefax, fax, poştă electronică sau prin alte mijloace ce asigură transmiterea textului cererii şi confirmarea primirii acestuia, dacă furnizorul de servicii tehnice de securitate cibernetică a indicat, în prealabil, autorităţii prevăzute la art. 10 din Legea nr. 58/2023, care formulează cererea, datele corespunzătoare în acest scop;

d) prin Platforma naţională pentru raportarea incidentelor de securitate cibernetică, denumită în continuare PNRISC, dacă furnizorul de servicii tehnice de securitate cibernetică este în prealabil interconectat la aceasta;

e) prin platforma de contact pusă la dispoziţie de către autoritatea prevăzută la art.10 din Legea nr. 58/2023 care formulează cererea şi la care furnizorul de servicii tehnice de securitate cibernetică este în prealabil interconectat;

(3) Cererile formulate prin mijloacele prevăzute la alin. (2) lit. a) şi b) se consideră comunicate la momentul datei prevăzute în dovada de primire, respectiv în procesul-verbal.

(4) Cererile formulate prin mijloacele prevăzute la alin. (2) lit. c)-e) se consideră comunicate la momentul la care au primit mesaj din partea sistemului folosit că au ajuns la destinatar, potrivit datelor furnizate de acesta.

(5) Dacă comunicarea prin mijloacele prevăzute la alin. (2) lit. c)-e) nu este posibilă din cauza lipsei datelor în acest sens sau sistemul folosit indică eroare în transmitere, cererea se va comunica potrivit prevederilor alin. (2) lit a) sau b).

Art. 3. - În termen de maximum 48 de ore de la primirea cererii cu privire la incidente de securitate cibernetică, potrivit prevederilor art. 2, furnizorii de servicii tehnice de securitate cibernetică transmit autorității solicitante, în scris, prin mijloace electronice sau prin orice altă modalitate stabilită, în prealabil, de comun acord, în formatul şi structura conforme raportării în PNRISC, un răspuns care să cuprindă cel puțin următoarele elemente:

a) data, ora, minutul descoperirii incidentului;

b) serviciile şi/sau rețelele care sunt afectate de incident;

c) estimarea ariei geografice afectate, precum şi a efectelor incidentului asupra furnizării oricărei rețele sau oricărui sistem informatic dintre cele prevăzute la art. 3 alin. (1) din Legea nr. 58/2023, precum şi interconectarea acestora cu terții şi cu utilizatorii finali;

d) datele şi informațiile privind cauza/cauzele care a/au provocat incidentul;

e) estimarea graficului de restabilire a funcționării rețelelor şi sistemelor informatice care fac parte dintre cele prevăzute la art. 3 alin. (1) din Legea nr. 58/2023, precum şi interconectarea acestora cu terții şi cu utilizatorii finali, respectiv estimarea revenirii furnizării serviciilor în parametrii normali de funcționare;

f) îndrumările oferite utilizatorilor şi acțiunile întreprinse de furnizorii de servicii tehnice de securitate cibernetică în vederea minimizării efectelor incidentului, dacă este cazul;

g) informațiile oferite publicului cu privire la existența unui incident, modalitatea de comunicare, data şi ora la care au fost comunicate informațiile, dacă acest lucru s-a întâmplat;

h) datele de contact – nume, prenume, număr de telefon, număr de fax, adresă de poştă electronică - ale persoanei/persoanelor care poate/pot da mai multe informații privind incidentul.

Art. 4. – (1) În termen de maximum 5 zile de la primirea unei cereri cu privire la amenințări, riscuri sau vulnerabilități, potrivit prevederilor art. 2, furnizorii de servicii tehnice de securitate cibernetică transmit autorității solicitante, în scris, prin mijloace electronice sau prin orice altă modalitate stabilită, în prealabil, de comun acord, un răspuns care să cuprindă cel puțin următoarele elemente:

a) date ce pot ajuta la identificarea vectorului de amenințare sau atac cibernetic;

b) scopul şi/sau motivația vectorului de amenințare sau atac cibernetic;

c) date care pot ajuta la contextualizarea şi descrierea incidentului vizat de vectorul de amenințare sau atac;

d) tehnici, tactici şi proceduri utilizate pentru activități nelegitime;

e) indicatori tehnici ai activităților nelegitime derulate de vectori de amenințare sau atac cibernetic sau celor aferente derulării incidentului, identificați în rețelele și sistemele informatice;
f) date și informații ce pot ajuta în evaluarea și cuantificarea impactului incidentului vizat sau potențialul impact al riscului;
g) soluții hardware și software ce pot fi afectate;
h) vulnerabilități identificate, date și informații cu privire la categorii de victime și entități vizate sau potențial afectate.

(2) Datele și informațiile prevăzute la alin. (1) sunt folosite exclusiv în vederea și în scopul asigurării securității și apărării cibernetice la nivel național, în conformitate cu atribuțiile specifice ale autorităților competente prevăzute la art. 10 alin. (1) din Legea nr. 58/2023.

Art. 5. – (1) În vederea stabilirii mijloacelor și metodelor de transmitere a datelor și informațiilor prevăzute la art. 3 și art. 4, furnizorii de servicii tehnice de securitate cibernetică și autoritățile prevăzute la art. 10 din Legea nr. 58/2023 vor utiliza unul dintre mijloacele de comunicare prevăzute la art. 2 alin. (2).

(2) În cazul imposibilității stabilirii de comun acord și prealabil, independent de culpa vreuneia dintre părți, a unuia dintre mijloacele și metodele de comunicare prevăzute la alin. (1), furnizorii de servicii tehnice de securitate cibernetică au obligația transmiterii datelor și informațiilor prin orice mijloc de comunicare care permite transmiterea, precum și confirmarea primirii acestora de către autoritățile solicitante, în termenele prevăzute la art. 3 și art. 4.

(3) În procesul de transmitere a datelor și informațiilor solicitate, se vor utiliza modalități tehnice adecvate, care să asigure confidențialitatea, integritatea, autenticitatea și non-repudierea datelor și informațiilor transmise.