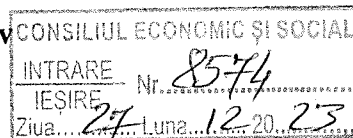


**Secțiunea 1:**  
**Titlul proiectului de act normativ**



**HOTĂRÂRE**

**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**

**Secțiunea a 2-a:**  
**Motivul emiterii actului normativ**

**2.1 Sursa proiectului de act normativ**

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

Ministerul Cercetării Inovării și Digitalizării, denumit în continuare MCID, a inițiat *Legea nr. 58/2023*, în calitate de coordonator de reformă pe Componenta C7 - Transformare digitală, din Programul Național de Redresare și Reziliență, prevederilor Anexei la *Ordonanța de Urgență a Guvernului nr. 124/2021 privind stabilirea cadrului instituțional și financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare și reziliență, precum și pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului național de redresare și reziliență necesar României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de redresare și reziliență, cu modificările și completările ulterioare* coroborat cu Acordul de finanțare dintre Ministerul Investițiilor și Proiectelor Europene și MCID: Reforma 3 privind Asigurarea securității cibernetice a entităților publice și private care dețin infrastructuri cu valențe critice, Jalonul 151 privind intrarea în vigoare a Legii privind apărarea și securitatea cibernetică a României.

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

**2.2 Descrierea situației actuale**

Securitatea cibernetică reprezintă o provocare globală în creștere, iar amenințările, riscurile sau vulnerabilitățile la adresa rețelelor și sistemelor informatice constituie o problemă serioasă, cu un impact major asupra securității naționale și a activităților economice.

*Legea nr. 58/2023* a reprezentat un pas important în reglementarea acestui domeniu, stabilind cadrul juridic de funcționare a furnizorilor de servicii tehnice de securitate cibernetică și obligațiile acestora de a furniza date și informații privind incidentele cibernetice, amenințările, riscurile sau vulnerabilitățile la adresa rețelelor și 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 cibernetică 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 cibernetică (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 fapte 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 "Infrațiuni contra siguranței și integrității sistemelor și datelor informatice" al titlului VII "Infrațiuni 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 și a Directivei (UE) 2018/1772 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), care va fi transpusă în legislația națională și de România, până la 17 octombrie 2024, scoate în evidență necesitatea și obligativitatea schimbului de informații tehnice necesare în tratarea riscurilor care decurg din amenințările cibernetice, astfel:

*”(85) Abordarea riscurilor care decurg din lanțul de aprovizionare al unei entități și din relația acesteia cu furnizorii săi, cum ar fi furnizorii de servicii de stocare și de prelucrare de date sau furnizorii de servicii de securitate gestionate și editorii de software, este deosebit de importantă, având în vedere prevalența incidentelor în care entitățile au fost victime ale atacurilor cibernetice și în care actori răuvoitori au fost în măsură să compromită securitatea rețelelor și a sistemelor informatice ale unei entități prin exploatarea vulnerabilităților care afectează produsele și serviciile unei părți terțe.*

*(119) Amenințările cibernetice devenind tot mai complexe și mai sofisticate, eficacitatea măsurilor de detectare a unor astfel de amenințări și prevenirea lor depinde în mare măsură de schimbul regulat de informații privind amenințările și vulnerabilitățile care are loc între entități. Schimbul de informații contribuie la creșterea gradului de sensibilizare cu privire la amenințările cibernetice, ceea ce, la rândul său, consolidează capacitatea entităților de a preveni materializarea unor astfel de amenințări în incidente și le permite entităților să controleze mai bine efectele incidentelor și să se redreseze mai eficient.”*

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

În plus, protecția datelor cu caracter personal și respectarea drepturilor fundamentale, precum dreptul la viață privată, secretul corespondenței și libertatea de exprimare, constituie un aspect central în cadrul oricărei activități de procesare a datelor și informațiilor.

Lipsa de claritate și uniformitate în ceea ce privește procedurile de solicitare și comunicare a datelor și informațiilor, precum și de garanții specifice privind respectarea drepturilor fundamentale, pot duce la incertitudini, posibile încălcări ale legii și riscuri de securitate.

Experiența altor state membre ale Uniunii Europene arată că reglementarea clară și uniformă a acestor proceduri, precum și stabilirea unor garanții specifice privind respectarea drepturilor fundamentale, pot contribui semnificativ la eficiența și securitatea activităților de securitate cibernetică.

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

Această reglementare va contribui la creșterea eficienței și securității activităților de securitate cibernetică, la asigurarea respectării drepturilor fundamentale și la consolidarea cadrului juridic de funcționare a furnizorilor de servicii tehnice de securitate cibernetică. Prin urmare, adoptarea prezentului proiect de hotărâre a Guvernului este necesară și oportună pentru a aborda aceste probleme, pentru a asigura un cadru clar, uniform și eficient pentru solicitarea și comunicarea

datelor și informațiilor în domeniul securității cibernetice, precum și pentru a proteja drepturile fundamentale ale persoanelor fizice și juridice.

### **2.3 Schimbări preconizate**

În contextul evoluției tehnologice și a amplificării amenințărilor la adresa securității cibernetice, este evident că procedurile existente în prezent sunt insuficiente pentru a face față provocărilor curente. Prin urmare, este esențială reglementarea clară și uniformă a solicitării și comunicării datelor și informațiilor între autoritățile menționate la art. 10 din *Legea nr. 58/2023* și furnizorii de servicii tehnice de securitate cibernetică.

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

Proiectul de hotărâre prevede faptul că solicitarea datelor și informațiilor relevante pentru securitatea cibernetică se va realiza de către autoritățile enumerate la art. 10 din *Legea nr. 58/2023*, iar furnizorii de servicii de securitate cibernetică vor avea obligația de a răspunde acestor solicitări. Este important de menționat că solicitarea nu vizează date cu caracter personal sau date de conținut, ci informații strict necesare pentru asigurarea securității cibernetice.

Proiectul de hotărâre introduce criterii clare pentru evaluarea gravității incidentelor de securitate cibernetică, în funcție de impactul acestora asupra funcționării normale a rețelelor și sistemelor informatice. Acest lucru va permite o abordare mai eficientă și 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 autoritățile competente. De asemenea, se oferă un cadru clar cu privire la tipul de informații care trebuie să fie incluse în aceste notificări.

Punerea în aplicare a acestor norme metodologice va aduce mai multă claritate și va eficientiza procesul de gestionare a securității cibernetice în România. Aceasta va asigura un nivel mai ridicat de protecție pentru rețelele și sistemele informatice, va îmbunătăți capacitatea de răspuns în cazul incidentelor de securitate cibernetică și va contribui la dezvoltarea unui mediu cibernetic mai sigur pentru toți utilizatorii.

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

Proiectul prevede reguli stricte privind protecția datelor cu caracter personal și a secretului corespondenței. În acest sens, prevederile proiectului vizează asigurarea unui echilibru între nevoia de securitate cibernetică și respectarea drepturilor fundamentale ale individului. Proiectul reglementează modul de colaborare între autorități și furnizorii de servicii tehnice de securitate cibernetică, bazat pe transparență, responsabilitate și cooperare activă. Astfel, se urmărește

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) **Sanțiuni 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. Implementarea 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

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 cibernetică, 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 și 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 cibernetică 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 cadru 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

c) bugetul asigurărilor sociale de stat: i. cheltuieli de personal bunuri și servicii						
d) alte tipuri de cheltuieli (se va menționa 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 creșterii cheltuielilor bugetare						
4.5 Propuneri pentru a compensa reducerea veniturilor bugetare						
4.6 Calcule detaliate privind fundamentarea modificărilor veniturilor și/sau cheltuielilor bugetare						
4.7 Prezentarea, în cazul proiectelor de acte normative a căror adoptare atrage majorarea cheltuielilor bugetare, a următoarelor documente: a) fișa financiară prevăzută la art.15 din <i>Legea nr. 500/2002 privind finanțele publice</i> , cu modificările și completările ulterioare, însoțită de ipotezele și metodologia de calcul utilizată; b) declarație conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele și prioritățile strategice specificate în strategia fiscal-bugetară, cu legea bugetară anuală și cu plafoanele de cheltuieli prezentate în strategia fiscal-bugetară.						
4.8 Alte informații						
<b>Secțiunea a 5-a: Efectele proiectului de act normativ asupra legislației în vigoare</b>						
<b>5.1 Măsurile normative necesare pentru aplicarea prevederilor proiectului de act normativ</b>						
Nu este cazul.						
<b>5.2 Impactul asupra legislației în domeniul achizițiilor publice</b>						
Nu este cazul.						
<b>5.3 Conformitatea proiectului de act normativ cu legislația UE (în cazul proiectelor ce transpun sau asigură aplicarea unor prevederi de drept UE).</b>						
Nu este cazul.						
<b>5.3.1 Măsurile normative necesare transpunerii directivelor UE</b>						

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

Nu este cazul.

**Secțiunea a 7-a:  
Activități de informare publică privind elaborarea și implementarea proiectului de act normativ**

**7.1 Informarea societății civile cu privire la elaborarea proiectului de act normativ**

Pentru proiectul de act normativ a fost îndeplinită procedura stabilită prin dispozițiile *Legii nr. 52/2003 privind transparența decizională în administrația 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 situației actuale în domeniul securității cibernetice, atât în România, cât și la nivel global.

În primul rând, trebuie subliniat faptul că amenințările cibernetice au devenit tot mai prezente și sofisticate în ultimii ani. Atacurile cibernetice împotriva instituțiilor guvernamentale, companiilor private și persoanelor cresc în număr și în intensitate, punând în pericol securitatea națională, economia și drepturile și libertățile individuale ale cetățenilor. Acest fapt este bine documentat de numeroase rapoarte naționale și internaționale, inclusiv de către Directoratul Național pentru Securitate Cibernetică și de către Europol.

În al doilea rând, situația actuală în materie de securitate cibernetică în România impune adoptarea de soluții imediate. În prezent, există lacune semnificative în cadrul legislativ și în capacitatea instituțiilor responsabile de a face față amenințărilor cibernetice. Aceste lacune pot duce la o vulnerabilitate crescută în fața atacurilor cibernetice, ceea ce poate avea consecințe grave asupra interesului public.

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

Prin urmare, având în vedere situația urgentă și excepțională în materie de securitate cibernetică și necesitatea adoptării de soluții imediate pentru a evita o gravă atingere adusă interesului public, proiectul de hotărâre a Guvernului respectă criteriile de excepție prevăzute la art. 7 alin. (13) *Legea nr. 52/2003* și, în consecință, poate fi supus adoptării și 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 societății civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum și efectele asupra sănătății și securității cetățenilor sau diversității biologice.**

Nu este cazul.

**Secțiunea a 8-a:  
Măsuri privind implementarea, monitorizarea și evaluarea proiectului de act normativ**

**8.1 Măsurile de punere în aplicare a proiectului de act normativ**

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

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  
MIRCEA CĂTĂLIN PREDOIU**

**DIRECTORUL  
SERVICIULUI DE TELECOMUNICAȚII SPECIALE  
IONEL SORIN BĂLAN**

**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**

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 BALAN**

**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 CĂCIU**

**MINISTRUL FINANTELOR  
MARCEL-IOAN BOLOȘ**

**MINISTRUL AFACERILOR EXTERNE  
LUMINIȚA-TEODORA ODOBESCU**

**MINISTRUL APĂRĂRII NAȚIONALE  
ANGEL TÎLVAR**

**MINISTRUL JUSTIȚIEI  
ALINA-ȘTEFANIA GORGHIU**

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

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 PAHOŢU**

**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.
<b>8.2 Alte informații</b> 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 PAZA  
LUCIAN SILVAN PATRONTU**

**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 CĂCIU**

**MINISTRUL FINANȚELOR  
MARCEL-IOAN BOLOȘ**

**MINISTRUL AFACERILOR EXTERNE  
LUMINIȚA-TEODORA ODOBESCU**

**MINISTRUL APĂRĂRII NAȚIONALE  
ANGEL TÎLVAR**

**MINISTRUL JUSTIȚIEI  
ALINA-ȘTEFANIA GORGHIU**

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

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**

**p. DIRECTORUL  
SERVICIULUI DE INFORMAȚII EXTERNE  
GABRIEL YLASE**



**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 CĂCIU**

**MINISTRUL FINANȚELOR  
MARCEL-IOAN BOLOȘ**

**MINISTRUL AFACERILOR EXTERNE  
LUMINIȚA-TEODORA ODOBESCU**

**MINISTRUL APĂRĂRII NAȚIONALE  
ANGEL TÎLVAR**

**MINISTRUL JUSTIȚIEI  
ALINA-ȘTEFANIA GORGHIU**

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

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 BETRESCU**

**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 CĂCIU**

**MINISTRUL FINANȚELOR  
MARCEL-IOAN BOLOȘ**

**MINISTRUL AFACERILOR EXTERNE  
LUMINIȚA-TEODORA ODOBESCU**

**MINISTRUL APĂRĂRII NAȚIONALE  
ANGEL TÎLVAR**

**MINISTRUL JUSTIȚIEI  
ALINA-ȘTEFANIA GORGHIU**

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

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 CĂCIU**

**MINISTRUL FINANȚELOR  
MARCEL-IOAN BOLOȘ**

**MINISTRUL AFACERILOR EXTERNE  
LUMINIȚA-TEODORA ODOBESCU**

**MINISTRUL APĂRĂRII NAȚIONALE  
ANGEL TÎLVAR**

**MINISTRUL JUSTIȚIEI  
ALINA-ȘTEFANIA GORGHIU**

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

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**

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  
VALEERIU ȘTEFAN ZGONEA**

**MINISTRUL INVESTIȚIILOR ȘI  
PROIECTELOR EUROPENE  
ADRIAN CĂCIU**

**MINISTRUL FINANTELOR  
MARCEL-IOAN BOLOȘ**

**MINISTRUL AFACERILOR EXTERNE  
LUMINIȚA-TEODORA ODOBESCU**

**MINISTRUL APĂRĂRII NAȚIONALE  
ANGEL TÎLVAR**

**MINISTRUL JUSTIȚIEI  
ALINA-ȘTEFANIA GORGHIU**

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

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, ÎNOVĂRII 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 CĂCIU**

**MINISTRUL FINANȚELOR  
MARCEL-IOAN BOLOȘ**

**MINISTRUL AFACERILOR EXTERNE  
LUMINIȚA-TEODORA ODOBESCU**

**MINISTRUL APĂRĂRII NAȚIONALE  
ANGEL TÎLVAR**

**MINISTRUL JUSTIȚIEI  
ALINA-ȘTEFANIA GORGHIU**

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

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 CĂCIU**

**MINISTRUL FINANȚELOR  
MARCEL-IOAN BOLOȘ**

**MINISTRUL AFACERILOR EXTERNE  
LUMINIȚA-TEODORA ODOBESCU**

**MINISTRUL APĂRĂRII NAȚIONALE  
ANGEL TÎLVAR**

**MINISTRUL JUSTIȚIEI  
ALINA-ȘTEFANIA GORGHIU**

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

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 ȚILVĂR**

**MINISTRUL JUSTIȚIEI  
ALINA-ȘTEFANIA GORGHIU**

ANEXA nr. S6

ANEXA nr. S6  
la SG 10.265. din 27. NOV 2023

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

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 PAHOŢU

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 CĂCIU

~~MINISTRUL FINANTELOR  
MARCEL IOAN BOLOS~~

MINISTRUL AFACERILOR EXTERNE  
LUMINIȚA-TEODORA ODOBESCU

MINISTRUL APARĂRII NAȚIONALE  
ANGEL TÎLVAR

MINISTRUL JUSTIȚIEI  
ALINA-ȘTEFANIA GORGHIU

Nu este cazul.
----------------

<b>8.2 Alte informații</b>
----------------------------

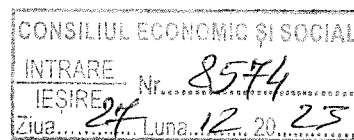
Nu este cazul.
----------------

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**

# GVERNUL ROMÂNIEI



## HOTĂRÂRE

**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**

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

**Guvernul României adoptă prezenta hotărâre.**

**Articol unic** –Se aprobă Normele 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, prevăzute în anexa care face parte integrantă din prezenta hotărâre.

**PRIM-MINISTRU  
ION-MARCEL CIOLACU**

**NORME 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**

**Art. 1.** - Prezentele Norme 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, denumite în continuare Norme metodologice, au ca obiect stabilirea modului de îndeplinire a obligațiilor ce le revin autorităților prevăzute la art. 10 din Legea nr. 58/2023 și furnizorilor de servicii tehnice de securitate cibernetică în procesul de solicitare și comunicare de date și informații privind incidente, respectiv privind amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau un sistem informatic dintre cele prevăzute la art. 3 alin. (1) din Legea nr. 58/2023, precum și interconectarea acestora cu terții și cu utilizatorii finali.

**Art. 2. – (1)** În vederea asigurării rezilienței și protecției rețelelor și sistemelor informatice ce susțin funcțiile de apărare, securitate națională, ordine publică și guvernare, precum și pentru asigurarea unei reacții rapide și eficiente la amenințările provenite din spațiul cibernetic național, autoritățile competente stabilite la art. 10 alin. (1) din Legea nr. 58/2023, în îndeplinirea responsabilităților acestora în domeniile securității și apărării cibernetică, pot solicita furnizorilor de servicii tehnice de securitate cibernetică, prin cerere motivată, date și informații privind incidente de securitate cibernetică, amenințări, riscuri sau vulnerabilități, a căror manifestare poate afecta cel puțin 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)** Cererea prevăzută la alin. (1) este transmisă prin oricare dintre următoarele mijloace de comunicare la distanță, dacă asigură primirea acesteia de către destinatar, astfel:

- a)** prin poștă, cu scrisoare recomandată, cu confirmare de primire, în plic închis, la care se atașează dovada de primire/procesul-verbal;
- b)** prin afișare la domiciliul sau la sediul furnizorului de servicii tehnice de securitate cibernetică, activitate care se consemnează într-un proces-verbal, semnat de cel puțin un martor;
- c)** prin telefon mobil, telefax, fax, poștă electronică sau prin alte mijloace ce asigură transmiterea textului cererii și confirmarea primirii acestuia, dacă furnizorul de servicii tehnice de securitate cibernetică a indicat, în prealabil, autorității prevăzute la art. 10 din Legea nr. 58/2023, care formulează cererea, datele corespunzătoare în acest scop;
- d)** prin Platforma națională 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 dispoziție de către autoritatea prevăzută la art. 10 din Legea nr. 58/2023 care formulează cererea și la care furnizorul de servicii tehnice de securitate cibernetică este în prealabil interconectat;

(3) Cererile formulate prin mijloacele prevăzute la alin. (2) lit. a) și 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 stabilă, în prealabil, de comun acord, în formatul și structura conforme raportării în PNRISC, un răspuns care să cuprindă cel puțin următoarele elemente:

- a) data, ora, minutul descoperirii incidentului;
- b) serviciile și/sau rețelele care sunt afectate de incident;
- c) estimarea ariei geografice afectate, precum și 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 și interconectarea acestora cu terții și cu utilizatorii finali;
- d) datele și informațiile privind cauza/cauzele care a/au provocat incidentul;
- e) estimarea graficului de restabilire a funcționării rețelelor și sistemelor informatice care fac parte dintre cele prevăzute la art. 3 alin. (1) din Legea nr. 58/2023, precum și interconectarea acestora cu terții și cu utilizatorii finali, respectiv estimarea revenirii furnizării serviciilor în parametrii normali de funcționare;
- f) îndrumările oferite utilizatorilor și 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 și 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 poștă 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 stabilă, 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 și/sau motivația vectorului de amenințare sau atac cibernetic;
- c) date care pot ajuta la contextualizarea și descrierea incidentului vizat de vectorul de amenințare sau atac;
- d) tehnici, tactici și 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.