**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**

**ANEXĂ**

**NORME METODOLOGICE**
**privind solicitarea și comunicarea datelor și informațiilor prevăzute la art. 25 alin. (1) din Legea nr. 58/2023**

**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 cibernetice, 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. Operațiunea de afișare 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 stabilită, 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 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 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) artefacte aferente activităților nelegitime derulate de vectori de amenințare sau atac cibernetic sau celor aferente derulării incidentului;
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.

**Art. 6. –** (1) Persoanele fizice și juridice au dreptul de a contesta orice încălcare a drepturilor lor, în condițiile prevăzute de Ordonanța Guvernului nr. 27/2002 privind reglementarea activității de soluționare a petițiilor, cu modificările și completările ulterioare.

(2) În cazul primirii unei astfel de contestații, autoritățile și furnizorii de servicii tehnice de securitate cibernetică sunt obligați să examineze contestația și să ofere, pe lângă răspunsul formulat în termenul legal, și o soluție pentru prevenirea sau remedierea pretinsei încălcări a drepturilor petenților.