

MONITORUL OFICIAL

AL

ROMÂNIEI

Anul 191 (XXXV) — Nr. 167

PARTEA I
LEGI, DECRETE, HOTĂRĂRI ȘI ALTE ACTE

Luni, 27 februarie 2023

SUMAR

<u>Nr.</u>		<u>Pagina</u>
DECIZII ALE PRIM-MINISTRULUI		
55.	— Decizie privind exercitarea, cu caracter temporar, de către doamna Gabriela-Andreea Nica a funcției publice vacante din categoria înalților funcționari publici de secretar general adjunct al Ministerului Muncii și Solidarității Sociale	2
56.	— Decizie privind exercitarea, cu caracter temporar, prin detașare, de către domnul Alexandru-Sorin Bordei-Gheorghisor a funcției publice vacante din categoria înalților funcționari publici de secretar general al Autorității Naționale pentru Protecția Drepturilor Persoanelor cu Dizabilități	2
ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE		
20.281.	— Ordin al ministrului cercetării, inovării și digitalizării privind procedura, metodele și instrumentele încetării utilizării produselor și serviciilor provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărui capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă	3–7
ACTE ALE BĂNCII NAȚIONALE A ROMÂNIEI		
1.	— Ordin privind completarea Ordinului Băncii Naționale a României nr. 27/2010 pentru aprobarea Reglementărilor contabile conforme cu Standardele Internaționale de Raportare Financiară și completarea Ordinului Băncii Naționale a României nr. 6/2015 pentru aprobarea Reglementărilor contabile conforme cu directivele europene	8–15
ACTE ALE AUTORITĂȚII DE SUPRAVEGHERE FINANCIARĂ		
8.	— Normă pentru modificarea Normei nr. 16/2010 privind prospectul schemei de pensii facultative, aprobată prin Hotărârea Comisiei de Supraveghere a Sistemului de Pensii Private nr. 27/2010	16

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

MINISTERUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

ORDIN

privind procedura, metodele și instrumentele încetării utilizării produselor și serviciilor provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărui capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă

Având în vedere necesitatea prevenirii și contracarării amenințărilor cibernetice derulate de Federația Rusă, precum și de actori statali și nonstatali aflați sub controlul Federației Ruse asupra infrastructurilor de comunicații și tehnologia informației cu valențe critice pentru securitatea națională,

având în vedere faptul că autoritățile și instituțiile publice trebuie să beneficieze de proceduri unitare, clare, previzibile, transparente și calitative privind deconectarea, respectiv dezinstalarea produselor și serviciilor provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărui capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă,

ținând cont de faptul că Ministerul Cercetării, Inovării și Digitalizării este organ de specialitate al administrației publice centrale, cu rol de elaborare și implementare, la nivel național, a politicii, strategiei și reglementărilor specifice de dezvoltare și de armonizare ale activităților în cadrul politicii generale a Guvernului, precum și de faptul că îndeplinește rolul de autoritate de stat în domeniul securității cibernetice, conform prevederilor art. 1 alin. (3) și art. 4 alin. (1) din Hotărârea Guvernului nr. 371/2021 privind organizarea și funcționarea Ministerului Cercetării, Inovării și Digitalizării, cu modificările și completările ulterioare,

în vederea aplicării prevederilor art. 5 alin. (1) din Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei,

în temeiul art. 12 alin. (3) din Hotărârea Guvernului nr. 371/2021 privind organizarea și funcționarea Ministerului Cercetării, Inovării și Digitalizării, cu modificările și completările ulterioare,

ministrul cercetării, inovării și digitalizării emite prezentul ordin.

Art. 1. — Se aprobă procedura, metodele și instrumentele încetării utilizării produselor și serviciilor provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărui capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă, prevăzute în anexa nr. 1 care face parte integrantă din prezentul ordin.

Art. 2. — (1) Prezentul ordin se aplică autorităților și instituțiilor publice de la nivel central și local, precum și persoanelor fizice și juridice care dețin rețele și sisteme informatice prin care se gestionează informații clasificate.

(2) Prezentul ordin nu este obligatoriu pentru autoritățile și instituțiile publice cu atribuții proprii în domeniul securității naționale, în domeniul securității cibernetice, apărării naționale și ordinii publice, cu excepția situației în care conducătorul autorității sau instituției respective decide aplicarea lui.

Art. 3. — Se aprobă chestionarul privind produsele și serviciile software care îndeplinesc criteriile prevăzute de Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate

de Federația Rusă împotriva Ucrainei, prevăzut în anexa nr. 2 care face parte integrantă din prezentul ordin.

Art. 4. — (1) Chestionarul prevăzut la art. 3 se publică în secțiunea dedicată autorităților și instituțiilor publice din cadrul Sistemului electronic de Achiziții publice — „Autorități contractante”, în termen de 5 zile de la data publicării prezentului ordin în Monitorul Oficial al României, Partea I.

(2) Autoritățile și instituțiile publice au obligația completării chestionarului prevăzut la art. 3 în termen de 30 de zile de la data publicării prezentului ordin în Monitorul Oficial al României, Partea I.

(3) Datele chestionarului sunt transmise, în format electronic, Ministerului Cercetării, Inovării și Digitalizării, Autorității pentru Digitalizarea României, Directoratului Național de Securitate Cibernetică, Serviciului Român de Informații, Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază și Oficiului Registrului Național al Informațiilor Secrete de Stat.

Art. 5. — Direcțiile de specialitate din cadrul Ministerului Cercetării, Inovării și Digitalizării, cu sprijinul autorităților și instituțiilor prevăzute la art. 2 alin. (3) și (4) din Legea nr. 354/2022, duc la îndeplinire prezentul ordin.

Art. 6. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Ministrul cercetării, inovării și digitalizării,
Sebastian-Ioan Burduja

PROCEDURA, METODELE ȘI INSTRUMENTELE
încetării utilizării produselor și serviciilor provenind direct sau indirect din Federația Rusă
sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice
din Federația Rusă sau al cărui capital este constituit cu participație provenind în mod direct sau prin firme interpuse
din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă

Art. 1. — (1) Prezenta procedură se aplică tuturor autorităților și instituțiilor publice de la nivel central și local, precum și persoanelor fizice și juridice care dețin rețele și sisteme informatice prin care se gestionează informații clasificate, denumite în continuare *entități*.

(2) Prezenta procedură nu este obligatorie pentru autoritățile și instituțiile publice cu atribuții proprii în domeniul securității naționale, în domeniul securității cibernetice, apărării naționale și ordinii publice, cu excepția situației în care conducătorul autorității sau instituției respective decide altfel.

(3) În vederea aplicării prezentei proceduri, autoritățile și instituțiile publice prevăzute la alin. (2) au în vedere să nu le fie afectate următoarele:

- a) activitatea de cercetare-dezvoltare și inovare;
- b) activitatea de informații și contrainformații;
- c) misiunile operative și tactice;
- d) personalul, metodele, mijloacele sau procedurile specifice exercitării atribuțiilor;
- e) respectarea regimului juridic al informațiilor clasificate;
- f) capacitățile de răspuns la amenințări, vulnerabilități sau riscuri la adresa securității naționale a României.

Art. 2. — (1) Entitățile analizează și constată dacă produsele și serviciile software aflate în proprietatea, administrarea sau folosința acestora sunt de tipul celor prevăzute la art. 2 alin. (1) din Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei, denumită în continuare *Lege*, și dacă acestea provin de la persoanele prevăzute la art. 1 alin. (1) și (3) din Lege.

(2) Entitățile stabilesc necesitățile de înlocuire a produselor și serviciilor software de tipul celor prevăzute la art. 2 alin. (1) din Lege și pe care le au în proprietate, administrare sau folosință.

Art. 3. — Entitățile constată încetarea contractelor încheiate cu operatorii economici.

Art. 4. — (1) Entitățile elaborează o procedură internă de încetare a utilizării, respectiv de deconectare/dezinstalare a produselor și serviciilor software interzise de Lege și o pun în aplicare în termen de 60 de zile de la intrarea în vigoare a prezentului ordin.

(2) Entitățile elaborează un plan propriu de înlocuire a produselor și serviciilor software interzise de Lege cu unele legale și compatibile din punct de vedere tehnic și operațional, în acord cu necesitățile fiecărei entități.

(3) În vederea implementării prevederilor alin. (2), entitățile trebuie să respecte cumulativ cel puțin următoarele obligații:

- a) perioada de tranziție între produsele și serviciile software interzise și cele legale și compatibile să fie cât mai scurtă posibil, astfel încât să nu se compromită buna funcționare a rețelelor și sistemelor informatice;
- b) produsele și serviciile software achiziționate să fie instalate în mediul de test, înainte de dezinstalarea/decuplarea celor interzise de Lege;
- c) să se asigure prevenirea și combaterea atacurilor cibernetice pe perioada de tranziție, luând în calcul toate posibilitățile disponibile în piață.

Art. 5. — Instalarea produselor și serviciilor software legale și compatibile se realizează cu respectarea următorilor pași tehnici:

1. se copiază local, pe sistemul informatic, fișierele necesare pentru instalarea produsului antivirus substituent, în funcție de tipul sistemului de operare. Fișierele de instalare se vor descărca de pe pagina oficială a producătorului, împreună cu manualul de instalare și utilizare a produsului;

2. se izolează sistemul informatic de la orice sursă de internet, indiferent de mediul de comunicații (de exemplu, infraroșu, laser), inclusiv de la rețeaua internă/locală din care face parte sistemul informatic, pentru a nu interacționa cu alte dispozitive în timpul procesului de dezinstalare/instalare a produsului antivirus;

3. pe toată durata activității de dezinstalare și instalare a produsului antivirus nu se vor efectua alte operațiuni la nivelul sistemului informatic, precum conectarea altor dispozitive de stocare, instalarea altor programe, deschiderea fișierelor stocate pe sistem sau instalarea și pornirea altor aplicații;

4. se urmează procedura standard de dezinstalare a antivirusului existent la nivelul sistemului informatic, în funcție de sistemul de operare și tipul produsului antivirus;

5. la finalizarea procesului de dezinstalare se repornește sistemul informatic;

6. după repornire se instalează produsul antivirus substituent conform pașilor recomandați de către producător și se efectuează o primă scanare rapidă a sistemului informatic pentru validarea funcționării corespunzătoare a noului antivirus și pentru identificarea posibilelor fișiere infectate la nivelul sistemului;

7. în cazul în care nu sunt detectate fișiere infectate se continuă procesul cu pasul 9;

8. în situația în care au fost identificate fișiere suspecte sau infectate, acestea se transmit personalului specializat pentru analiză suplimentară. Până la stabilirea unui verdict, sistemul informatic nu va fi reconectat la rețeaua din care face parte și nu se va continua procesul. În funcție de tipul de malware și capacitățile acestuia, se procedează la ștergerea fișierelor infectate sau, după caz, la reinstalarea sistemului de operare și se revine la pasul 6;

9. se reconectează sistemul informatic la rețeaua din care face parte sau la o sursă cu conexiune la internet, protejată, de preferat, cel puțin cu o soluție de tip firewall;

10. se actualizează semnăturile din baza de date a produsului antivirus și se scanează complet sistemul informatic pentru detecția eventualelor fișiere infectate.

Art. 6. — (1) În termen de 30 de zile de la data intrării în vigoare a ordinului de aprobare a prezentei proceduri, entitățile demarează procedura de achiziție a produselor și serviciilor software compatibile și legale, cu respectarea legislației privind achizițiile publice, pentru asigurarea continuității activității, cu încadrarea în bugetul propriu.

(2) Documentația de atribuire trebuie să cuprindă elemente suficiente și necesare care să excludă posibilitatea achiziționării produselor și serviciilor software interzise de Lege.

(3) În cadrul documentației de atribuire pentru achiziția de produse și servicii de tipul celor prevăzute la art. 2 alin. (1) din Lege, entitățile sunt obligate să prevadă excluderea de la

procedura de achiziție a persoanelor prevăzute de art. 1 alin. (1) și (3) din Lege, respectiv:

a) operatorilor economici aflați sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă;

b) operatorilor al căror capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă;

c) operatorilor economici din ale căror organe de administrare fac parte persoane din Federația Rusă.

Art. 7. — (1) Entitățile care au în proprietate, administrare sau folosință produse și servicii interzise de lege comunică Ministerului Cercetării, Inovării și Digitalizării, Autorității pentru Digitalizarea României, denumită în continuare *ADR*, și Directoratului Național de Securitate Cibernetică cel puțin următoarele:

a) tipul de produs sau serviciu software interzis de Lege și aflat în proprietate, administrare sau folosință;

b) operatorul economic de la care a achiziționat produsul sau serviciul software;

c) operatorul economic care a fabricat produsul sau serviciul software;

d) data efectivă a dezinstalării/deconectării produselor și serviciilor software interzise prin Lege;

e) procedura internă prevăzută la art. 4 alin. (1);

f) planul de înlocuire prevăzut la art. 4 alin. (2);

g) solicitare expresă, dacă este cazul, pentru suport tehnic în ceea ce privește asigurarea securității cibernetice a rețelelor și sistemelor informatice conectate cu produsele și serviciile software interzise de Lege.

(2) Comunicarea prevăzută la alin. (1) se transmite prin completarea unui formular online administrat de ADR prin Sistemul electronic de achiziții publice, care conține întrebările prevăzute în anexa nr. 2 la ordin.

ANEXA Nr. 2

CHESTIONAR ONLINE

pentru identificarea situației la nivel național privind utilizarea de produse și servicii software care îndeplinesc criteriile prevăzute de Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei

A. Secțiunea date de identificare

• A.1 Secțiunea date de identificare. Completați numele și prenumele persoanei de contact din cadrul organizației dumneavoastră

• A.2 Secțiunea date de identificare. Completați numărul de telefon al persoanei de contact

• A.3 Secțiunea date de identificare. Completați e-mailul persoanei de contact

B. Secțiunea profilul organizației (număr de utilizatori)

Care este numărul aproximativ de utilizatori IT&C din organizația dumneavoastră?

— Selectați o valoare:

- o 1—10 utilizatori
- o 10—50 de utilizatori
- o 50—100 de utilizatori
- o 100—500 de utilizatori
- o 500—1.000 de utilizatori
- o Peste 1.000 de utilizatori
- o N/A

C. Secțiunea informații privind categoriile de produse și servicii software

Care dintre următoarele categorii de produse și servicii software sunt utilizate în organizația dumneavoastră?

MULTI-SELECT

CHECKBOX

- Produse privind securitatea dispozitivului, securitatea punctului final/device security, endpoint security products
- Aplicații și programe software de detecție antivirus/antivirus software
- Aplicații și programe software antimalware, firewall pentru aplicații web, firewall-as-a-service/antimalware software applications, web application firewall (WAF), firewall-as-a-service
- Rețele virtuale private/virtual private networks (VPN)
- Sisteme de detecție și răspuns pentru endpoint/endpoint detection and response systems (EDR)

D. Secțiunea informații privind produse și servicii software specifice

Care dintre următoarele produse și servicii software specifice sunt instalate în infrastructura dumneavoastră?

CHECKBOX

- a) Kaspersky Security
- b) Infotecs
- c) XSIGNAL
- d) Metascan
- e) Dr. Web
- f) RPA RusBITech JSC

- . g) RusBITech Astra
- . h) Era Technopolis
- . i) Pasit Ao
- . j) Neobit, 000
- . k) Advanced System Technology, Ao
- . l) Positive Technologies, Ao
- . m) Altele, care nu se regăsesc în lista de mai sus
- . n) Nu dețin niciuna din cele de mai sus.

D0. **Confirm că am parcurs lista de la secțiunea D.**

— Selecție simplă

D1. **Dacă la întrebarea de la secțiunea D ați selectat opțiunea „Altele, care nu se regăsesc în lista de mai sus”, vă rugăm să detaliați. Dacă nu ați selectat, vă rugăm să completați „Nu este cazul.”**

· **FREE-TEXT**

D2. **Dacă la întrebarea de la secțiunea D ați selectat lit. a) Kaspersky Security, vă rugăm să selectați una sau mai multe din opțiunile de mai jos, potrivit celor deținute de entitatea dumneavoastră.**

MULTI-SELECT

CHECKBOX

- § Kaspersky Anti-Virus
- § Kaspersky Internet Security
- § Kaspersky Total Security
- § Kaspersky Security Cloud Personal
- § Kaspersky VPN Secure Connection
- § Kaspersky Password Manager
- § Kaspersky Safe Kids
- § Kaspersky Internet Security for Mac
- § Kaspersky Internet Security for Android
- § Kaspersky Virus Removal Tool
- § Kaspersky Rescue Disk
- § Altele
- § Nu dețin niciuna din cele de mai sus.

D2.1. **Dacă la întrebarea de la secțiunea D2 ați selectat „Altele”, vă rugăm să detaliați. Dacă nu ați selectat, vă rugăm să completați „Nu este cazul.”**

· **FREE-TEXT**

D3. **Dacă la întrebarea de la secțiunea D lit. b) ați selectat Infotecs, vă rugăm să selectați una sau mai multe din opțiunile de mai jos, potrivit celor deținute de entitatea dumneavoastră.**

MULTI-SELECT

CHECKBOX

- § ViPNet Coordinator HW
- § ViPNet xFirewall
- § ViPNet EndPoint Protection
- § ViPNet EndPoint Protection
- § ViPNet Client for mobile platforms
- § ViPNet Client for workstations
- § ViPNet Coordinator IG/HW/KB/VA
- § ViPNet Personal Firewall
- § ViPNet SIES/OSSL/TIAS
- § Altele
- § Nu dețin niciuna din cele de mai sus.

D3.1. **Dacă la întrebarea de la secțiunea D3 ați selectat „Altele”, vă rugăm să detaliați. Dacă nu ați selectat, vă rugăm să completați „Nu este cazul.”**

· **FREE-TEXT**

D4. **Dacă la întrebarea de la secțiunea D lit. e) ați selectat Dr. Web, vă rugăm să selectați una sau mai multe din opțiunile de mai jos, potrivit celor deținute de entitatea dumneavoastră.**

o MULTI-SELECT sau CHECKBOX

- § Dr. Web Control Center
- § Dr. Web Desktop Security Suite
- § Dr. Web Server Security Suite
- § Dr. Web Mail Security Suite

- § Dr. Web Gateway Security Suite
- § Dr. Web Mobile Security Suite
- § Dr. Web KATANA
- § Dr. Web Security Space (for Windows)
- § Dr. Web Security Space (for Linux)
- § Dr. Web Security Space (for macOS)
- § Dr. Web Security Space (for MS-DOS, OS/2)
- § Dr. Web Security Space (for Android)
- § Altele
- § Nu dețin niciuna din cele de mai sus.

D4.1. Dacă la întrebarea de la secțiunea D4 ați selectat „Altele”, vă rugăm să detaliați. Dacă nu ați selectat, vă rugăm să completați „Nu este cazul.”

· **FREE-TEXT**

E. Secțiunea date privind suportul/mentenanța produselor și serviciilor software specifice

În prezent, există suport/mentenanță pentru produsele sau serviciile identificate anterior?

- . DROP LIST Selectați o valoare
 - o Da
 - o Nu
 - o Nu știu.
 - o Nu este cazul. Nu dețin produse sau servicii care intră sub incidența Legii nr. 354/2022.

F. Secțiunea date privind inventarul de produse și servicii software

Aveți întocmit, la acest moment, în organizația dumneavoastră un inventar al produselor și serviciilor software utilizate sau achiziționate?

- . DROP LIST Selectați o valoare
 - o Da
 - o Nu
 - o Nu știu.

G. Secțiunea date privind modul de achiziție a produselor și serviciilor software

Cum achiziționați în organizația dumneavoastră produsele și serviciile software?

MULTI-SELECT

CHECKBOX

- . Ca licențe software achiziționate direct de organizație
- . Ca licențe software achiziționate în numele organizației de o altă instituție, for superior, autoritate contractantă etc.
- . Ca parte a unor contracte de prestări servicii
- . Ca parte a implementării de proiecte
- . Alte situații

H. Secțiunea date privind operatorii economici ce furnizează produse și servicii software

Organizația dumneavoastră utilizează, după informațiile disponibile la acest moment, furnizori de produse și servicii software cu sediul în Federația Rusă sau care se cunosc a fi sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă conform definițiilor de la art. 1 al Legii nr. 354/2022?

- . Selectați o valoare
 - o Da
 - o Nu
 - o Nu știu.

H.1. Dacă la întrebarea anterioară ați selectat opțiunea „Da”, completați numele furnizorului utilizat. Dacă nu ați selectat, vă rugăm să completați „Nu este cazul.”

· **FREE-TEXT**

Numele furnizorului/Nu este cazul.

I. Ați efectuat dezinstalarea/deconectarea produselor și serviciilor software interzise prin Legea nr. 354/2022?

- Selectați o valoare
 - o Da
 - o Nu
 - o Nu este cazul. Nu dețin produse sau servicii care intră sub incidența Legii nr. 354/2022.

J. Secțiunea alte informații relevante

- . Alte informații relevante

· **FREE-TEXT**