GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din 2025

Chișinău

cu privire la aprobarea Conceptului tehnic al Sistemului informațional „Controlul comerțului cu mărfuri strategice” și a Regulamentului cu privire la modul de ținere a Registrului de stat al controlului comerțului cu mărfuri strategice

În temeiul art.16 alin. (1) și art.17 alin. (1) din Legea nr.71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314), cu modificările ulterioare, și art.22 lit. d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările ulterioare, Guvernul HOTĂRĂȘTE:

1. Se aprobă:

1.1. Conceptul tehnic al Sistemului informațional „Controlul comerțului cu mărfuri strategice”, conform anexei nr. 1;

1.2. Regulamentul cu privire la modul de ținere a Registrului de stat al controlului comerțului cu mărfuri strategice, conform anexei nr. 2;

2. Instituția publică „Agenția Servicii Publice”, în calitate de posesor și deținător al Sistemului informațional „Controlul comerțului cu mărfuri strategice”, va asigura administrarea, mentenanța, funcționarea și dezvoltarea continuă a Sistemului informațional „Controlul comerțului cu mărfuri strategice” în conformitate cu prezenta Hotărâre.

3. Dezvoltarea și mentenanța Sistemului informațional „Controlul comerțului cu mărfuri strategice”, pentru un an de zile de la data dării în exploatare a sistemului, se va realiza în condițiile atașate la Acordul de transfer de proprietate EXBS (nr. S-PMECO-24-PT-007), încheiat între Departamentul de Stat al Statelor Unite ale Americii și Guvernul Republicii Moldova.

4. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova,

Prim-ministru **DORIN RECEAN**

Contrasemnează:

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării **Doina NISTOR**

Anexa nr. 1
la Hotărârea Guvernului
nr. ___/2025

CONCEPTUL TEHNIC
al Sistemului informațional „Controlul comerțului cu mărfuri strategice” (SI CCMS)

Capitolul I
INTRODUCERE

Implementarea Sistemului informațional „Controlul comerțului cu mărfuri strategice” *(în continuare - SI CCMS)* în Republica Moldova reprezintă un pas esențial în alinierea țării noastre la standardele internaționale în domeniul controlului comerțului cu mărfuri strategice. Acest sistem, fiind un rezultat al unui parteneriat eficient și strategic cu Statele Unite ale Americii, își propune să modernizeze și să eficientizeze procesele de autorizare și monitorizare a exporturilor, reexporturilor, importurilor și tranzitului de mărfuri strategice.

Necesitatea unui astfel de sistem este dictată de complexitatea crescândă a comerțului internațional și de riscurile asociate proliferării armelor de distrugere în masă și a tehnologiilor cu potențial militar. Prin intermediul Sistemului informațional „Controlul comerțului cu mărfuri strategice”, Republica Moldova își va consolida capacitatea de a preveni transferurile ilicite de bunuri și tehnologii sensibile, contribuind astfel la asigurarea securității naționale și internaționale.

Implementarea SI CCMS va permite o mai bună aliniere a Republicii Moldova la acquis-ul Uniunii Europene și la atingerea obiectivelor majore în domeniul controlului comerțului cu mărfuri strategice:

- **simplificarea procedurilor** – accelerarea proceselor de autorizare, oferind operatorilor economici un mediu de lucru mai transparent și mai eficient;
- **îmbunătățirea transparenței** – asigurarea accesului facil la informații privind reglementările în domeniul comerțului strategic și statusul cererilor de autorizare;
- **consolidarea controlului** – implementarea unui sistem de monitorizare în timp real a fluxurilor comerciale, permițând identificarea rapidă a eventualelor încălcări;
- **asigurarea conformității** – alinierea la standardele internaționale în domeniul controlului exporturilor, precum și la cerințele impuse de partenerii de dezvoltare;
- **îmbunătățirea cooperării internaționale** – facilitarea schimbului de informații cu alte țări și organizații internaționale în domeniul controlului comerțului cu mărfuri strategice.

Capitolul II
DISPOZIȚII GENERALE

1. Sistemul informațional „Controlul comerțului cu mărfuri strategice” este un sistem informațional de control destinat evidenței autorizațiilor pentru comerțul cu mărfuri strategice și a actelor conexe în conformitate cu prevederile actelor normative în domeniul controlului comerțului cu mărfuri strategice.

2. Agenția Servicii Publice (*în continuare – autoritate emitentă*), în baza deciziilor Comisiei naționale de control al comerțului cu mărfuri strategice (*în continuare - Comisie*), va asigura emiterea, eliberarea și evidența autorizațiilor pentru comerțul cu mărfuri strategice și a actelor conexe.

3. Scopurile atinse de SI CCMS:

3.1. asigurarea constituirii resursei informaționale unice privind autorizațiile pentru comerțul cu mărfuri strategice și a actelor conexe;

3.2. asigurarea furnizării informației autorităților administrației publice, pentru eficientizarea activității de realizare a politicilor de stat în domeniul controlului comerțului cu mărfuri strategice.

4. Principiile de bază ale SI CCMS:

4.1. *principiul legalității* – crearea și exploatarea SI CCMS în conformitate cu legislația;

4.2. *principiul veridicității* – evidența datelor se realizează în baza actelor justificative prezentate;

4.3. *principiul integrității* – păstrarea conținutului datelor și interpretarea lor univocă în condițiile unor acțiuni accidentale. Integritatea datelor se consideră a fi păstrată dacă datele nu au fost denaturate sau distruse;

4.4. *principiul autenticității* - toate datele din SI CCMS se prezumă a fi autentice, integre și veridice;

4.5. *principiul plenitudinii* – asigurarea volumului complet al informației gestionate de SI CCMS, în conformitate cu actele normative;

4.6. *principiul confidențialității informației* – restricționarea accesului persoanelor neautorizate la informația cu accesibilitate limitată;

4.7. *principiul securității informaționale* – asigurarea nivelului integrității, exclusivității, accesibilității și eficienței protecției datelor împotriva pierderii, alterării, denaturării, deteriorării, modificării, accesului și utilizării neautorizate. Securitatea SI CCMS presupune rezistența la atacuri, protecția integrității informației și pregătirea pentru lucru atât la nivel de sistem, cât și la nivelul de date prezentate în această informație;

4.8. *principiul compatibilității* – SI CCMS trebuie să fie compatibil cu sistemele informaționale de stat existente;

4.9. *principiul dezvoltării* – SI CCMS poate fi dezvoltat prin prisma apariției unor obiecte noi;

4.10. *principiul modularității și scalabilității* – posibilitatea de a dezvolta SI CCMS fără modificarea componentelor create anterior;

4.11. *principiul neexcesivităţii si pertinenței prelucrării datelor cu caracter personal* - necesitatea limitării volumului datelor cu caracter personal prelucrate, în așa fel încât să fie prelucrate doar informațiile relevante și necesare în contextul realizării sarcinilor SI CCMS.

5. Noțiunile utilizate în prezentul Concept, dacă nu este definit altfel, au semnificațiile prevăzute în Legea nr. 213/2024 privind controlul comerțului cu mărfuri strategice și Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, precum și următoarele noțiuni:

5.1. *solicitanți* – sunt persoane fizice sau unități de drept, care în vederea obținerii certificatului de înregistrare prealabilă *(în continuare - CIP)*, autorizației pentru comerțul cu mărfuri strategice sau actelor conexe, depun cereri online sau pe suport de hârtie direct la sediul autorității emitente personal sau prin intermediul unui reprezentant împuternicit conform legii.

5.2. *eveniment (operație tehnologică)* – unul dintre scenariile comportamentului obiectului informațional, scontat în sistemul informațional. Lista evenimentelor cuprinde tot ciclul de viață al obiectului în resursa informațională respectivă, începând cu luarea primară în evidență și finalizând cu radierea din evidență. Totodată, evenimentul înregistrat sau produs în alt sistem informațional de stat, care interacționează cu SI CCMS, poate genera modificări în datele obiectului informațional conținut în SI CCMS;

5.3. *formular electronic* – modelul electronic al serviciului, ce conține toate atributele suficiente pentru crearea, actualizarea datelor unui obiect informațional în resursele informaționale, precum și alte date conexe, necesare pentru îndeplinirea și auditarea proceselor tehnologice.

Capitolul III
SPAȚIUL JURIDICO-NORMATIV AL FUNCȚIONĂRII SI CCMS

6. Crearea, funcționarea și actualizarea SI CCMS este reglementată de următoarele acte normative:

6.1. Constituția Republicii Moldova;

6.2. Legea nr. 358/2004 cu privire la implementarea Convenției privind interzicerea dezvoltării, producerii, stocării și folosirii armelor chimice și distrugerea acestora;

6.3. Legea nr.133/2011 privind protecția datelor cu caracter personal;

6.4.Legea nr.160/2011 privind reglementarea prin autorizare a activității de întreprinzător;

6.5.Legea nr.161/2011 privind implementarea ghișeului unic în desfășurarea activității de întreprinzător;

6.6. Legea nr. 132/2012 privind desfășurarea în siguranță a activităților nucleare și radiologice;

6.7. Legea nr. 172/2014 privind aprobarea Nomenclaturii combinate a mărfurilor;

6.8. Legea nr. 100/2017 cu privire la actele normative;

6.9. Legea nr. 195/2024 privind protecția datelor cu caracter personal (în vigoare din 23.08.2026).

6.10. Legea nr. 213/2024 privind controlul comerțului cu mărfuri strategice;

6.11. Hotărârea Guvernului nr. 1392/2005 pentru aprobarea Normelor metodologice privind procedurile tehnice de aplicare a prevederilor Legii nr.358-XV din 5 noiembrie 2004 cu privire la implementarea Convenției privind interzicerea dezvoltării, producerii, stocării și folosirii armelor chimice și distrugerea acestora;

6.12. Hotărârea Guvernului nr. 727/2014 pentru aprobarea Regulamentului privind autorizarea activităților nucleare și radiologice;

6.13. Hotărârea Guvernului nr. 314/2017 privind constituirea Agenției Servicii Publice;

6.14. Hotărârea Guvernului nr. 966/2020 cu privire la serviciile prestate de către Agenția Servicii Publice;

6.15. Hotărârea Guvernului nr. 24/2025 cu privire la Sistemul național de control al comerțului cu mărfuri strategice în Republica Moldova.

7. Actele normative în domeniul tehnologiei informației și comunicațiilor sunt următoarele:

7.1. Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;

7.2. Legea nr. 71/2007 cu privire la registre;

7.3. Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

7.4. Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;

7.5. Legea nr. 148/2023 privind accesul la informațiile de interes public;

7.6. Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;

7.7. Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);

7.8.Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);

7.9. Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);

7.10. Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);

7.11. Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;

7.12. Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;

7.13. Hotărârea Guvernului nr. 375/2020 pentru aprobarea Conceptului Sistemului informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) și a Regulamentului privind modul de ținere a Registrului împuternicirilor de reprezentare în baza semnăturii electronice;

7.14. Hotărârea Guvernului nr. 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);

7.15. Hotărârea Guvernului nr. 712/2020 cu privire la serviciul guvernamental de plăți electronice (MPay);

7.16. Ordinul ministrului dezvoltării informaționale nr. 78/2006 cu privire la aprobarea reglementării tehnice „Procesele ciclului de viață al software-ului” RT 38370656-002:2006;

7.17. Standardul Republicii Moldova SM ISO/CEI 12207:2014 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului”;

7.18. Standardul Republicii Moldova SM ISO/CEI/IEEE 15288:2015 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului”;

7.19. Standardul Republicii Moldova SM ISO/CEI 27002:2017 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației.”

Capitolul IV
SPAȚIUL FUNCȚIONAL AL SI CCMS

Secțiunea 1
Funcțiile de bază

8. Funcțiile de bază ale SI CCMS sunt următoarele:

8.1. Formarea resursei informaționale (*bazei de date)* – SI CCMS:

8.1.1. Funcțiile principale la formarea bazei de date a sistemului, tipice oricărui sistem sunt: înregistrarea inițială, actualizarea datelor și radierea din evidență a obiectelor informaționale (modificarea statutului obiectului). Evidența datelor obiectului informațional include introducerea în baza de date a tuturor atributelor proprii obiectului indicat. Funcțiile respective sunt realizate în cadrul scenariilor de bază asociate obiectelor informaționale.

8.1.2. Datele sunt stocate în sistem în ordine cronologică.

8.2. Organizarea accesului la date – accesarea și utilizarea datelor în scopuri legale în conformitate cu drepturile atribuite:

8.2.1. Datele conținute în SI CCMS nu sunt disponibile pentru organizarea procesului de consum și/sau schimb informațional public. Utilizatorii (intern/extern) de date al SI CCMS vor avea acces limitat și vor utiliza aceste date în conformitate cu drepturile atribuite, în urma autentificării prin mecanisme speciale;

8.3. Jurnalizarea evenimentelor – asigurarea jurnalizării automatizate a tuturor evenimentelor de business print mecanisme speciale de verificare și audit (MLog etc.);

8.4. Asigurarea calității informației – asigurarea calității informației din contul creării și menținerii componentelor sistemului calității, bazat pe abordare procesuală;

8.5. Securitatea și confidențialitatea – corespunderea cerințelor în materie de securitate și confidențialitate, și anume:

8.5.1. Protejarea datelor subiectului de date cu caracter personal, prin mecanisme adecvate de securitate;

8.5.2. Integritatea informațiilor și autenticitatea utilizatorilor prin mecanisme de autentificare care prevăd utilizarea certificatelor calificate ale cheilor publice, eliberate în condițiile actelor normative în domeniul semnăturii electronice și documentului electronic (MPass);

8.5.3. Aplicarea politicii corespunzătoare de securitate la nivelul serviciilor web;

8.6. Administrarea și monitorizarea – asigurarea următoarelor funcții specifice:

8.6.1. Administrarea utilizatorilor, rolurilor și accesului la sistem;

8.6.2. Asigurarea integrității logice a sistemului;

8.6.3. Administrarea bazelor de date ale sistemului;

8.6.4. Gestionarea clasificatoarelor;

8.6.5. Gestionarea copiilor de rezervă;

8.6.6. Monitorizarea performanței sistemului;

8.6.7 Suport tehnic și mentenanță.

Secțiunea 2
Funcțiile specifice

9. În cadrul funcționării SI CCMS trebuie îndeplinite următoarele funcții specifice ale sistemului, structurate în contururi funcționale specifice, și anume:

9.1. Conturul **„CERERE”** – asigură evidența cererilor și documentelor anexate de solicitant, depuse la autoritatea emitentă, în vederea obținerii autorizației pentru comerțul cu mărfuri strategice și actelor conexe, precum și a funcțiilor conexe, și anume:

9.1.1. cererea privind eliberarea certificatul de înregistrare prealabilă;

9.1.2. cerere pentru eliberarea autorizației:

9.1.2.1. generală națională de export al mărfurilor strategice;

9.1.2.2. globală de export al mărfurilor strategice;

9.1.2.3. individuală de export al mărfurilor strategice;

9.1.2.4. individuală de import al mărfurilor strategice;

9.1.2.5. individuală de tranzit al mărfurilor strategice;

9.1.2.6. individuală de transbordare a mărfurilor strategice;

9.1.2.7. individuală de transportare a produselor militare;

9.1.2.8. individuală de asistența tehnică a mărfurilor strategice;

9.1.2.9. individuală de servicii de intermediere a mărfurilor strategice;

9.1.3. cerere pentru eliberarea actelor conexe:

9.1.3.1. certificat internațional de import;

9.1.3.2. certificat al utilizatorului final;

9.1.3.3. certificat de verificare a livrării;

9.1.3.4. notificare;

9.1.4. cererea de suspendare temporară a autorizației;

9.1.5. cererea de reluare a valabilității autorizației;

9.1.6. cererea privind prelungirea termenului de valabilitate al autorizației;

9.1.7. cerere pentru reperfectarea autorizației pentru comerțul cu mărfuri strategice/ actelor conexe;

9.1.8. cerere pentru eliberarea duplicatului autorizației/ actului conex;

certificat constatator;

9.1.9. avizele consultative (pozitive/ negative) ale autorităților implicate de autoritatea emitentă;

9.1.10. returnarea de către autoritatea emitentă a cererii depuse cu încălcarea prevederilor actelor normative în domeniul controlului comerțului cu mărfuri strategice.

9.2. Conturul **„PARTICIPANT AL SISTEMULUI”** – asigură evidența participanților sistemului:

9.2.1. solicitanților de autorizații pentru comerțul cu mărfuri strategice;

9.2.2. solicitanților de acte conexe;

9.2.3. membrilor Comisiei naționale;

9.2.4. specialiștilor desemnați de către instituțiile membre ale Comisiei.

9.3. Conturul **„DECIZIA”** – asigură evidența deciziilor luate de Comisie și autoritatea emitentă, și anume:

9.3.1. evidența deciziilor adoptate de către Comisie privind:

9.3.1.1. eliberarea autorizațiilor;

9.3.1.2. prelungirea autorizațiilor ;

9.3.1.3. suspendarea temporară autorizațiilor;

9.3.1.4. retragerea autorizațiilor;

9.3.1.5. anularea autorizațiilor;

9.3.1.6. refuzul eliberării autorizațiilor conform prevederilor actelor normative în domeniul controlului comerțului cu mărfuri strategice;

9.3.1.7. retragerea certificatului de înregistrare prealabilă;

9.3.2. evidența deciziilor autorității emitente privind:

9.3.2.1. eliberarea, prelungirea, suspendarea temporară, reluarea valabilității, reperfectarea, retragerea și anularea actelor conexe;

9.3.2.2. reluarea valabilității autorizațiilor;

9.3.2.3. reperfectarea autorizațiilor;

9.3.2.4. refuzul emis unilateral de către autoritatea emitentă cu privire la eliberarea autorizației pentru comerțul cu mărfuri strategice sau a actelor conexe dacă, în ultimele două luni, Comisia a adoptat o decizie de refuz sau de retragere a autorizației cu privire la aceeași tranzacție cu mărfuri strategice indicată în cererea depusă de către solicitant;

9.3.2.5. refuzul acceptării cererii în cazul insuficienței informației necesare pentru identificarea solicitantului;

9.3.2.6. refuzul înregistrării prealabile a solicitantului;

9.3.2.7. eliberarea, prelungirea, suspendarea temporară, reluarea valabilității, reperfectarea și anularea certificatului de înregistrare prealabilă;

9.3.3. avizele consultative *(pozitive/ negative)* ale membrilor Comisiei;

9.3.4. avizele consultative *(pozitive/ negative)* ale autorităților implicate de Comisie.

9.4. Conturul **„CIP/ AUTORIZAȚIE/ ACT CONEX”** – asigură evidența emiterii certificatului de înregistrare prealabilă, autorizațiilor pentru comerțul cu mărfuri strategice și actelor conexe, și anume:

9.4.1. certificatul de înregistrare prealabilă;

9.4.2. autorizațiilor individuale de import, de export, de tranzit, de transbordare, de transportare, asistența tehnică, de furnizare serviciilor de intermediare;

9.4.3. autorizațiilor globale de export;

9.4.4. autorizațiilor generale naționale de export;

9.4.5. actelor conexe: certificatul internațional de import, certificatul al utilizatorului final, certificatul de verificare a livrării, notificarea.

9.5. **Funcțiile comune tuturor contururilor:**

9.5.1. furnizarea datelor statistice și rapoarte;

9.5.2. filtrarea masivelor de date conform criteriilor prestabilite, inclusiv căutarea datelor.

Capitolul V
STRUCTURA ORGANIZAȚIONALĂ AL SI CCMS

10. **Proprietarul resursei informaționale** (SI CCMS) și sistemului informațional aferent acesteia (SI CCMS) este statul.

11. **Posesorul și Deținătorul** resursei informaționale (SI CCMS) și sistemului informațional aferent acesteia (SI CCMS) este Instituția publică „Agenția Servicii Publice”, care asigură buna funcționare a SI CCMS.

12. **Administratorul tehnic al SI CCMS** este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, în calitate de Posesor al platformei tehnologice guvernamentale comune (MCloud) – își exercită atribuțiile în conformitate cu actele normative în domeniul administrării tehnice și menținerii resurselor și sistemelor informaționale de stat.

13. **Registratorii datelor în SI CCMS:**

13.1.**Agenția Servicii Publice**, prin intermediul personalului din cadrul subdiviziunilor structurale asigură înregistrarea datelor cu privire la:

13.1.1. solicitanții, care au obținut certificatul de înregistrare prealabilă pentru desfășurarea activității de comerț cu mărfuri strategice;

13.1.2. solicitanții, care au obținut autorizații și acte conexe;

13.1.3. cererile depuse de către solicitant pentru obținerea certificatul de înregistrare prealabilă;

13.1.4. cererile depuse de către solicitant pentru obținerea autorizației privind comerțul cu mărfuri strategice sau actelor conexe;

13.1.5. documente anexate de solicitant la cerere;

13.1.6. certificatului constatator;

13.1.7. deciziile de eliberare, prelungire, suspendare a temporară, reluare, reperfectare, retragere, anulare a actelor conexe;

13.1.8. autorizații și acte conexe eliberate;

13.1.9. certificatul de înregistrare prealabilă;

13.1.10. refuzul înregistrării prealabile a solicitantului;

13.1.11. eliberarea, prelungirea, suspendarea temporară, reluarea valabilității, reperfectarea și anularea a certificatului de înregistrare prealabilă;

13.1.12. refuzul emis unilateral cu privire la eliberarea autorizației pentru comerțul cu mărfuri strategice sau a actelor conexe dacă, în ultimele două luni, Comisia a adoptat o decizie de refuz sau de retragere a autorizației cu privire la aceeași tranzacție cu mărfuri strategice indicată în cererea depusă de către solicitant;

13.1.13. refuzul de acceptare a cererii solicitantului în cazul insuficienței informației necesare pentru identificarea solicitantului.

13.2. **Comisia națională de control al comerțului cu mărfuri strategice**, prin persoanele desemnate, asigură înregistrarea datelor cu privire la:

13.2.1. avizele consultative *(pozitive/ negative)* ale membrilor Comisiei;

13.2.2. procesele verbale ale ședințelor comisiei privind deciziile de:

13.2.2.1. eliberarea autorizațiilor;

13.2.2.2. prelungirea autorizațiilor;

13.2.2.3. suspendarea temporară a autorizațiilor;

13.2.2.4. reluarea autorizațiilor;

13.2.2.5. reperfectarea autorizațiilor;

13.2.2.6. retragerea autorizațiilor;

13.2.2.7. retragerea certificatului de înregistrare prealabilă;

13.2.2.8. anulare a autorizațiilor;

13.2.2.9. refuz emis de către Comisie conform prevederilor actelor normative în domeniul controlului comerțului cu mărfuri strategice.

14. **Furnizori ai datelor pentru SI CCMS** sunt **Solicitanții** care asigură furnizarea datelor cu privire la:

14.1. cereri privind eliberarea, prelungirea, suspendarea temporară, reluarea valabilității, reperfectarea și anularea a certificatului de înregistrare prealabilă;

14.2. cereri privind eliberarea, prelungirea, suspendarea a temporară, reluarea, reperfectarea, retragerea autorizațiilor pentru comerțul cu mărfuri strategice sau actelor conexe;

14.3. documentele anexate la cerere.

15. **Destinatari ai datelor din SI CCMS** sunt:

15.1. membrii Comisiei;

15.2. specialiștii desemnați de către instituțiile membre ale Comisiei;

15.3. solicitanții autorizațiilor pentru comerțul cu mărfuri strategice sau actelor conexe.

16. Resursa informațională SI CCMS este ținută în limba română.

17. Conținutul SI CCMS se aprobă și se modifică prin hotărârea Guvernului, la propunerea Instituției publice „Agenția Servicii Publice”.

Capitolul VI
DOCUMENTE

18. În SI CCMS se conțin date referitor la următoarele categorii de documente:

18.1. documente de intrare, ce reprezintă temeiul legal pentru înregistrarea datelor în sistem;

18.2. documente de ieșire, obținute în rezultatul funcționării sistemului;

18.3. documente tehnologice, ce conțin informația privind descrierea proceselor tehnologice.

19. Documentele de intrare:

19.1. cererea solicitantului:

19.1.1. pentru eliberarea, prelungirea, suspendarea temporară, reluarea valabilității, reperfectarea și anularea certificatului de înregistrare prealabilă;

19.1.2. pentru eliberarea autorizației:

19.1.2.1. generală națională de export al mărfurilor strategice;

19.1.2.2. globală de export al mărfurilor strategice;

19.1.2.3. individuală de export al mărfurilor strategice;

19.1.2.4. individuală de import al mărfurilor strategice;

19.1.2.5. individuală de tranzit al mărfurilor strategice;

19.1.2.6 individuală de transbordare a mărfurilor strategice;

19.1.2.7. individuală de transportare a produselor militare;

19.1.2.8. individuală de asistența tehnică a mărfurilor strategice;

19.1.2.9. individuală de servicii de intermediere a mărfurilor strategice;

19.1.3. pentru eliberarea actelor conexe:

19.1.3.1. certificat internațional de import;

19.1.3.2. certificat al utilizatorului final;

19.1.3.3. certificat de verificare a livrării;

19.1.3.4. notificare;

19.1.4. pentru suspendarea temporară a autorizației;

19.1.5. pentru reluarea valabilității autorizației;

19.1.6. pentru prelungirea termenului de valabilitate al autorizației;

19.1.7. pentru reperfectarea autorizației pentru comerțul cu mărfuri strategice și a actelor conexe;

19.1.8. pentru eliberarea duplicatului autorizației;

19.2. certificatul de înregistrare pentru desfășurarea activității de comerț cu mărfuri strategice;

19.3. documentele anexate de solicitant la cererea depusă, care sunt prevăzute în Hotărârea Guvernului nr. 24/2025 cu privire la Sistemul național de control al comerțului cu mărfuri strategice în Republica Moldova.

20. Documentele de ieșire sunt:
20.1. certificatul de înregistrare prealabilă;
20.2. certificatul constatator;
20.3. autorizația:
20.3.1. generală națională de export al mărfurilor strategice;
20.3.2. globală de export al mărfurilor strategice;
20.3.3. individuală de export al mărfurilor strategice;
20.3.4. individuală de import al mărfurilor strategice;
20.3.5. individuală de tranzit al mărfurilor strategice;
20.3.6. individuală de transbordare a mărfurilor strategice;
20.3.7. individuală de transportare a produselor militare;
20.3.8. individuală de asistența tehnică a mărfurilor strategice;
20.3.9. individuală de servicii de intermediere a mărfurilor strategice;
20.4. actul conex:
20.4.1. certificat internațional de import;
20.4.2. certificat al utilizatorului final;
20.4.3. certificat de verificare a livrării;
20.4.4. notificarea;
20.5. deciziile de refuz pentru eliberarea, prelungirea, suspendarea temporară, reluarea valabilității, reperfectarea și anularea.

21. Documentele tehnologice:
21.1. modele și formulare electronice destinate proceselor de prestare a serviciilor publice, inclusiv cele pentru autentificare, validare, verificare și arhivare electronică.
21.2. ghiduri și proceduri tehnice pentru instalarea, configurarea și administrarea sistemului informațional, cu detalii despre cerințele de infrastructură hardware și software.
21.3. instrucțiuni pentru utilizatori finali care să includă descrieri detaliate ale funcționalităților, proceduri pas-cu-pas și soluții pentru probleme comune.
21.4. manuale de administrare și mentenanță cuprinzând proceduri de copii de rezervă, restaurare în caz de dezastru, gestionarea actualizărilor și monitorizarea performanței.
21.5. protocoale de securitate și conformitate care să includă măsuri pentru protecția datelor, autentificare și autorizare, precum și cerințe legale și standarde internaționale aplicabile.

Capitolul VII
SPAȚIUL INFORMAȚIONAL

Secțiunea 1
Obiectele informaționale gestionate

22. Totalitatea obiectelor informaționale de bază, care reprezintă resursa informațională formată de SI CCMS, se determină în funcție de destinația acestuia și include:

22.1. **cerere**;

22.2. **solicitant**:

22.2.1. persoana fizică;

22.2.2. unitate de drept;

22.3. **decizie**;

22.4. **CIP/ autorizație/ act conex**;

22.5. **document** (*documente anexate la cererea solicitantului, depuse la autoritatea emitentă, în vederea obținerii autorizației pentru comerțul cu mărfuri strategice și actelor conexe*);

22.6. **eveniment** (*operație tehnologică*);

22.7. **formular electronic** (*document tehnologic*).

Secțiunea 2
Identificatorul obiectului informațional

23. Principiul de bază a integrării resurselor informaționale de stat sunt realizate prin intermediul introducerii sistemului de stat de identificatori.

24. Identificatorul obiectului informațional „Cerere” este un număr de identificare unic, generat de sistem.

25. Indicele de bază de identificare a obiectului „Solicitant” este:

25.1. pentru persoane fizice - numărul de identificare de stat al persoanei fi-zice (*IDNP, identificat în Registrul de stat al populației*);

25.2. pentru unitații de drept - numărul de identificare de stat al unităților de drept (*IDNO, identificat în Registrul de stat al unităților de drept*).

26. Identificatorul obiectului informațional „Decizie” este un număr de identificare unic, generat de sistem.

27. Identificatorul obiectului informațional „CIP/Autorizația/Act conex” este un număr de identificare unic, generat de sistem.

28. Identificatorul obiectului informațional „Document” este un număr de identificare unic, generat de sistem.

29. Identificatorul obiectului informațional „Eveniment” este un număr de identificare unic, generat de sistem.

30. Identificatorul obiectului informațional „Formular electronic” este un număr de identificare unic, generat de sistem.

31. Identificarea obiectelor informaționale, propusă la etapa descrierii Conceptului, este opțională și poate fi revizuită în procesul elaborării sarcinii tehnice.

Secțiunea 3

Scenariile asociate obiectelor informaționale

32. Scenariile de bază reprezintă un șir de evenimente, aferente obiectului informațional luat în evidentă în SI CCMS (înregistrarea, actualizarea, radierea obiectelor informaționale). Grupul de scenarii, relaționate cu înregistrarea și actualizarea informației, interacționează cu obiectele informaționale ale sistemului în modul urmă-tor:

32.1. **pentru obiectul informațional „Cerere”**:

32.1.1. Înregistrarea inițială se efectuează la depunerea cererii conform cerințelor legislației naționale.

32.1.2. Actualizarea datelor se efectuează la suplinirea setului de documente anexate, depuse incomplect.

32.1.3. Radierea din evidență a cererii se efectuează la:

32.1.3.1. refuzul emis unilateral de către autoritatea emitentă;

32.1.3.2. refuzul emis de către Comisia națională.

32.2. **pentru obiectul informațional „Solicitant”:**

32.2.1. Înregistrarea inițială a solicitantului (persoană fizică/unitatea de drept) se efectuează la prima solicitare.

32.2.2. Actualizarea datelor se operează în procesul examinării cererilor depuse:

32.2.2.1. de persoana fizică – la modificarea datelor personale conform proceselor business prestabilite în Registrul de stat al populației;

32.2.2.2. de unitatea de drept – la modificarea datelor conform proceselor business prestabili-te în Registrul de stat al unităților de drept.

32.2.3. Radierea din evidență a solicitantului se operează la expirarea termenului de valabilitate a CIP.

32.3. **pentru obiectul informațional „Decizie”:**

32.3.1. Înregistrarea inițială se realizează la aprobarea procesului-verbal al ședinței Comisiei sau la aprobarea deciziei autorității emitente.

32.4. **pentru obiectul informațional „CIP/Autorizație/act conex”:**

32.4.1. Înregistrarea inițială se operează la eliberarea CIP/Autorizației/actului conex solicitantului.

32.4.2. Actualizarea datelor privind CIP/Autorizația/actul conex se realizează prin procesul de luare a deciziei de modificare a statutului documentului:

32.4.2.1. privind prelungirea CIP/Autorizației/actului conex;

32.4.2.2. privind suspendarea temporară a CIP/Autorizației/actului conex;

32.4.2.3. privind reluarea valabilității CIP/Autorizației/ actului conex;

32.4.3. Radierea din evidență a CIP/Autorizației/actului conex se operează:

32.4.3.1. la expirarea termenului de valabilitate a CIP/Autorizației/actului conex.

32.4.3.2. la anularea CIP/Autorizației/actului conex;

32.4.3.3. la retragerea CIP/Autorizației/actului conex:

32.4.3.4. reperfectarea CIP/Autorizației/actului conex.

32.5. **pentru obiectul informațional „Document”:**

32.5.1. Înregistrarea inițială se efectuează la anexarea documentelor necesare la cererea depusă pentru eliberarea CIP/Autorizației/actului conex.

32.5.2. Radierea din evidență se operează:

32.5.2.1. la plasarea eronată a documentului în sistem;

32.5.2.2. la refuzul cererii.

32.6. **pentru obiectul informațional „Eveniment” și „Formular electronic”:**

32.6.1. Înregistrarea inițială – are loc la introducerea primară a evenimentului în sistem.

32.6.2. Actualizarea datelor – la luarea deciziei de către persoana responsabilă.

32.6.3. Radierea din evidență – la anularea evenimentului (*la decizia autorității emitente*).

Secțiunea 4
Datele obiectelor informaționale

33. Obiectele informaționale reprezintă un ansamblu de atribute ce le caracterizează:

33.1. **datele despre obiectul informațional „Cerere”:**

33.1.1. numărul de identificare a cererii;

33.1.2. tipul cererii (pentru CIP/Autorizației/act conex);

33.1.3. număr și data de înregistrare a cererii la solicitant (conform tipului de activitate);

33.1.4. număr și data de înregistrare a cererii la Agenția Servicii Publice;

33.1.5. textul cererii în format digital;

33.1.6. IDNO și/ sau IDNP al solicitantului;

33.1.7. datele reprezentantului:

33.1.7.1.1. IDNO și/ sau IDNP al reprezentantului;

33.1.7.1.2. ID împuternicirii de reprezentare din SIA „MPower” sau datele procurii prezentate;

33.1.8. termenul de examinare a cererii și emitere a CIP/Autorizației/act conex;

33.1.9. ID documentelor anexate pentru eliberarea CIP/Autorizației/act conex;

33.1.10. textul documentelor anexate la cerere în format digital;

33.1.11. tip de activitate solicitat (import, export, intermediere, transbordare, transportare, tranzit, furnizare de asistență tehnică);

33.1.12. parteneri externi/ țara;

33.1.13. țara plătitoare și codul țării;

33.1.14. țara exportatoare și codul țării;

33.1.15. țara importatoare și codul țării;

33.1.16. țara de destinație finală și codul țării;

33.1.17. țara de origine/țara de amplasament al produselor care fac obiectul serviciilor de intermediere și codul țării;

33.1.18. statul în care se află sau se vor afla mărfurile strategice și codul țării;

33.1.19. statul în care se intenționează parcurgerea procedurii vamale de export și codul țării;

33.1.20. moneda plății și codul;

33.1.21. transportator:

33.1.21.1. denumirea transportatorului;

33.1.21.2. mijloc de transport;
33.1.21.3. traseu de tranzit pe teritoriu Republicii Moldova;
33.1.22. destinatar final;
33.1.23. agent/reprezentant (dacă diferă de exportator);
33.1.24. biroul vamal:
33.1.24.1. biroul vamal de intrare;
33.1.24.2. biroul vamal de ieșire;
33.1.25. alte precizări ale solicitantului;
33.1.26. date despre marfa strategică:
33.1.26.1. numărul conform listelor de mărfuri strategice supuse controlului;
33.1.26.2. codul potrivit nomenclaturii combinat a mărfurilor;
33.1.26.3. denumirea comercială;
33.1.26.4. cantitatea mărfii (cod UM/tone, kg; cod UM supl./ cantit.supl./ altă unitate de măsură cu indicarea acesteia);
33.1.26.5. valoarea în moneda plății;
33.1.27. ID certificatului de constatare.
33.2. **datele despre obiectul informațional „Solicitant”:**
33.2.1. date despre „persoană fizică”:
33.2.1.1. numărul de identificare de stat al persoanei fizice (IDNP);
33.2.1.1.1. numele;
33.2.1.1.2. prenumele;
33.2.1.1.3. date privind domiciliul și/sau reședința temporară;
33.2.1.2. datele de contact (*număr telefon, e-mail*);
33.2.2. datele despre „unitate de drept”:
33.2.2.1. numărul de identificare de stat al unității de drept (IDNO);
33.2.2.2. denumirea;
33.2.2.3. sediul (adresa poștală, telefon, adresa electronică).
33.3. **date despre obiectul informațional „Decizie”**
33.3.1. ID deciziei;
33.3.2. tipul deciziei;
33.3.3. textul deciziei în format digital;
33.3.4. data adoptării;
33.3.5. emitentul deciziei;
33.3.6. măsurile restrictive internaționale;
33.3.7. ID avizului consultativ (pozitiv/negativ) al membrului Comisiei;
33.3.8. ID avizului consultativ (pozitiv/negativ) al autorității implicată de Comisie.
33.4. **date privind obiectul informațional „CIP/Autorizație/act conex”:**
33.4.1. numărul de identificare a CIP/Autorizației/actului conex;
33.4.2. tipul autorizației/actului conex;
33.4.3. data eliberării;
33.4.4. termen de valabilitate solicitat;
33.4.5. termenul de valabilitate acordat;
33.4.6. temei pentru eliberarea autorizației/actului conex;

33.4.7. ID solicitantului;
33.4.8. ID cererii.

Secțiunea 5
Clasificatoarele

34. În vederea asigurării veridicității și reducerii volumului informației păstrate în sistem, precum și pentru o clasificare corectă a obiectelor în sistem, se utilizează sistemul de clasificatoare:

34.1. clasificatoarele internaționale;
34.2. clasificatoarele naționale ale Republicii Moldova;
34.3. clasificatoarele interne.

35. Clasificatoarele interne se elaborează și se utilizează în cadrul SI CCMS doar în cazurile absenței clasificatoarelor naționale și internaționale aprobate.

Secțiunea 6
Interacțiunea cu alte sisteme informaționale de stat relevante și cu sisteme informaționale partajate

36. Pentru buna funcționare SI CCMS interacționează cu alte sisteme informaționale de stat:

36.1. **SI Registrul de stat al populației** – pentru schimbul automatizat de date privind persona fizică.

36.2. **SI Registrul de stat al unității de drept** – pentru schimbul automatizat de date privind unitatea de drept.

37. SI CCMS interacționează cu următoarele sisteme informaționale partajate și sisteme informaționale din posesia altor autorități publice:

37.1. **serviciul electronic guvernamental de autentificare și control al accesului (MPass)** – pentru autentificarea și controlul accesului în cadrul sistemului pe bază de roluri;

37.2. **serviciul electronic guvernamental integrat de semnătură electronică (MSign)** – pentru semnarea electronică a înregistrărilor;

37.3. **sistemul informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice" (MPower)** – pentru validarea împuternicirilor de reprezentare în procedura de înregistrare de stat;

37.4. **serviciul electronic guvernamental de notificare (MNotify)** – pentru notificarea beneficiarilor serviciilor publice prestate în baza datelor din SI CCMS;

37.5. **serviciul guvernamental de plăți electronice (MPay)** – pentru achitarea și, respectiv, încasarea plăților de la persoanele fizice în procesul prestării serviciilor;

37.6. **serviciul electronic guvernamental de jurnalizare (MLog)** – pentru asigurarea evidenței evenimentelor de creare/modificare/anulare în contextul utilizării SI CCMS;

37.7. **portalul guvernamental al cetățeanului (MCabinet)** – pentru plasarea documentelor electronice rezultate din prestarea serviciilor publice din SI CCMS;

Capitolul VIII
SPAȚIUL TEHNOLOGIC

Secțiunea 1
Dispoziții generale

38. SI CCMS utilizează standarde deschise și care sunt compatibile cu sisteme care, la fel, utilizează standarde non-proprietare, cât și cu standardele deja existente.

39. Arhitectura complexului software-hardware, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale sunt determinate de Posesor.

40. Sistemul de comunicații este bazat pe infrastructura și echipamentul rețelelor guvernamentale, care includ posibilitatea conectării la internet. Infrastructura existentă este planificată în modul corespunzător, care oferă nivele adecvate de performanță și capacitate.

Secțiunea 2
Platforma tehnologică

41. SI CCMS este găzduit pe platforma tehnologică guvernamentală comună (MCloud), care permite accesul, la cerere, pe bază de rețea la totalitatea configurabilă a resurselor de calcul virtualizabile (*de exemplu rețele, servere, echipamente de stocare, aplicații și servicii*), ce pot fi puse la dispoziție cu un efort minim de administrare sau interacțiune cu furnizorul acestor servicii. În acest fel, SI CCMS poate fi ușor extins pe verticală, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori, atât în regim normal de lucru, cât și în perioadele de vârf.

42. Interfața de utilizare a SI CCMS se va adapta automat la diverse rezoluții de afișare și va fi disponibilă, inițial, în cel puțin două limbi: română (*ISO 639-1:„RO”)* și engleză (*ISO 639-1:„EN”*).

43. Având în vedere importanța și rolul SI CCMS, accesul la datele din SI CCMS este asigurat în mod continuu și neîntrerupt. Se asigură funcționarea non-stop a SI CCMS , precum și a tuturor operațiunilor tehnice, fără a fi necesar să se întrerupă accesul subiecților raporturilor juridice și/sau activitățile din cadrul sistemului. Din acest motiv, întreaga soluție este construită în regim de înaltă disponibilitate (*24 de ore pe zi, 7 zile pe săptămână*).

Capitolul IX
ASIGURAREA SECURITĂȚII INFORMAȚIONALE

44. Securitatea informației presupune protecția SI CCMS la orice etapă a proceselor de creare, procesare, stocare și transmitere a datelor, de acțiuni accidentale sau intenționate cu caracter artificial sau natural, care au ca rezultat cauzarea

prejudiciului posesorului și utilizatorilor resurselor informaționale și infrastructurii informaționale.

45. Asigurarea securității informației este realizată în conformitate cu Hotărârea Guvernului nr. 201/2017 privind aprobarea cerințelor minime obligatorii de securitate cibernetică, aprobate prin. Pentru gestiunea riscurilor de securitate este pus în aplicare sistemul de management al securității informațiilor pentru a asigura îndeplinirea obiectivelor și principiilor de intervenție definite prin politica de securitate. Pentru a asigura un nivel de securitate corespunzător, personalul implicat în utilizarea și administrarea SI CCMS este instruit în ceea ce privește riscurile de securitate la care poate fi expus. Politica de securitate include prevederi referitoare la organizarea auditurilor periodice de securitate pentru a verifica politica și conformitatea cu regulile de securitate, precum și a stabili domeniile care necesită efectuarea acțiunilor corective.

46. Pericolele securității informaționale:

46.1. colectarea și utilizarea ilegală a datelor;

46.2. încălcarea tehnologiei de prelucrare a datelor;

46.3. implementarea în produsele software și hardware a componentelor care îndeplinesc funcții neprevăzute în documentația aferentă acestor produse;

46.4. elaborarea și răspândirea programelor ce afectează funcționarea normală a sistemelor informaționale și a comunicațiilor electronice, precum și a sistemelor securității informaționale;

46.5. nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor și sistemelor de prelucrare a datelor și comunicațiilor electronice;

46.6. influențarea sistemelor cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a datelor;

46.7. compromiterea cheilor și mijloacelor de protecție criptografică a informației;

46.8. scurgerea informației prin canale tehnice;

46.9. implementarea dispozitivelor electronice pentru interceptarea informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor utilizând sistemele de comunicații, precum și în încăperile de serviciu ale autorităților administrației publice;

46.10. nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;

46.11. interceptarea datelor în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acestor date și impunerea unor date false;

46.12. utilizarea tehnologiilor informaționale naționale și internaționale necertificate, a mijloacelor de protecție a informației și a mijloacelor de informatizare la crearea și dezvoltarea infrastructurii informaționale de comunicații electronice;

46.13. încălcarea restricțiilor legale privind răspândirea informației;

46.14. încălcarea prevederilor Legii nr.133/2011 privind protecția datelor cu caracter personal.

47. SI CCMS asigură următoarele obiective de securitate:

47.1. autentificarea – garantează că zonele restricționate ale SI CCMS vor fi accesibile utilizatorilor interni/externi cu o identitate verificată prin mecanisme speciale (MPass, etc.);

47.2. autorizarea – garantează că utilizatorii autentificați prin mecanisme speciale pot accesa serviciile și datele care corespund drepturilor lor de acces:

47.3. confidențialitatea – garantează că datele înregistrate în SI CCMS nu pot fi accesate de o parte terță neautorizată;

47.4. integritatea – garantează că datele înregistrate în SI CCMS nu au fost modificate sau alterate de o parte terță neautorizată;

47.5. non-repudierea – garantează că datele înregistrate în SI CCMS nu pot fi negate mai târziu.

Capitolul X
ÎNCHEIERE

48. Implementarea SI CCMS reprezintă și o investiție strategică în viitorul Republicii Moldova și este un pas important în modernizarea administrației publice și în consolidarea securității naționale a Republicii Moldova. Prin intermediul acestui sistem, țara noastră va deveni un partener mai responsabil în domeniul controlului comerțului strategic, contribuind astfel la stabilitatea regională și internațională.

49. Totodată, proiectul de implementare a SI CCMS este asociat cu anumite riscuri, cum ar fi întârzieri în procesul de dezvoltare și ajustare la cerințele expuse în actele normative naționale, probleme de compatibilitate cu alte sisteme sau rezistența la schimbare a utilizatorilor. Pentru a mitiga aceste riscuri, se vor implementa următoarele măsuri:

49.1. **planificare detaliată**: – elaborarea de către autoritatea emitentă a unui plan de proiect detaliat și monitorizarea constantă a progresului de implementare a sistemului.

49.2. **comunicare eficientă:** – asigurarea unei comunicări transparente și eficiente între toate părțile implicate în proiect.

49.3. **testare riguroasă:** – efectuarea de teste amănunțite în toate etapele proiectului: îndeosebi teste funcționale, de performanță și de securitate.

49.4. **instruirea utilizatorilor:** – organizarea de sesiuni de instruire pentru a asigura o utilizare corectă a sistemului.

50. Pe termen lung, SI CCMS va fi integrat cu alte sisteme informaționale relevante, creând astfel un mediu de afaceri mai transparent și mai eficient. Acest sistem va beneficia atât autoritățile de control, cât și operatorii economici, precum și cetățenii Republicii Moldova.

Anexa nr. 2
la Hotărârea Guvernului
nr.___/2025

REGULAMENT
cu privire la modul de ținere a Registrului de stat al controlului comerțului cu mărfuri strategice (RS CCMS)

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul cu privire la modul de ținere a Registrului de stat al controlului comerțului cu mărfuri strategice (*în continuare – Regulament*) este elaborat în conformitate cu prevederile Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova nr.6-12 art.44 din 01.01.2004), Legii nr. 71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova nr.70-73 art.314 din 25.05.2007) cu modificările și completările ulterioare, și Conceptul Sistemului informațional „Controlul comerțului cu mărfuri strategice" (*în continuare - SI CCMS*) din Anexa nr.1 din prezenta hotărâre.

2. Prezentul Regulament stabilește modul de utilizare, administrare și dezvoltare a Registrului de stat al controlului comerțului cu mărfuri strategice (în continuare – *RS CCMS*), precum și atribuțiile, drepturile și responsabilitățile subiecților raporturilor juridice (*sau subiecți sau utilizatori ai RS CCMS*) în domeniul creării, administrării, mentenanței și dezvoltării RS CCMS.

3. RS CCMS este resursa informațională de bază care conține date sistematizate despre eliberarea, prelungirea, suspendarea sau anularea autorizațiilor de export, reexport, import și tranzit al mărfurilor strategice, precum și monitorizarea procedurii de control asupra exportului, reexportului, importului și tranzitului de mărfuri strategice.

4. RS CCMS este parte componentă a resurselor informaționale de stat și are ca obiectiv principal asigurarea necesităților informaționale ale utilizatorilor RS CCMS în procesul de autorizare a comerțului cu mărfuri strategice.

5. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută la art.3 din Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat, precum și noțiunile utilizate în Conceptul SI CCMS.

Capitolul II
SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII, ADMINISTRĂRII, MENTENANȚEI ȘI DEZVOLTĂRII RS CCMS

6. Subiecții raporturilor juridice din domeniul creării, administrării, mentenanței și dezvoltării RS CCMS sunt:

6.1. Proprietarul RS CCMS;

6.2. Posesorul RS CCMS;

6.3. Deținătorul RS CCMS;

6.4. Registratorul datelor în RS CCMS;

6.5. Administratorul tehnic al RS CCMS;

6.6. Furnizorul datelor în RS CCMS;

6.7. Destinatarul datelor din RS CCMS.

7. Proprietarul RS CCMS își realizează drepturile de proprietate, de gestionare și de utilizare a datelor înregistrate în resursa informațională.

8. Posesorul RS CCMS asigură condițiile juridice, financiare și organizatorice pentru administrarea, mentenanța și dezvoltarea resursei informaționale RS CCMS.

9. Deținătorul RS CCMS asigură buna funcționare și gestionează complexul de software și hardware aferent (sistemul informațional), acordă drepturi de acces utilizatorilor, exercită atribuții de nivel tehnic.

10. Registratorii de date în RS CCMS sunt persoane juridice de drept public și privat, cărora Posesorul le-a acordat drepturi respective de înregistrare, actualizare (completare/modificare) și radiere a datelor obiectului informațional al RS CCMS, conform prevederilor Conceptului SI CCMS. Atribuțiile se transmit în baza și în conformitate cu prezentul Regulament sau cu acordurile încheiate cu Posesorul RS CCMS.

11. Administratorul tehnic al RS CCMS exercită atribuții în conformitate cu actele normative în domeniul administrării, menținerii și dezvoltării infrastructurii de tehnologie a informației precum și implementării cerințelor de securitate stabilite de actele normative în domeniul securității cibernetice.

12. Furnizorii de date în RS CCMS sunt persoanele fizice și juridice de drept public și privat, care prezintă date despre obiectul înregistrării în baza și în conformitate cu prezentul Regulament sau cu acordurile încheiate cu Posesorul RS CCMS.

13. Destinatarii datelor RS CCMS sunt persoanele juridice de drept public și privat, mandatate cu dreptul de a consuma datele din RS CCMS, conform actelor normative.

Capitolul III
DREPTURILE SI OBLIGATIILE SUBIECȚILOR RAPORTURILOR JURIDICE

Secțiunea 1
Drepturile si obligațiile Posesorului RS CCMS

14. Posesorul RS CCMS are următoarele drepturi:

14.1. stabilirea procedurilor pentru accesarea și vizualizarea datelor din RS CCMS;

14.2. verificarea respectării condițiilor juridice, financiare, organizatorice, de funcționare și exploatare a sistemului informațional de către Deținător și alți utilizatori, în limita rolului atribuit;

14.3. supravegherea respectării cerințelor de securitate a informației de către utilizatorii RS CCMS, fixarea cazurilor și tentativelor de încălcare a acestora;

14.4. solicitarea de la Registratori și Furnizorii de date completarea sau actualizarea datelor din RS CCMS;

14.5. solicitarea de la Registratori și Furnizori, remedierea erorilor și omisiunilor, actualizarea și corectarea datelor înregistrate în RS CCMS;

14.6. elaborarea și/sau aprobarea, conform competențelor, cadrului normativ cu privire la RS CCMS;

14.7. înaintarea deținătorului RS CCMS a propunerilor și soluțiilor de perfecționare și eficientizare a procesului business de actualizare a RS CCMS;

14.8. efectuarea permanentă a controlului intern al RS CCMS;

14.9. inițierea procedurii de revocare a drepturilor de acces la RS CCMS pentru subiecții raporturilor juridice care nu respectă regulile stabilite, prevederile standardelor și normelor general acceptate în domeniul securității informaționale;

14.10. deținerea altor drepturi stabilite în conformitate cu Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat.

15. Posesorul RS CCMS are următoarele obligații:

15.1. asigurarea condițiilor organizatorice, juridice, si financiare pentru crearea, administrarea, mentenanța și dezvoltarea RS CCMS;

15.2. aprobarea instrucțiunilor privind înregistrarea, păstrarea, completarea, corectarea, radierea și utilizarea datelor din RS CCMS;

15.3. stabilirea și asigurarea implementării măsurilor organizatorice și tehnice necesare pentru asigurarea protecției și confidențialității datelor cu caracter personal bazate pe un sistem consistent de profiluri și autorizații de acces;

15.4. elaborarea și dezvoltarea cadrului normativ cu privire la RS CCMS, prin intermediul Cancelariei de Stat conform competențelor deținute;

15.5. aprobarea și coordonarea cu Administratorul tehnic executarea modificărilor/rectificărilor privind neconformitățile de sistem, neconformitățile cauzate de factorul uman, incidentele de infrastructură care afectează funcționarea corespunzătoare a acestuia;

15.6. asigurarea dezvoltării continue a RS CCMS prin adăugarea de noi componente;

15.7. autorizarea, suspendarea și revocarea dreptului de acces la RS CCMS în condițiile prezentului Regulament;

15.8. informarea utilizatorilor RS CCMS despre reglementările normative, modificările condițiilor tehnice de funcționare a acestuia;

15.9. asigurarea ținerii RS CCMS în conformitate cu actele normative în domeniul ținerii registrelor și prezentul Regulament;

15.10. utilizarea datelor obținute din RS CCMS în scopuri legale și în conformitate cu actele normative;

15.11. exercitarea altor obligații necesare asigurării funcționării corespunzătoare a RS CCMS.

Secțiunea 2
Drepturile si obligațiile Deținătorului RS CCMS

16. Deținătorul RS CCMS are următoarele drepturi:

16.1. monitorizarea exploatării SI CCMS de către utilizatori;

16.2. gestionarea și utilizarea datelor din RS CCMS;

16.3. supravegherea respectării cerințelor de securitate a informației de către utilizatorii RS CCMS, identificarea cazurilor și tentativelor de încălcare a cerințelor;

16.4. verificarea autenticității și veridicității datelor înregistrate de registratorii RS CCMS;

16.5. solicitarea, de la Registratori și Furnizori, actualizarea sau corectarea datelor din RS CCMS, în caz de depistare a neconformităților;

16.6. suspendarea sau revocarea dreptului de acces la RS CCMS pentru utilizatorii, care nu respectă condițiile de securitate și regulile de exploatare a acestuia, precum și regulile, standardele și normele general acceptate în domeniul securității informaționale;

16.7. participarea la implementarea și dezvoltarea continuă a RS CCMS;

16.8. înaintarea propunerilor de ordin normativ, tehnic și organizatoric în vederea îmbunătățirii și sporirii eficacități funcționarii SI CCMS;

16.9. solicitarea respectării de către subiecții raporturilor juridice a cerințelor de securitate privind accesul la resursa informațională și regulile de exploatare a sistemului informațional în procesul de înregistrare, vizualizare, completare, modificare, procesare, extragere, validare/invalidare și radiere a datelor în RS CCMS;

16.10. solicitarea de la Registratori și Furnizori a informațiilor suplimentare despre obiectele suspuse înregistrării în RS CCMS;

16.11. exercitarea altor activități necesare asigurării bunei funcționari a RS CCMS.

17. Deținătorul RS CCMS are următoarele obligații:

17.1. exploatarea RS CCMS în corespundere cu actele normative și prezentul Regulament;

17.2. asigurarea administrării RS CCMS în conformitate cu prezentul Regulament, precum și cu alte acte normative;

17.3. asigurarea masurilor tehnice și organizatorice de protecție și securitate a datelor RS CCMS;

17.4. monitorizarea și supravegherea accesării datelor din RS CCMS și identificarea neconformitățile comise;

17.5. asigurarea plenitudinii și integrității datelor înregistrate în RS CCMS, neadmiterea modificării neautorizate ale acestora;

17.6. asigurarea, în condițiile și în limitele cadrului normativ, a suportului metodologic și practic utilizatorilor RS CCMS;

17.7. asigurarea autenticității accesului Registratorilor, Furnizorilor, Destinatarilor în conformitate cu drepturile de acces stabilite și atribuțiile delegate;

17.8. asigurarea monitorizării modului de furnizare a datelor în/din RS CCMS;

17.9. notificarea Administratorului tehnic al RS CCMS pentru întreprinderea măsurilor în vederea depistării sursei de producere a incidentelor și remedierii acestora, în cazul incidentelor de securitate, deficiențelor și defecțiunilor apărute în funcționarea RS CCMS;

17.10. gestionarea și păstrarea înregistrărilor de audit intern și extern ale securității operațiilor de prelucrare a datelor cu caracter personal în cadrul SI CCMS;

17.11. asigurarea păstrării RS CCMS până la adoptarea deciziei privind lichidarea acestuia. În cazul lichidării, datele și documentele înregistrate în acesta se transmit în arhivă, conform actelor normative;

17.12. asigurarea ținerii RS CCMS în conformitate cu prezentul Regulament;

17.13. asigurarea funcționării în timp real (online, 7/7, 24/24) a RS CCMS în conformitate cu cadrul normativ;

17.14. informarea utilizatorilor RS CCMS despre reglementările normative, modificările condițiilor tehnice de funcționare a acestuia;

17.15. utilizarea datelor consumate din RS CCMS în scopuri legale și în conformitate cu actele normative;

17.16. exercitarea altor obligații necesare asigurării funcționării corespunzătoare a RS CCMS.

Secțiunea 3
Drepturile si obligațiile Administratorului tehnic

18. Administratorul tehnic are drepturi și obligații expres stipulate în Statutul Instituției publice „Serviciul Tehnologia Informației și Securitate Cibernetică”, conform Anexei nr.1 la Hotărârea Guvernului nr.414/2018.

Secțiunea 4
Drepturile si obligațiile Registratorului RS CCMS

19. Registratorul RS CCMS are următoarele drepturi:

19.1. accesarea, vizualizarea, înregistrarea, actualizarea datelor în limitele competențelor deținute și rolului atribuit în RS CCMS;

19.2. înaintarea către Posesorul RS CCMS de propuneri privind modificarea actelor normative care reglementează funcționarea RS CCMS;

19.3. solicitarea și recepționarea de la Deținătorul RS CCMS a suportului metodologic și practic necesar privind funcționarea RS CCMS;

19.4. înaintarea către Posesorul/Deținătorul RS CCMS a propunerilor de ordin normativ, tehnic și organizatoric în vederea îmbunătățirii și sporirii eficacității funcționarii SI CCMS.

20. Registratorul RS CCMS are următoarele obligații:

20.1. înregistrarea, actualizarea (completarea, modificarea), radierea datelor obiectelor informaționale și atributelor aferente acestora, conform prevederilor Conceptului SI CCMS și rolului atribuit în SI CCMS;

20.2. desemnarea persoanelor responsabile de înregistrare, actualizare (completare, modificare), radiere a obiectelor informaționale și atributelor aferente;

20.3. asigurarea corectitudinii, autenticității și veridicității datelor înregistrate în RS CCMS;

20.4. asigurarea respectării cerințelor privind protecția datelor cu caracter personal prelucrate în cadrul RS CCMS, în conformitate cu prevederile actelor normative;

20.5. informarea Posesorului/Deținătorului și Administratorului tehnic al RS CCMS despre problemele identificate în funcționarea sistemului informațional;

20.6. întreprinderea măsurilor privind prevenirea accesului neautorizat la datele din RS CCMS de către persoanele terțe;

20.7. întreprinderea măsurilor de prevenire a incidentelor de securitate;

20.8. raportarea Posesorului/Deținătorului RS CCMS cu privire la incidentele de infrastructură, erorile de sistem sau erorile cauzate de factorul uman în scopul remedierii acestora;

20.9. înaintarea către Posesorul/Deținătorul RS CCMS a demersurilor privind autorizarea, modificarea, suspendarea și revocarea dreptului de acces la SI CCMS al Registratorilor, Furnizorilor și Destinatarilor acestuia;

20.10. utilizarea datelor obținute din RS CCMS în scopuri legale și în conformitate cu actele normative;

20.11. exercitarea altor obligații necesare asigurării funcționării corespunzătoare a RS CCMS.

Secțiunea 5
Drepturile si obligațiile Furnizorului de date în RS CCMS

21. Furnizorul de date în RS CCMS are următoarele drepturi:

21.1. accesarea și vizualizarea datelor din RS CCMS în limitele competențelor deținute și conform rolului atribuit în SI CCMS;

21.2. solicitarea de la Posesorul/Deținătorul RS CCMS a informațiilor complete privind datele obiectelor informaționale care se conțin în RS CCMS și care au fost prezentate de către acest Furnizor;

21.3. solicitarea și recepționarea suportului de la Deținătorul RS CCMS privind utilizarea corectă a SI CCMS.

21.4. înaintarea către Posesorul/Deținătorul RS CCMS a propunerilor de ordin normativ, tehnic și organizatoric în vederea îmbunătățirii și sporirii eficacității funcționarii SI CCMS.

22. Furnizorul de date în RS CCMS are următoarele obligații:

22.1. asigurarea corectitudinii, autenticității și confidențialității datelor furnizate pentru a fi înregistrate în RS CCMS;

22.2. asigurarea prezentării imediate a datelor actualizate pentru înregistrare în RS CCMS sau în conformitate cu periodicitatea preconizată în acte normative sau acord;

22.3. informarea Posesorului RS CCMS despre modificarea actelor normative aferente datelor înregistrate în RS CCMS;

22.4. informarea Posesorului/Deținătorului RS CCMS despre orice situație care face imposibila furnizarea datelor în RS CCMS;

22.5. raportarea către Deținător despre problemele de funcționalitate a componentelor RS CCMS;

22.6. desemnarea, și informarea Posesorului/Deținătorului RS CCMS, despre persoanele împuternicite cu dreptul de a transmite date pentru înregistrarea în RS CCMS;

22.7. utilizarea datelor consumate din RS CCMS în scopuri legale și în conformitate cu actele normative;

22.8. exercitarea altor obligații necesare asigurării funcționării corespunzătoare a RS CCMS.

Secțiunea 6
Drepturile si obligațiile Destinatarului de date RS CCMS

23. Destinatarul de date RS CCMS are următoarele drepturi:

23.1. solicitarea și recepționarea de la Posesorul/Deținătorul RS CCMS a datelor necesare și a suportului privind utilizarea corectă a RS CCMS;

23.2. solicitarea și recepționarea de la Posesorul/Deținătorul RS CCMS a datelor cu privire la acordarea accesului la datele înregistrate, pornind de la atribuțiile și funcțiile deținute, precum și în conformitate cu scopul prelucrării;

23.3. vizualizarea datelor din RS CCMS în conformitate cu rolul atribuit și fără dreptul de a modifica aceste date;

23.4. înaintarea către Posesorul/Deținătorul RS CCMS a propunerilor de ordin normativ, tehnic și organizatoric în vederea îmbunătățirii și sporirii eficacități funcționarii SI CCMS.

24. Destinatarul de date RS CCMS are următoarele obligații:

24.1. asigurarea accesării și utilizării datelor din RS CCMS în conformitate cu competențele și scopul legitim de utilizare a acestora;

24.2. asigurarea respectării cerințelor privind protecția datelor cu caracter personal utilizate în cadrul RS CCMS, în conformitate cu prevederile actelor normative;

24.3. asigurarea protecției, securității și confidențialității datelor accesate (vizualizate, consumate) în RS CCMS;

24.4. întreprinderea măsurilor de prevenire a incidentelor de securitate;

24.5. informarea Posesorului/Deținătorului despre neconformitățile depistate;

24.6. utilizarea datelor consumate din RS CCMS în scopuri legale și în conformitate cu actele normative;

24.7. exercitarea altor obligații necesare asigurării bunei funcționari a RS CCMS.

Capitolul IV
ȚINEREA SI ASIGURAREA FUNCTIONARII RS CCMS

25. RS CCMS se ține în format electronic. Datele cuprinse în RS CCMS sunt înscrise cu caracterele alfabetului latin extins, cu diacritice.

26. Structura RS CCMS se aprobă și se modifică prin hotărârea Guvernului, la propunerea Instituției publice „Agenția Servicii Publice”.

27. Funcțiile de administrare a SI CCMS sunt delegate de către Posesor subdiviziunii de resort.

28. RS CCMS este găzduit pe platforma tehnologică guvernamentală comună (MCloud) în conformitate cu Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud).

29. RS CCMS funcționează zilnic (7/7, 24/24), cu excepția timpului rezervat pentru lucrări de mentenanță, care sunt programate, cu unele excepții, în afara orelor de program sau în zilele de odihnă ori de sărbătoare.

30. Schimbul de date dintre RS CCMS și sisteme și resurse informaționale deținute de Agenția Servicii Publice poate fi realizat și în afara platformei de interoperabilitate în conformitate cu prevederile art.6 din Legea nr.142/2018 cu privire la schimbul de date și interoperabilitate.

31. Păstrarea RS CCMS este asigurată de către deținător până la adoptarea deciziei Guvernului de lichidare a acestuia.

32. Zonele restricționate ale RS CCMS vor fi accesibile utilizatorilor interni/externi cu o identitate verificată prin mecanisme speciale (MPass etc.).

33. Înregistrarea, actualizarea și radierea din evidență a obiectelor informaționale și atributelor aferente în RS CCMS este asigurată de către Registratori în temeiul documentelor justificative disponibile, precum și după examinarea și validarea datelor parvenite de la Furnizori.

34. Obiectele informaționale și scenariile de bază asociate obiectelor informaționalele din RS CCMS sunt descrise în Conceptul SI CCMS.

35. Evidentă obiectelor informaționale se ține conform instrucțiunilor elaborate de Deținătorul RS CCMS și aprobate în comun cu Registratorii implicați.

36. La înregistrarea inițială în RS CCMS fiecărui obiect informațional i se atribuie, în mod obligatoriu, un identificator unic, care rămâne invariabil pe parcursul ciclului de viață al obiectului.

37. Înregistrarea repetată a obiectului informațional în RS CCMS sau acumularea repetată a datelor despre el în RS CCMS, se interzice.

38. Procedura de înregistrare, actualizare și radiere a datelor include principalele etape de autentificare în sistem a Registratorului RS CCMS și de accesare a componentelor RS CCMS destinate înregistrării datelor, de completare a câmpurilor obligatorii ale formularului electronic și, după caz, a celor opționale.

39. Datele din RS CCMS reprezintă totalitatea obiectelor informaționale și atributelor acestora. Obiectele informaționale pot fi proprii sau împrumutate. Atributele proprii pot fi modificate, iar atributele împrumutate pot fi doar vizualizate.

40. Modificarea/completarea/radierea datelor din RS CCMS se realizează de către Registratorii care le-au înregistrat. În cazul radierii datelor, acestea își vor schimba statutul.

41. Toate modificările operate în RS CCMS se păstrează în ordine cronologică, cu păstrarea nemijlocită a istoricului acestora.

42. În cazul constatării incorectitudinii sau inexactității datelor înregistrate sau recepționate pentru înregistrare de la Furnizori, Registratorul este obligat să întreprindă măsuri pentru identificarea cauzei și remedierea situației, cu informarea și implicarea Furnizorului, în caz de necesitate.

43. Pentru utilizarea datelor în RS CCMS se impun următoarele restricții:

43.1. Registratorii pot vizualiza, modifica și radia datele doar în conformitate cu atribuțiile pe care le au în cadrul RS CCMS în temeiul unor motive şi/sau al documentelor justificative;

43.2.Destinatarii datelor nu sunt în drept să modifice datele obținute din RS CCMS.

44. Termenul de păstrare a documentelor semnate electronic este identic cu termenul prevăzut de cadrul normativ pentru păstrarea documentelor echivalente pe suport de hârtie.

45. Furnizorii de date sunt obligați să asigure plenitudinea, corectitudinea și autenticitatea datelor prezentate pentru a fi înregistrate în RS CCMS, precum și să asigure actualizarea acestora în modul stabilit de cadrul normativ sau în baza acordurilor cu privire la schimbul de date și interoperabilitate.

46. Înregistrarea datelor neveridice în RS CCMS este interzisă.

47. Registratorii desemnează persoanele responsabile de verificarea veridicității și înregistrarea datelor în SI CCMS.

48. Jurnalizarea evenimentelor produse în RS CCMS este asigurată de către Deținătorul acestuia, prin intermediul modului de jurnalizare intern al sistemului informațional, iar în cazul integrării cu serviciul electronic guvernamental de

jurnalizare (MLog) – în conformitate cu cadrul normativ care reglementează sistemul informațional partajat respectiv.

49. La înregistrarea, actualizarea și radierea datelor în RS CCMS, Registratorii se conduc de actele normative respective (regulamente, instrucțiuni etc.).

50. În cadrul operațiilor de prelucrare a datelor cu caracter personal efectuate conform prezentului Regulament se asigură respectarea drepturilor utilizatorilor de date cu caracter personal, în conformitate cu prevederile actelor normative privind protecția datelor cu caracter personal.

Capitolul V
MANAGEMENTUL UTILIZATORILOR ÎN CADRUL RS CCMS ȘI PROCESELE DE ADMINISTRARE

51. Managementul utilizatorilor va fi efectuat prin gestiunea rolurilor și utilizatorilor din cadrul RS CCMS de către Deținător.

52. Atât pentru asigurarea posibilității de intervenție operativă, cât și pentru descentralizarea gestionării utilizatorilor și a drepturilor de acces, Deținătorul va realiza distribuirea drepturilor conform proceselor de administrare:

52.1. administrare sistem/infrastructură;

52.2. administrare conținut;

52.3. administrare utilizatori;

52.4. administrare securitate.

53. Administrarea de sistem/infrastructură necesită gestionarea sistemelor operaționale, sistemului informațional (părți componente) al RS CCMS, bazelor de date, copierea rezervă/restabilirea, resursele de rețea.

54. Administrarea de conținut necesită configurarea proceselor prin care se gestionează, organizează, actualizează și monitorizează datele disponibile în cadrul RS CCMS.

55. Administrarea de utilizatori necesită configurarea rolurilor atribuite și este efectuată la nivel central în conformitate cu acordurile încheiate cu subiecții raporturilor juridice.

56. Administrarea de securitate se va asigura prin monitorizarea acțiunilor utilizatorilor, accesarea și furnizarea datelor de audit.

57. Procesele de administrare pe domeniile de competentă se efectuează cu ajutorul procedurilor de administrare aprobate.

57.1. Utilizarea procedurilor de administrare care nu sânt aprobate se admite numai în situații de forță majoră.

57.2. Modificări în procedura de administrare se admit numai după aprobarea lor de către Posesorul RS CCMS.

57.3. Procedurile de administrare se elaborează de către Deținător pentru fiecare proces de administrare. Toate procedurile de administrare se documentează în formă de regulamente/instrucțiuni și se aprobă de către Posesorul RS CCMS.

58.În procesul de administrare a sistemului informațional, Deținătorul asigură:

58.1. să asigure funcționarea și ținerea RS CCMS în conformitate cu procedurile de administrare și prezentul Regulament;

58.2. să asigure colectarea datelor de la Furnizori, înregistrarea și stocarea lor în banca centrală de date, menținerea și actualizarea acestora;

58.3. să verifice autenticitatea și integritatea prezentării de către utilizatori a datelor în banca centrală de date a RS CCMS;

58.4. să asigure utilizatorii RS CCMS acces la date din banca centrală de date în conformitate cu actele normative. În caz de modificare a drepturilor de acces, Deținătorul trebuie să ia decizia cu privire la reconfigurarea acestora, la necesitate;

58.5. să asigure asistență informațională utilizatorilor RS CCMS în modul stabilit;

58.6. să efectueze măsurile necesare privind protecția și confidențialitatea datelor din RS CCMS împotriva acțiunilor neautorizate (acces, actualizare, radiere și transmitere de date);

58.7. să asigure măsurile organizatorico-tehnice necesare pentru protecția datelor în conformitate cu cerințele privind protecția datelor RS CCMS și respectarea acestor măsuri;

58.8. să protejeze, prin măsuri adecvate, datele colectate, echipamentele tehnice și produsele de program utilizate pentru administrarea acestora, asigurând securitatea și integritatea datelor înregistrate în banca centrală de date a RS CCMS împotriva riscurilor de pierdere, distrugere, precum și împotriva folosirii neautorizate sau divulgării lor;

58.9. să monitorizeze acțiunile persoanelor autorizate în RS CCMS, inclusiv să supravegheze accesările datelor;

58.10. să efectueze activități de audit al securității categoriilor speciale de date cu caracter personal înregistrate în RS CCMS;

58.11. să asigure serviciul de copiere de rezervă a întregului RS CCMS pentru continuitatea operațională în cazul apariției unui incident și restabilirea rapidă a funcționalității RS CCMS fără pierdere de date în mai puțin de o oră, cu excluderea/limitarea extinderii defecțiunilor în cadrul RS CCMS, cu minimizarea impactului negativ asupra activității utilizatorilor;

58.12. să acorde suportul necesar pentru conectarea acestora la RS CCMS;

58.13. să informeze utilizatorii despre modificările condițiilor tehnice de funcționare a RS CCMS.

59. Dezvoltarea RS CCMS include activități ce țin de dezvoltarea sistemului informațional, structurilor bazelor de date, rapoartelor generate din RS CCMS, elaborarea web serviciilor, managementul proceselor business.

60. Funcțiile de dezvoltare a RS CCMS sunt executate de către Deținătorul acestuia.

Capitolul VI
REGIMUL JURIDIC DE UTILIZARE A DATELOR DIN RS CCMS

61. Accesul la datele din RS CCMS, precum și punerea la dispoziție a datelor din RS CCMS sunt limitate și se efectuează în baza actelor normative care prevăd aceste proceduri, în special: Legea nr.142/2018 cu privire la schimbul de date și interoperabilitate și Legea nr. 148/2023 privind accesul la informațiile de interes public.

62. Utilizatorii au drept de acces la datele din RS CCMS în limitele competențelor deținute și rolului atribuit în SI CCMS, cu respectarea regimului juridic al datelor accesate. Nivelul de acces la date pentru fiecare utilizator corespunde funcției deținute și profilului de acces.

63. Dreptul de acces la RS CCMS este segmentat pe unități de conținut, atribuind prerogative partajate, si anume: înregistrare, vizualizare, actualizare, procesare, extragere, validare/invalidare și radiere.

64. Accesul la RS CCMS este segmentat pe utilizatori, ale căror drepturi de acces sunt definite în acte normative și poate fi activ sau pasiv.

65. Registratorul, de regulă, are acces la datele din RS CCMS, ceea ce presupune posibilitatea de înregistrare, actualizare și radiere din oficiu a datelor înregistrate de acesta, în limita scopului și atribuțiilor acordate prin prezentul Regulament și stipulate în acte normative.

66. Furnizorul de date și Destinatarul au acces pasiv la datele din RS CCMS, ceea ce presupune vizualizarea datelor numai în formatul individual permis pentru fiecare în parte. Respectiv și Registratorul, va avea rol cu acces pasiv la datele străine.

67. Furnizorul de date poate modifica și radia datele înregistrate de aceștia în RS CCMS, prin intermediul Registratorului.

68. Destinatarul datelor din RS CCMS nu este în drept să modifice datele consumate.

69. Destinatarul poate consuma datele înregistrate în RS CCMS conform rolurilor atribuite.

70. Accesul la RS CCMS și exploatarea acestuia fără autorizare nominală sunt strict interzise și sunt calificate ca acces neautorizat la informația cu caracter personal, atribuită categoriei de informație cu caracter limitat.

71. Dreptul de acces la RS CCMS nu este unul permanent, acesta poate fi suspendat sau revocat.

72. Înregistrarea, vizualizarea, actualizarea, procesarea, extragerea, validarea/invalidarea datelor în/din RS CCMS de pe un nume sau profil de utilizator străin sunt strict interzise și calificate ca acces neautorizat.

73 Revocarea dreptului de acces la RS CCMS se efectuează la cererea Registratorului, adresată Deținătorului sistemului, în una dintre următoarele situații:

73.1. la încetarea/suspendarea raportului de serviciu/de muncă al utilizatorului;

73.2. la intervenirea modificărilor în raportul de serviciu/de muncă, când noile atribuții nu impun accesul la datele din RS CCMS;

73.3. la constatarea încălcării măsurilor de protecție și/sau a regulilor de securitate a datelor din RS CCMS;

73.4. în alte cazuri, conform actelor normative.

74. Datele consumate din RS CCMS nu pot participa la transmiterea transfrontalieră, dacă actele normative sau tratatele internaționale la care Republica Moldova este parte nu prevăd altfel.

Capitolul VII
ASIGURAREA PROTECTIEI SI SECURITATII DATELOR DIN RS CCMS

Secțiunea 1
Securitatea informației în RS CCMS

75. Datele din RS CCMS fac parte din categoria datelor cu acces limitat, care necesită a fi protejate. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul RS CCMS se efectuează de către utilizatori cu drepturi de acces la sistem informațional și cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

76. Măsurile de protecție și securitate a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, administrare, mentenanță și dezvoltare a RS CCMS și se efectuează neîntrerupt de către Deținătorul RS CCMS.

77. Obiecte ale asigurării protecției și securității datelor din RS CCMS se consideră tot complexul de mijloace software și hardware care asigură realizarea proceselor informaționale, și anume:

77.1. baza de date, sistemele informaționale, sistemele operaționale, sistemele de gestiune a bazelor de date, sistemele de evidență și alte aplicații care asigură funcționarea RS CCMS;

77.2. sistemele de telecomunicații, rețelele, serverele, calculatoarele și alte mijloace tehnice de prelucrare a datelor.

78. Protecția datelor cu caracter personal din RS CCMS la nivel de Deținător se efectuează prin următoarele metode:

78.1. prevenirea conexiunilor neautorizate la rețelele de transport de date guvernamentale și interceptării cu ajutorul mijloacelor tehnice specifice a datelor din RS CCMS transmise prin aceste rețele;

78.2. asigurarea măsurilor de protecție a datelor prin folosirea metodelor criptografice de transmitere a datelor prin rețelele de transport de date guvernamentale;

78.3. excluderea accesului neautorizat la datele din RS CCMS prin utilizarea funcționalităților de autorizare ale serviciului guvernamental MPass;

78.4. prevenirea acțiunilor speciale tehnice și de program care duc la distrugerea, denaturarea datelor sau cauzează defecțiuni în funcționarea complexului tehnic si de program;

78.5. efectuarea periodică planificată a copiilor de siguranță a datelor și fișierelor mijloacelor de program;

78.6. efectuarea tuturor masurilor aferente asigurării restabilirii si continuității funcționarii RS CCMS în cazul incidentelor.

79. Posesorul/ Deținătorul/ Registratorul al RS CCMS elaborează și implementează politica de securitate informațională pentru asigurarea respectării regulilor, standardelor si normelor în domeniul securității informaționale, incluzând:

79.1. identitatea persoanei responsabile de politica de securitate;

79.2. principalele măsuri tehnico-organizatorice necesare asigurării funcționarii RS CCMS;

79.3. procedurile interne ce exclud cazurile de modificare nesancționată a mijloacelor software și/sau a informației din RS CCMS;

79.4. responsabilitățile personalului utilizatorului RS CCMS privind asigurarea securității informaționale.;

79.5. procedurile de control intern al utilizatorului RS CCMS privind respectarea condițiilor de securitate informațională.

80. Securitatea informațională a RS CCMS se asigură prin aplicarea metodelor și efectuarea acțiunilor descrise în planul de continuitate al RS CCMS și, după caz, a procedurilor operaționale.

81. Securitatea informațională se menține pe parcursul întregului ciclu de viață al Sistemului informațional SI CCMS și se perfecționează continuu pentru prevenirea noilor pericole.

82. Fiecare subiect al raporturilor juridice asigură prevenirea, informarea sau, după caz, instruirea personalului implicat privind metodele si procedeele de contracarare a pericolelor informaționale.

83. Toți utilizatorii RS CCMS poartă răspundere disciplinară, civilă, contravențională sau penală în conformitate cu actele normative, pentru prelucrarea, divulgarea, transmiterea datelor din RS CCMS persoanelor terțe contrar prevederilor legislației.

84. Funcționarea RS CCMS se suspendă de către Deținătorul sistemului informațional din inițiativă proprie sau la demersul Posesorului, în una dintre următoarele situații:

84.1. în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al SI CCMS;

84.2. la apariția circumstanțelor de forță majoră;

84.3. la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea SI CCMS;

84.4. în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SI CCMS;

84.5. la decizia Posesorului/Deținătorului.

85. Lucrările profilactice planificate în complexul de mijloace software și hardware se efectuează după notificarea Registratorilor de către Posesor/Deținător, în baza unui plan, cu cel puțin două zile lucrătoare înainte de inițierea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil. Lucrările profilactice neplanificate se efectuează la necesitate ca urmare a identificării unor deficiențe în baza sesizărilor subiecților raporturilor juridice, după coordonarea prealabilă cu Posesorul/Deținătorul în situația nefuncționării sau funcționării necorespunzătoare a complexului de mijloace software și hardware.

86. În cazul apariției circumstanțelor de forță majoră și a dificultăților tehnice în funcționarea complexului de mijloace software și hardware al RS CCMS din vina persoanelor terțe este posibilă suspendarea funcționării SI CCMS, cu informarea utilizatorilor RS CCMS prin mijloacele tehnice disponibile.

Secțiunea 2
Protecția datelor cu caracter personal din RS CCMS

87. Datele de identificare și individualizare fac parte din categoria datelor cu caracter personal. Asigurarea securității, confidențialității și a integrității datelor prelucrate în cadrul RS CCMS se efectuează de către utilizatori cu drepturi de acces la sistem cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

88. Dreptul de informare a utilizatorului datelor cu caracter personal, dreptul de acces la datele cu caracter personal, dreptul de intervenție asupra datelor cu caracter personal, dreptul de opoziție al utilizatorului datelor cu caracter personal și alte aspecte ce țin de domeniul protecției datelor cu caracter personal se vor realiza în condițiile prevederilor actelor normative ce fac obiectul de reglementare în domeniul respectării drepturilor utilizatorului de date cu caracter personal.

89. Prelucrarea de date din RS CCMS trebuie să garanteze respectarea următoarelor principii privind protecția datelor cu caracter personal:

89.1. specificarea și limitarea scopului;

89.2. adoptarea de masuri tehnice și organizaționale în scopul asigurării unui nivel adecvat de protecție a datelor cu caracter personal, în conformitate cu actele normative.

90. În cazul incidentelor de securitate, subiecții raporturilor juridice vor întreprinde măsuri necesare pentru depistarea sursei de producere a incidentului, vor efectua analiza acestuia și vor înlătura cauzele incidentului de securitate, cu informarea Centrului National pentru Protecția Datelor cu Caracter Personal.

Capitolul VIII
CONTROLUL ȘI RESPONSABILITATEA

91. RS CCMS este supus unui control intern și extern. Controlul intern este efectuat permanent de către Posesor, iar controlul extern este efectuat de către instituțiile abilitate și certificate în domeniul auditului.

92. Responsabilitatea pentru organizarea funcționării RS CCMS aparține Posesorului/Deținătorului acestuia.

93. La organizarea controlului extern a RS CCMS Posesorul/Deținătorul este obligat să asigure dreptul de acces la complexul de mijloace software și hardware ale RS CCMS.

94. Responsabilitatea pentru ținerea RS CCMS revine deținătorului. Deținătorul este obligat să întreprindă masurile de rigoare pentru eliminarea neconformităților depistate, cu ulterioara informare a organului de control.

95. Controlul legalității operațiunilor de prelucrare a datelor cu caracter personal desfășurate în RS CCMS se efectuează de către Centrul National pentru Protecția Datelor cu Caracter Personal.

96. Utilizatorii RS CCMS care consumă date cu caracter personal sunt responsabili, în conformitate cu actele normative, pentru divulgarea, transferul către persoane terțe și utilizarea acestora în scopuri personale.

97. Subiecții raporturilor juridice responsabili pentru administrarea RS CCMS, înregistrarea datelor, furnizarea datelor și asigurarea funcționării RS CCMS, poartă răspundere personală în conformitate cu actele normative, pentru completitudinea, autenticitatea, veridicitatea, integritatea datelor, precum și pentru păstrarea și utilizarea acestora.