Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr.____

din _____ 2026

privind sistemul informațional ”Decizii vamale”

În temeiul art.18 alin.(1) și art.22 lit. c) și 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

HOTĂRĂŞTE:

1. Se instituie Sistemul informațional „Decizii vamale”.
2. Se aprobă:

2.1. Conceptul Sistemului informațional „Decizii vamale”, conform anexei nr. 1;

2.2. Regulamentul resursei informaționale formate de Sistemul informațional „Decizii vamale”, conform anexei nr.2.

3. Serviciul Vamal, în calitate de posesor și deținător al Sistemului informațional „Decizii vamale”, va asigura, conform competențelor legale, crearea și implementarea acestuia, precum și administrarea, mentenanța și dezvoltarea sa ulterioară din contul și în limitele mijloacelor financiare alocate anual din bugetul de stat, precum și din alte surse, conform legislației.
4. Controlul asupra executării prezentei hotărâri se pune în sarcina Serviciului Vamal.
5. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

Prim-ministru **Alexandru MUNTEANU**

Ministrul finanțelor Andrian GAVRILIȚĂ

Anexa nr. 1 la
Hotărârea Guvernului nr. _____/2026

CONCEPTUL
Sistemului informațional ”Decizii vamale”

INTRODUCERE

În conformitate cu angajamentele asumate de Republica Moldova în cadrul procesului de aderare la Uniunea Europeană, inclusiv cu prevederile Programului național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029, aprobat prin Hotărârea Guvernului nr. 306/2025 (Monitorul Oficial al Republicii Moldova, 2025, nr. 269–288, art.319), precum și ale Hotărârii Guvernului nr. 260/2025 cu privire la aprobarea Agendei de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025–2027 (Monitorul Oficial al Republicii Moldova, 2025, nr. 215–222, art.256), se impune armonizarea procedurilor vamale naționale cu standardele și cerințele comunitare, atât prin adaptarea cadrului normativ intern, cât și prin dezvoltarea sistemelor informatice corespunzătoare.

În acest context, se prevede dezvoltarea și implementarea unui sistem informațional național echivalent cu Sistemul informațional de Decizii Vamale (CDS) utilizat la nivelul Uniunii Europene, care la momentul aderării Republicii Moldova la Uniunea Europeană, să funcționeze drept componentă națională a acestuia și să asigure interoperabilitatea deplină cu infrastructura informatică europeană relevantă.

Sistemul Informațional ”Decizii vamale” constituie o platformă digitală centralizată, destinată optimizării și automatizării proceselor aferente gestionării deciziilor vamale. Sistemul asigură depunerea și procesarea cererilor, precum și emiterea, reevaluarea, modificarea, suspendarea, anularea și revocarea deciziilor vamale, inclusiv evidența, monitorizarea, schimbul de informații și trasabilitatea acestora.

Implementarea Sistemului Informațional ”Decizii Vamale” *(în continuare SI ”Decizii vamale”)* va contribui la aplicarea uniformă a legislației vamale naționale și la consolidarea transparenței, securității și eficienței proceselor administrative în domeniul vamal. Totodată, sistemul va oferi autorității vamale și operatorilor economici un instrument modern și sigur pentru gestionarea proceselor relevante deciziilor vamale, bazat pe utilizarea exclusivă a tehnicilor de prelucrare electronică a datelor.

Instituirea acestui sistem reprezintă un pas esențial în procesul de implementare a cadrului legal național armonizat cu acquis-ul comunitar și constituie o etapă pregătitoare în perspectiva aderării la Uniunea Europeană. Aceasta va asigura capacitatea tehnică și juridică necesară aplicării Regulamentului (UE) nr. 952/2013 al Parlamentului European și al Consiliului din 9 octombrie 2013 de stabilire a Codului vamal al Uniunii și Regulamentului de punere în aplicare (UE) 2025/512 al Comisiei din 13 martie 2025 privind modalitățile tehnice pentru dezvoltarea, întreținerea și utilizarea sistemelor electronice destinate schimbului și stocării de informații în temeiul Regulamentului (UE) nr. 952/2013 al Parlamentului European și al Consiliului (Jurnalul Oficial al Uniunii Europene L 2025/512, 20.3.2025).

Componenta națională a sistemului va deveni operațională anterior aderării, permițând aplicarea legislației naționale, iar ulterior, după aderare, odată cu conectarea la infrastructura informatică a Uniunii Europene și asigurarea interoperabilității sistemelor informatice, va facilita integrarea completă a fluxurilor de date și aplicarea uniformă a cadrului legislativ vamal. Această abordare va contribui la reducerea sarcinilor administrative, la consolidarea cooperării interinstituționale, la creșterea transparenței proceselor în raport cu mediul de afaceri și la facilitarea comerțului internațional.

Prezentul concept are drept obiectiv definirea cadrului detaliat al sistemului, incluzând arhitectura propusă, funcționalitățile esențiale, mecanismele de gestionare a fluxurilor de date și modalitățile de integrare cu infrastructura informatică națională și cu platformele corespunzătoare la nivelul Uniunii Europene. Implementarea acestei soluții va asigura compatibilitatea, interoperabilitatea și sustenabilitatea pe termen lung a sistemului, reprezentând un instrument esențial pentru modernizarea și eficientizarea activității vamale în Republica Moldova.

Capitolul I
DISPOZIȚII GENERALE

1. Conceptul SI ”Decizii vamale” (în continuare - *Concept*) stabilește spațiul funcțional, structura organizatorică, spațiul informațional, spațiul tehnologic, securitatea sistemului informațional și protecția informației în cadrul SI „Decizii Vamale”.

2. SI ”Decizii vamale” reprezintă o soluție informatică din categoria Guvern către Guvern (G2G), Guvern către Business (G2B) și Guvern către Cetățeni (G2C) și constituie totalitatea mijloacelor software, hardware și de infrastructură ale utilizatorului, destinate formării resursei informaționale privind deciziile vamale, precum și schimbul de informații cu alte autorități vamale.

3. În contextul Conceptului sunt utilizate următoarele noțiuni:

3.1 autorizare – proces al SI ”Decizii vamale” care determină nivelul de acces atribuit unui utilizator autentificat pentru a accesa resurse securizate, controlate de sistem;

3.2 concept – document care descrie într-o formă generalizată trăsăturile esențiale ale SI ”Decizii vamale” ca totalitate de viziuni interconectate de funcționare a sistemului;

3.3 obiect informațional – reflectare virtuală a obiectului înregistrării în cadrul resursei informaționale;

3.4 platforma MConnect – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);

3.5 serviciul MLog – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);

3.6 serviciul MPass – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass).

4. SI ”Decizii vamale” este parte componentă a Sistemului Informațional Integrat Vamal.

5. SI ”Decizii vamale” înglobează posibilități funcționale de gestionare a fluxurilor de lucru, schimb de informații, notificarea utilizatorilor, precum și pentru stocarea datelor și depunerea online a cererilor, necesare procesării acestora și emiterii deciziilor.

6. SI ”Decizii vamale” pune la dispoziția utilizatorilor următoarele servicii:

6.1 depunerea online a cererilor;

6.2 acces la toate informațiile privind procesarea cererii și decizia vamală emisă;

6.3 evidența strictă a cererilor și deciziilor vamale.

7. Obiectivele SI ”Decizii vamale” sunt:

7.1 crearea și operarea unui sistem informațional stabil, sigur și fiabil pentru evidența, gestiunea și trasabilitatea deciziilor vamale, asigurând transparența, corectitudinea și securitatea procesului decizional, prin digitalizarea completă a proceselor și arhivarea electronică a datelor;

7.2 facilitarea comunicării electronice și a schimbului securizat de date și documente între Serviciul Vamal, mediul de afaceri și autoritățile vamale internaționale, asigurând interoperabilitatea sistemului la nivel național și european, promovând cooperarea transfrontalieră;

7.3 optimizarea și automatizarea proceselor de gestionare a deciziilor vamale, reducând intervenția umană în etapele critice, crescând eficiența operațională, reducând timpul de procesare și costurile pentru mediul de afaceri și facilitând comerțul internațional;

7.4 consolidarea capacității decizionale a Serviciului Vamal prin centralizarea și trasabilitatea informațiilor relevante, astfel încât să permită luarea rapidă, informată și eficientă a deciziilor și gestionarea riscurilor vamale;

7.5 implementarea noilor instrumente internaționale în domeniul vamal.

8. Principiile de bază ale SI ”Decizii vamale” sunt următoarele:

8.1 principiul legalității - presupune crearea și exploatarea sistemului informațional în conformitate cu legislația națională și a normelor și standardelor internaționale recunoscute în domeniu;

8.2 principiul independenței de platformă - interfața utilizator a sistemului informațional nu va impune o anumită platformă software și hardware pentru calculatorul utilizatorului;

8.3 principiul datelor sigure - dispune introducerea datelor în sistem doar prin canalele autorizate și autentificate;

8.4 principiul securității informaționale - presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și de acces nesancționat;

8.5 principiul accesibilității informației cu caracter public - presupune implementarea procedurilor de asigurare a accesului utilizatorilor la informația cu caracter public, furnizată de soluția informațională;

8.6 principiul transparenței - presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informaționale și de telecomunicații;

8.7 principiul extensibilității - stipulează posibilitatea extinderii și completării sistemului informațional cu noi funcții sau îmbunătățirea celor existente;

8.8 principiul scalabilității - presupune asigurarea unei performanțe similare a soluției informaționale pentru volumele mici/mari de date și accesări la sistem;

8.9 principiul integrării cu sistemele existente - presupune posibilitatea soluției informaționale de a se integra și interacționa cu aplicațiile deja implementate;

8.10 principiul simplității și comodității utilizării - presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor Sistemului, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție.

8.11 principiul conformității prelucrării datelor cu caracter personal - prelucrarea datelor cu caracter personal ale persoanelor implicate în procesul de obținere are loc în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

9. Noțiunile utilizate în Concept corespund celor reglementate de Codul vamal al Republicii Moldova nr. 95/2021, de Legea nr. 467/2003 privind informatizarea și resursele informaționale de stat, precum și de Hotărârea Guvernului nr. 92/2023 privind punerea în aplicare a Codului vamal nr. 95/2021 și alte acte normative în materie.

Capitolul II
SPAȚIUL JURIDICO-NORMATIV AL SI ”DECIZII VAMALE”

10. Cadrul normativ al SI ”Decizii vamale” este format din legislația națională, tratatele la care Republica Moldova este parte. Crearea și funcționarea SI ”Decizii vamale” sunt reglementate de următoarele acte normative:

10.1 Constituția Republicii Moldova nr. 1/1994;

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

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

10.4 Legea nr. 302/2017 cu privire la Serviciul Vamal;

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

10.6 Codul vamal al Republicii Moldova nr. 95/2021;

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

10.8 Hotărârea Guvernului nr. 561/2007 cu privire la Sistemul Informațional Integrat Vamal;

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

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

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

10.12 Hotărârea Guvernului nr.708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);Hotărârea Guvernului nr. 92/2023 cu privire la punerea în aplicare a Codului vamal nr. 95/2021;

10.13 Hotărârea Guvernului nr.650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030;

10.14 Hotărârea Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice;

10.15 Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design.

11. La dezvoltarea și implementarea SI ”Decizii vamale” se vor respecta următoarele reglementări tehnice și standarde aplicabile privind dezvoltarea soluțiilor informatice:

11.1 Reglementarea tehnică „Procesele ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006;

11.2 Reglementarea tehnică „Modul de evidență a serviciilor publice electronice”, aprobată prin Ordinul viceministrului dezvoltării informaționale nr.94/2009 cu privire la aprobarea unor reglementări tehnice;

11.3 Reglementarea tehnică „Prestarea serviciilor publice electronice. Cerințe tehnice”, aprobată prin Ordinul viceministrului dezvoltării informaționale nr.94/2009 cu privire la aprobarea unor reglementări tehnice;

11.4 Reglementarea tehnică „Asigurarea securității informaționale la prestarea serviciilor publice electronice. Cerințe tehnice”, aprobată prin Ordinul viceministrului dezvoltării informaționale nr. 94/2009 cu privire la aprobarea unor reglementări tehnice;

11.5 Reglementarea tehnică „Determinarea costului de elaborare şi implementare a sistemelor informaționale automatizate. Normativele şi estimarea cheltuielilor de lucru”, aprobată prin Ordinul viceministrului dezvoltării informaționale nr. 94/2009 cu privire la aprobarea unor reglementări tehnice;

11.6 SM ISO/CEI 27002:2014 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației”;

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

11.8 SM ISO/CEI 15408-1 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 1: Introducere și model general”;

11.9 SM ISO/CEI 15408-2 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 2: Cerințe funcționale de securitate”;

11.10 SM ISO/CEI 15408-3 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 3: Cerințe de asigurare a securității”;

11.11 SM EN ISO/IEC 27002 „Securitatea informației, securitatea cibernetică și protecția vieții private. Mijloace de control al securității informației”.

Capitolul III
SPAŢIUL FUNCŢIONAL AL SI ”DECIZII VAMALE”

12. SI ”Decizii vamale” va asigura îndeplinirea atât a funcțiilor de bază ale sistemului informațional tip, cât și a funcțiilor specifice, determinate de destinația SI ”Decizii vamale”, care sunt grupate în blocuri funcționale specializate.

13. Funcțiile de bază ale SI ”Decizii vamale” sunt următoarele:

13.1 Formarea și gestionarea băncii de date a sistemului, inclusiv colectarea, stocarea, structurarea și actualizarea informațiilor, în conformitate cu cerințele legale;

13.2 Organizarea asigurării informaționale și a suportului decizional, astfel încât să fie garantat accesul autorizat la date și sprijinul proceselor decizionale ale Serviciului Vamal, inclusiv prin:

13.2.1. definirea clară a drepturilor și responsabilităților utilizatorilor;

13.2.2. implementarea mecanismelor de control și monitorizare a fluxurilor de date;

13.2.3. furnizarea rapoartelor, analizelor și indicatorilor relevanți pentru toate nivelurile de management;

13.2.4. menținerea integrității, consistenței și actualizării continue a datelor;

13.2.5. garantarea disponibilității informațiilor critice prin măsuri de securitate, continuitate a activității și planuri de backup;

13.2.6. facilitarea schimbului de informații cu alte sisteme interne sau externe, prin interoperabilitate standardizată și protecție a datelor sensibile.

13.3 Asigurarea protecției și calității informațiilor, inclusiv:

13.3.1. protecția datelor în toate etapele de procesare, stocare și transmitere, conform legislației privind datele cu caracter personal și regimul informațiilor clasificate, dacă este cazul;

13.3.2. implementarea unui sistem de management al calității bazat pe abordarea de proces, conform Standardului Național SM EM ISO 9001:2002 „Sisteme de management al calității. Cerințe”.

13.4. Asigurarea funcționării integrate a sistemului, inclusiv interoperabilitatea subsistemelor, integritatea fluxurilor informaționale și sprijinul proceselor decizionale ale Serviciului Vamal;

13.5. Automatizarea proceselor de activitate ale Serviciului Vamal și tranziția la fluxuri de lucru exclusiv digitale, cu creșterea transparenței și a accesului la servicii electronice pentru toți subiecții implicați;

13.6. Supravegherea, controlul și managementul riscului în domeniile de competență ale Serviciului Vamal;

13.7. Administrarea sistemului în condiții optime, astfel încât să fie garantată continuitatea, securitatea și eficiența funcționării acestuia.

14. În cadrul funcționării SI ”Decizii vamale” se realizează funcții specifice, grupate în contururi funcționale speciale:

14.1. depunerea și procesarea cererilor depuse de utilizatori;

14.2. administrarea și monitorizarea acțiunilor utilizatorilor.

15. Conturul funcțional “Depunerea cererilor” include următoarele funcții:

15.1. depunerea cererilor, modificarea cererilor și vizualizarea statutelor lor;

15.2. trimiterea, primirea și răspunderea la mesaje;
15.3. retragerea cererilor depuse;
15.4. vizualizarea deciziilor și statutelor lor;
15.5. comunicarea prin intermediul notificărilor SI ”Decizii vamale”.
16. Conturul funcțional “Gestiunea deciziilor vamale” include următoarele funcții:
16.1. procesarea cererilor și emiterea deciziilor vamale;
16.2. acceptarea cererilor depuse;
16.3. respingerea cererilor depuse;
16.4. intrarea în vigoare a deciziei vamale;
16.5. anularea deciziei vamale;
16.6. revocarea deciziei vamale;
16.7. modificarea deciziei vamale;
16.8. reevaluarea deciziei vamale;
16.9. suspendarea deciziei vamale;
16.10. menținerea deciziei vamale;
16.11. trimiterea, primirea și răspunderea la mesaje;
16.12. comunicarea prin intermediul notificărilor SI ”Decizii vamale”.
17. Conturul funcțional “Administrarea și monitorizarea acțiunilor utilizatorilor” include următoarele funcții:
17.1. asigurarea integrității logice a SI ”Decizii vamale”;
17.2. administrarea bazelor de date ale SI ”Decizii vamale”;
17.3. elaborarea și mentenanța ghidurilor de sistem și a clasificatoarelor;
17.4. delimitarea drepturilor de acces pentru utilizatori;
17.5. asigurarea securității, protecției și integrității informației în SI ”Decizii vamale” în baza standardului național SM EN ISO/IEC 27001:2017 “Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe”;
17.6. asigurarea respectării cerințelor sistemului de protecție a datelor cu caracter personal.

Capitolul IV
STRUCTURA ORGANIZATORICĂ A SI ”DECIZII VAMALE”

18. Funcțiile de bază privind formarea și exploatarea SI ”Decizii vamale” sunt divizate între:
18.1. proprietarul SI ”Decizii vamale”;
18.2. posesorul SI ”Decizii vamale”;
18.3. deținătorul SI ”Decizii vamale”;
18.4. administratorul tehnic SI ”Decizii vamale”;
18.5. furnizorii de date/registratorii de date pentru SI ”Decizii vamale”;
18.6. utilizatorii SI ”Decizii vamale”.
19. Proprietarul SI ”Decizii vamale” este statul.
20. Posesorul și deținătorul al SI ”Decizii vamale” este Serviciul Vamal din subordinea Ministerului Finanțelor, care asigură condiţiile financiare, juridice şi organizatorice, precum şi realizarea nemijlocită a competenţelor de creare, administrare, mentenanţă şi dezvoltarea sistemului.
21. Inițial, administratorul tehnic al SI „Decizii vamale” este Serviciul Vamal. Ulterior, după migrarea sistemului informațional și încheierea Acordului privind prestarea serviciilor platformei tehnologice guvernamentale comune (MCloud) cu posesorul platformei și a Acordului privind administrarea tehnică și menținerea sistemului informațional, administratorul tehnic al SI „Decizii vamale” va fi Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, care își va exercita atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a sistemelor informaționale de stat.

22. Deținătorul al SI ”Decizii vamale” va dispune de un mecanism de înregistrare și administrare a profilurilor utilizatorilor sistemului, implicați în sistem. Acest mecanism va permite definirea parametrilor de acces la interfață, servicii, fișiere și conținutul bazei de date.

23. Furnizori de date pentru SI ”Decizii vamale” sunt:

23.1. Agenția Servicii Publice – furnizează date cu privire la persoanele fizice luate în evidență în Registrul de stat al populației și datele cu privire la unitățile de drept luate în evidență în Registrul de stat al unităților de drept;

23.2. Serviciul Vamal – furnizează date despre operatorii economici, înregistrați ca operatori economici care efectuează activități economice externe, și date despre autorizațiile Operatorilor Economici Autorizați.

24. Registratorii SI ”Decizii vamale” reprezintă funcționarii vamali cu drept de întocmire a deciziilor vamale, de modificare, de suspendare, de reevaluare și de menținere a acestora.

25. Utilizatorii SI ”Decizii vamale” sunt persoanele fizice, persoanele juridice și funcționarii vamali beneficiari ale serviciilor SI ”Decizii vamale” sau ale raporturilor juridice de gestionare automatizată a SI ”Decizii vamale”.

Capitolul V
DOCUMENTELE SI ”DECIZII VAMALE”

26. Documentele SI ”Decizii vamale” reprezintă totalitatea documentelor procedurale necesare pentru ținerea evidenței, monitorizarea și emiterea deciziilor vamale.

27. În cadrul SI ”Decizii vamale” se folosesc următoarele categorii de documente:

27.1. *documente de intrare*, care sunt relevante pentru emiterea deciziilor vamale;

27.2. *documente de ieșire*, care se consideră documente finale ce pot fi utilizate și care reprezintă deciziile vamale, notificările privind emiterea deciziilor vamale la adresa de e-mail. SI „Decizii vamale” gestionează următoarele decizii vamale:

27.2.1. autorizația pentru statutul de destinatar agreat (ACE);

27.2.2. autorizația pentru statutul de expeditor agreat (ACR);

27.2.3. autorizația pentru statutul de destinatar agreat în sensul TIR (ACT);

27.2.4. autorizația pentru utilizarea garanției globale, inclusiv cu cuantum redus, sau exonerarea de la aceasta (CGU);

27.2.5. autorizația pentru funcționarea spațiilor de depozitare a mărfurilor într-un antrepozit vamal:

27.2.5.1. autorizația pentru funcționarea spațiilor de depozitare a mărfurilor într-un antrepozit vamal – Tipul 1 (CW1);

27.2.5.2. autorizația pentru funcționarea spațiilor de depozitare a mărfurilor într-un antrepozit vamal – Tipul 2 (CW2);

27.2.5.3. autorizația pentru funcționarea spațiilor de depozitare a mărfurilor într-un antrepozit vamal – Privat (CWP);

27.2.6. autorizația pentru funcționarea spațiilor de depozitare a mărfurilor într-un depozit temporar (TST);

27.2.7. autorizația pentru amânarea plăților (DPO);

27.2.8. autorizația pentru depunerea declarației simplificate sub forma unei înscrieri în evidențele declarantului (EIR);

27.2.9. autorizația pentru utilizarea unui document electronic de transport ca declarație vamală (ETD);

27.2.10. autorizația pentru utilizarea regimului vamal de destinație finală (EUS);

27.2.11. autorizația pentru utilizarea regimului vamal de perfecționare activă (PA);

27.2.12. autorizația pentru utilizarea regimului vamal de perfecționare pasivă (PP);

27.2.13. autorizația pentru utilizarea declarației simplificate (SDE);

27.2.14. autorizația pentru utilizarea sigiliilor speciale (SSE);

27.2.15. autorizația pentru utilizarea regimului vamal de admitere temporară (TEA);

27.2.16. autorizația pentru utilizarea declarației de tranzit cu un set redus de date (TRD);

27.2.17. autorizația pentru simplificarea determinării sumelor care fac parte din valoarea în vamă a mărfurilor (CVA);

27.2.18. autorizația pentru statutul de exportator aprobat.

27.3. *documente tehnologice,* care include rapoarte de analiză, rapoarte de monitorizare, lista utilizatorilor și drepturile acestora, documentele ce conțin înregistrări de audit privind acțiunile utilizatorilor, erorile de sistem, precum și ghidurile de utilizare a SI ”Decizii vamale”.

Capitolul VI
SPAȚIUL INFORMAȚIONAL AL SI ”DECIZII VAMALE”

Secțiunea 1
Obiectele informaționale ale SI ”Decizii vamale”

28. Resursa informațională a SI ”Decizii vamale” este reprezentată de un ansamblu de obiecte informaționale și interacțiunea acestora. Obiectele informaționale SI ”Decizii vamale” includ:

28.1. cererile;

28.2. profilurile utilizatorilor;

28.3. persoanele juridice;

28.4. decizii;

28.5. persoanele fizice.

29. Identificarea obiectelor SI ”Decizii vamale” se efectuează prin utilizarea pentru fiecare dintre ele a numărului de identificare unic generat și atribuit de sistem, cu excepția identificatorilor obiectelor informaționale împrumutate din alte resurse informaționale de stat.

30. Identificatorul obiectului informațional „cereri” este cheia unică formată din litere și cifre generată de sistem.

31. Identificatorul obiectului informațional „persoanele juridice”:

31.1. pentru rezidenții Republicii Moldova – este numărul de identificare de stat al persoanelor juridice (IDNO), preluat din Registrul de stat al unităților de drept. Adițional se va indica separat și numărul de identificare EORI (Economic operators registration and identification number);

31.2. pentru nerezidenți – este numărul de identificare EORI (Economic operators registration and identification number);

31.3. Identificatorul obiectului informațional „persoane fizice” și „Profilurile utilizatorilor” este numărul de identificare de stat al persoanei fizice (IDNP), preluat din Registrul de stat al populației.

32. Persoanele fizice reprezintă un obiect informațional care include date privind persoanele delegate ale persoanei juridice. Obiectul informațional conține următoarele date:

32.1. IDNP-ul, numele și prenumele, data nașterii, naționalitatea și genul persoanei fizice;

32.2. datele de contact: telefon, e-mail;

32.3. pentru nerezidenți – este numărul de identificare EORI (Economic operators registration and identification number).

33. Decizii - reprezintă obiectul informațional principal al sistemului, care este de următoarele tipuri și subtipuri:

33.1. Autorizația pentru statutul de destinatar agreat" (ACE);

33.2. Autorizația pentru statutul de expeditor agreat" (ACR);

33.3. Autorizația pentru statutul de destinatar agreat în sensul TIR (ACT);

33.4. Autorizația pentru utilizarea garanției globale, inclusiv cu cuantum redus, sau exonerarea de garanție (CGU);

33.5. Autorizația pentru funcționarea spațiilor de depozitare a mărfurilor într-un antrepozit vamal:

33.5.1. Autorizația pentru funcționarea spațiilor de depozitare a mărfurilor într-un antrepozit vamal – Tipul 1 (CW1);

33.5.2. Autorizația pentru funcționarea spațiilor de depozitare a mărfurilor într-un antrepozit vamal – Tipul 2 (CW2);

33.5.3. Autorizația pentru funcționarea spațiilor de depozitare a mărfurilor într-un antrepozit vamal – Privat (CWP).

33.6. Autorizația pentru funcționarea spațiilor de depozitare a mărfurilor într-un depozit temporar (TST);

33.7. Autorizația pentru amânarea plății (DPO);

33.8. Autorizația pentru depunerea declarației simplificate sub forma unei înscrieri în evidențele declarantului (EIR);

33.9. Autorizația pentru utilizarea unui document electronic de transport ca declarație vamală (ETD);

33.10. Autorizația pentru utilizarea regimului vamal de destinație finală (EUS);

33.11. Autorizația pentru utilizarea regimului vamal de perfecționare activă (PA);

33.12. Autorizația pentru utilizarea regimului vamal de perfecționare pasivă (PP);

33.13. Autorizația pentru utilizarea declarației simplificate (SDE);

33.14. Autorizația pentru utilizarea sigiliilor speciale (SSE);

33.15. Autorizația pentru utilizarea regimului vamal de admitere temporară (TEA);

33.16. Autorizația pentru utilizarea declarației de tranzit cu un set redus de date (TRD);

33.17. Autorizația pentru simplificarea determinării sumelor care fac parte din valoarea în vamă a mărfurilor (CVA).

33.18. Autorizația pentru statutul de exportator aprobat.

34. Entitățile juridice - reprezintă un obiect informațional (preluat din Registrul de Stat al Unităților de Drept) care conține următoarele date:

34.1. denumirea operatorului economic;

34.2. IDNO/EORI - numărul de identificare al operatorului economic;

34.3. adresa juridică - raionul, localitatea, strada, numărul casei, blocului, apartamentului și codul poștal;

34.4. administrator - IDNP, numele, prenumele și data nașterii a administratorului operatorului economic;

34.5. telefon - numărul de telefon al operatorului economic;

34.6. email - adresa de email a operatorului economic.

35. Profilurile utilizatorilor - reprezintă un obiect informațional care constă din totalitatea datelor aferente utilizatorilor autorizați gestionați prin intermediul serviciul electronic guvernamental de autentificare și control al accesului (MPass). Profilul utilizatorului va conține totalitatea informației aferentă acestuia în dependență de tipul utilizatorului (informație pentru autorizarea în sistem, nume, prenume, date de identificare, adresa poștală, telefon de contact, email, la care entitate economică este atașat sau la care birou/post vamal este atașat) și a

funcționalităților SI ”Decizii vamale” accesibile utilizatorului (drepturile și rolurile aferente acestuia). Profilul utilizatorului va livra istoria activității acestuia în cadrul SI ”Decizii vamale”.

Secțiunea a 2-a
Scenariile de bază utilizate în cadrul SI ”Decizii vamale”

36. Scenariile de bază utilizate în cadrul SI ”Decizii vamale” sunt dezvoltate și relaționate obiectelor informaționale ale sistemului, având la bază necesitățile de ținere a evidenței, monitorizării și emiterii deciziilor vamale.

37. În SI ”Decizii vamale” se utilizează următoarele scenarii de bază:

37.1. scenariul de depunere a cererii presupune parcurgerea următorilor pași:

37.1.1. operatorul economic accesează portalul electronic și completează cererea pentru obținerea deciziei vamale, anexând datele și documentele justificative necesare;

37.1.2. este permisă depunerea concomitentă a mai multor cereri pentru diferite tipuri de decizii vamale;

37.1.3. cererea se înregistrează și se atribuie subdiviziunii vamale, în funcție de locul permanent de desfășurare a activității economice a solicitantului sau la subdiviziunea responsabilă de gestionarea deciziilor;

37.1.4. operatorul economic primește o notificare de primire a cererii, moment din care se inițiază procesul de verificare de către autoritatea vamală.

37.2. scenariul de verificare și acceptare a cererii presupune parcurgerea următorilor pași:

37.2.1. cererea pentru obținerea deciziei vamale este supusă unui proces preliminar de verificare, denumit procesul de acceptare a cererii, care are ca scop validarea unei serii inițiale de condiții (condițiile de acceptare);

37.2.2. în cazul în care toate condițiile de acceptare sunt îndeplinite, cererea este considerată acceptată și trece la etapa următoare a procesului de examinare;

37.2.3. în cazul în care una sau mai multe condiții de acceptare nu sunt îndeplinite, cererea nu este acceptată, iar operatorul economic primește o notificare care indică motivele neacceptării;

37.2.4. în cazul în care autoritatea vamală solicită informații suplimentare, operatorul economic transmite datele și documentele solicitate în termenul stabilit;

37.2.5. durata maximă a procesului de acceptare a cererii este stabilită prin lege, cu posibilitatea prelungirii acesteia în situația în care autoritatea vamală solicită informații suplimentare de la operatorul economic.

37.3. scenariul de luare a deciziei presupune parcurgerea următorilor pași:

37.3.1. procesul de luare a deciziei începe după finalizarea acceptării cererii și constă în analiza detaliată a cererii de către autoritatea vamală;

37.3.2. autoritatea vamală verifică dacă solicitantul îndeplinește condițiile și criteriile necesare pentru acordarea deciziei vamale;

37.3.3. autoritatea vamală poate solicita, după caz:

37.3.3.1. sprijinul autorităților statelor membre implicate, după aderarea Republicii Moldova la Uniunea Europeană;

37.3.3.2. informații suplimentare de la operatorul economic;

37.3.4. operatorul economic are dreptul să transmită modificări sau clarificări referitoare la cererea sa, în vederea sprijinirii luării deciziei;

37.3.5. în cazul în care autoritatea vamală intenționează să emită o decizie nefavorabilă, operatorului economic i se acordă dreptul la replică, pentru a prezenta observații sau informații suplimentare înainte de luarea deciziei finale;

37.3.6. decizia vamală favorabilă este înregistrată cu un număr unic și dată, care servește drept referință oficială pentru toate acțiunile ulterioare legate de decizie.

37.4. scenariul de gestionare a deciziilor vamale presupune parcurgerea următorilor pași:

37.4.1. depunerea cererii – reprezintă etapa inițială prin care operatorul economic solicită acordarea deciziei vamale, fiind punctul de pornire pentru întregul ciclu de emitere și gestionare a deciziei.

37.4.2. anularea deciziei vamale – încetarea definitivă a valabilității deciziei, astfel încât aceasta să nu mai poată fi utilizată de operatorul economic. Anularea poate fi dispusă în situații precum constatarea unor erori fundamentale la momentul emiterii deciziei sau încetarea activității operatorului economic.

37.4.3. revocarea deciziei vamale – încetarea utilizării deciziei, însă păstrând evidența acesteia în registrele autorității vamale. Aceasta poate fi aplicată atunci când se constată nerespectarea condițiilor de acordare sau alte circumstanțe care justifică retragerea dreptului de utilizare, fără a șterge istoricul deciziei.

37.4.4. modificarea deciziei vamale – actualizarea unuia sau mai multor elemente de date ale deciziei, cum ar fi informațiile despre operator, condițiile speciale aplicabile sau alte detalii relevante, menținând valabilitatea generală a deciziei.

37.4.5. reevaluarea deciziei vamale – procesul continuu de verificare a respectării condițiilor și criteriilor inițiale care au stat la baza emiterii deciziei, pentru a asigura conformitatea permanentă a operatorului economic.

37.4.6. suspendarea deciziei vamale – oprirea temporară a valabilității deciziei, fără a o anula definitiv, aplicată în cazuri de neconformitate temporară sau verificări suplimentare.

37.4.7. menținerea deciziei vamale – decizia rămâne conformă și activă, fără efectuarea de modificări, confirmând respectarea continuă a condițiilor și criteriilor stabilite inițial.

Secțiunea a 3-a
Interacțiunea cu alte sisteme informaționale

38. Pentru asigurarea formării corecte a resursei informaționale a SI ”Decizii vamale”, este necesară organizarea accesului la resursele informaționale ale următoarelor sisteme informaționale automatizate:

38.1. sisteme informaționale partajate:

38.1.1. serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea și controlul accesului în SI „Decizii vamale”;

38.1.2. Serviciul electronic guvernamental integrat de semnătură electronică (MSign) - utilizat pentru semnarea documentelor în cadrul sistemului;

38.1.3. serviciul electronic guvernamental de jurnalizare (MLog)- pentru asigurarea jurnalizării evenimentelor produse în SI „Decizii vamale”;

38.1.4. Serviciul electronic guvernamental de notificare (MNotify) - utilizat pentru notificarea utilizatorilor sistemului despre evenimentele produse în sistem;

38.1.5. Portalul guvernamental al antreprenorului – pentru accesarea și evidența notificărilor de către cetățeni și persoanele juridice care desfășoară activități de antreprenoriat;

38.1.6. Platforma de interoperabilitate (MConnect) – pentru schimbul de date cu sistemele și resursele informaționale de stat;

38.1.7. Portalul guvernamental integrat EVO - pentru accesul la datele despre persoane fizice și juridice aferente utilizării SI „Decizii vamale”, precum și pentru accesul la serviciile publice electronice prestate prin intermediul SI „Decizii vamale”.

38.2. alte sisteme informaționale de stat:

38.2.1. Sistemul Informațional Integrat Vamal – pentru obținerea accesului la datele despre operatorii economici, înregistrați ca operatori economici care efectuează activități economice externe, pentru verificarea datelor indicate în cereri;

38.2.2. Sistemul informațional e-AEO – pentru obținerea listei Operatorilor Economici Autorizați, datelor cu privire la autorizații și statutul acestora;

38.2.3. Sistemul informațional automatizat "Registrul de stat al unităților de drept", care conține date despre toate categoriile de unități de drept, constituite în bază legală - în scopul preluării și validării datelor despre persoanele juridice privind corectitudinea combinațiilor de IDNO, denumire, cod CUATM, cod CAEM necesare înregistrărilor, modificărilor sau radierilor, care conțin date despre persoane juridice;

38.2.4. Sistemul informațional automatizat "Registrul de stat al populației", care include date despre persoanele fizice - în vederea preluării și validării înregistrărilor, modificărilor sau radierilor, care conțin date despre persoane fizice, și a verificării acestora privind corectitudinea combinațiilor de IDNP, nume, prenume, act de identitate, data nașterii;

38.2.5. alte sisteme informaționale în scopul consumului de date necesar realizării funcționalităților SI „Decizii vamale", în conformitate cu cadrul normativ.

39. Schimbul de date dintre SI „Decizii vamale" și alte sisteme informaționale se asigură prin intermediul platformei guvernamentale de interoperabilitate (MConnect), precum și prin intermediul componentei MConnect Events, pentru expunerea evenimentelor în timp real în contextul realizării servicii proactive. În acest sens Serviciul Vamal înregistrează activele semantice utilizate în SI „Decizii vamale" în cadrul Sistemului informațional „Catalogul semantic".

Capitolul VII
SPAȚIUL TEHNOLOGIC AL SI "DECIZII VAMALE"

40. Inițial, SI „Decizii vamale" este găzduit pe infrastructura tehnologică dedicată a Serviciului Vamal. Ulterior, după încheierea Acordului privind prestarea serviciilor platformei tehnologice guvernamentale comune (MCloud) cu posesorul platformei, SI „Decizii vamale" va fi găzduit pe platforma tehnologică guvernamentală comună (MCloud) și va fi compatibil cu platforma de găzduire bazată pe tehnologii de tip container, care permite utilizarea eficientă a resurselor.

41. Arhitectura SI "Decizii vamale" urmează să fie orientată spre prestarea serviciilor (SOA (Service-Oriented Archiecture)), ceea ce permite ca SI "Decizii vamale" să fie integrat cu toate sistemele informaționale partajate precum: (MSign), (MPass), (MLog) și (MNotify) și cu alte sisteme informaționale ale altor autorități publice.

42. Datorită faptului că interfața de client a SI "Decizii vamale" este preconizată să fie navigatorul (browser) web, nu sunt necesare resurse hardware și software adăugătoare semnificative.

43. La toate etapele de proiectare, dezvoltare și actualizare a SI "Decizii vamale" se va utiliza Modelul unitar de design conform Hotărârii Guvernului nr.677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice şi aprobarea măsurilor necesare pentru implementarea modelului unitar de design.

Capitolul VIII
ASIGURAREA SECURITĂȚII INFORMAȚIONALE A SI "DECIZII VAMALE"

44. Esența securității informaționale a SI ”Decizii vamale” constă în următoarele:

44.1. prin securitate informațională se înțelege protecția resurselor și a infrastructurii informaționale a SI ”Decizii vamale” împotriva acțiunilor premeditate sau accidentale cu caracter natural sau artificial, care au ca rezultat cauzarea prejudiciului participanților la procesul de schimb informațional;

44.2. noțiunea de securitate informațională a SI ”Decizii vamale” include o serie de termeni, cum ar fi: măsuri, politici, tehnologii, puncte de control, structură organizatorică, atribuții și funcții în sistem. Este necesară identificarea acestor mijloace de control pentru a asigura securitatea informațională și pentru a le implementa în SI ”Decizii vamale”;

44.3. colectarea, prelucrarea, stocarea și furnizarea datelor cu caracter personal se efectuează în conformitate cu prevederile Legii nr. 133/2011 privind protecția datelor cu caracter personal;

44.4. pentru a atinge un nivel sporit al securității informaționale trebuie să se țină cont de cele două părți componente ale acesteia – securitatea fizică și securitatea informațională:

44.4.1. securitatea fizică se referă la protejarea infrastructurii fizice a sistemului, a utilizatorilor sistemului și a componentelor fizice (puncte de acces în incinta clădirilor, acces la calculatoare, imprimante) prin aplicarea tuturor măsurilor de securitate;

44.4.2. securitatea informațională presupune protejarea informației prin aplicarea unor măsuri de securizare la nivel logic, prin utilizarea tehnologiilor informaționale. Aceasta include programele antivirus, delimitarea logică a subrețelelor, firewall, controlul asupra folosirii programelor piratate, evidența și actualizarea licențelor produselor software.

45. Pericolul informațional reprezintă un eveniment sau o acțiune posibilă, orientată spre cauzarea unui prejudiciu resurselor sau infrastructurii informaționale. Principalele pericole pentru securitatea informațională a SI ”Decizii vamale” sunt:

45.1. colectarea și utilizarea ilegală a informației;

45.2. încălcarea tehnologiei de prelucrare a informației;

45.3. implementarea în produsele software și hardware a componentelor care realizează funcții neprevăzute în documentația care însoțește aceste produse;

45.4. elaborarea și răspândirea programelor ce pot afecta funcționarea normală a sistemelor informaționale și de comunicații, precum și a sistemelor de protecție a informației;

45.5. nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor hardware și/sau software de prelucrare a informației;

45.6. compromiterea credențialelor, a cheilor și a mijloacelor de protecție criptografică a informației;

45.7. scurgerea de informație prin canale tehnice;

45.8. implementarea dispozitivelor electronice de interceptare a informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor prin canalele de comunicații;

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

45.10. tentativele de interceptare, interceptarea informației în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acestei informații și impunerea informației false;

45.11. utilizarea tehnologiilor informaționale necertificate, a mijloacelor de protecție a datelor, a mijloacelor de informatizare, de comunicații electronice și comunicații la crearea și dezvoltarea infrastructurii informaționale;

45.12. accesul neautorizat la resursele informaționale care se află în băncile și bazele de date;

45.13. încălcarea restricțiilor legale ce țin de răspândirea informației.

46. Modurile de realizare a pericolelor:

46.1. accesul nesancționat;

46.2. influența fizică asupra componentelor infrastructurii informaționale;

46.3. organizarea scurgerii informației prin canale diferite;

46.4. mituirea și intimidarea personalului.

47. Surse ale pericolelor sunt infractorii, funcționarii de stat corupți și utilizatorii de rea-credință.

48. SI ”Decizii vamale” prevede următoarele cerințe și sarcini privind asigurarea securității informaționale:

48.1. securitatea informațională trebuie să fie conformă cerințelor legislației Republicii Moldova, precum și standardelor internaționale care nu contravin legii și permit sporirea gradului de securitate;

48.2. securitatea informațională trebuie să asigure:

48.2.1. confidențialitatea informației, care presupune limitarea, după caz, interzicerea accesului la informație pentru persoanele fără drepturi și împuterniciri corespunzătoare;

48.2.2. integritatea logică a informației, adică prevenirea introducerii, modificării, copierii, actualizării și nimicirii neautorizate a informației;

48.2.3. integritatea fizică a informației;

48.2.4. protecția infrastructurii informaționale împotriva deteriorării și încercărilor de modificare a funcționării.

49. SI „Decizii vamale” asigură realizarea următoarelor obiective de securitate:

49.1. autentificarea - garantează că accesul la zonele restricționate ale SI „Decizii vamale” este permis doar utilizatorilor cu identitate verificată, prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass);

49.2. autorizarea - garantează că utilizatorii autentificați prin serviciul electronic guvernamental de autentificare și control al accesului (MPass) pot accesa serviciile și datele care corespund drepturilor lor de acces;

49.3. confidențialitatea – garantează că datele generate în SI ”Decizii vamale” nu pot fi accesate de o parte terță neautorizată;

49.4. integritatea – garantează că datele generate în SI ”Decizii vamale” nu au fost modificate sau alterate de o parte terță neautorizată.

50. Controlul riguros asupra acțiunilor care au loc în SI ”Decizii vamale” pentru a putea depista la o fază mai timpurie unele încercări de a accesa date confidențiale sau de a aduce un prejudiciu premeditat sau accidental integrității informației se realizează prin intermediul jurnalizării evenimentelor. Setul de acțiuni supuse monitorizării poate fi extins de către administratorul de sistem al SI ”Decizii vamale”.

51. Toate înregistrările privind acțiunile utilizatorilor în sistem și acțiunile care provin din exteriorul sistemului, trebuie să constituie subiect al unei analize detaliate în cazul depistării unor nereguli sau tentative de corupere ori acces neautorizat la datele din SI ”Decizii vamale”.

52. Jurnalizarea evenimentelor în SI ”Decizii vamale” se efectuează prin mijloace proprii, precum și prin integrarea sistemului cu serviciul (MLog).

Capitolul IX
CADRUL DE INTEGRARE A SI „DECIZII VAMALE” ÎN SISTEMUL DECIZII VAMALE AL UNIUNII EUROPENE

53. La momentul aderării Republicii Moldova la Uniunea Europeană, SI „Decizii vamale” se consideră sistem național de gestionare a deciziilor vamale („CDMS național”) și constituie componenta națională în raport cu Sistemul de Decizii Vamale (CDS) al Uniunii Europene, în sensul prevederilor Regulamentului de punere în aplicare (UE) 2025/512 al Comisiei din 13 martie 2025 privind modalitățile tehnice pentru dezvoltarea, întreținerea și utilizarea sistemelor electronice destinate schimbului și stocării de informații în temeiul Regulamentului (UE) nr.

952/2013 al Parlamentului European și al Consiliului (Jurnalul Oficial al Uniunii Europene RO L 2025/512, 20.3.2025).

54. În situația prevăzută la pct. 53, deciziile vamale enumerate la pct. 27.2 se gestionează în cadrul SI „Decizii vamale”.

55. În situația prevăzută la pct. 53, următoarele decizii vamale se gestionează în componenta comună a Sistemului de Decizii Vamale (CDS) al Uniunii Europene:

55.1. autorizația de instituire a unor servicii de transport maritim regulat (RSS);

55.2. autorizația pentru statutul de emitent autorizat (ACP);

55.3. autorizația de vămuire centralizată (CCL);

55.4. autorizația de autoevaluare (SAS);

55.5. autorizația pentru statutul de cântăritor autorizat de banane (AWB).

56. La momentul aderării Republicii Moldova la Uniunea Europeană, Serviciul Vamal va asigura interoperabilitatea între SI „Decizii vamale” și Portalul de Informații Comerciale (considerat Portal național pentru comercianți), pe de o parte, și Sistemul de Decizii vamale (CDS) al Uniunii Europene și Portalul Uniunii Europene pentru comercianți, pe de altă parte, precum și alte sisteme informaționale relevante.

57. În situația descrisă în punctul 53, Serviciul Vamal va asigura dezvoltarea rolurilor, funcțiilor și scenariilor relevante procesului de consultare și coparticipare la luarea deciziilor vamale de comun cu alte autorități vamale ale Uniunii Europene.

Anexa nr. 2 la
Hotărârea Guvernului nr. _____ /2026

REGULAMENTUL
resursei informaționale formate de
Sistemul informațional „Decizii vamale”

Capitolul I
DISPOZIȚII GENERALE

1. Prezentul Regulament stabilește drepturile și obligațiile subiecților raporturilor juridice aferente creării, exploatării și utilizării resursei informaționale „Decizii vamale” *(*în continuare – *RIDV)* formate de Sistemul informațional „Decizii vamale” (în continuare – *SI „Decizii vamale”*), procedura de înregistrare, modificare, completare și radiere a datelor, procedura de interacțiune cu furnizorii de date, măsurile privind asigurarea securității RIDV.

2. RIDV este o resursă informațională de stat creată pentru înregistrarea, evidența și accesarea datelor privind deciziile vamale.

3. Noțiunile utilizate în cuprinsul prezentului Regulament corespund noțiunilor reglementate în anexa nr. 1.

Capitolul II
SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL ȚINERII RIDV

4. Subiecții raporturilor juridice sunt:

4.1.proprietarul;

4.2.posesorul;

4.3.deținătorul;

4.4.registratorul;

4.5.furnizorul datelor;

4.6.destinatarul datelor.

5. Proprietarul RIDV este statul, care își exercită dreptul de posesie și de gestionare asupra conținutului informațional aferent deciziilor vamale.

6. Posesorul și deținătorul RIDV este Serviciul Vamal al Republicii Moldova din subordinea Ministerului Finanțelor.

7. Registratorii RIDV sunt funcționarii vamali cu drept de întocmire a deciziilor vamale, de modificare, de suspendare, de reevaluare și de menținere a acestora, care asigură înregistrarea datelor în RIDV.

8. Furnizorii de date pentru RIDV sunt:

8.1. Agenția Servicii Publice – furnizează date cu privire la persoanele fizice luate în evidență în Registrul de stat al populației și datele cu privire la unitățile de drept luate în evidență în Registrul de stat al unităților de drept;

8.2. Serviciul Vamal – furnizează date despre operatorii economici, înregistrați ca operatori economici care efectuează activități economice externe, și date despre autorizațiile Operatorilor Economici Autorizați.

8.3. Destinatarii RIDV sunt persoanele fizice, autoritățile/instituțiile publice și persoanele juridice de drept public din Republica Moldova sau din alte state, mandatate să acceseze datele privind deciziile vamale conform legislației privind accesul la informație și schimbul de date.

Capitolul III
DREPTURILE, ATRUBUȚIILE ȘI OBLIGAȚIILE SUBIECȚILOR RIDV

9. Subiecții RIDV beneficiază de drepturi de acces conform atribuțiilor și funcțiilor deținute. Nivelul de acces la informație este determinat în funcție de responsabilitățile fiecărui participant și de criteriile de acces stabilite.

10. Accesul la RIDV este segmentat conform unităților de conținut, fiind reglementat prin atribuirea unor drepturi specifice, precum: vizualizare, adăugare, modificare și eliminare a datelor.

Secțiunea 1
Drepturile și obligațiile posesorului RIDV

11. Posesorul RIDV are dreptul:

11.1. să dezvolte, în funcție de competențele sale, cadrul normativ cu privire la RIDV;

11.2. să propună și să pună în aplicare soluții pentru îmbunătățirea și eficientizarea ținerii RIDV;

11.3. să supravegheze acuratețea și actualitatea informațiilor conținute în RIDV;

11.4. să delege atribuții deținătorului, referitoare la dezvoltarea, actualizarea și menținerea RIDV;

11.5. să solicite de la deținător corectarea erorilor admise în procesul de înregistrare și actualizare a datelor RIDV.

12. Posesorul RIDV are următoarele obligații:

12.1. asigură condițiile juridice, organizatorice și financiare pentru crearea și ținerea RIDV;

12.2. organizează crearea SI „Decizii vamale”;

12.3. asigură înregistrarea obiectelor supuse înregistrării, conform cadrului normativ aplicabil;

12.4. asigură autenticitatea, plenitudinea și integritatea datelor înscrise în RIDV, prevenind modificările neautorizate;

12.5. adoptă măsuri tehnice și organizatorice pentru protejarea și securitatea datelor conținute în RIDV, prevenind accesul neautorizat și pierderea informațiilor;

12.6. monitorizează și reglementează accesul la datele din RIDV, asigurând respectarea drepturilor de acces pentru destinatarii autorizați, conform prevederilor legale și regulilor aplicabile;

12.7. asigură corectarea datelor în caz de depistare a omiterilor sau a erorilor;

12.8. utilizează datele RIDV doar în scopurile stabilite de prezentul Regulament;

12.9. asigură dezvoltarea continuă a SI „Decizii vamale” prin adăugarea noilor sisteme informaționale care asigură interoperabilitatea cu SI „Decizii vamale” și pot fi utilizate de către subiecți;

12.10. asigură tuturor destinatarilor acces la datele din RIDV în conformitate cu legea și cu regulile de ținere a registrelor;

12.11. exercită alte atribuții necesare pentru menținerea, protecția și utilizarea corespunzătoare a RIDV.

Secțiunea a 2-a
Drepturile și obligațiile deținătorului RIDV

13. Deținătorul RIDV are dreptul:

13.1. să restricționeze temporar accesul la RIDV în cazul unei situații excepționale stabilite conform actelor normative aplicabile, în cazul unor incidente majore sau al existenței unor riscuri semnificative de securitate;

13.2. să supravegheze respectarea regulilor și cerințelor privind ținerea și utilizarea RIDV;

13.3. să supravegheze respectarea cerințelor privind structura, completitudinea și actualizarea metadatelor de către responsabilii desemnați;

13.4. să monitorizeze utilizarea RIDV de către utilizatori, în scopul prevenirii utilizării necorespunzătoare și al asigurării conformității cu regulamentele aplicabile;

13.5. să solicite de la persoanele responsabile (registratori, furnizori de date) actualizarea sau corectarea informațiilor în RIDV, în cazul identificării unor omisiuni sau erori;

13.6. să suspende temporar sau să revoce definitiv dreptul de acces al unui utilizator la RIDV în cazul în care acesta încalcă regulile de acces, cerințele de securitate ori normele legale privind protecția informațiilor. Exercitarea acestei măsuri se realizează conform procedurii și condițiilor prevăzute la pct. 23, pentru a asigura proporționalitatea și legalitatea intervenției;

13.7. să desfășoare alte activități necesare pentru menținerea integrității, securității și utilizării eficiente a RIDV.

14. Deținătorul RIDV este obligat:

14.1. să stabilească planurile de dezvoltare ale RIDV, în conformitate cu cerințele posesorului și cu prevederile legale aplicabile;

14.2. să gestioneze drepturile de acces ale utilizatorilor, iar în acest scop, deținătorul va autoriza accesul utilizatorilor îndreptățiți și va dispune, după caz, suspendarea temporară sau revocarea definitivă a drepturilor de acces, în conformitate cu prezentul Regulament și cu normele legale aplicabile privind accesul la date;

14.3. să raporteze posesorului necesitățile de dezvoltare și de îmbunătățire a RIDV;

14.4. să asigure păstrarea și protecția datelor din RIDV prevenind orice modificare neautorizată a acestora;

14.5. să acorde suport metodologic și tehnic registratorilor în procesul de încărcare a datelor în RIDV, asigurând respectarea cerințelor privind acuratețea și structura informației;

14.6. să asigure veridicitatea, plenitudinea informației conținute în RIDV, prevenind omisiunile și inexactitățile în procesul de actualizare a datelor;

14.7. să asigure păstrarea și protecția metadatelor din RIDV, prevenind orice modificare neautorizată sau alterare a acestora;

14.8. să acorde suport metodologic și tehnic registratorilor în procesul de creare sau actualizare a metadatelor;

14.9. să elaboreze, să actualizeze și să mențină ghidul utilizatorilor RIDV, oferind instrucțiuni clare privind accesul și utilizarea datelor;

14.10. să monitorizeze și să supravegheze accesările și utilizarea RIDV, prevenind utilizările neautorizate și identificând eventualele breșe de securitate;

14.11. să implementeze măsurile organizatorice și tehnice necesare pentru protecția și confidențialitatea informațiilor stocate în RIDV, prevenind distrugerea, modificarea, blocarea, copierea, răspândirea sau alte acțiuni ilicite, și asigurând un nivel adecvat de securitate în raport cu riscurile asociate prelucrării datelor;

14.12. să exercite alte atribuții necesare pentru menținerea integrității, securității și gestionării eficiente a RIDV, în conformitate cu actele normative aplicabile.

Secțiunea a 3-a
Drepturile și obligațiile registratorului RIDV

15. Registratorul RIDV are dreptul:

15.1. să înregistreze, să vizualizeze și să editeze informațiile din RIDV în limitele rolului atribuit și conform competențelor delegate;

15.2. să acceseze RIDV, în conformitate cu drepturile de acces stabilite de posesor și deținător;

15.3. să acceseze informațiile ce se conțin în RIDV care au fost prezentate sau introduse de către acesta, în conformitate cu regulamentele aplicabile;

15.4. să înainteze posesorului propuneri privind modificarea actelor normative care reglementează ținerea acestuia;

15.5. să solicite și să primească de la posesor și deținător suport metodologic și tehnic privind utilizarea RIDV;

15.6. să solicite și să primească de la posesor informații referitoare la nivelul agreat al serviciilor conform indicatorilor stabiliți în cadrul normativ;

15.7. să înainteze posesorului și deținătorului propuneri privind îmbunătățirea și sporirea eficacității ținerii RIDV.

16. Registratorul RIDV este obligat:

16.1. să înregistreze datele în RIDV în conformitate cu prevederile legale;

16.2. să asigure corectitudinea, autenticitatea și veridicitatea datelor introduse, prevenind erorile și informațiile inexacte;

16.3. să asigure actualizarea în timp real a datelor introduse în RIDV exclusiv în baza informațiilor documentate, recepționate de la deținătorii sau furnizorii oficiali de date, utilizând mecanismele de interoperabilitate prevăzute de cadrul normativ;

16.4. să întreprindă măsuri pentru prevenirea accesului neautorizat al persoanelor terțe la datele din RIDV;

16.5. să utilizeze informațiile RIDV în exclusivitate conform destinației acestora și în strictă conformitate cu legislația..

Secțiunea a 4-a
Drepturile și obligațiile furnizorului de date RIDV

17. Furnizorul de date are dreptul:

17.1. să participe la procesul de ținere și utilizare a RIDV, contribuind la îmbunătățirea calității și actualității informațiilor conținute;

17.2. să înainteze posesorului propuneri privind modificarea actelor normative care reglementează ținerea și utilizarea RIDV;

17.3. să înainteze posesorului propuneri privind îmbunătățirea și sporirea eficacității procesului de ținere și utilizare a RIDV.

18. Furnizorul de date este obligat:

18.1. să asigure corectitudinea, autenticitatea, veridicitatea și integritatea datelor furnizate;

18.2. să asigure actualitatea datelor furnizate, conform cerințelor stabilite de posesorul și deținătorul RIDV, respectând termenele și procedurile legale;

18.3. să implementeze măsuri organizatorice necesare pentru asigurarea furnizării corecte și sigure a datelor pe care le deține către RIDV;

18.4. să asigure, în conformitate cu cadrul normativ privind schimbul de date și interoperabilitate, disponibilitatea datelor din registrele și sistemele informaționale pe care le deține, prin servicii informaționale web expuse în platforma de interoperabilitate (MConnect);

18.5. să asigure măsurile necesare pentru protecția și securitatea informațiilor furnizate către RIDV, să documenteze orice încercare de acces neautorizat și să adopte măsurile necesare pentru prevenirea și remedierea incidentelor de securitate.

Secțiunea a 5-a
Drepturile și obligațiile destinatarului datelor din RIDV

19. Destinatarul datelor are dreptul:

19.1. să acceseze și să utilizeze date din RIDV, în conformitate cu necesitățile sale profesionale și cu drepturile de acces stabilite prin cadrul normativ aplicabil;

19.2. să înainteze posesorului RIDV propuneri privind modificarea actelor normative care reglementează ținerea și utilizarea acestuia;

19.3. să solicite și să primească de la posesorul și de la deținătorul RIDV ajutor metodologic și practic privind utilizarea acestuia;

19.4. să solicite și să primească de la posesorul RIDV informații referitoare la nivelul agreat al serviciilor conform cadrului normativ;

19.5. să solicite și să primească de la posesor accesul la datele/informațiile RIDV în conformitate cu scopul prelucrării și cu rolul atribuit;

19.6. să vizualizeze datele/informațiile/documentele din RIDV în conformitate cu drepturile de acces stabilite în baza atribuțiilor și funcțiilor deținute, fără dreptul de a modifica aceste date/informații/documente;

19.7. să prezinte posesorului RIDV propuneri privind îmbunătățirea și eficientizarea procesului de ținere și utilizare a acestuia.

20. În funcție de rolurile atribuite, destinatarul este obligat:

20.1. să asigure confidențialitatea datelor/informațiilor/documentelor obținute din RIDV în conformitate cu normele legale privind protecția informației și a datelor cu caracter personal;

20.2. să asigure accesarea și utilizarea datelor/informațiilor/documentelor din RIDV în conformitate cu rolul atribuit și cu scopul legitim de utilizare a acestora;

20.3. să implementeze măsuri pentru protecția și securitatea informațiilor din RIDV, să documenteze incidentele de securitate și să întreprindă măsurile necesare pentru prevenirea și remedierea acestora;

20.4. să respecte regulile de acces și exploatare a RIDV, asigurând utilizarea corectă și protejată a informațiilor conținute;

20.5. să utilizeze informația obținută doar în scopurile stabilite de legislație;

20.6. să informeze posesorul RIDV, în termen de o zi lucrătoare, despre orice incident care ar putea afecta negativ exercitarea funcțiilor sale sau utilizarea RIDV.

21. Utilizarea RIDV fără autorizare nominală este interzisă și urmează a fi considerată ca acces neautorizat la un sistem informațional public.

22. Dreptul de acces la RIDV nu este unul permanent, acesta poate fi suspendat sau revocat de către deținător. Introducerea și/sau modificarea informațiilor în RIDV de pe un nume sau profil de utilizator străin este interzisă, urmând a fi considerată ca acces neautorizat. Utilizatorii urmează să se asigure de faptul că profilul de utilizator, precum și semnătura electronică sunt confidențiale.

23. Dreptul de acces la RIDV are caracter nepermanent și poate fi limitat, suspendat sau retras de către deținător, în condițiile prezentului Regulament. Suspendarea ori revocarea dreptului de acces al unui utilizator se dispune de către deținător în următoarele situații:

23.1. la încetarea raporturilor de serviciu sau de muncă ale utilizatorului, ori la suspendarea temporară a acestora (de exemplu, concediu fără plată, detașare), caz în care accesul se retrage corespunzător duratei/necesității;

23.2. la modificarea atribuțiilor de serviciu/de muncă ale utilizatorului, când noile responsabilități nu mai necesită acces la datele din RIDV;

23.3. dacă posesorul sau deținătorul constată că utilizatorul a accesat RIDV fără autorizare ori a permis accesul nesancționat al altor persoane;

23.4. dacă posesorul sau deținătorul constată încălcarea măsurilor de securitate informațională de către utilizator, punând în pericol integritatea sau confidențialitatea datelor.

24. Lucrările de mentenanță planificate în complexul de mijloace software a SI „Decizii vamale" se efectuează după notificarea, în scris sau prin e-mail, a registratorilor de către deținător cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil. Lucrările de mentenanță neplanificate se efectuează la solicitarea utilizatorilor și coordonarea prealabilă cu posesorul în situația nefuncționării sau funcționării necorespunzătoare a complexului de mijloace software.

Capitolul IV
ȚINEREA ȘI GESTIONAREA RIDV

25. RIDV, fiind interoperabil, prin intermediul platformei de interoperabilitate (MConnect) cu alte sisteme și resurse informaționale de stat, asigură un mediu informațional securizat, complet și transparent..

26. Evidența obiectelor informaționale este asigurată conform prevederilor Conceptului Sistemului informațional "Decizii vamale", precum și instrucțiunilor elaborate de posesor și aprobate împreună cu deținătorul.

27. În cadrul RIDV, datele cu caracter personal sunt utilizate exclusiv în scopul pentru care sunt notificate, fără a se urmări obținerea de informații în interes personal.

28. RIDV se ține în limba română.

29. Utilizarea RIDV este asigurată de către posesor, cu respectarea cerințelor legale aplicabile privind infrastructura tehnologică guvernamentală și securitatea sistemelor informaționale.

30. Introducerea datelor în RIDV se va efectua în conformitate cu ghidurile de utilizare, prezentul Regulament și actele normative emise de posesor.

31. În cazul depistării unor erori sau inexactități în documentele sau datele primite, deținătorul RIDV este obligat să informeze despre aceasta furnizorul și destinatarii cărora le-au fost transmise date eronate.

32. Dacă furnizorul de date constată necesitatea rectificării unor informații eronate sau inexacte, acesta poate face un demers argumentat, iar registratorul din cadrul RIDV va efectua corectările necesare și va informa furnizorul despre modificările realizate.

33. Păstrarea și administrarea datelor din RIDV este asigurată de către deținător până la adoptarea deciziei de lichidare a acestuia. În cazul lichidării acestuia, datele și documentele conținute în RIDV se transmit în arhivă conform legislației.

Capitolul V
INTERACȚIUNEA CU FURNIZORII DE DATE DIN CADRUL RIDV

34. Pentru asigurarea gestionării eficiente și continue a RIDV, schimbul de date între participanții acestuia este asigurat în regim nonstop.

35. Lucrările de mentenanță și verificările tehnice periodice se execută după notificarea utilizatorilor, în scris sau prin e-mail, cu cel puțin o zi înainte de începerea lucrărilor, cu indicarea

termenelor de finalizare, cu excepția situațiilor neprevăzute de suspendare temporară a accesului la RIDV.

36. Schimbul informațional al resursei informaționale formate de SI „Decizii vamale” se realizează prin intermediul platformei de interoperabilitate (MConnect) sau prin intermediul Sistemului de telecomunicații al autorităților administrației publice.

37. Răspunderea pentru veridicitatea și corectitudinea RIDV le revine deținătorului și, respectiv, registratorilor de date.

38. RIDV conține un depozit de date care permite realizarea unor analize complexe ale informațiilor, precum și generarea rapoartelor și a indicatorilor de performanță. Accesul la rapoarte și la indicatorii de performanță este disponibil pentru utilizatorii RIDV, în funcție de rolurile atribuite și drepturile de acces stabilite.

Capitolul VI
INTEROPERABILITATEA CU ALTE SISTEME INFORMAȚIONALE

39. Pentru asigurarea actualizării operative și automate a conținutului informațional al RIDV cu informație veridică, poate fi efectuată interacțiunea și sincronizarea acestuia cu alte registre și resurse informaționale, importându-se automat sau exportându-se date spre verificare și/sau completare a conținutului informațional al acestuia.

40. Pentru preluarea datelor cu conținut informațional relevant, RIDV interacționează, prin intermediul platformei de interoperabilitate (MConnect), cu următoarele sisteme și resurse informaționale de stat:

40.1. Registrul de stat al unităților de drept;

40.2. Registrul de stat al populației;

40.3. Sistemul Informațional Integrat Vamal;

40.4. Sistemul Informațional ASYCUDA World;

40.5. Sistemul informațional e-AEO;

40.6. Sistemul informațional ”Noul sistem computerizat de tranzit”;

40.7. alte resurse informaționale relevante.

41. Pentru asigurarea autenticității, integrității și securității accesului la date, RIDV utilizează următoarele servicii informaționale partajate::

41.1. serviciul electronic guvernamental de autentificare și control al accesului (MPass);

41.2. serviciul electronic guvernamental integrat de semnătură electronică (MSign);

41.3. serviciul electronic guvernamental de jurnalizare (MLog);

41.4. serviciul guvernamental de notificare electronică (MNotify);

41.5. platforma de interoperabilitate (MConnect).

42. În scopul asigurării interoperabilității și a schimbului de date cu alte sisteme și resurse informaționale de stat, Posesorul înregistrează activele semantice utilizate în Sistemul informațional „Catalogul semantic”.

Capitolul VII
ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI RIDV

43. Datele conținute în RIDV fac parte din categoria datelor care necesită protecție. Asigurarea securității, confidențialității și integrității acestor date este responsabilitatea subiecților

cu drepturi de acces la RIDV, care trebuie să respecte cerințele legale privind protecția datelor cu caracter personal în procesul de prelucrare a acestora.

44. Măsurile de protecție și de securitate a datelor din RIDV reprezintă totalitatea acțiunilor juridice, organizatorice, economice și tehnologice orientate spre prevenirea pericolelor asociate resurselor și infrastructurii informaționale.

45. Obiectele asigurării protecției și securității datelor din RIDV sunt considerate toate mijloacele software și infrastructurile tehnologice utilizate pentru realizarea proceselor informaționale, în conformitate cu cerințele legale aplicabile privind securitatea sistemelor informaționale. În această categorie se includ:

45.1. baza de date, sistemele informaționale, sistemele operaționale, sistemele de gestiune a bazelor de date, sistemele de evidență și alte aplicații care asigură gestionarea RIDV;

45.2. sistemele de comunicații electronice, rețelele, serverele, calculatoarele și alte mijloace tehnice de prelucrare a datelor.

46. Securitatea informațională a RIDV se efectuează prin aplicarea metodelor și prin efectuarea acțiunilor descrise în Planul de continuitate al acestuia și, după caz, a procedurilor operaționale.

47. Protecția datelor cu caracter personal sunt asigurate prin următoarele acțiuni:

47.1. posesorul, deținătorul, registratorii și furnizorii de date vor prelucra doar acele date cu caracter personal care sunt strict necesare, neexcesive scopului prestabilit, conform competențelor atribuite și respectând principiile stabilite de cadrul normativ privind protecția datelor cu caracter personal;

47.2. în procesul de prelucrare a datelor cu caracter personal, posesorii, deținătorii, registratorii și furnizorii vor asigura măsuri organizatorice și tehnice necesare pentru a proteja datele cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii sau a altor acțiuni ilegale. Aceste măsuri asigură un nivel adecvat de securitate, corespunzător riscurilor asociate prelucrării și caracterului datelor prelucrate.

48. Respectarea drepturilor subiectului de date cu caracter personal se realizează în conformitate cu prevederile cadrului legislativ.

49. Serviciul Vamal dispune sau contractează personal calificat pentru efectuarea auditului privind securitatea informațională, verificarea conformității și instruirea continuă în domeniul asigurării securității informaționale.

50. Persoana responsabilă de protecția datelor cu caracter personal notifică Centrului Național pentru Protecția Datelor cu Caracter Personal orice indicii sau incidente care ar putea indica încălcări ale legislației privind protecția datelor cu caracter personal.

51. Protecția datelor RIDV se efectuează prin următoarele metode:

51.1. prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor, care pot duce la distrugerea sau denaturarea datelor;

51.2. utilizarea obligatorie a produselor de program licențiate și aprobate;

51.3. monitorizarea procesului de utilizare a RIDV prin intermediul mecanismului de jurnalizare, gestionat de deținătorul acestuia.

52. Subiecții, la utilizarea și exploatarea SI „Decizii vamale”, asigură implementarea normelor de securitate, acestea urmând să conțină acte ce confirmă:

52.1. identitatea persoanei responsabile de implementarea normelor de securitate și împuternicirile acesteia;

52.2. implementarea principalelor măsuri tehnico-organizatorice necesare pentru protecția RIDV;

52.3. implementarea procedurilor interne pentru prevenirea modificărilor neautorizate asupra conținutului informațional;

52.4. informarea utilizatorilor interni și instruirea acestora cu privire la modalitățile și mecanismele de asigurare a securității informaționale;

52.5. procedurile de control intern ale subiecților care accesează RIDV privind respectarea condițiilor de securitate informațională.

53. Schimbul informațional se efectuează cu utilizarea mijloacelor software și a infrastructurilor tehnologice autorizate, prin canale securizate, asigurând integritatea și securitatea datelor, în conformitate cu cerințele legale aplicabile.

54. Serviciul Vamal desemnează o persoană sau un grup de persoane, subordonată nemijlocit conducătorului instituției, responsabilă de implementarea și monitorizarea respectării normelor de securitate informațională.

55. Normele de securitate informațională se aduc la cunoștința fiecărui utilizator intern și se semnează de acesta. Fiecare utilizator intern este obligat să cunoască normele securității informaționale, procedurile pe care trebuie să le respecte în strictă conformitate cu politica de securitate.

56. Utilizatorii interni asigură instruirea angajaților privind metodele și procedeele de contracarare a pericolelor informaționale.

Capitolul VIII
ASIGURAREA CONTROLULUI INTERN ȘI EXTERN AL RIDV

57. Ținerea SI „Decizii vamale” este supusă controlului intern și extern. Controlul intern privind organizarea și gestionarea RIDV se efectuează de către posesor. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea RIDV se efectuează de către instituții abilitate și certificate în domeniul auditului.

58. RIDV se înregistrează în Registrul resurselor și sistemelor informaționale de stat.

59. Responsabilitatea pentru organizarea și gestionarea RIDV aparține deținătorului acestuia.

60. Anual, până la data de 31 ianuarie, posesorul prezintă Centrului Național pentru Protecția Datelor cu Caracter Personal un raport generalizat despre incidentele de securitate din cadrul RIDV, în conformitate cu prevederile cadrului normativ.

61. Controlul legalității operațiilor de prelucrare a datelor cu caracter personal realizate în RIDV se efectuează de către Centrul Național pentru Protecția Datelor cu Caracter Personal.

62. În cazul apariției unor circumstanțe excepționale și dificultăți tehnice care afectează infrastructura de suport a RIDV, inclusiv deficiențe ale platformei tehnologice guvernamentale comune (MCloud), funcționalitatea acestuia poate fi suspendată temporar. În astfel de cazuri, subiecții RIDV vor fi informați prin intermediul mijloacelor tehnice disponibile.

63. Toți subiecții RIDV poartă răspundere disciplinară, civilă, administrativă sau penală, conform legislației, pentru prelucrarea, divulgarea și transmiterea informației cu caracter personal din RIDV persoanelor terțe, contrar prevederilor legislației.

64. Utilizatorii implicați în întreținerea RIDV, introducerea datelor, furnizarea informațiilor și gestionarea acestuia poartă răspundere personală, în conformitate cu legislația, pentru integralitatea, autenticitatea și veridicitatea informațiilor gestionate în RIDV, precum și pentru păstrarea și utilizarea corespunzătoare a informațiilor, conform normelor de securitate și protecție a datelor.