Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr.____

din _____ 2026

privind sistemul informațional „Noul sistem computerizat de tranzit”

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 „Noul sistem computerizat de tranzit”.
2. Se aprobă:

2.1. Conceptul Sistemului informațional „Noul sistem computerizat de tranzit”, conform anexei nr.1;

2.2. Regulamentul resursei informaționale formate de Sistemul informațional „Noul sistem computerizat de tranzit”, conform anexei nr.2.

3. Serviciul Vamal, în calitate de posesor și deținător al Sistemului informațional „Noul sistem computerizat de tranzit”, 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
la Hotărârea Guvernului nr. _____/2026

CONCEPTUL
Sistemului informațional „Noul sistem computerizat de tranzit”

INTRODUCERE

În conformitate cu art.193 alineat (4) al Acordului de Asociere între Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de o parte, și Republica Moldova, pe de altă parte, semnat la Bruxelles la 27 iunie 2014, Republica Moldova și-a asumat angajamentul de aderare la Convenția privind regimul de tranzit comun, încheiată la Interlaken 1987.

Prin Hotărârea Guvernului nr.750/2022 (Monitorul Oficial al Republicii Moldova, 2022, nr.343-348, art.828), a fost aprobată semnarea Acordului de finanțare dintre Guvernul Republicii Moldova și Comisia Europeană privind Programul „UE pentru redresare și reziliență”, iar unul din proiectele incluse, reprezintă dezvoltarea și implementarea Noului sistem computerizat de tranzit în Republica Moldova. Noul sistem computerizat de tranzit este unul dintre principalele sisteme vamale ale Uniunii Europene.

Pentru a acoperi noile funcționalități și proceduri impuse de Convenția privind regimul de tranzit comun, a fost dezvoltată aplicația națională de tranzit pe baza specificațiilor tehnice obligatorii pentru domeniul comun și specificațiile tehnice recomandate pentru domeniul extern și domeniul național, ambele definite de Direcția Generală Impozitare și Uniune Vamală (în continuare - DG TAXUD).

Principalul obiectiv al Noului sistem computerizat de tranzit este asigurarea unui sistem electronic unificat pentru gestionarea rapidă, sigură și eficientă a regimului de tranzit între toate părțile contractante la Convenția privind regimul de tranzit comun. Totodată, în temeiul art.296 Cod vamal, nr.95/2021, Noul sistem computerizat de tranzit este utilizat pentru mișcările de tranzit pe teritoriul național, asigurând alinierea procedurii de tranzit reglementată de legislația națională cu procedura de tranzit comun.

Noul sistem computerizat de tranzit este un instrument de facilitare a comerțului internațional ce oferă beneficii tuturor părților implicate. Aplicarea sistemului, asigură raționalizarea controalelor la frontieră printr-o gestionare eficientă a riscurilor, reducerea timpului și a costurilor pentru întreprinderi, accelerarea procesului de trecere a frontierei, sincronizarea datelor (trasabilitatea datelor, reutilizarea datelor, calitatea datelor).

Prezentul concept tehnic 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 „Noul sistem computerizat de tranzit” (în continuare - *Concept*) stabilește spațiul funcțional, structura organizatorică, spațiul informațional, spațiul tehnologic, securitatea sistemului informațional și protecția informației în cadrul SI „Noul sistem computerizat de tranzit”.

2. SI „Noul sistem computerizat de tranzit” (în continuare – *NCTS*) reprezintă o soluție informatică din categoria Guvern către Guvern (G2G) și Guvern către Business (G2B) și constituie totalitatea mijloacelor software, hardware și de infrastructură ale utilizatorului, destinate formării resursei informaționale privind declarațiile de tranzit, precum și schimbul de informații cu alte autorități vamale.

3. În contextul Conceptului sunt utilizate următoarele noțiuni:

3.1.autorizare – proces al NCTS 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 NCTS 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. NCTS este parte componentă a Sistemului Informațional Integrat Vamal.

5. NCTS înglobează posibilități funcționale de gestionare a fluxurilor de lucru, schimb de informații, funcții de înștiințare, depozitare a datelor și prelucrarea declarațiilor de tranzit.

6. NCTS pune la dispoziția utilizatorilor următoarele servicii:

6.1. depunerea declarațiilor de tranzit standard sau declarațiilor de tranzit combinate cu o declarație sumară de intrare;

6.2. modificarea declarațiilor de tranzit;

6.3. invalidarea declarațiilor de tranzit

6.4. prelucrarea declarațiilor de tranzit;

6.5. acces la toate informațiile privind prelucrarea declarațiilor de tranzit;

6.6. monitorizarea declarațiilor de tranzit;

6.7. înregistrarea incidentelor;

6.8. cercetarea operațiunilor de tranzit;

6.9. recuperarea datoriei vamale.

7. Obiectivele NCTS sunt:

7.1. crearea și operarea unui sistem informațional stabil, sigur și fiabil pentru evidența, gestiunea și trasabilitatea declarațiilor de tranzit, asigurând transparența, corectitudinea și securitatea procesului de prelucrare a declarațiilor vamale, 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 declarațiilor de tranzit, 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. excluderea manipulării frauduloase a documentelor;

7.5. reducerea numărului de investigări;

7.6. controale bazate pe analiza riscului;

7.7. mai bună planificare și utilizare a resurselor umane;

7.8. implementarea noilor instrumente internaționale în domeniul vamal.

8. Principiile de bază ale NCTS 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 expansibilității - 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 NCTS

10. Cadrul normativ al NCTS este format din legislația națională, tratatele la care Republica Moldova este parte. Crearea și funcționarea NCTS 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. Legea nr.169/2025 pentru aderarea Republicii Moldova la Convenția privind regimul de tranzit comun;

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

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

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

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

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

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

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

10.15. Hotărârea Guvernului nr.211/2019 privind platforma de interoperabilitate (MConnect);

10.16. 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);

10.17. Hotărârea nr.153/2021 pentru aprobarea Conceptului Sistemului informațional „Registrul resurselor și sistemelor informaționale de stat” și a Regulamentului privind modul de ținere a Registrului resurselor și sistemelor informaționale de stat;

10.18. Hotărârea Guvernului nr. 323/2021 pentru aprobarea Conceptului Sistemului informațional „Catalogul semantic” și a Regulamentului privind modul de ținere a Registrului format de Sistemul informațional „Catalogul semantic”;

10.19. Hotărârea Guvernului nr. 92/2023 cu privire la punerea în aplicare a Codului vamal nr. 95/2021;

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

10.21. 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;

10.22. 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 NCTS 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 NCTS

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

13. Funcțiile de bază ale NCTS 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, 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, 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 NCTS se realizează funcții specifice, grupate în contururi funcționale speciale:

14.1. depunerea și prelucrarea declarațiilor;

14.2. analiza riscurilor;

14.3. gestiunea garanțiilor;

14.4. gestiunea controalelor;

14.5. gestiunea incidentelor;

14.6. înregistrarea traversării frontierei;

14.7. gestionarea procesului de sosire a mărfii;

14.8. cercetarea mișcării de tranzit;

14.9. recuperarea datoriei vamale;

14.10. administrarea și monitorizarea acțiunilor utilizatorilor.

15. Conturul funcțional „Depunerea și prelucrarea declarațiilor” include următoarele funcții:

15.1. depunerea declarațiilor de tranzit și vizualizarea statutelor lor;

15.2. modificarea declarațiilor depuse;

15.3. anularea declarațiilor depuse;

15.4. invalidarea declarațiilor de tranzit;

15.5. prelucrarea declarațiilor de către funcționarii vamali;

15.6. comunicarea prin intermediul notificărilor NCTS.

16. Conturul funcțional “Analiza riscurilor” include următoarele funcții:

16.1. configurarea regulilor de risc;

16.2. declanșarea procesului de analiză a riscurilor;

16.3. înregistrarea rezultatelor controlului vamal bazat pe analiza riscurilor.

16.4. comunicarea prin intermediul notificărilor NCTS.

17. Conturul funcțional „Gestiunea garanțiilor” include următoarele funcții:

17.1. înregistrarea garanțiilor și vizualizarea statutelor lor;

17.2. modificarea garanțiilor;

17.3. suspendarea garanțiilor;

17.4. retragerea garanțiilor;

17.5. comunicarea prin intermediul notificărilor NCTS.

18. Conturul funcțional „Gestiunea controalelor” include următoarele funcții:

18.1. luarea deciziei de a efectua controlul;

18.2. înregistrarea rezultatelor controlului;

18.3. comunicarea prin intermediul notificărilor NCTS.

19. Conturul funcțional „Înregistrarea traversării frontierei” include următoarele funcții:

19.1. identificarea Avizului anticipat de tranzit și examinarea acestuia;

19.2. înregistrarea traversării frontierei;

19.3. refuzul înregistrării traversării frontierei;

19.4. oprirea mișcării de tranzit;

19.5. comunicarea prin intermediul notificărilor NCTS.

20. Conturul funcțional „Gestionarea procesului de sosire a mărfii” include următoarele funcții:

20.1. transmiterea notificării de sosire a mărfurilor;

20.2. decizia de control;

20.3. înregistrarea rezultatelor controlului la destinație;

20.4. comunicarea prin intermediul notificărilor NCTS.

21. Conturul funcțional „Cercetarea mișcării de tranzit” include următoarele funcții:

21.1. interogare informații privind operațiunea de tranzit;

21.2. încheierea regimului de tranzit în baza probelor alternative;

21.3. comunicarea prin intermediul notificărilor NCTS.

22. Conturul funcțional „Recuperarea datoriei vamale” include următoarele funcții:

22.1. inițierea procedurii de recuperare;

22.2. înregistrarea recuperării datoriei vamale;

22.3. comunicarea prin intermediul notificărilor NCTS.

23. Conturul funcțional „Gestiunea incidentelor” include următoarele funcții:

23.1. interogare mișcare;

23.2. înregistrarea incidentelor și vizualizarea categoriei lor;

23.3. comunicarea prin intermediul notificărilor NCTS.

24. Conturul funcțional „Administrarea și monitorizarea acțiunilor utilizatorilor” include următoarele funcții:

24.1. asigurarea integrității logice a NCTS;

24.2. administrarea bazelor de date ale NCTS;

24.3. elaborarea și mentenanța ghidurilor de sistem și a clasificatoarelor;

24.4. delimitarea drepturilor de acces pentru utilizatori;

24.5. asigurarea securității, protecției și integrității informației în NCTS în baza standardului național SM EN ISO/IEC 27001:2017 „Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe”;

24.6. asigurarea respectării cerințelor sistemului de protecție a datelor cu caracter personal.

Capitolul IV
STRUCTURA ORGANIZATORICĂ A NCTS

25. Funcțiile de bază privind formarea și exploatarea NCTS sunt divizate între:

25.1. proprietarul NCTS;

25.2. posesorul NCTS;

25.3. deținătorul NCTS;

25.4. administratorul tehnic NCTS;

25.5. furnizorii de date pentru NCTS;

25.6. registratorii de date pentru NCTS;

25.7. utilizatorii NCTS.

26. Proprietarul NCTS este statul.

27. Posesorul și deținătorul al NCTS este Serviciul Vamal din subordinea Ministerului Finanțelor, care asigură condițiile financiare, juridice și organizatorice, precum și realizarea nemijlocită a competențelor de creare, administrare, mentenanță și dezvoltarea sistemului .

28. Inițial, administratorul tehnic al NCTS 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 NCTS 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.

29. Deținătorul al NCTS 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.

30. Furnizori de date pentru NCTS sunt:

30.1. Agenția Serviciilor 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;

30.2. Serviciul Vamal – furnizează date despre operatorii economici, înregistrați ca operatori economici care efectuează activități economice externe, și date despre autorizațiile Operatorilor Economici Autorizați, date din declarațiile vamale și deciziile vamale.

31. Registratorii NCTS reprezintă persoanele fizice și juridice sau reprezentanții acestora care depun declarațiile de tranzit, precum funcționarii vamali cu drept de prelucrare a declarațiilor de tranzit.

32. Utilizatorii NCTS sunt persoanele juridice, persoanele fizice, brokerii vamali și funcționarii vamali beneficiari ale serviciilor NCTS sau ale raporturilor juridice de gestionare automatizată a NCTS.

Capitolul V
DOCUMENTELE NCTS

33. Documentele NCTS reprezintă totalitatea documentelor procedurale necesare pentru ținerea evidenței, prelucrării și monitorizarea declarațiilor de tranzit.

34. În cadrul NCTS se folosesc următoarele categorii de documente:

34.1. *documente de intrare,* care sunt relevante pentru prelucrarea declarațiilor de tranzit sau incidente;

34.2. *documente de ieșire*, care se consideră documente finale ce pot fi utilizate și care reprezintă declarațiile de tranzit prelucrate, notificările privind statutul declarațiilor de tranzit la adresa de e-mail;

34.3. *documente tehnologice*, care include lista utilizatorilor și drepturile acestora, documentele ce conțin înregistrări de audit privind acțiunile utilizatorilor, erorile de sistem, precum și ghidurile de utilizare a NCTS.

Capitolul VI
SPAȚIUL INFORMAȚIONAL AL NCTS

Secțiunea 1
Obiectele informaționale ale NCTS

35. Resursa informațională a NCTS este reprezentată de un ansamblu de obiecte informaționale și interacțiunea acestora. Obiectele informaționale NCTS includ:

35.1. declarații;

35.2. profilurile utilizatorilor;

35.3. entitățile juridice;

35.4. persoanele fizice;

35.5. documente;

35.6. incidente.

36. Identificarea obiectelor NCTS 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 corespunzătoare persoanelor fizice sau juridice.

37. Identificatorul obiectului informațional „entități juridice”:

37.1. pentru rezidenții Republicii Moldova – este numărul de stat de identificare al unității de drept (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);

37.2. pentru nerezidenți – este numărul de identificare EORI (Economic Operators Registration and Identification).

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

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

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

40.1. declarația de tranzit;

40.2. documentul de însoțire a tranzitului.

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

41.1. denumirea operatorului economic;

41.2. IDNO – numărul de identificare de stat al unității de drept (operator economic rezident al Republicii Moldova);

41.3. EORI – numărul de identificare al operatorului economic nerezident;

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

41.5. administrator - IDNP, numele și prenumele administratorului operatorului economic;

41.6. telefon - numărul de telefon al operatorului economic;

41.7. email - adresa de email a operatorului economic.

42. Persoanele fizice – reprezintă un obiect informațional care include date privind persoanele delegate ale entității juridice. Obiectul informațional conține următoarele date:

42.1. IDNP-ul și inițialele persoanei fizice (rezident al Republicii Moldova);

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

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

43. Documente – reprezintă setul de documente care se atașează la declarație (scrisoare de transport internațional - CMR, invoice și după caz actul permisiv pentru plasarea mărfurilor în regim vamal de tranzit), precum și cele formate/atașate pe parcursul procesării declarației (de ex. garanție, decizie de control).

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

45. Incidente – reprezintă un obiect informațional care include un set de date utilizat pentru înregistrarea și raportarea evenimentelor neprevăzute, care apar pe parcursul unei operațiuni de tranzit, între biroul vamal de plecare și cel de destinație (schimbarea mijlocului de transport, deteriorarea sau ruperea sigiliilor vamale, orice alt eveniment care afectează integritatea mărfurilor sau a datelor declarației de tranzit).

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

47. 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 (informație pentru autorizarea în sistem, nume, prenume, date de identificare, adresa poștală, telefon de contact, email, la care entitate economică este atașat) și a funcționalităților NCTS accesibile utilizatorului (drepturile și rolurile aferente acestuia). Profilul utilizatorului va livra istoria activității acestuia în cadrul NCTS.

Secțiunea a 2-a
Scenariile de bază utilizate în cadrul NCTS

48. Scenariile de bază utilizate în cadrul NCTS sunt dezvoltate și relaționate obiectelor informaționale ale sistemului, având la bază necesitățile de ținere a evidenței, prelucrării și monitorizării declarațiilor de tranzit.

49. În NCTS se utilizează următoarele scenarii de bază:

49.1. scenariul de depunere a declarației de tranzit presupune parcurgerea următorilor pași:

49.1.1. titularul regimului accesează sistemul și depune declarația de tranzit;

49.1.2. dacă declarația de tranzit este validă din punct de vedere a structurii mesajului, regulilor, condițiilor, biroul vamal confirmă acceptarea declarației de tranzit, alocând un număr principal de identificare;

49.1.3. biroul vamal examinează declarația de tranzit și ia decizia privind inițierea sau nu a controlului;

49.1.4. în cazul în care NCTS nu identifică niciun risc pentru mișcarea de tranzit, iar biroul vamal de plecare decide să nu controleze mișcarea, funcționarul vamal înregistrează garanția, iar sistemul verifică dacă aceasta este una conformă tranzacției în cauză;

49.1.5. după înregistrarea garanției, biroul vamal de plecare decide să acorde liber de vamă în tranzit, acordă termenul de prezentare a mărfurilor la destinație și indică numărul sigiliului aplicat, după caz;

49.1.6. titularul regimului primește o notificare privind statutul declarației.

49.2. scenariul de modificare a declarației presupune parcurgerea următorilor pași:

49.2.1. titularul regimului poate solicita modificarea uneia sau mai multor date din declarația de tranzit după acceptarea acesteia de către biroul vamal de plecare;

49.2.2. biroul vamal de plecare întreprinde măsurile de identificare pe care le consideră necesare și introduce datele corespunzătoare în declarația de tranzit;

49.2.3. dacă biroul vamal de plecare acceptă modificarea declarației, titularul regimului primește notificarea despre acceptarea modificării, în caz contrar – notificarea privind respingerea modificării cu indicarea motivelor.

49.3. scenariul de procesare automatizată a declarației conform procedurii simplificate:

49.3.1. la biroul vamal de plecare de la primirea declarației, înregistrarea garanției până la acordarea liberului de vamă în tranzit;

49.3.2. la biroul vamal de destinație de la notificarea prezentării mărfii în locul autorizat până la încheierea regimului de tranzit.

Fluxul operațional automatizat se va efectua numai în următoarele condiții stricte:

49.3.2.1. la biroul vamal de plecare - declarația este validă din punct de vedere a structurii mesajului, regulilor, condițiilor, este depusă în orele indicate în autorizație și a fost atribuită pe culoar verde;

49.3.2.2. la biroul vamal de destinație - notificarea de sosire este transmisă în orele indicate în autorizație, declarația vamală a fost atribuită pe culoar verde, iar observațiile privind descărcarea mărfurilor nu sunt.

49.3.3. titularul regimului poate solicita modificarea uneia sau mai multor date din declarația de tranzit după acceptarea acesteia de către biroul vamal de plecare;

49.3.4. biroul vamal de plecare întreprinde măsurile de identificare pe care le consideră necesare și introduce datele corespunzătoare în declarația de tranzit;

49.3.5. dacă biroul vamal de plecare acceptă modificarea declarației, titularul regimului primește notificarea despre acceptarea modificării, în caz contrar – notificarea privind respingerea modificării cu indicarea motivelor.

49.4. scenariul de înregistrare a incidentelor presupune parcurgerea următorilor pași:

49.4.1. funcționarul vamal înregistrează incidentul aferent declarației de tranzit;

49.4.2. funcționarul vamal examinează incidentul raportat și întreprinde măsuri, dacă e cazul.

49.5. scenariul de gestionare a sosirii mărfurilor presupune parcurgerea următorilor pași:

49.5.1. biroul vamal de destinație transmite notificarea de prezentare a mărfurilor;

49.5.2. în cazul în care NCTS nu identifică niciun risc pentru mișcarea de tranzit, iar biroul vamal de destinație decide să nu controleze mișcarea, mărfurile sunt eliberate din tranzit;

49.5.3. în cazul în care biroul vamal de destinație decide să efectueze control, înregistrează rezultatele controlului la destinație, iar după caz, transmite rezultatul nesatisfăcător biroului vamal de plecare pentru rezolvarea discrepanțelor constatate.

49.6. scenariul de cercetare a mișcării de tranzit include următoarele acțiuni:

49.6.1. în cazul în care biroul vamal de destinație nu a transmis notificarea de sosire a mărfurilor sau rezultatele controlului în termenul stabilit, subdiviziunea competentă pentru cercetare inițiază procedura de cercetare prin transmiterea cererii de interogare către titularul regimului de tranzit sau către biroul vamal de destinație.

49.6.2. în cazul în care informațiile obținute nu sunt suficiente pentru încheierea regimului de tranzit, subdiviziunea competentă transmite cererea de solicitare a informațiilor suplimentare;

49.6.3. în baza dovezilor alternative prezentate, regimul de tranzit este încheiat corespunzător.

49.7. scenariul de recuperare a datoriei vamale presupune parcurgerea următorilor pași:

49.7.1. inițierea procedurii de recuperare a datoriei vamale;

49.7.2. transmiterea cererii de transfer a competenței de recuperare a datoriei vamale;

49.7.3. recuperarea completă a datoriei vamale.

Secțiunea a 3-a
Interacțiunea cu alte sisteme informaționale

50. Pentru asigurarea formării corecte a resursei informaționale a NCTS, este necesară organizarea accesului la resursele informaționale ale următoarelor sisteme informaționale automatizate:

50.1. sistemele informaționale partajate:

50.1.1. serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea și controlul accesului în NCTS;

50.1.2. serviciul electronic guvernamental de semnătură electronică (MSign) - utilizat pentru semnarea documentelor în cadrul sistemului;

50.1.3. serviciul electronic guvernamental de jurnalizare (MLog)- pentru asigurarea jurnalizării evenimentelor produse în NCTS;

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

50.1.5. „Portalul guvernamental integrat EVO - pentru accesul la datele despre persoane fizice și juridice aferente utilizării NCTS, pentru accesul la serviciile publice electronice prestate prin intermediul NCTS, precum și pentru accesarea și evidența notificărilor de către cetățeni și persoanele juridice care desfășoară activități de antreprenoriat;

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

50.2. alte sisteme informaționale de stat:

50.2.1. 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 declarații;

50.2.2. Sistemul Informațional ASYCUDA World – pentru obținerea datelor din declarațiile de import/export;

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

50.2.4. Sistemul informațional „Decizii vamale" – pentru obținerea accesului la datele despre deciziile vamale, pentru verificarea datelor indicate în declarații;

50.2.5. 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;

50.2.6. 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;;

50.2.7. alte sisteme informaționale de stat, în scopul consumului de date necesar realizării funcționalităților SI „Nou sistem computerizat de tranzit", în conformitate cu cadrul normativ.

51. Schimbul de date dintre NCTS 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 NCTS în cadrul Sistemului informațional „Catalogul semantic".

52. NCTS este interoperabil cu Portalul vamal pentru comercianți și este utilizat de către Serviciul Vamal sau de către părțile contractante la Convenția privind regimul de tranzit comun, pentru a depune și a prelucra declarația de tranzit.

Capitolul VII
SPAȚIUL TEHNOLOGIC AL NCTS

53. Inițial, NCTS este găzduit pe infrastructura tehnologică dedicată a Serviciului Vamal. Ulterior, după încheierea Acordului privind prestarea serviciilor platformei tehnologice guvernamentale comune (MCloud) cu posesorul platformei, NCTS 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.

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

55. Datorită faptului că interfața de client a NCTS este preconizată să fie navigatorul (browser) web, nu sunt necesare resurse hardware și software adăugătoare semnificative.

56. La toate etapele de proiectare, dezvoltare și actualizare a NCTS 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 și aprobarea măsurilor necesare pentru implementarea modelului unitar de design.

Capitolul VIII
ASIGURAREA SECURITĂȚII INFORMAȚIONALE A NCTS

57. Esența securității informaționale a NCTS constă în următoarele:

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

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

57.3. colectarea, prelucrarea, stocarea și furnizarea datelor cu caracter personal se efectuează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal;

57.4. 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:

57.4.1. 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;

57.4.2. 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.

58. Pericolul informațional reprezintă un eveniment sau o acțiune posibilă, orientată spre cauzarea unui prejudiciu resurselor sau infrastructurii informaționale. Principalele pericole pentru securitatea informațională a NCTS sunt:

58.1. colectarea și utilizarea ilegală a informației;

58.2. încălcarea tehnologiei de prelucrare a informației;

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

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

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

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

58.7. scurgerea de informație prin canale tehnice;

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

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

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

58.11.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;

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

58.13.încălcarea restricțiilor legale ce țin de răspândirea informației.

59. Modurile de realizare a pericolelor:

59.1. accesul nesancționat;

59.2. influența fizică asupra componentelor infrastructurii informaționale;

59.3. organizarea scurgerii informației prin canale diferite;

59.4. mituirea și intimidarea personalului.

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

61. NCTS prevede următoarele cerințe și sarcini privind asigurarea securității informaționale:

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

61.2. securitatea informațională trebuie să asigure:

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

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

61.2.3. integritatea fizică a informației;

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

62. NCTS asigură realizarea următoarelor obiective de securitate:

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

62.2. 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;

62.3. confidențialitatea – garantează că datele generate în NCTS nu pot fi accesate de o parte terță neautorizată;

62.4. integritatea – garantează că datele generate în NCTS nu au fost modificate sau alterate de o parte terță neautorizată.

63. Controlul riguros asupra acțiunilor care au loc în NCTS 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 tehnic de sistem al NCTS.

64. 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 NCTS.

65. Jurnalizarea evenimentelor în NCTS se efectuează prin mijloace proprii, precum și prin integrarea sistemului cu serviciul (MLog).

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

REGULAMENTUL
resursei informaționale formate de
Sistemul informațional „Noul sistem computerizat de tranzit”

Capitolul I
DISPOZIȚII GENERALE

1. Prezentul Regulament stabilește drepturile și obligațiile subiecților raporturilor juridice aferente creării, exploatării și utilizării Resursei informaționale al declarațiilor de tranzit *(*în continuare – *RIDT)* formate de Sistemul informațional „Noul sistem computerizat de tranzit” (în continuare – *NCTS*), procedura de înregistrare, modificare, completare și radiere a datelor, procedura de interacțiune cu furnizorii de date; măsurile privind asigurarea securității RIDT.

2. RIDT este o resursă informațională de stat creată pentru depunerea, procesarea, controlul și evidența declarațiilor de tranzit.

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

Capitolul II
SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL ȚINERII RIDT

4. Subiecții raporturilor juridice sunt :
4.1. proprietarul;
4.2. posesorul;
4.3. deținătorul;
4.4. furnizorul de date;
4.5. registratorul;
4.6. destinatarul datelor.

5. Proprietarul RIDT este statul, care își exercită dreptul de posesie și de gestionare asupra conținutului informațional aferent declarațiilor de tranzit.

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

7. Registratorii RIDT sunt persoanele fizice și juridice sau reprezentanții acestora care depun declarațiile de tranzit, precum și funcționarii vamali cu drept de prelucrare a declarațiilor de tranzit, care asigură înregistrarea datelor în RIDT.

8. Furnizorii de date pentru RIDT sunt:

8.1. Agenția Serviciilor 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, date despre autorizațiile Operatorilor Economici Autorizați, date din declarațiile vamale și deciziile vamale.

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

Capitolul III
DREPTURILE, ATRUBUȚIILE ȘI OBLIGAȚIILE SUBIECȚILOR RIDT

9. Subiecții RIDT 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 RIDT 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 RIDT

11. Posesorul RIDT are dreptul:

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

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

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

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

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

12. Posesorul RIDT are următoarele obligații:

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

12.2. organizează crearea NCTS;

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

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

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

12.6. monitorizează și reglementează accesul la datele din RIDT, 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 RIDT doar în scopurile stabilite de prezentul Regulament;

12.9. asigură dezvoltarea continuă a NCTS prin adăugarea noilor sisteme informaționale care asigură interoperabilitatea cu NCTS și pot fi utilizate de către subiecți;

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

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

Secțiunea a 2-a

Drepturile și obligațiile deținătorului RIDT

13. Deținătorul RIDT are dreptul:

13.1. să restricționeze temporar accesul la RIDT 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 RIDT;

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

13.4. să monitorizeze utilizarea RIDT 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 RIDT, în cazul identificării unor omisiuni sau erori;

13.6. să suspende temporar sau să revoce definitiv dreptul de acces al unui utilizator la RIDT 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 RIDT.

14. Deținătorul RIDT este obligat:

14.1. să stabilească planurile de dezvoltare ale RIDT, 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 RIDT;

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

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

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

14.7. să asigure păstrarea și protecția metadatelor din RIDT, 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 RIDT, oferind instrucțiuni clare privind accesul și utilizarea datelor;

14.10. să monitorizeze și să supravegheze accesările și utilizarea RIDT, 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 RIDT, 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 RIDT, în conformitate cu actele normative aplicabile.

Secțiunea a 3-a
Drepturile și obligațiile registratorului RIDT

15. Registratorul RIDT are dreptul:

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

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

15.3. să acceseze informațiile ce se conțin în RIDT 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 RIDT;

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 RIDT.

16. Registratorul RIDT este obligat:

16.1. să înregistreze datele în RIDT 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 RIDT 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 RIDT;

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

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

17. Furnizorul de date are dreptul:

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

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

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

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 RIDT, 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 RIDT;

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 RIDT, 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 RIDT

19. Destinatarul datelor are dreptul:

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

19.2. să înainteze posesorului RIDT 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 RIDT ajutor metodologic și practic privind utilizarea acestuia;

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

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

19.6. să vizualizeze datele/informațiile/documentele din RIDT 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 RIDT 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 RIDT 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 RIDT în conformitate cu rolul atribuit și cu scopul legitim de utilizare a acestora;

20.3. să implementeze măsuri pentru protecția și securitatea informațiilor din RIDT, 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 RIDT, 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 RIDT, în termen de o zi lucrătoare, despre orice incident care ar putea afecta negativ exercitarea funcțiilor sale sau utilizarea RIDT.

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

22. Dreptul de acces la RIDT nu este unul permanent, acesta poate fi suspendat sau revocat de către deținător. Introducerea și/sau modificarea informațiilor în RIDT 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 RIDT are caracter temporar și poate fi limitat, suspendat sau retras de către deținător, în condițiile prezentului Regulament.

24. Dreptul de acces la RIDT se suspendă de către deținător în următoarele cazuri:

24.1. neactualizarea datelor de autentificare sau expirarea certificatelor digitale utilizate la accesul în RIDT;

24.2. suspiciunea rezonabilă privind utilizarea abuzivă sau neautorizată a datelor din RIDT;

24.3. detectarea unor breșe de securitate care impun limitarea temporară a accesului până la remedierea riscului;

24.4. solicitarea expresă a organelor de control, în baza constatării unor abateri semnificative;

24.5. încălcarea obligațiilor de utilizare a RIDT, stabilite prin cadrul normativ;

24.6. utilizarea unor echipamente sau aplicații neautorizate care pun în pericol funcționalitatea NCTS;

24.7. introducerea repetată de date eronate sau incomplete de către utilizator;

24.8. transmiterea accesului de utilizator către terțe persoane;

24.9. suspendarea temporară a activității utilizatorului în cadrul instituției de proveniență;

24.10. deficiențe tehnice în infrastructura utilizatorului care compromit securitatea NCTS.

25. Dreptul de acces la RIDT se retrage de către deținător în următoarele cazuri:

25.1. încălcări grave și repetate ale regulilor de utilizare a RIDT;

25.2. utilizarea RIDT în scopuri ilicite, inclusiv falsificarea sau manipularea datelor;

25.3. divulgarea cu bună știință a informațiilor confidențiale către entități fără drept;

25.4. refuzul de a se conforma cerințelor de securitate, stabilite de posesor sau de deținător;

25.5. hotărâri executorii ale instanțelor sau decizii administrative de retragere a accesului;

25.6. încetarea calității de angajat sau colaborator al unei entități cu acces la RIDT;

25.7. producerea unor daune sistemului din culpă sau prin neglijență gravă;

25.8. refuzul repetat de a corecta erorile semnalate de deținător, posesor sau registratori;

25.9. pierderea valabilității certificatelor de semnătură digitală sau altor instrumente de autentificare;

25.10. lipsa de activitate a contului pe o perioadă extinsă, stabilită de posesor;

25.11. desfășurarea unor activități incompatibile cu buna funcționare și legalitatea RIDT;

25.12. în baza cererii/solicitării conducătorilor persoanelor juridice, în cazul utilizatorilor angajați;

25.13. la modificarea raporturilor de muncă, când noile responsabilități nu presupun accesul la datele RIDT;

25.14. la constatarea încălcării securității informaționale de utilizatorul RIDT.

26. Lucrările de mentenanță planificate în complexul de mijloace software a NCTS 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 RIDT

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

28. Evidența obiectelor informaționale este asigurată conform prevederilor Conceptului Sistemului informațional „Noul sistem computerizat de tranzit”, precum și instrucțiunilor elaborate de posesor și aprobate împreună cu deținătorul.

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

30. RIDT se ține în limba română.

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

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

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

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

35. Toate modificările operate în NCTS se păstrează în ordine cronologică, cu păstrarea nemijlocită a istoricului acestora, pe un termen de 6 ani, după expirarea căruia, datele cu caracter personal trebuie să fie depersonalizate ireversibil, păstrându-se exclusiv metadatele statistice necesare pentru audit și raportare. Cu titlu de excepție, termenul de 6 ani poate fi prelungit doar în cazurile justificate, prin necesitatea soluționării unor cauze penale, contravenționale sau litigii civile. Modificarea sau completarea datelor nu afectează accesarea și vizualizarea informației din NCTS.

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

Capitolul V
INTERACȚIUNEA CU FURNIZORII DE DATE DIN CADRUL RIDT

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

38. 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 NCTS.

39. Schimbul informațional al resursei informaționale formate de NCTS se realizează prin intermediul platformei de interoperabilitate (MConnect).

40. Răspunderea pentru veridicitatea și corectitudinea RIDT le revine deținătorului și, respectiv, registratorilor de date.

41. RIDT 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 RIDT, în funcție de rolurile atribuite și drepturile de acces stabilite.

Capitolul VI
INTEROPERABILITATEA CU ALTE SISTEME INFORMAȚIONALE

42. Pentru asigurarea actualizării operative și automate a conținutului informațional al RIDT 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.

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

43.1. Registrul de stat al unităților de drept;

43.2. Registrul de stat al populației;

43.3. Sistemul Informațional Integrat Vamal;

43.4. Sistemul Informațional ASYCUDA World;

43.5. Sistemul informațional e-AEO;

43.6. Sistemul informațional ”Decizii vamale”;

43.7. alte resurse informaționale relevante.

44. Pentru asigurarea autenticității, integrității și securității accesului la date, RIDT utilizează următoarele sisteme informaționale partajate:

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

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

44.3. serviciul electronic guvernamental de jurnalizare (MLog);

44.4. serviciul guvernamental de notificare electronică (MNotify);

44.5. platforma de interoperabilitate (MConnect);

44.6. alte sisteme informaționale partajate, conform cadrului normativ.

45. 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 RIDT

46. Datele conținute în RIDT fac parte din categoria datelor care necesită protecție. Asigurarea securității, confidențialității și integrității acestor date este responsabilitatea subiecților cu drepturi de acces la RIDT, care trebuie să respecte cerințele legale privind protecția datelor cu caracter personal în procesul de prelucrare a acestora.

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

48. Obiectele asigurării protecției și securității datelor din RIDT 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:

48.1. baza de date, sistemele informaționale, sistemele operaționale, sistemele de gestiune a bazelor de date, sistemele de evidență și alte aplicații care asigură gestionarea datelor din NCTS;

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

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

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

50.1. 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;

50.2. 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.

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

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

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

54. Protecția datelor din cadrul NCTS se efectuează prin următoarele metode:

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

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

54.3. monitorizarea procesului de utilizare a RIDT prin intermediul mecanismului de jurnalizare, gestionat de deținătorul acestuia.

55. Subiecții, la utilizarea și exploatarea NCTS, asigură implementarea normelor de securitate, acestea urmând să conțină acte ce confirmă:

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

55.2. implementarea principalelor măsuri tehnico-organizatorice necesare pentru protecția RIDT;

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

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

55.5. procedurile de control intern ale subiecților care accesează RIDT privind respectarea condițiilor de securitate informațională.

56. 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.

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

58. 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.

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

Capitolul VIII
ASIGURAREA CONTROLULUI INTERN ȘI EXTERN AL RIDT

60. Ținerea RIDT este supusă controlului intern și extern. Controlul intern privind organizarea și gestionarea RIDT se efectuează de către posesor. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea RIDT se efectuează de către instituții abilitate și certificate în domeniul auditului.

61. RIDT se înregistrează în Registrul resurselor și sistemelor informaționale de stat.

62. Responsabilitatea pentru organizarea și gestionarea RIDT aparține deținătorului acestuia.

63. 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 RIDT, în conformitate cu prevederile cadrului normativ.

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

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