

**REGULAMENT**  
**privind organizarea și funcționarea Sistemului informațional**  
**„Registrul cererilor de intervenție”**

**I. DISPOZIȚII GENERALE**

1. Regulamentul privind organizarea și funcționarea Sistemului informațional „Registrul cererilor de intervenție” (în continuare – *Regulament*) stabilește modul de organizare, funcționare și conținutul informațional al sistemului, subiecții raporturilor juridice în domeniul creării și funcționării Sistemului informațional „Registrul cererilor de intervenție” (în continuare – *SI e-RCI*), drepturile și obligațiile acestora, obiectele informaționale și lista datelor incluse în acestea, procedurile de colectare și gestiune a datelor, accesul la datele SI e-RCI, interoperabilitatea cu alte registre și sisteme informaționale, modalitatea de ținere și asigurare a funcționării sistemului, formele de exercitare a controlului și responsabilitatea pentru organizarea și funcționarea SI e-RCI.

2. În sensul prezentului Regulament, termenii și noțiunile de mai jos au următoarea semnificație:

*Sistemul informațional „Registrul cererilor de intervenție”* (în continuare - *SI e-RCI*) – sistem informațional, parte a platformei informaționale în domeniul protecției drepturilor de proprietate intelectuală, destinat spre a fi utilizat de titularii de drepturi de proprietate intelectuală pentru depunerea în adresa Serviciului Vamal a cererilor de intervenție, în conformitate cu Capitolul XII al Codului Vamal, precum și utilizarea de către Serviciul Vamal pentru organizarea procesului de management și gestionare a cererilor de intervenție, începând de la recepționarea electronică a acestor cereri și până la reflectarea deciziei luate prin completarea Registrului cererilor de intervenție;

*participanții SI e-RCI* – posesorul, deținătorul, utilizatorii sistemului;

*operatorul tehnico-tehnologic al SI e-RCI* – Serviciul Tehnologia Informației și Securitate Cibernetică, care funcționează în conformitate cu legislația Republicii Moldova și care asigură gestionarea și administrarea tehnică necesară funcționării SI e-RCI, conform indicatorilor de performanță și nivelului agreat de servicii;

*administratorul SI e-RCI* – persoana autorizată, desemnată expres de către deținătorul SI e-RCI, care are acces nelimitat la toate compartimentele în cadrul Sistemului în vederea gestionării depline a acestuia;

*prelucrare automatizată de date* – orice operațiune sau serie de operațiuni care se efectuează asupra datelor prin mijloace automatizate, precum: colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

*securitate* – nivel necesar de integritate, selectivitate pentru protejarea datelor împotriva pierderilor, alterărilor, deteriorărilor și a accesului neautorizat. Securitatea sistemului presupune faptul că acesta este rezistent la atacuri, informația este confidențială, integră și în stare de lucru, atât la nivel de sistem, cât și la nivel de date;

*ansamblu de mijloace software și hardware* – totalitate a programelor și mijloacelor tehnice care asigură realizarea proceselor informaționale;

*bază de date* – colecție de date organizată conform unei structuri conceptuale, care descrie caracteristicile acestor date și relațiile dintre entitățile lor componente, destinată unuia sau mai multor domenii de aplicație;

*identificator de obiect informațional* – unul dintre atributele obiectului informațional, care este unic și rămâne invariabil pe parcursul întregii perioade de existență a obiectului în SI e-RCI;

*clasificator* – totalitate a semnificațiilor anumitor caracteristici ale obiectului și codurilor digitale sau literale ce corespund acestora;

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

*resursă informațională* – totalitate de informații conținute în SI e-RCI, organizată în conformitate cu legislația și cerințele stabilite;

*obiecte de proprietate intelectuală (în continuare - OPI)* – orice rezultat al activității intelectuale, confirmat și protejat prin drepturile corespunzătoare privind utilizarea acestuia, care se divizează în obiecte de proprietate industrială (invenții, soiuri de plante, topografii de circuite integrate, mărci, desene și modele industriale, indicații geografice, denumiri de origine și specialități tradiționale garantate) și obiecte ale dreptului de autor (opere literare, artistice și științifice exprimate în diferite forme, prevăzute prin lege) și ale drepturilor conexe (interpretări, fonograme, videograme și emisiuni ale organizațiilor de difuziune);

*cerere de intervenție* – solicitare prezentată Serviciului Vamal pentru a interveni în cazul mărfurilor susceptibile de a aduce atingere unui drept de proprietate intelectuală;

*date privind încălcările drepturilor de proprietate intelectuală* – cereri de intervenție referitoare la obiectele de proprietate intelectuală depuse la Serviciul vamal, OPI ce beneficiază de protecție la frontieră, rețineri înregistrate și rezultatul reținerilor; cereri (sesizări) referitoare la obiectele de proprietate intelectuală depuse la Inspectoratul General al Poliției, procedura de control efectuată, actul de constatare, procedura de ridicare a produselor și dosare înregistrate (contravenționale și penale); cereri (sesizări) referitoare la obiectele de proprietate intelectuală depuse la Procuratura Generală, procedura de control efectuată, actul de constatare, procedura de ridicare a produselor, dosare înregistrate și hotărâri judecătorești.

## II. SARCINILE ȘI FUNCȚIILE SI e-RCI

3. Sarcinile de bază ce urmează a fi realizate la exploatarea SI e-RCI sunt:

1) eficientizarea procesului de implementare a mecanismelor de protecție a drepturilor de proprietate intelectuală;

2) standardizarea procedurilor, formularelor, nomenclatoarelor, seturilor de date, la nivelul întregului sistem;

3) optimizarea comunicării și coordonării interinstituționale prin automatizarea procesului de colectare și transmitere a datelor relevante procesului de aplicare a mecanismelor de protecție a drepturilor de proprietate intelectuală de către autoritățile implicate în implementarea legilor și actelor normative guvernamentale privind drepturile de proprietate intelectuală din Republica Moldova;

4) creșterea gradului de transparență și accesibilitate a informațiilor prin asigurarea mijloacelor de acces unificat la baza de date privind OPI înregistrate în Republica Moldova, dar și la datele despre încălcările asupra drepturilor de proprietate intelectuală;

5) securizarea informațiilor cu accesibilitate limitată, prin implementarea unei politici de acces în sistem pentru fiecare utilizator în funcție de competențe și atribuții specifice;

6) asigurarea mecanismelor corespunzătoare de monitorizare și audit prin implementarea instrumentelor terțe, externe de asigurare a redundanței informațiilor și evenimentelor jurnalizate;

7) asigurarea interoperabilității cu alte sisteme informaționale pentru a prelua și a transmite informații.

4. Sistemul asigură realizarea funcțiilor de bază ale unui sistem informațional, conform legislației, precum și funcțiile specifice ce reies din destinația sistemului, după cum urmează:

1) *inițierea procedurii de protecție* – crearea interfeței pentru depunerea de către titularul de drepturi la Serviciul Vamal a cererii de intervenție, monitorizarea statutului cererilor depuse;

2) *managementul cererilor de intervenție* – oferirea spațiului tehnologic pentru Serviciul Vamal, în scopul organizării procesului de examinare și acceptare a cererilor de intervenție, stabilire a perioadei de intervenție;

3) *formarea resursei informaționale unice în domeniul cererilor de intervenție acceptate* și obiectelor de proprietate intelectuală ce beneficiază de această măsură de protecție;

4) *formarea resursei informaționale unice privind măsurile de protecție prin reținerea mărfurilor* susceptibile a aduce atingere dreptului de proprietate intelectuală, precum și privind aplicarea măsurilor asupra mărfurilor în privința cărora s-a dovedit că aduc atingere unui drept de proprietate intelectuală;

5) *asigurarea accesului la informație*. Informația din SI e-RCI este pusă la dispoziția autorităților implicate, titularilor de drepturi. Nivelul de acces al beneficiarilor la informația din SI e-RCI este stabilit de legislație, în dependență de statutul său juridic și regimul juridic al informației. Fiecare beneficiar este obligat să utilizeze informația strict în scopurile legale;

6) *asigurarea securității și protecției informației*. Asigurarea securității și protecției informației, la toate etapele de prelucrare a resurselor informaționale se efectuează conform legislației și standardelor de securitate, bunelor practici în domeniul dat, cu utilizarea metodelor avansate de autentificare și de autorizare a utilizatorilor, conform rolului atribuit în SI e-RCI, precum și cu utilizarea mecanismelor de protecție a datelor și a canalelor de conexiune, de monitorizare și jurnalizare a evenimentelor produse în cadrul sistemului;

7) *administrarea sistemului*, care include următoarele acțiuni de administrare a rolurilor și drepturilor utilizatorilor, administrarea nomenclatoarelor, alte activități de administrare și acces la funcționalitățile SI e-RCI;

8) *asigurarea calității informațiilor*, utilizând componentele sistemului de management al calității.

5. În cadrul funcționării SI e-RCI vor fi realizate funcții specifice, grupate în module și contururi funcționale, după cum urmează:

1) **Modulul funcțional al titularului de drepturi de proprietate intelectuală**. În cadrul acestui modul sunt operaționale următoarele contururi funcționale:

- a) conturul „CERERI DE INTERVENȚIE”;
- b) conturul „REGISTRUL CERERILOR DE INTERVENȚIE”;
- c) conturul „NOTIFICĂRI”;
- d) conturul „INCIDENTE”.

2) **Modulul funcțional al Serviciului Vamal**. Acest modul reprezintă spațiul de lucru destinat reprezentanților Serviciului Vamal pentru organizarea procesului de examinare, acceptare a cererilor de intervenție, gestionarea Registrului cererilor de intervenție și măsurilor de reținere aplicate. În cadrul acestui modul sunt operaționale următoarele contururi funcționale:

- a) conturul „CERERI DE INTERVENȚIE”;
- b) conturul „REGISTRUL CERERILOR DE INTERVENȚIE”;
- c) conturul „REȚINERI”;
- d) conturul „NOTIFICĂRI”;
- e) conturul „INCIDENTE”.

3) **Modulul funcțional de administrare și monitorizare** asigură interacțiunea informațională a tuturor participanților sistemului, reprezintă un subsistem integrat de control și monitorizare a formării și utilizării resursei informaționale și include următoarele funcții:

- a) asigurarea integrității logice a SI e-RCI;
- b) administrarea bazelor de date ale SI e-RCI;
- c) elaborarea și mentenanța ghidurilor de sistem și a clasificatoarelor;
- d) delimitarea drepturilor de acces pentru utilizatori;
- e) monitorizarea respectării regulilor de autentificare și autorizare, management al utilizatorilor;

f) asigurarea securității, protecției și integrității informației în sistem conform cerințelor standardelor naționale SM EN ISO/IEC 27001:2017 „Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe”;

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

### III. SPAȚIUL INFORMAȚIONAL, OBIECTELE INFORMAȚIONALE SI e-RCI

**6. Modulul funcțional al titularului de drepturi de proprietate intelectuală**, reprezintă interfața destinată titularilor de drepturi pentru depunerea cererilor de intervenție, monitorizarea statutului acestor cereri, consultarea Registrului cererilor de intervenție, recepționarea notificărilor, raportarea incidentelor, informarea privind drepturile de proprietate intelectuală.

**6.1. Conturul „CERERI DE INTERVENȚIE”** (titular), oferă următoarele funcționalități:

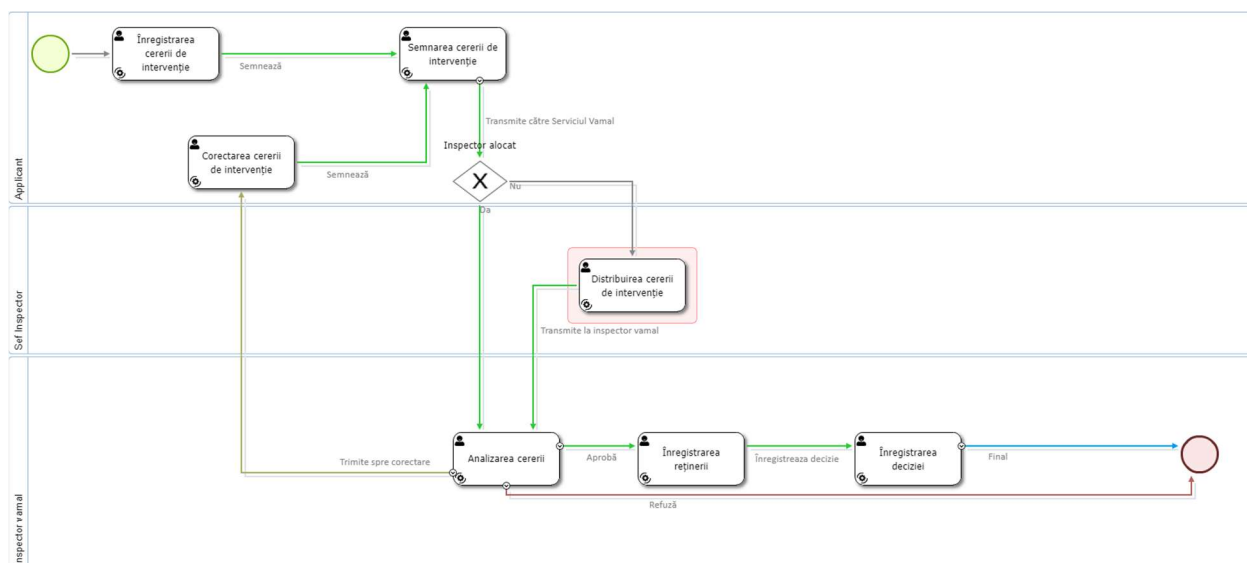
- căutarea unei cereri de intervenție după: numărul cererii, titularul de drepturi, numărul de înregistrare al OPI;

- vizualizarea rezultatului căutării reprezintă informații despre cererile de intervenție inițiate de titularul de drepturi;

- adăugarea unei înregistrări – funcționalitate care permite inițierea, completarea unei cereri de intervenție, atașarea documentelor conform prevederilor legale, semnarea electronică a cererii și remiterea în adresa Serviciului Vamal. Informația despre obiectele de proprietate intelectuală sunt preluate în mod automatizat, prin servicii informaționale, din Sistemul informațional în domeniul protecției obiectelor de proprietate intelectuală (în continuare – SI e-OPI), gestionat de AGEPI;

- organizarea cererilor de intervenție ale titularului în:

- Cereri în lucru – reflectă cererile inițiate, cererile completate ce pot fi semnate electronic, cererile semnate electronic de titular;
- Cereri transmise – reflectă cererile transmise către Serviciul Vamal și permite vizualizarea în timp real a statutului cererii transmise (Figura 1);
- Cereri incomplete – reflectă cererile transmise către Serviciul Vamal și returnate de către acesta pentru corectări, completări;
- Cereri acceptate – reflectă cererile care au fost aprobate de către Serviciul Vamal;
- Cereri respinse – reflectă cererile ce au fost respinse de către Serviciul Vamal;
- Cereri anulate – reflectă cererile anulate în conformitate cu prevederile legale;
- Cereri suspendate - reflectă cererile suspendate în conformitate cu prevederile legale;
- Cereri în curs de expirare - reflectă cererile în curs de anulare;
- Cereri expirate – reflectă cererile care deja au expirat.



**Figura 1.** Exemplu privind rezultatul operațiunii de monitorizare a statutului cererii de intervenție transmise de titular.

În cadrul conturului informațional „**CERERE de INTERVENȚIE**” sunt configurate date despre următoarele obiecte informaționale:

**a) obiectul informațional „Intervenție”,** care conține următoarele date:

- numărul cererii;
- data depunerii cererii;
- data transmiterii;
- numărul de intrare al cererii;
- statutul solicitantului;
- mențiunea privind solicitarea utilizării procedurii de la art. 305<sup>1</sup> Cod Vamal;
- inspectorul vamal responsabil/alocat;
- data deciziei;
- perioada de valabilitate a protecției;
- informații privind decizia de refuzare;
- documente generate (Declarația titularului, în sensul art. 302<sup>1</sup> Cod Vamal și Cererea de intervenție, în sensul art. 303 Cod Vamal).

**b) obiectul informațional „Solicitant”,** care conține următoarele date:

- jurisdicția persoanei;
- statutul persoanei;
- calitatea persoanei;
- funcția;
- IDNO/IDNP;
- denumirea persoanei juridice/Nume, prenumele persoanei fizice;
- date de contact (localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

**c) obiectul informațional „Persoane de contact”,** care conține următoarele date:

- jurisdicția persoanei;
- statutul persoanei;
- calitatea persoanei;
- responsabilitatea persoanei (probleme administrative/tehnice);
- IDNP;
- nume, prenumele persoanei fizice;
- date de contact (localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

**d) obiectul informațional „Obiectul de proprietate intelectuală”,** preluat din SI e-OPI, și conține următoarele date:

- numărul cererii de intervenție;
- numărul înregistrării OPI;
- data înregistrării OPI;
- termenul de valabilitate al înregistrării OPI;
- statutul OPI;
- originea cererii de înregistrare;
- denumirea OPI;
- tipul OPI;
- clasele de protecție/clasificare Nice;
- imaginea grafică;
- datele titularului OPI/rezentantului (Jurisdicția persoanei; Statutul persoanei; Calitatea persoanei; Funcția; IDNO; Denumirea persoanei juridice; Date de contact: localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

**e) obiectul informațional „Documente atașate”,** care conține următoarele date:

- numărul documentului;
- tipul documentului;
- numele fișierului;

- autorul documentului;
- data creării documentului;
- mărimea fișierului.

**f) obiectul informațional „Rețineri”**, care va conține următoarele date:

- numărul cererii de intervenție;
- subdiviziunea organului vamal;
- data reținerii/suspendării;
- procedura aplicată (cerere de intervenție/ex officio);
- tipul produsului;
- starea bunului;
- OPI;
- proprietarul bunurilor;
- titularul de drepturi;
- țara de origine;
- țara de destinație;
- tipul de transport;
- acțiunea întreprinsă (tipul acțiunii, data dispunerii acțiunii, data aplicării acțiunii).

**g) obiectul informațional „Contestații”**, care conține următoarele date:

- numărul cererii de intervenție;
- tipul/obiectul contestației;
- rezultatul contestației.

**6.2. Conturul „REGISTRUL CERERILOR DE INTERVENȚIE”** oferă titularului de drepturi funcționalități de:

- Căutare avansată în Registrul cererilor de intervenție;
- Consultare, vizualizare a datelor din Registrul cererilor de intervenție și acces direct către detaliile cererii de intervenție;
- Căutare punctuală în Registrul cererilor de intervenție;
- Exportarea informațiilor din Registrul cererilor de intervenție (format Word, Excel, PowerPoint, PDF, TIFF file, MHTML, CSV, XML file, Data feed);
- Imprimarea informațiilor din Registrul cererilor de intervenție.

În cadrul conturului informațional „REGISTRUL CERERILOR DE INTERVENȚIE”, sunt configurate următoarele date:

- numărul cererii de intervenție;
- data depunerii cererii;
- statut solicitant;
- persoană fizică/persoană juridică;
- național/străin;
- numele persoanei responsabile de examinare din cadrul Serviciului Vamal;
- statutul cererii;
- informația despre OPI relaționat cererii de intervenție (tipul OPI, numărul înregistrării, nume titular de drepturi, clasele de protecție/clasificare Nice, imaginea grafică).

**6.3. Conturul funcțional „NOTIFICĂRI”**, oferă titularului de drepturi recepționarea notificărilor privind acțiunile întreprinse în contextul inițierii, depunerii unei cereri de intervenție, acțiunile întreprinse de Serviciul Vamal în legătura cu cererea titularului și statutul de examinare a acesteia.

Conturul conține următoarele tipuri de notificări:

- notificare privind inițierea cererii de intervenție;
- notificare privind cererea de intervenție pregătită pentru a fi semnată electronic;
- notificare privind semnarea electronică de către titular a cererii de intervenție;
- notificare privind transmiterea cererii de intervenție către Serviciul Vamal;
- notificare privind expedierea/returnarea cererii de intervenție pentru modificări, corectări, completări;
- notificare privind inspectorul vamal alocat;

- notificare privind acceptarea cererii de intervenție;
- notificare privind refuzarea cererii de intervenție;
- notificare privind anularea cererii de intervenție;
- notificare privind suspendarea cererii de intervenție;
- notificare privind expirarea cererii de intervenție.

**6.4.** Conturul funcțional „**INCIDENTE**”, permite titularului de drepturi raportarea unor incidente, probleme apărute în procesul de utilizare a sistemului informațional.

Incidentele raportate sunt clasificate în următoarele tipuri:

- Cerință tehnică anterior nedefinită;
- Cerință tehnică neimplementată (eroare logică);
- Îmbunătățire minoră de utilizare;
- Eroare de soft ce determină funcționarea inadecvată a sistemului (bug);
- Solicitare de clarificare;
- Solicitare de suport tehnic;
- Solicitare de training.

La fel, în cadrul conturului funcțional titularul are posibilitatea de a căuta un anumit incident, în baza unor parametri dinamici, precum și de a monitoriza statutul incidentului raportat:

- Depus;
- În progres;
- În proces de testare;
- Suspendat;
- Anulat;
- Soluționat.

**7. Modulul funcțional al Serviciului Vamal**, reprezintă spațiul de lucru destinat reprezentanților Serviciului Vamal pentru organizarea procesului de examinare, acceptare a cererilor de intervenție, gestionarea Registrului cererilor de intervenție și măsurilor de reținere aplicate. În cadrul acestui modul sunt operaționale următoarele contururi funcționale:

**7.1.** Conturul „**CERERI DE INTERVENȚIE**” (Serviciul Vamal), oferă următoarele funcționalități:

Pentru inspectorul vamal șef:

- căutarea unei cereri de intervenție după: numărul cererii, titularul de drepturi, numărul de înregistrare al OPI;
- vizualizarea rezultatului căutării, care reprezintă informații despre cererile de intervenție inițiate de titularul de drepturi;
- recepționarea și vizualizarea cererilor de intervenție depuse de titulari;
- alocarea unui inspector vamal și transmiterea spre examinare de către acesta a cererii de intervenție;
- gestionarea cererilor de intervenție aflate în examinare la inspectorii vamali și funcționalitatea de realocare a inspectorului;
- gestionarea cererilor de intervenție pe suport de hârtie, examinate de inspectorii vamali;
- gestionarea cererilor de intervenție acceptate, funcționalitatea de realocare a inspectorului vamal;
- gestionarea cererilor de intervenție respinse, suspendate și anulate.

Pentru inspectorul vamal:

- căutarea unei cereri de intervenție după: numărul cererii, titularul de drepturi, numărul de înregistrare al OPI;
- vizualizarea rezultatului căutării, care reprezintă informații despre cererile de intervenție inițiate de titularul de drepturi;
- recepționarea și vizualizarea cererilor de intervenție depuse de titulari și repartizate de inspectorul vamal șef;
- gestionarea cererilor de intervenție electronice și pe hârtie, repartizate spre examinare de inspectorul vamal șef prin funcționalitatea de „Acceptarea cererii”, „Refuzarea cererii”;

- gestionarea cererilor de intervenție acceptate prin funcționalitatea de „Anularea cererii” și „Suspendarea cererii”;
- gestionarea cererilor de intervenție respinse, suspendate și anulate.

În cadrul conturului informațional „**CERERI DE INTERVENȚIE**” (Serviciul Vamal), sunt configurate date despre următoarele obiecte informaționale:

**a) obiectul informațional „Intervenție”,** care conține următoarele date:

- numărul cererii;
- data depunerii cererii;
- data transmiterii;
- numărul de intrare al cererii;
- statutul solicitantului;
- mențiunea privind solicitarea utilizării procedurii de la art. 305<sup>1</sup> Cod Vamal;
- inspectorul vamal responsabil/alocat;
- data deciziei;
- perioada de valabilitate a protecției;
- informații privind decizia de refuzare;
- documente generate (Declarația titularului, în sensul art. 302<sup>1</sup> Cod Vamal și Cererea de intervenție, în sensul art. 303 Cod Vamal).

**b) obiectul informațional „Solicitant”,** care conține următoarele date:

- jurisdicția persoanei;
- statutul persoanei;
- calitatea persoanei;
- funcția;
- IDNO/IDNP;
- denumirea persoanei juridice/Nume, prenumele persoanei fizice;
- date de contact (localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

**c) obiectul informațional „Persoane de contact”,** care conține următoarele date:

- jurisdicția persoanei;
- statutul persoanei;
- calitatea persoanei;
- responsabilitatea persoanei (probleme administrative/tehnice);
- IDNP;
- nume, prenumele persoanei fizice;
- date de contact (localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

**d) obiectul informațional „Obiectul de proprietate intelectuală”,** preluat din SI e-OPI, și conține următoarele date:

- numărul cererii de intervenție;
- numărul înregistrării OPI;
- data înregistrării OPI;
- termenul de valabilitate al înregistrării OPI;
- statutul OPI;
- originea cererii;
- denumirea OPI;
- tipul OPI;
- clasele de protecție/clasificare;
- imaginea grafică;
- datele titularului OPI/reprezentantului (Jurisdicția persoanei; Statutul persoanei; Calitatea persoanei; Funcția; IDNO; Denumirea persoanei juridice; Date de contact: localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

**e) obiectul informațional „Documente atașate”,** care conține următoarele date:

- numărul documentului;
- tipul documentului;



- numele fișierului;
- autorul documentului;
- data creării documentului;
- mărimea fișierului.

**f) obiectul informațional „Rețineri”**, care va conține următoarele date:

- numărul cererii de intervenție;
- subdiviziunea organului vamal;
- data reținerii/suspendării;
- procedura aplicată (cerere de intervenție/ex officio);
- tipul produsului;
- starea bunului;
- OPI;
- proprietarul bunurilor;
- titularul de drepturi;
- țara de origine;
- țara de destinație;
- tipul de transport;
- acțiunea întreprinsă (tipul acțiunii, data dispunerii acțiunii, data aplicării acțiunii).

**g) obiectul informațional „Contestații”**, care conține următoarele date:

- numărul cererii de intervenție;
- tipul/obiectul contestației;
- rezultatul contestației.

**7.2. Conturul „REGISTRUL CERERILOR DE INTERVENȚIE”** (Serviciul Vamal) oferă reprezentatului Serviciul Vamal funcționalități de:

- Căutare avansată în Registrul cererilor de intervenție;
- Consultare, vizualizare a datelor din Registrul cererilor de intervenție și acces direct către detaliile cererii de intervenție;
- Căutare punctuală în Registrul cererilor de intervenție;
- Exportarea informațiilor din Registrul cererilor de intervenție (format Word, Excel, PowerPoint, PDF, TIFF file, MHTML, CSV, XML file, Data feed);
- Imprimarea informațiilor din Registrul cererilor de intervenție.

În cadrul conturului informațional „REGISTRUL CERERILOR DE INTERVENȚIE” (Serviciul Vamal), sunt configurate următoarele date:

- numărul cererii de intervenție;
- data depunerii cererii;
- statutul solicitantului;
- persoană fizică/persoană juridică;
- național/străin;
- numele persoanei responsabile de examinare din cadrul Serviciului Vamal;
- statutul cererii;
- informația despre OPI relaționat cererii de intervenție (tipul OPI, numărul înregistrării, nume titular de drepturi, clasele de protecție/clasificare, imaginea grafică).

**7.3. Conturul funcțional „REȚINERI”** (Serviciul Vamal), reprezintă instrumentarul necesar reprezentanților Serviciului Vamal pentru gestionarea și monitorizarea procedurilor de reținere a bunurilor în privința cărora există suspecții că aduc atingere drepturilor de proprietate intelectuală.

Conturul pune la dispoziție reprezentantului Serviciului Vamal funcționalități de:

1) inițiere a procedurii ex officio. Astfel, la inițierea unei noi înregistrări privind procedura ex officio, sunt configurate următoarele câmpuri de date:

- numărul cererii de intervenție;
- subdiviziunea organului vamal;
- data reținerii/suspendării;
- procedura aplicată;

- tipul produsului;
- starea bunului (contrafăcut, falsificat, original);
- țara de origine;
- țara de destinație;
- tipul transportului (aerian, maritim, rutier, poștal, cale ferată).

2) Vizualizare, consultare a reținerilor dispuse de Serviciul Vamal, unde sunt disponibile următoarele date:

- numărul cererii de intervenție;
- subdiviziunea organului vamal;
- data reținerii/suspendării;
- procedura aplicată;
- tipul produsului;
- starea bunului (contrafăcut, falsificat, original);
- obiectul de proprietate intelectuală;
- proprietarul bunurilor;
- titularul de drepturi;
- țara de origine;
- țara de destinație;
- tipul transportului (aerian, maritim, rutier, poștal, cale ferată);
- acțiuni dispuse, cu posibilitatea de redactare, adăugare a unei noi acțiuni.

**7.4. Conturul funcțional „NOTIFICĂRI”** (Serviciul Vamal), oferă reprezentantului Serviciului Vamal recepționarea notificărilor privind acțiunile întreprinse în contextul inițierii, depunerii unei cereri de intervenție, acțiunile întreprinse de Serviciul Vamal în legătura cu cererea titularului și statutul de examinare a acesteia.

Conturul conține următoarele tipuri de notificări:

- notificare privind cererea de intervenție pregătită pentru a fi semnată electronic;
- notificare privind semnarea electronică de către titular a cererii de intervenție;
- notificare privind transmiterea cererii de intervenție către Serviciul Vamal;
- notificare privind expedierea/returnarea cererii de intervenție pentru modificări, corectări, completări;
- notificare privind inspectorul vamal alocat;
- notificare privind aprobarea cererii de intervenție;
- notificare privind refuzarea cererii de intervenție;
- notificare privind anularea cererii de intervenție;
- notificare privind suspendarea cererii de intervenție;
- notificare privind expirarea cererii de intervenție.

**7.5. Conturul funcțional „INCIDENTE”**, permite reprezentantului Serviciului Vamal raportarea unor incidente, probleme apărute în procesul de utilizare a sistemului informațional.

Incidentele raportate sunt clasificate în următoarele tipuri:

- Cerință tehnică anterior nedefinită;
- Cerință tehnică neimplementată (eroare logică);
- Îmbunătățire minoră de utilizare;
- Eroare de soft ce determină funcționarea inadecvată a sistemului (bug);
- Solicitare de clarificare;
- Solicitare de suport tehnic;
- Solicitare de training.

La fel, în cadrul conturului funcțional titularul are posibilitatea de a căuta un anumit incident, în baza unor parametri dinamici, precum și de a monitoriza statutul incidentului raportat:

- Depus;
- În progres;
- În proces de testare;
- Suspendat;
- Anulat;

- Soluționat.

#### **IV. SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII, EXPLOATĂRII ȘI UTILIZĂRII SI e-RCI**

**8.** Subiecții în domeniul creării, exploatării și utilizării conținutului SI e-RCI sunt:

- 1) proprietarul;
- 2) posesorul;
- 3) deținătorul;
- 4) operatorul tehnico-tehnologic;
- 5) utilizatorii;

**9.** *Proprietarul* este statul care realizează dreptul de proprietate, de gestionare și utilizare a datelor din SI e-RCI.

**10.** *Posesorul și deținătorul*, cu drept de creare, gestionare, utilizare și deținere a resursei informaționale este Serviciul Vamal.

**11.** Posesorul și deținătorul (Serviciul Vamal) exercită următoarele atribuții:

- a) asigură condițiile organizatorice și financiare pentru funcționarea SI e-RCI;
- b) stabilește scopurile și sarcinile funcționale ale SI e-RCI;
- c) determină obiectele informaționale supuse înregistrării în SI e-RCI și conținutul acestora;
- d) monitorizează procesul de înregistrare și prelucrare a datelor în SI e-RCI;
- e) gestionează activitatea de exploatare și ținere a conținutului informațional al SI e-RCI;
- f) asigură securitatea și protecția datelor din SI e-RCI prin intermediul structurilor de stat specializate;
- g) aprobă și coordonează cu operatorul tehnico-tehnologic executarea modificărilor, rectificărilor solicitate în cererile privind erorile de sistem ale SI e-RCI, erorile cauzate de factorul uman în SI e-RCI, incidentele de infrastructură care afectează funcționarea normală a SI e-RCI;
- h) autorizează, suspendă și revocă dreptul de acces în SI e-RCI;
- i) stabilește măsurile tehnice și organizatorice de protecție și securitate a SI e-RCI;
- j) monitorizează și, după caz, ajustează cerințele de securitate și conformitate a SI e-RCI la domeniul protecției datelor cu caracter personal;
- k) exercită alte atribuții necesare asigurării bunei funcționări a SI e-RCI.

**12.** Posesorul asigură păstrarea SI e-RCI pînă la adoptarea deciziei despre lichidarea acestuia. În cazul lichidării, datele și documentele conținute în acesta se transmit în arhivă, conform legislației.

**13.** *Operatorul tehnico-tehnologic* este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”.

**14.** Operatorul tehnico-tehnologic are următoarele atribuții:

- a) asigură administrarea tehnică a SI e-RCI, inclusiv funcționalitatea și securitatea logică și cibernetică în conformitate cu actele normative în domeniu;
- b) controlează și asigură funcționarea e-RCI;
- c) execută modificările/rectificările solicitate în demersurile primite referitoare la erorile de sistem ale SI e-RCI, erorile cauzate de factorul uman în SI e-RCI, incidentele de infrastructură care afectează funcționarea normală a SI e-RCI, cu condiția primirii în prealabil a aprobării posesorului, în rezultatul verificării de către posesor a corespunderii solicitării cu prevederile legislației;
- d) asigură autorizarea accesului, precum și suspendarea și revocarea drepturilor de acces în SI e-RCI, cu condiția primirii în prealabil a aprobării posesorului în rezultatul verificării de către posesor a corespunderii solicitării cu prevederile legislației;

- e) elaborează și aprobă în comun cu posesorul Planul de continuitate al SI e-RCI, instituie activități de control menite să diminueze riscurile privind integritatea datelor SI e-RCI;
- f) adresează posesorului demersuri privind autorizarea accesului, precum și suspendarea și revocarea drepturilor de acces și întocmește lista nominală a angajaților acestuia cu drepturi în sistem și datele de contact, care este transmisă posesorului de fiecare dată când datele se modifică;
- g) alte atribuții necesare asigurării bunei funcționări a SI e-RCI.

**15.** Administrarea SI e-RCI include asigurarea funcționalității, disponibilității și continuității SI e-RCI în conformitate cu Planul de continuitate al SI e-RCI, precum și procedurile operaționale ale deținătorului tehnic.

**16.** Activitatea deținătorului tehnic se supune auditului extern.

**17.** *Utilizatori* ai SI e-RCI sunt titularii de drepturi și Serviciul Vamal din cadrul Ministerului Finanțelor, prin intermediul angajaților acestora împuterniciți cu atribuții de acces în sistem, în baza atribuțiilor acordate prin lege.

**18.** Utilizatorii SI e-RCI au următoarele atribuții:

- a) asigură colectarea, introducerea și prelucrarea informației relevante în baza de date a SI e-RCI, în termenele și condițiile stabilite;
- b) asigură autenticitatea, plenitudinea, integritatea datelor din SI e-RCI;
- c) asigură securitatea și confidențialitatea informației introduse în SI e-RCI;
- d) asigură introducerea și prelucrarea datelor și monitorizează procesul de introducere a acestora;
- e) raportează de fiecare dată posesorului incidentele de infrastructură, erorile de sistem sau erorile cauzate de factorul uman în scopul remedierii acestora;
- f) solicită posesorului autorizarea accesului, precum și suspendarea și revocarea drepturilor de acces în SI e-RCI;
- g) adresează posesorului cereri de modificare a drepturilor de acces/rolurilor unor utilizatori;
- h) raportează posesorului sau operatorului tehnico-tehnologic problemele de sistem în utilizarea SI e-RCI;
- i) înaintează demersuri privind necesitatea de dezvoltare și îmbunătățire a SI e-RCI;
- j) participă în grupurile de lucru organizate în scopul dezvoltării și îmbunătățirii SI e-RCI.

**19.** Utilizatorii din cadrul Serviciului Vamal desemnează și informează posesorul despre numărul, numele, prenumele angajaților acestora cu atribuții de introducere nemijlocită a datelor în baza de date și împuterniciri specifice ce sînt delegate în sensul îndeplinirii atribuțiilor legate de gestionarea spațiului de lucru în SI e-RCI.

## **V. MODUL DE ACCESARE ȘI UTILIZARE A SI e-RCI**

**20.** Accesul la resursele informaționale ale SI e-RCI este segmentat pentru utilizatorii interni și utilizatorii externi.

**21.** Utilizatori interni ai SI e-RCI sînt posesorul/deținătorul, operatorul tehnico-tehnologic, utilizatorul din cadrul Serviciului Vamal, ale căror drepturi de acces sînt definite în acte normative.

**22.** Utilizatori externi ai SI e-RCI sînt titularii de drepturi.

**23.** Utilizatorii beneficiază de drepturi de acces la informația din SI e-RCI conform atribuțiilor și funcțiilor deținute și regimul juridic al informației accesate. Nivelul de acces la informație pentru fiecare participant corespunde funcției de serviciu și/sau profilului de acces.

**24.** Posesorul va asigura conectarea participanților la SI e-RCI, în scopul exercitării de către aceștia a obligațiilor prevăzute de legislația.

**25.** Utilizatorii se vor conecta la SI e-RCI prin intermediul Serviciului electronic guvernamental de autentificare și control al accesului (MPass).

**26.** Posesorul are acces cu drept de vizualizare a datelor din SI e-RCI, în limita scopului și atribuțiilor legale prevăzute de legislația.

**27.** Operatorul tehnico-tehnologic are acces tehnic la datele din SI e-RCI, în scopul prestării serviciilor de administrare, inclusiv mentenanță adaptivă și perfectivă a SI e-RCI.

**28.** Utilizatorul are acces tehnic la datele din SI e-RCI, ceea ce implică introducerea, modificarea și radierea informației înregistrate. Un utilizator nu poate modifica informațiile documentate în SI e-RCI de către alt registrator.

**29.** Terții au acces informațional la datele din SI e-RCI, ceea ce presupune vizualizarea informației numai în formatul individual permis pentru fiecare utilizator în parte, întrucât conținutul informațional al SI e-RCI este determinat atât de date publice, cât și de date cu acces limitat.

**30.** Dreptul de acces la SI e-RCI nu este unul permanent, acesta poate fi suspendat sau revocat în circumstanțele prevăzute în prezentul Regulament. Introducerea și/sau modificarea datelor în e-RCI de pe un profil de utilizator străin este strict interzisă, urmînd a fi considerată ca acces neautorizat. Utilizatorii urmează să se asigure de faptul că profilul de utilizator, precum și semnătura electronică sînt confidențiale.

**31.** Revocarea dreptului de acces la SI e-RCI se efectuează la demersul motivat către posesor, în una dintre următoarele situații:

- a) la încetarea/suspendarea raporturilor de serviciu/ de muncă ale utilizatorului;
- b) la intervenirea modificărilor raporturilor de serviciu/de muncă cînd noile atribuții nu impun accesul la datele din SI e-RCI;
- c) la constatarea de către posesor a încălcării securității informaționale;
- d) în alte cazuri, în limitele prevederilor legislației.

**32.** Lucrările profilactice planificate în complexul de mijloace software și hardware se efectuează după notificarea, în scris sau prin e-mail, a registratorilor de către posesor, în baza planului coordonat cu operatorul tehnico-tehnologic cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil. Lucrările profilactice neplanificate se efectuează la solicitarea utilizatorilor și coordonarea prealabilă cu posesorul în situația nefuncționării sau funcționării necorespunzătoare a complexului de mijloace software și hardware.

## **VI. ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI ȘI RESURSELOR INFORMAȚIONALE ALE SI e-RCI**

**33.** Măsurile de protecție și securitate a informației din SI e-RCI reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a SI e-RCI și se efectuează neîntrerupt de către posesorul/deținătorul Sistemului.

**34.** Obiecte ale asigurării protecției și securității informației din SI e-RCI se consideră:

- 1) masivele informaționale, indiferent de formele păstrării, bazele de date, suporturile materiale care conțin informații privind date cu caracter personal;
- 2) sistemele informaționale, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații care asigură activitatea SI e-RCI;
- 3) sistemele de telecomunicații, rețelele, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

**35.** Protecția informației cu caracter personal din SI e-RCI se efectuează prin următoarele metode:

1) prevenirea conexiunilor neautorizate la rețelele tele-comunicaționale și a interceptării cu ajutorul mijloacelor tehnice a datelor din Sistem transmise prin aceste rețele, asigurată prin folosirea metodelor de cifrare și criptare a acestei informații, inclusiv cu utilizarea măsurilor organizatorice, tehnice și de regim;

2) excluderea accesului neautorizat la datele din Sistem, asigurată prin folosirea mijloacelor speciale tehnice și de program, cifrarea acestor informații, inclusiv prin măsurile organizatorice și de regim;

3) prevenirea acțiunilor intenționate și/sau neintenționate ale participanților la Sistem care pot conduce la distrugerea sau modificarea datelor acestuia, prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizarea sistemului de control al securității softului și efectuarea periodică a copiilor de siguranță.

**36.** Posesorul SI e-RCI elaborează, aprobă și organizează implementarea documentului care stabilește politica de securitate informațională pentru asigurarea respectării regulilor, standardelor și normelor general acceptate în domeniul securității informaționale, cu indicarea:

1) identității persoanei responsabile de politica de securitate;

2) principalelor măsuri tehnico-organizatorice necesare de asigurare a funcționării SI e-RCI;

3) procedurilor interne ce exclud cazurile de modificare neautorizată a mijloacelor software și/sau a informației din Sistem;

4) nivelului necesar de securitate pentru fiecare categorie de utilizatori ai Sistemului;

5) listei nominale a utilizatorilor autorizați să acceseze datele din Sistem;

6) responsabilităților utilizatorilor Sistemului privind asigurarea securității informaționale;

7) procedurilor de control intern al utilizatorilor Sistemului privind respectarea condițiilor de securitate informațională.

**37.** Posesorul SI e-RCI desemnează o persoană subordonată nemijlocit conducătorului instituției, responsabilă de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate informațională.

**38.** Persoana responsabilă de politica securității informaționale asigură definirea clară a tuturor responsabilităților cu privire la securitatea informației din SI e-RCI (prevenire, supraveghere, detectare și prelucrare), precum și operarea cu ele.

**39.** În cazul operării cu informația din SI e-RCI ce a devenit cunoscută utilizatorului acestui sistem în urma activității sale, este asigurat regimul de confidențialitate, care presupune următoarele acțiuni:

1) limitarea numărului persoanelor cu drept de acces la datele din SI e-RCI;

2) monitorizarea procedurii de admitere și delimitarea funcțională a responsabilităților persoanelor care au acces la informația din SI e-RCI;

3) identificarea și autentificarea participanților la SI e-RCI cu folosirea mijloacelor moderne de autentificare;

4) executarea măsurilor de protecție a informației în cadrul păstrării, prelucrării și transmiterii acesteia prin intermediul canalelor de comunicații.

**40.** 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 concordanță cu politica de securitate.

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

## **VII. PROTECȚIA DATELOR CU CARACTER PERSONAL, CONTROLUL ȘI RESPONSABILITATEA**

**42.** Prelucrarea datelor cu caracter personal se efectuează în conformitate cu legislația în domeniul protecției datelor cu caracter personal.

**43.** Persoanele împuternicite cu drept de acces la SI e-RCI sînt obligate de a nu divulga informația cu accesibilitate limitată la care au primit acces în legătură cu exercitarea atribuțiilor funcționale, inclusiv după încetarea activității. Pentru încălcarea clauzei de confidențialitate, persoanele vinovate poartă răspundere în conformitate cu legislația.

**44.** Responsabilitatea pentru organizarea și funcționarea SI e-RCI se atribuie posesorului, care elaborează tipul și modelul documentelor aferente, instrucțiunile privind modul de completare și alte materiale necesare pentru funcționarea acestui sistem.

**45.** Ținerea SI e-RCI este supusă controlului intern și extern. Controlul intern privind organizarea și funcționarea SI e-RCI se efectuează de către posesor. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea SI e-RCI se efectuează de către instituții abilitate și certificate în domeniul auditului.

**46.** Utilizatorii în atribuțiile cărora intră ținerea SI e-RCI, introducerea datelor, furnizarea informațiilor și asigurarea funcționării SI e-RCI poartă răspundere personală în conformitate cu legislația, pentru completitudinea, autenticitatea, veridicitatea, integritatea informației, precum și pentru păstrarea și utilizarea ei.

**47.** Toți subiecții SI e-RCI, precum și solicitantul informațiilor ce conțin date cu caracter personal poartă răspundere conform legislației pentru prelucrarea, divulgarea, transmiterea informației din sistem persoanelor terțe, cu încălcarea prevederilor legale.

**48.** Anual, pînă la data de 31 ianuarie, posesorul prezintă Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova un raport generalizat despre incidentele de securitate din cadrul SI e-RCI, în conformitate cu prevederile Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr. 1123/2010.

**49.** Pentru asigurarea funcționalității eficiente și neîntreprute a SI e-RCI, schimbul informațional de date SI e-RCI este asigurat în regim non-stop.

**50.** Funcționarea SI e-RCI se suspendă de către operatorul tehnico-tehnologic sau la demersul utilizatorului, după coordonarea prealabilă cu posesorul, în caz de apariție a uneia dintre următoarele situații:

- a) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al SI e-RCI;
- b) la apariția circumstanțelor de forță majoră;
- c) la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea SI e-RCI;
- d) în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SI e-RCI;
- e) la cererea scrisă a posesorului.

**51.** În cazul apariției circumstanțelor de forță majoră și a dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SI e-RCI din vina terțelor persoane, este posibilă suspendarea funcționării SI e-RCI, cu informarea subiecților SI e-RCI prin mijloacele tehnice disponibile.