Anexa nr.4
la Hotărîrea Guvernului
nr._____ din _____2019

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

I. DISPOZIŢII 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 şi funcţionarea 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;

administratorul tehnic al SI e-RCI – Centrul de Tehnologii Informaţionale în Finanţe, 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;

prelucrarea datelor cu caracter personal – 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, atît la nivel de sistem, cît și la nivel de date;

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 protecţie la frontieră, reţineri înregistrate şi rezultatul reţinerilor; cereri (sesizări) referitoare la obiectele de proprietate intelectuală depuse la Inspectoratul General al Poliției, procedura de verificare efectuată, actul de constatare, procedura de ridicare a produselor și dosare înregistrate (contravenționale şi penale); sesizări referitoare la obiectele de proprietate intelectuală adresate Procuraturii Generale în conformitate cu prevederile Codului de procedură penală, procese penale înregistrate, procese contravenţionale pornite, cauze penale pornite şi hotărâri judecătoreşti.

II. SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII, EXPLOATĂRII ȘI UTILIZĂRII SI e-RCI

3. Subiecții în domeniul creării, exploatării și utilizării conținutului SI e-RCI sunt:
1) proprietarul;
2) posesorul;
3) deținătorul;
4) administratorul tehnic;
5) utilizatorii;

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

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

6. Posesorul și deținătorul (Serviciul Vamal) exercită următoarele atribuții:
1) asigură condițiile organizatorice şi financiare pentru funcționarea SI e-RCI;
2) stabilește scopurile și sarcinile funcționale ale SI e-RCI;
3) determină obiectele informaționale supuse înregistrării în SI e-RCI și conținutul acestora;
4) monitorizează procesul de înregistrare și prelucrare a datelor în SI e-RCI;
5) gestionează activitatea de exploatare și ținere a conținutului informațional al SI e-RCI;
6) asigură securitatea și protecția datelor din SI e-RCI prin intermediul structurilor de stat specializate;
7) aprobă și coordonează cu administratorul tehnic 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;
8) autorizează, suspendă și revocă dreptul de acces în SI e-RCI;
9) stabilește măsurile tehnice și organizatorice de protecție și securitate a SI e-RCI;
9) monitorizează și, după caz, ajustează cerințele de securitate și conformitate a SI e-RCI la domeniul protecției datelor cu caracter personal;
10) exercită alte atribuții necesare asigurării bunei funcționări a SI e-RCI.

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

8. *Administratorul tehnic* este Instituţia Publică „Centrul de Tehnologii Informaţionale în Finanţe”.

9. Administratorul tehnic are următoarele atribuții:
1) asigură administrarea tehnică a SI e-RCI, inclusiv funcționalitatea și securitatea logică și cibernetică în conformitate cu actele normative în domeniu;
2) controlează și asigură funcționarea e-RCI;
3) 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;

4) 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;

5) 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;

6) 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 cînd datele se modifică;

7) alte atribuții necesare asigurării bunei funcționări a SI e-RCI.

10. 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.

11. Activitatea deținătorului tehnic se supune auditului extern.

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

13. Utilizatorii SI e-RCI au următoarele atribuții:

1) asigură colectarea, introducerea și prelucrarea informației relevante în baza de date a SI e-RCI, în termenele și condițiile stabilite;

2) asigură autenticitatea, plenitudinea, integritatea datelor din SI e-RCI;

3) asigură securitatea și confidențialitatea informației introduse în SI e-RCI;

4) asigură introducerea și prelucrarea datelor și monitorizează procesul de introducere a acestora;

5) raportează de fiecare dată posesorului incidentele de infrastructură, erorile de sistem sau erorile cauzate de factorul uman în scopul remedierii acestora;

6) solicită posesorului autorizarea accesului, precum și suspendarea și revocarea drepturilor de acces în SI e-RCI;

7) adresează posesorului cereri de modificare a drepturilor de acces/rolurilor unor utilizatori;

8) raportează posesorului sau administratorului tehnic problemele de sistem în utilizarea SI e-RCI;

9) înaintează demersuri privind necesitatea de dezvoltare și îmbunătățire a SI e-RCI;

10) participă în grupurile de lucru organizate în scopul dezvoltării și îmbunătățirii SI e-RCI.

14. 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.

III. MODUL DE ACCESARE ŞI UTILIZARE A SI e-RCI

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

16. Utilizatori interni ai SI e-RCI sînt posesorul/deținătorul, administratorul tehnic, utilizatorul din cadrul Serviciului Vamal, ale căror drepturi de acces sînt definite în acte normative.

17. Utilizatori externi ai SI e-RCI sunt titularii de drepturi.

18. 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.

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

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

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

22. Administratorul tehnic are acces tehnic la datele din SI e-RCI, în scopul prestării serviciilor de administrare, inclusiv mentenanță adaptivă și perfectivă a SI e-RCI.

23. 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.

24. 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.

25. 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, urmând a fi considerată ca acces neautorizat. Utilizatorii urmează să se asigure de faptul că profilul de utilizator, precum și semnătura electronică sînt confidențiale.

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

1) la încetarea/suspendarea raporturilor de serviciu/ de muncă ale utilizatorului;

2) la intervenirea modificărilor raporturilor de serviciu/de muncă când noile atribuții nu impun accesul la datele din SI e-RCI;

3) la constatarea de către posesor a încălcării securității informaționale;

4) în alte cazuri, în limitele prevederilor legislației.

27. 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 administratorul tehnic 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.

IV. ASIGURAREA PROTECŢIEI ŞI SECURITĂŢII INFORMAŢIEI ŞI RESURSELOR INFORMAŢIONALE ALE SI e-RCI

28. 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.

29. 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.

30. Protecția datelor 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.

31. 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.

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

33. 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.

34. 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.

35. 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.

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

V. PROTECŢIA DATELOR CU CARACTER PERSONAL, CONTROLUL ŞI RESPONSABILITATEA

37. Prelucrarea datelor cu caracter personal se efectuează în conformitate cu legislaţia în domeniul protecției datelor cu caracter personal.

38. Datele cu caracter personal prelucrate în cadrul SI e-RCI sunt stocate pe o perioadă ce nu depășește durata de protecție a obiectelor de proprietate intelectuală, stabilită de legislația în vigoare. La expirarea termenului de stocare, datele cu caracter personal, rămîn la păstrare, primind statutul de document de arhivă, cu excepția obiectelor dreptului de autor, care intră în domeniul public, odată cu expirarea termenului de protecție a drepturilor patrimoniale. Regulamentul privind prelucrarea informațiilor ce conțin date cu caracter personal în cadrul Sistemului informațional în „Registrul cererilor de intervenție ” se aprobă prin Ordinul Directorului Serviciului Vamal.

39. 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.

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

41. 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.

42. 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.

43. 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.

44. 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.

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

46. Funcționarea SI e-RCI se suspendă de către administratorul tehnic sau la demersul utilizatorului, după coordonarea prealabilă cu posesorul, în caz de apariție a uneia dintre următoarele situații:

1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al SI e-RCI;

2) la apariția circumstanțelor de forță majoră;

3) la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea SI e-RCI;

4) în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SI e-RCI;

5) la cererea scrisă a posesorului.

47. 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 terților persoane, este posibilă suspendarea funcționării SI e-RCI, cu informarea subiecților SI e-RCI prin mijloacele tehnice disponibile.