*Anexa*

 *la Hotărârea Guvernului nr.\_\_\_\_\_din\_\_\_\_\_\_\_\_\_*

**Conceptul tehnic al Sistemului informațional automatizat**

**„Registrul amenzilor contravenționale”**

**Introducere**

 Procesul contravenţional este activitatea desfăşurată de autoritatea competentă, cu participarea părţilor şi a altor persoane titulare de drepturi şi de obligaţii, avînd ca scop constatarea contravenţiei, examinarea şi soluţionarea cauzei contravenţionale, constatarea cauzelor şi condiţiilor care au contribuit la săvîrşirea contravenţiei.

 Autoritățile competente să soluționeze cauzele contravenționale sunt prevăzute la art.393 alin.(1) din Codul contravențional.

 Ca urmare a examinării cauzei contravenționale, autoritățile competente soluționează cauza prin adoptarea deciziei asupra cauzei contravenționale, una din care poate fi aplicarea amenzii contravenționale în cuantumul reglementat de Codul contravențional.

 La etapa actuală, fiecare autoritate cu drept de soluționare a cauzelor contravenționale, ține separat evidența amenzilor contravenționale aplicate. Cu toate acestea, autoritățile care au aplicat amenzi contravenționale nu dețin informația cu privire la sumele amenzilor contravenționale achitate, informație care este deținută de Serviciul Fiscal de Stat.

 Deci, suntem în prezența situației când informația despre suma amenzii contravenționale aplicate este deținută de către o autoritate publică, iar informația despre suma amenzii achitate – de către o altă autoritate publică.

 Situația respectivă nu permite o bună evidență a sumelor amenzilor contravenționale aplicate și achitate/neachitate, deoarece există o ruptură între deținătorul informației cu privire la suma aplicată și a celei cu privire la suma achitată.

 Respectiv, se impune necesitatea creării și implementării unui sistem informațional care să asigure vizualizarea de către deținător atît a informației cu privire la sumele amenzilor contravenționale aplicate, cît și a celor achitate.

 Implementarea Sistemului informațional automatizat “Registrul amenzilor contravenționale” (*în continuare SIA „RAC”*) va asigura evidența analitică conformă privind calcularea și achitarea amenzilor aplicate în cadrul procesului contravențional, precum și urmăririi plenitudinii încasărilor efectuate și raportării acestora.

 Implementarea unui sistem informatic care va gestiona întreg fluxul de documente în procesul evidenței amenzilor contravenționale, oferă un instrument puternic de gestionare a acțiunilor autorităților competente să soluționeze cauzele contravenționale și, totodată, permite ținerea evidenței și efectuarea raportării statistice și analitice cu o mai mare eficacitate și eficiență.

 Astfel, *SIA „RAC”* este un instrument-cheie de asigurare a evidenței amenzilor contravenționale, poate asigura accesul on-line la dosarul electronic al procedurii și, în același timp, poate îndeplini cerințele strategiei naționale de migrare a sistemelor informaționale pe platforma MCloud, schimbul de date cu alte sisteme informaționale prin intermediul platformei MConnect și integrarea lor cu serviciile de platformă precum MSign, MPass, MPay, MNotify și MLog.

**Conceptul tehnic al SIA „RAC”** (în continuare – Concept) stabileşte scopurile, sarcinile şi funcţiile sistemului, structura organizaţională şi baza juridico-normativă, necesare pentru crearea şi exploatarea lui, obiectele informaţionale şi lista datelor care se păstrează în sistem, infrastructura tehnologică şi măsurile de asigurare a securităţii şi protecţiei informaţiei, precum şi măsurile legate de crearea, implementarea, exploatarea şi menţinerea sistemului.

**Capitolul I. Dispoziții generale**

1. **Definirea sistemului**

 SIA „RAC” reprezintă o soluţie informatică din categoria Guvern pentru Guvern (G4G) și are ca principal obiectiv asigurarea necesităților informatice și informaționale a actorilor implicați în procesul contravențional.

1. **Caracteristicile de bază ale sistemului**

SIA „RAC” este o platformă unică de generare și înregistrare exclusiv în format electronic, stocare și verificare a informației cu privire la amenzile contravenționale.

 SIA „RAC” creează un mediu informaţional accesibil, modern şi securizat pentru asigurarea evidenței amenzilor contravenționale aplicate și achitate/neachitate.

 Implementarea SIA „RAC” va asigura ținerea evidenței analitice conforme privind calcularea și achitarea amenzilor aplicate în cadrul procesului contravențional, precum și va avea impact benefic asupra urmăririi plenitudinii încasărilor efectuate și raportării acestora.

1. **Locul sistemului în spațiul informațional unic**

 SIA „RAC” este o parte componentă a resursei informaționale integrate a Sistemului Informațional al Serviciului Fiscal de Stat.

 Datorită poziţiei sale în cadrul resurselor informaţionale ale statului, implementarea SIA „RAC” va spori deschiderea informaţională şi transparenţa activităţilor de administrare statală, fiind parte componentă a guvernării electronice, bazat pe informaţie şi tehnologii informaționale și ale comunicației.

SIA „RAC” este integrat cu alte sisteme informaţionale cu care autoritățile competente să soluționeze cauzele contravenționale interacţionează pentru exercitarea obligaţiunilor și atribuțiilor sale.

1. **Noțiuni**

 În sensul prezentului Concept, noţiunile utilizate semnifică:

**bază de date** - ansamblu de date organizate conform structurii conceptuale care descrie caracteristicile de bază și relația dintre entități;

**clasificator** - document care reprezintă o culegere sistematizată a denumirilor şi codurilor grupelor de clasificare şi/sau obiectelor de clasificare;

**date** - unităţi informaţionale elementare despre persoane, entităţi, evenimente, procese și obiecte, prezentate într-o formă care permite gestiunea lor;

**document electronic** - informaţie în formă electronică, creată, structurată, prelucrată, păstrată, transmisă cu ajutorul computerului, altor dispozitive electronice sau mijloacelor software şi hardware, semnată cu semnătură electronică;

**gestiunea documentelor** - setul de proceduri utilizate pentru captarea, gestionarea, stocarea, menţinerea, livrarea şi distrugerea documentelor în cadrul unei organizaţii; noţiunea de “documente” poate fi atribuită unui număr vast de active informaţionale, inclusiv imagini, documente textuale, grafică şi desene, precum şi unor obiecte informaţionale moderne cum ar fi paginile web, mesajele e-mail, mesajele instant sau fişierele video;

**integritatea datelor** - stare a datelor, când acestea îşi păstrează conţinutul şi sunt interpretate univoc în cazuri de acţiuni aleatorii; integritatea se consideră păstrată dacă datele nu au fost alterate sau deteriorate (şterse);

**MCloud** - infrastructura informațională guvernamentală comună care funcționează în baza tehnologiei de „cloud computing”;

**MConnect** - soluție tehnică de interoperabilitate, parte a platformei tehnologice comune a Guvernului;

**MLog** (serviciul electronic guvernamental de jurnalizare*)* - serviciu centralizat, reutilizabil, găzduit pe platforma tehnologică guvernamentală comună (MCloud), care are scopul de a oferi un mecanism securizat şi flexibil de jurnalizare şi audit, asigurând evidenţa evenimentelor, în contextul utilizării sistemelor informaţionale;

**MPass** - serviciu reutilizabil, furnizat la nivelul platformei tehnologice comune a Guvernului, care are scopul de a oferi un mecanism integrator, securizat și flexibil de autentificare și control al accesului utilizatorilor în sistemele informaționale, inclusiv serviciile;

**MSign** - serviciu reutilizabil, furnizat la nivelul platformei tehnologice comune a Guvernului, care are scopul de a oferi un mecanism integrator, securizat și flexibil, al diferitelor soluții de aplicare și verificare a autenticității semnăturii electronice de către utilizatori, oferite de către furnizorii de semnătură electronică în conformitate cu legislația;

**obiect informațional** - reprezentare virtuală al entităților materiale și nemateriale existente;

**politică de securitate informaţională** - ansamblul unitar al normelor de drept şi etico-morale, al măsurilor organizatorico-administrative şi al mijloacelor tehnice de program, orientate spre contracararea pericolelor ce ameninţă sistemul şi spre minimizarea eventualelor prejudicii care ar putea fi cauzate posesorilor şi utilizatorilor de informaţii;

**Sistem Informațional Automatizat** - totalitatea integrată a infrastructurii informaționale de telecomunicații, a resurselor informaționale, a normelor de drept, a structurilor organizaționale și a infrastructurii utilizatorului, destinată pentru îndeplinirea sarcinilor trasate pentru utilizator;

**SLA (eng. Service Level Agreement)** - acord privind nivelul de calitate al serviciilor, încheiat între furnizorul de servicii şi client, prin intermediul căruia se specifică serviciul oferit, calitatea serviciului şi se stabilesc zonele de responsabilitate atât ale furnizorului de servicii cât şi ale clientului.

1. **Destinația sistemului**

 Destinația SIA „RAC” este generarea, colectarea, stocarea, actualizarea și analiza datelor despre amenzile contravenționale aplicate și achitate/neachitate și despre participanții la SIA „RAC”.

 SIA „RAC” servește drept instrument de susţinere și executare a tuturor activităţilor și proceselor de lucru la evidența amenzilor contravenționale, prin oferirea mijloacelor tehnice de schimb informaţional, colaborare şi transparentizare a activităţilor desfăşurate de părțile implicate în acest proces.

1. **Scopurile şi obiectivele creării sistemului**

 Scopul sistemului îl constituie automatizarea fluxurilor de procesare în cadrul procesului de evidență a amenzilor contravenționale, optimizarea cooperării dintre autoritățile care au aplicat amenzi contravenționale, prin implementarea unei soluţii moderne de e-guvernare ce va oferi un serviciu public calitativ şi va spori transparența procesului de evidență a amenzilor contravenționale.

 Obiectivul general al SIA „RAC” constă în îmbunătăţirea, automatizarea şi eficientizarea evidenței amenzilor contravenționale aplicate și achitate/neachitate.

 Prin intermediul SIA „RAC” se realizează următoarele obiective specifice:

a) eficientizarea activității de evidență a amenzilor contravenționale, prin automatizarea proceselor de lucru și acces în mod operativ la toate informațiile necesare desfășurării activității atât din sistemele interne cât și din surse externe de date;

b) uniformizarea procesului de evidență a amenzilor contravenționale și de comunicare între autoritățile care au aplicat amenzi contravenționale, precum și uniformizarea procedurilor adiacente aplicării amenzilor contravenționale;

c) automatizarea transferului de informații (creșterea gradului de interoperabilitate) între toate structurile instituțiilor beneficiare, ceea ce duce la îmbunătățirea comunicării, eficientizarea activităților specifice ale acestora și reducerea costurilor;

c) gestionarea unui volum mare de date și informații pe o perioadă lungă de timp și obținerea de rapoarte și situații pe baza acestora;

d) dezvoltarea serviciilor G2G prin implementarea suportului necesar dezvoltării serviciilor electronice ce au la bază informaţii corespunzătoare cu privire la amenzile contravenționale;

e) asigurarea încasării amenzilor contravenționale;

 f) asigurarea evidenței analitice conforme privind calcularea și achitarea amenzilor aplicate în cadrul procesului contravențional, precum și urmăririi plenitudinii încasărilor efectuate și raportării acestora.

1. **Principiile de bază ale creării sistemului**

 SIA „RAC” se bazează pe principiile care guvernează procesul contravențional: a legalității, egalității în fața legii, dreptății, caracterului personal al răspunderii contravenționale, individualizării răspunderii contravenţionale şi sancţiunii contravenţionale, imparţialității, a confidenţialității, a relevanţei, a transparenţei, a colaborării la nivel naţional și internaţional, precum și pe următoarele principii specifice:

a) principiul legalităţii, care presupune crearea şi exploatarea sistemului informațional în conformitate cu legislaţia naţională în vigoare, a normelor şi standardelor internaţionale recunoscute în domeniu;

b) principiul datelor sigure, presupune introducerea datelor în sistem doar prin canale autorizate, autentificate și criptate;

c) principiul securităţii informaţionale, presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate şi eficienţă pentru protecţia datelor de pierderi, alterări, deteriorări şi de acces nesancţionat;

d) principiul accesibilităţii informaţiei cu caracter public, care presupune implementarea procedurilor de asigurare a accesului solicitanţilor la informaţia cu caracter public furnizată de soluţia informatică;

e) principiul transparenţei, presupune proiectarea şi implementarea sistemului conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informaționale şi de telecomunicaţii;

f) principiul expansibilităţii, stipulează posibilitatea extinderii şi completării sistemului informațional cu noi funcţii sau îmbunătăţirea celor existente;

g) principiul integrării cu produsele de program existente, presupune posibilitatea soluției informatice de a se integra și interacționa cu aplicațiile, serviciile și bazele de date implementate în cadrul autorităților publice și instituțiilor din Republica Moldova;

h) principiul simplităţii şi comodităţii utilizării, presupune proiectarea şi realizarea tuturor aplicaţiilor, mijloacelor tehnice şi de program accesibile utilizatorilor sistemului, bazate pe principii exclusiv vizuale, ergonomice şi logice de concepţie;

i) principiul neutralitatii si adaptării tehnologice, presupune că sistemul trebuie să se orienteze pe cerințele funcționale, asigurând accesul la serviciul informatic public independent de tehnologii sau produse specifice;

j) principiul îmbinării publicităţii şi confidenţialităţii, prevede publicarea informaţiei general accesibile, cu excepţia informaţiei recunoscute ca fiind confidenţială, în modul stabilit de legislaţia naţională în vigoare;

k) principiul unităţii spaţiului informaţional, prevede utilizarea unui sistem unic de clasificatoare, formate de date, protocoale de interacţiune informaţională, standarde, documente normative şi metodice interdependente, condiţie care este necesară pentru formarea spaţiului informaţional unic al sistemului de prestare a serviciilor publice;

l) principiul protecţiei datelor cu caracter personal, prevede crearea şi exploatarea sistemului de evidenţă a serviciilor publice în conformitate cu acordurile şi convenţiile internaţionale, precum şi cu legislaţia naţională în vigoare în domeniul protecţiei datelor cu caracter personal;

m) principiul identificării unice, prevede faptul că toate obiectele informaţionale de evidenţă trebuie să aibă un număr unic de identificare;

n) principiul controlului, prevede controlul măsurilor ce asigură calitatea, fiabilitatea resurselor şi sistemelor informaţionale de stat, precum şi păstrarea şi utilizarea raţională a acestora.

1. **Sarcinile de bază realizate prin exploatarea sistemului**

 Prin exploatarea sistemului se soluţionează următoarele probleme de bază:

a) formarea resurselor informaţionale pentru susţinerea activității specifice de evidență a amenzilor contravenționale și a proceselor decizionale şi de conducere;

b) gestionarea procesului de bază, indicând expirarea termenelor legale și alte evenimente relevante în cazul amenzilor contravenționale;

c) generarea automată (pe bază de șabloane) a documentelor specifice procesului contravențional;

d) automatizarea colectării, stocării, procesării şi analizei datelor, a procesului de elaborare a rapoartelor analitice și statistice;

e) furnizarea informației analitice și statistice privind amenzile contravenționale în adresa autorităților și instituțiilor publice ale Republicii Moldova;

f) asigurarea accesului online la informația cu privire la amenzile contravenționale aplicate și achitate/neachitate;

g) reducerea timpului necesar pentru examinarea informației cu privire la amenzile contravenționale;

i) realizarea unui mecanism eficient de colaborare între autoritățile competente să soluționeze cauzele contravenționale;

j) asigurarea controlului accesului la date și asigurarea unei securități și confidențialități maxime a datelor colectate privind utilizatorii;

k) asigurarea informațională a activității de analiză, prognozare și cercetare științifică în domeniu;

l) colectarea, înregistrarea, prelucrarea, păstrarea şi actualizarea informaţiei cu privire la amezile contravenționale;

m) asigurarea la nivel de stat a evidenţei unice centralizate a amenzilor contravenționale;

n) asigurarea cu informaţie operativă şi statistică conducerea ţării, ministerele, autorităţile publice interesate, precum şi agenţii constatatori;

o) asigurarea schimbuluui de informaţie cu privire la amenzile contravenționale;

p) supravegherea respectării disciplinei de înregistrare şi evidenţă a amenzilor contravenționale, precum şi contribuirea la elaborarea şi realizarea măsurilor de reacţionare oportună la tendinţele şi manifestările negative;

r) asigurarea funcţionării complexului tehnic de program şi a reţelelor informaţionale utilizate în cadrul Sistemului.

**Capitolul II. Spațiul juridico-normativ al funcționării sistemului**

 **9. Cadrul juridico-normativ de activitate a sistemului**

 SIA „RAC” se conformează legilor şi reglementărilor din sfera dezvoltării sistemelor informatice şi a ciclului de viaţă al produselor software. În mod special, procesul care ghidează elaborarea concepţiilor este definit de reglementarea tehnică „Procesele ciclului de viaţă al software-ului” RT 38370656-002:2006, aprobată prin ordinul ministrului devoltării informaționale nr. 78 din 1 iunie 2006.

 Deciziile şi spaţiul soluţiilor disponibile rezultă din actele normative conexe ale Republicii Moldova, precum şi din standardele şi practicile internaţionale în domeniu.

1. **Spațiul juridico-normativ al SIA „RAC” include:**
2. Codul contravențional nr. 218-XVI din 24.10.2008 (Republicat: Monitorul Oficial al Republicii Moldova, 2017, nr.78-84, art.100);
3. Legea nr. 1069-XIV din 22 iunie 2000 cu privire la informatică (Monitorul Oficial al Republicii Moldova, 2001, nr. 73-74, art. 547);
4. Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44);
5. Legea nr. 71-XVI din 22 martie 2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314);
6. Legea nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2011, nr. 170-175, art. 492);
7. Legea nr. 91 din 29 mai 2014 privind semnătura electronică şi documentul electronic (Monitorul Oficial al Republicii Moldova, 2014, nr. 174-177, art. 397);
8. Hotărârea Guvernului nr. 735 din 11 iunie 2002 cu privire la sistemele speciale de telecomunicații ale Republicii Moldova (Monitorul Oficial al Republicii Moldova, 2002, nr. 79-81, art. 833);
9. Hotărârea Guvernului nr. 840 din 26 iulie 2004 cu privire la crearea Sistemului de telecomunicații al autorităților administrației publice (Monitorul Oficial al Republicii Moldova, 2004, nr. 130, art. 1013);
10. Hotărârea Guvernului nr. 1140 din 20.12.2017 pentru aprobarea Regulamentului privind activitatea prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice (Monitorul Oficial al Republicii Moldova, 2017, nr. 451-463 art. 1268);
11. Hotărârea Guvernului nr. 1123 din 14 decembrie 2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal (Monitorul Oficial al Republicii Moldova, 2010, nr. 254-256, art. 1282);
12. Hotărârea Guvernului nr. 710 din 20 septembrie 2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare) (Monitorul Oficial al Republicii Moldova, 2011, nr. 156-159, art. 780);
13. Hotărârea Guvernului nr. 656 din 5 septembrie 2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate (MConnect) (Monitorul Oficial al Republicii Moldova, 2012, nr. 186-189, art.708);
14. Ordinul ministrului dezvoltării informaționale nr. 94 din 17 septembrie 2009 cu privire la aprobarea unor reglementări tehnice (Monitorul Oficial al Republicii Moldova, 2010, nr. 58-60, art. 232);
15. Standardul Republicii Moldova SMV ISO CEI 15288:2009, „Ingineria sistemelor şi software-ului. Procesele ciclului de viaţă al sistemului”;
16. alte acte normative și standarde în vigoare în domeniul tehnologiei informației și comunicațiilor.

**Capitolul III. Spațiul funcțional al sistemului**

1. **Funcțiile standard ale sistemului**

 Funcționalitățile standard ale sistemului sunt:

1) Formarea repozitorului de date (baza de date) necesare pentru susținerea activității autorităților publice – funcții de introducere a datelor, modificări și/sau ștergeri, arhivare ale acestora;

2) Organizarea accesului la date. Datele conţinute în stocul de date a SIA „RAC” sunt puse la dispoziţia autorităților publice, persoanelor fizice şi juridice, şi pentru organizarea procesului de schimb informaţional. Fiecare utilizator de date ale sistemului urmează să utilizeze aceste date numai în scopuri legale în conformitate cu drepturile utilizatorului;

3) Interoperabilitatea. Sistemul asigură schimbul electronic de informații, prin intermediul platformei MConnect, cu toate Registrele de stat cu care autoritățile publice interacționează.

4) Administrarea sistemului. Aplicația informatică oferă facilități de:

a) administrarea rolurilor şi drepturilor utilizatorilor;

b) administrarea nomenclatoarelor;

c) administrarea modelelor de documente;

d) administrarea sumelor care urmează să fie încasate;

e) administrarea termenelor corespunzătoare diferitelor etape ale procesului contravențional și a procesului de executare a amenzilor contravenționale;

5) Arhivarea datelor și documentelor. Arhivarea datelor constă în scoaterea obiectului informațional din evidență și transferarea datelor despre acesta în arhivă prin efectuarea unei înscrieri speciale în baza de date, conform politicii de arhivare corespunzătoare a amenzilor contravenționale și a documentelor aferente.

6) Auditul utilizatorilor. Sistemul informatic conține un mecanism propriu de jurnalizare a tuturor evenimentelor de business aferente utilizării sale. Orice acțiune a utilizatorilor se documentează în registre electronice speciale, arătând momentul de timp și utilizatorul care a efectuat acțiunea. Pentru fiecare acțiune a utilizatorului se salvează în evenimentul jurnalizat datele care au fost modificate. Adițional, sistemul informatic dispune de un instrument eficient care oferă posibilitatea de a efectua o analiză a comportamentului utilizatorilor sau a productivității lor. Sistemul informatic jurnalizează în paralel prin intermediul serviciului guvernamental MLog evenimentele de business critice. Toate acțiunile care sunt jurnalizate în paralel prin intermediul MLog pot fi configurate în opțiunile de administrare.

7) Securitate și confidențialitate. SIA „RAC” trebuie să respecte următoarele prevederi în materie de securitate și confidențialitate:

a) să permită protejarea datelor depozitate sau în tranzit de către entităţile cărora nu le sunt adresate, prin mecanisme adecvate de securitate;

b) să asigure integritatea informaţiilor şi autenticitatea părţilor prin mecanisme adecvate de certificare electronică, respectiv aplicarea tehnologiei TLS/SSL. (Interacțiunea SIA „RAC” cu serviciile de platformă disponibile, precum MPass și MSign, oferite de Centrul de telecomunicații speciale va permite utilizarea semnăturii electronice);

c) generarea documentelor, în baza schimbului de date și a datelor noi;

d) să permită auditarea activităţilor efectuate în sistem, atât a utilizatorilor simpli, cât şi a utilizatorilor privilegiaţi;

e) să aplice politici corespunzătoare de securitate la nivelul serviciilor web.

1. **Funcții specifice ale sistemului**

 SIA „RAC” trebuie să asigure realizarea următoarelor funcţii specifice determinate de destinaţia sistemului şi grupate în următoarele contururi funcţionale:

1) Evidența amenzilor contravenționale aplicate. Toate documentele/informațiile aferente amenzii contravenționale aplicate sunt înregistrate în sistem. O parte din acestea parvin în cadrul schimbului de informații cu alte registre în format electronic, iar pentru acele documente venite în format hârtie, li se atașează atribute proprii (metadate) și sunt scanate. Documentele electronice scanate se atașează dosarului electronic, în spațiul de lucru corespunzător și se stochează în sistem. Pentru documentele create în sistem, utilizatorii au posibilitatea să aleagă șablonul corespunzător etapei procedurii.

2) Evidența sumelor amenzilor contravenționale achitate și neachitate. Se va ține evidența sumelor amenzilor contravenționale care au fost sau nu achitate. Se va asigura integrarea cu platforma MPay sau alte metode de plată pentru perceperea amenzilor, iar sistemul oferă informații referitoare la modul de îndeplinire a obligației de plată.

3) Evidența contravenienților. Înregistrarea, gestionarea și managementul participanților la procesul contravențional și a informației aferente fiecărui participant.

4) Evidența termenelor. Fiecare etapă a fluxurilor informaționale definite de sistem are termene de executare corespunzătoare. Aplicația trebuie să asocieze aceste termene dosarului electronic (în funcție de specificul acestuia) și să alerteze utilizatorii de apropierea și/sau depășirea termenelor. Totodată, aceste termene vor sta la baza remiterii către executorul judecătoresc a documentelor executorii ce vizează amenzi contravenționale neachitate în mod benevol.

5) Evidența acțiunilor de executare. Sistemul permite evidența acțiunilor de executare în cazul neachitării amenzilor contravenționale. Acestea se identifică unic și fac parte integrantă din procesul de executare a amenzilor contravenționale. Sistemul dă posibilitatea monitorizării termenelor de îndeplinire a actelor de executare în cadrul procedurii de executare a amenzilor contravenționale inclusiv prin primirea unor alerte personalizate în aplicație.

5) Evidența costurilor de executare. Costurile de executare se compun din sumele pasibile să fie achitate executorului judecătoresc în cazul în care amenzile nu vor fi achitate benevol și documentul executoriu va fi remis spre executare executorului judecătoresc (taxele, spezele procedurii de executare,onorariul executorului judecătoresc).

6) Implementarea fluxurilor de lucru și a mecanismelor de control privind executarea lor. Procesul de evidență a amenzilor contravenționale urmează să fie împărțită în pași, cu oferirea opțiunilor necesare etapei de lucru. Sistemul monitorizează etapa/situația la care se află amenda contravențională (achitat/neachitat) și oferă utilizatorului un număr restrâns de acte ce pot fi întocmite în această etapă. Fiecare etapă are o serie de atribute: acte posibile de întocmit, timp de executare. În implementarea fiecărui flux de proces de lucru se ţine cont de existenţa unor matrici RACI (Responsible, Accountable, Consulted, Informed – Responsabil, Răspunzător, Consultat, Informat) prin care se descriu rolurile şi responsabilităţile diverselor echipe sau persoane în derularea unui proces funcţional.

7) Furnizarea informațiilor depersonalizate pentru consultări on-line. Accesul va fi permis pe o bază de date tampon (Data HUB) unde sunt înregistrate documente depersonalizate. Datele de interes public (datele statistice, rapoartele KPI) se fac publice pe Portalul Datelor Deschise.

8) Generarea datelor statistice. Sistemul are un modul care permite realizarea de rapoarte analitice sau statistice, în funcție de rolul și responsabilitățile fiecărui utilizator.

1. **Contururile funcționale ale sistemului**

 Funcţiile specifice ale sistemului, determinate de destinaţia acestuia, sunt grupate în următoarele contururi funcţionale (module ale aplicației):

a) evidența amenzilor contravenționale aplicate;

b) evidența amenzilor contravenționale achitate/neachitate;

c) evidența contravenienților;

d) evidența și gestionarea acțiunilor de executare;

e) evidența cheltuielilor de executare și a plăților aferente;

f) evidența și gestionarea fluxurilor de lucru corespunzătoare procesului;

g) schimb de date și informații (interoperabilitate) cu ale sisteme informaționale ale statului;

h) acces on-line la dosar;

i) gestionarea și raportarea datelor statistice;

j) generarea documentelor;

k) administrarea sistemului.

 Fiecare din modulele date oferă un set clar de instrumente necesare în activitatea fiecărui tip de utilizator.

1. **Interacțiunea sistemului cu alte sisteme informatice**

SIA „RAC” asigură un sistem unitar de acces la datele privind amenzile contravenționale atât organelor care au aplicat amenda contravențională, cât şi a persoanelor (SFS, executorii judecătorești) care validează/notifică producerea unui eveniment care are impact asupra activităţilor de emitere și a procedurii ulterioare de executare.

 **15.** SIA „RAC” interacţionează cu sisteme informatice de stat, suport general pentru sistemele informatice dezvoltate de autoritățile și instituțiile publice, precum:

a) Autorităţi de certificare (Centrul de Telecomunicații Speciale, Serviciul Fiscal de Stat şi Agenția Servicii Publice) ce eliberează certificate electronice şi identifică utilizatorii şi sistemele ca părţi ale diferitor domenii;

b) MConnect - pentru schimbul de date între SIA „RAC” și sistemele informatice ale autorităților publice și prestatorilor de servicii;

c) MPass - pentru autentificare și autorizare pe bază de roluri;

d) MSign - pentru a permite semnarea electronică a deciziilor și pentru a valida semnăturile;

e) MPay - pentru gestionarea plăților efectuate;

f) MLog – pentru a asigura jurnalizarea, auditul și evidența evenimentelor, în contextul utilizării sistemelor informaţionale.

 **16.** Informația cu privire la amenzile contravenționale și documentele aferente acestora sunt generate de sistem prin intermediul a două canale:

a) Prin MConnect în cadrul schimbului de informații cu instituțiile ce au sisteme informatice conectate la platforma națională;

b) Prin transmiterea la Serviciul Fiscal de Stat;

 **17.** Pentru a prelua informaţii, date relevante, SIA „RAC” interacţionează cu resursele informaţionale administrative prin accesarea bazelor de date (registrelor) deţinute de instituţiile respective, utilizând serviciile WEB furnizate de acestea prin intermediul platformei de interoperabilitate platforma tehnologică MConnect.

 Pentru comunicarea între nivelurile sistemului se utilizează sistemul reţelelor de comunicaţii electronice administrate de Centrul de Telecomunicații Speciale, iar schimbul electronic de date se realizează prin utilizarea serviciilor web.

 **18.** Conexiunea la sistemul unic de prelucrare a informației se efectuează prin canale securizate, utilizatorii fiind grupaţi după entitatea pe care o reprezintă şi rolul pe care îl vor avea în sistem.

 Executorii judecătorești accesează SIA „RAC”, prin intermediul rețelei web, utilizând mijloacele de securizare a legăturii cu SIA „RAC”. Autentificarea în sistem se face utilizând semnăturile electronice prin intermediul platformei MSign.

 Baza de date SIA „RAC” furnizează informaţii autorităţilor publice, persoanelor juridice şi fizice în baza contractelor sau acordurilor respective, încheiate de părţi. Părțile interesate pot avea acces on-line la dosarul electronic, cu păstrarea cerințelor de securitate și confidențialitate a datelor cu caracter personal, pe baza de cerere adresată administratorului de sistem.

 În scopul asigurării securității și protecției datelor cu caracter personal, sistemul are prevăzută o bază de date tampon (BD consultare) unde sunt transferate datele ce fac obiectul consultării electronice. Aceste date sunt prelucrate în vederea depersonalizării lor.

**Capitolul IV. Spațiul organizațional al sistemului**

1. **Cadrul organizațional**

Proprietarul SIA „RAC” este statul, care îşi realizează dreptul de proprietate, de gestionare şi utilizare a datelor din sistemul informaţional.

 Posesorul SIA „RAC” este Serviciul Fiscal de Sat cu drept de gestionare a registrului şi utilizare a datelor din registru şi a resurselor, precum și asigură crearea și exploatarea acestui sistem.

 Administratorul SIA „RAC” este persoana cu un rol tehnic (desemnată de Posesor) cu drepturi administrative în sistem, abilitată să gestioneze alte entităţi, să acorde drepturi de acces altor utilizatori, să exercite alte atribuții la nivel tehnic.

 Utilizatorii SIA „RAC” sunt:

a) autoritățile competente să soluționeze cauzele contravenționale;

b) Serviciul Fiscal de Stat;

c) executorii judecătorești;

d)) persoanele angajate în cadrul birourilor executorilor judecătorești;

e) alte persoane cointeresate în obținerea datelor statistice din SIA „RAC”.

**20. Furnizorii de date**

Principalii furnizori de date pentru SIA „RAC” sunt :

a) Programul Integrat de Gestionare a Dosarelor (PIGD), un sistem multifuncțional de gestionare a dosarelor instalat și utilizat în fiecare instanță din Republica Moldova;

b) Registrul de stat a unităților de drept;

c) Sistemul informatic integrat „e-Rețineri”;

d) Registrul garanțiilor reale mobiliare;

e) Registrul de stat al persoanelor autorizate;

f) Registrul de stat al populației;

g) Registrul de stat al transportului auto;

h) Sistemul informațional Integrat al Poliției de Frontieră;

i) Registrul de stat al armelor;

j) Registrul bunurilor imobile.

 **21.** Informația furnizată de fiecare registru este prezentată în tabelul de mai jos.

|  |  |  |
| --- | --- | --- |
| **Instituția deținătoare** | **Registrul de stat** | **Tipul de informații** |
| Agenția Serviciilor Publice | Registrul de stat al populației | **Persoane fizice** (inclusiv cetăţeni străini, cu domiciliul în Republica Moldova):* numărul de identificare de stat - IDNP
* nume
* prenumele
* patronimicul
* data naşterii
* numărul, seria, valabilitatea documentului de identificare al persoanei
* imaginea grafică
 |
| Agenția Serviciilor Publice | Registrul de stat al transporturilor | **Unitatea de transport:*** caracteristicile tehnice ale autovehiculului (tipul UT, marca/modelul, culoarea, numărul de stat de înregistrare)
* datele agregatelor (numărul caroseriei, motorului, şasiului, codul VIN)
* numărul şi seria documentului de înmatriculare, posesorul
 |
| Agenția Serviciilor Publice | Registrul bunurilor imobile | **Bunuri imobile:*** numărul cadastral (numărul cadastral convenţional)
* modul de folosinţă al bunului imobil
* locul amplasării sau adresa bunului imobil
* numele şi prenumele proprietarului, data, luna şi anul naşterii, în cazul persoanei fizice (se indică toţi coproprietarii bunului imobil)
* denumirea de firmă, în cazul persoanei juridice
* numărul de identificare al persoanei fizice sau numărul şi data eliberării certificatului înregistrării de stat a persoanei juridice
* domiciliul persoanei fizice sau sediul persoanei juridice
* cota de proprietate în bunul imobil, în. cazul dreptului de proprietate comună în diviziune
* documentele ce confirmă drepturile în a căror bază a fost înscris dreptul de proprietate
* data naşterii dreptului de proprietate
* înscrieri referitoare la alte drepturi reale: superficia, uzufructul, uzul, abitația, servitutea ce grevează imobilul, ipoteca, folosinţa, concesiunea, gestiunea (administrarea) economică
* înscrieri referitoare la drepturile de creanţă, faptele sau raporturile juridice aferente bunurilor imobile
* tipul dreptului care grevează dreptul de proprietate şi/sau alt drept patrimonial asupra bunului imobil
* termenul pentru care a fost stabilită grevarea, în cazul în care acest termen a fost stabilit
* suma obligaţiei asigurată prin gaj/ipotecă
* date despre persoana în a cărei favoare a fost stabilită grevarea
* denumirea, numărul şi data eliberării [documentelor ce](http://documentelor.ee) confirmă drepturile în a căror bază a fost efectuată înregistrarea.
 |
| Agenția Serviciilor Publice | Registrul de stat a unităților de drept | **Unități de drept:*** numărul de identificare de stat al unității de drept -IDNO
* datele de identificare
* categoria unităţii de drept
* denumirea
* datele privind structura organizațional-juridică: tipul proprietăţii; forma organizaţional-juridică; finanţare bugetară/autogestiune
* datele privind crearea, reorganizarea şi lichidarea
* data, locul şi motivul creării, reorganizării sau lichidării; registratorul
* datele despre fondatori (numărul de identificare - IDNP (pentru persoanele fizice) sau IDNO (pentru unităţile de drept)
 |
| Ministerul Justiției | Registrul garanțiilor reale mobiliare | **Date despre gaj:*** obligaţia garantată cu gaj (temeiul obligației, valoarea acesteia și scadența obligației), tipul gajului
* avizul de înregistrare, modificare, executare sau de radiere a gajului
* contractul de gaj
 |
| Departamentul Instituțiilor Penitenciare | Registrul persoanelor reținute, arestate și condamnate | **Date privind persoane condamnate:*** datele generale despre condamnat
* instituția penitenciară în care se deține
 |
| Serviciul Fiscal de Stat | Registrul Fiscal de Stat | **Date privind informații fiscale:*** subdiviziunile agentului economic și adresele acestora, conturile bancare
* informație referitoare la amenzile  achitate, inclusiv amenzile și sancțiunile contravenționale calculate  și încasate  la BPN și administrate de Serviciul Fiscal de Stat
* locul de muncă curent al debitorului
 |

**Capitolul V. Documentele sistemului**

**22.** SIA „RAC” formează un dosar electronic pentru fiecare cauză contravențională care conţine formulare electronice perfectate, copii scanate ale documentelor colectate. Fiecare document inserat dispune de un set de metadate necesare identificării, clasificării și procesării automatizate.

**23.** Documentele de bază ale sistemului se clasifică, în funcție de faza procesului de executare, după cum urmează:

a) documente de intrare;

b) documente utilizate în procedura de lucru;

c) documente de ieșire;

d) documente tehnologice.

**24. Documentele de intrare**

Sunt considerate documente de intrare:

a) procesul-verbal cu privire la contravenție;

b) decizia asupra cauzei contravenționale;

c) fișa contravenției constatate;

d) fișa cu privire la derularea cauzei contravenționale;

**25.** **Documentele utilizate în procedura de lucru**

 O serie de documente se atașează la dosarul cauzei contravenționale, pe parcursul derulării activităților specifice și sunt, de regulă, documente primite de la terți sau documente elaborate de funcționarul SFS ca rezultat al efectuării actelor de procedură. Aceste documente sunt de tipul:

1) Documente primite de la terți:

a) rezultatul interogării diferitelor registre ale statului;

b) răspunsul la solicitări de informații transmise către autorități/instituții/persoane fizice sau juridice;

c) dovada plății amenzii.

2) Documente ce rezultă în cadrul efectuării actelor de procedură:

a) copii sau scanări ale unor acte;

b) declarații.

**26.** **Documentele de ieșire**

Documentele de ieșire sunt documentele produse de către funcționarul din cadrul SFS sau executorul judecătoresc și transmise către terți, ca rezultat al neachitării benevole a amenzii contravenționale.

 Acestea pot fi:

a) încheieri;

b) procese-verbale;

c) somații;

d) citații;

e) adrese către terți (autorități, instituții, părți);

f) cereri de informații;

g) notificări de încetare a procedurii de executare;

h) ordine incasso;

i) demersuri/interpelări;

j) borderouri;

k) comunicări către părți.

**27.** **Documentele tehnologice**

Pe lângă tipurile de documente menţionate anterior, sistemul include o serie de documente tehnologice:

1) semnăturile documentelor şi înregistrărilor semnate electronic;

2) certificatele electronice cu care au fost produse semnăturile electronice;

3) confirmările din partea sistemelor informatice ale autorităţilor publice sau angajaţilor acestora privind veridicitatea documentelor prezentate;

4) imaginile scanate ale documentelor;

5) lista utilizatorilor şi drepturilor acestora;

6) înregistrările de audit ale activităţii sistemului şi utilizatorilor;

7) versiunile documentelor şi istoricul modificărilor;

8) documentele tehnologice privind parametrii de sistem;

9) rapoartele şi statisticile agregate privind utilizarea sistemului.

 Sistemul poate genera următoarele rapoarte analitice și sintetice:

1) clasificarea și calcularea numărului cauzelor contravenționale, conform categoriilor;

2) indicatorul numeric al amenzilor contravenționale neachitate, inclusiv conform categoriilor (în perioada solicitată);

3) indicatorul numeric al documentelor executorii remise către executorul judecătoresc - numărul total și numărul documentelor executorii conform categoriilor (în perioada solicitată);

4) indicatorul numeric al documentelor executorii încheiate - numărul total și numărul documentelor executorii conform categoriilor (în perioada solicitată);

5) indicatorul numeric al documentelor executorii strămutate - numărul total și numărul documentelor executorii conform categoriilor (în perioada solicitată);

6) indicatorul numeric al documentelor executorii restituite (clasificarea conform motivului restituirii) - numărul total și numărul documentelor executorii conform categoriilor (în perioada solicitată);

7) numărul total al documentelor executorii suspendate (cu delimitarea suspendării: din oficiu sau de către instanța de judecată) - numărul total și numărul documentelor executorii conform categoriilor (în perioada solicitată);

8) informația privind sarcina lunară (în perioada solicitată) - individuală și medie; pe funcționar și pe SFS în general;

9) calcularea sumelor încasate în contextul fiecărei cauze contravenționale și a documentelor executorii încheiate/restituite/strămutate;

10) identificarea existenței amenzii contravenționale prin introducerea în motorul de căutare a contravenientului/numărului documentului executoriu și oferirea informației privind angajatul SFS sau a executorului judecătoresc care instrumentează cauza sau în arhiva căruia se află;

11) identificarea documentelor executorii conform sumei amenzii din acestea (cu formarea ad-hoc a filtrului), conform fiecărei categorii de dosare;

13) clasificarea documentelor executorii în funcție de emitent;

13) clasificarea documentelor executorii în contextul cărora au fost avansate/neavansate cheltuielile de către creditor;

14) clasificarea contravenienților juridic, conform categoriilor de dosare;

15) calcularea termenului de executare benevolă;

16) calcularea valorii medii a sumelor amenzilor contravenționale (calculate/achitate/neachitate);

17) obținerea informației privind numărul/tipul de măsuri întreprinse ;

18) restanța la începutul perioadei;

19) numărul de documente executorii restituite:

 a) conform cererii;

 b) din cauza anulării ulterioare a documentului executoriu;

 c) alte motive;

26) numărul de documente executorii suspendate;

28) termenul de executare a amenzii (zile, luni, ani).

**Capitolul VI. Spațiul informațional al sistemului**

1. **Obiectele informaționale**

 Totalitatea obiectelor informaționale este determinată de destinația SIA „RAC”, incluzând:

1) dosarul electronic al cauzei contravenționale, cu următoarele componente:

 a) proces-verbal cu privire la contravenție/decizie asupra cauzei contravenționale;

 b) somația de executare benevolă;

2) persoana fizică;

3) persoana juridică;

4) raport.

 Identificator al obiectului informațional „dosarul electronic al cauzei contravenționale” este constituit dintr-un număr de ordine unic și un cod de securitate unic, generate de sistem în momentul înregistrării cererii/solicitării.

 Identificator al obiectului informațional „persoana fizică” este numărul de identificare de stat al persoanei fizice (IDNP).

 Identificator al obiectului informațional „persoana juridică” este numărul de identificare de stat al persoanei juridice (IDNO).

 Identificator al obiectului informațional „raport” este constituit dintr-un număr de ordine unic, generat automat de sistem.

1. **Scenariile de bază**

 Scenariile de bază reprezintă o listă a evenimentelor aferente obiectului informaţional ale SIA „RAC”, după cum urmează:

1) cu privire la obiectul informațional „dosarul electronic al cauzei contravenționale”:

a) înregistrarea primară - în momentul înscrierii informației cu privire la amenda contravențională aplicată;

b) actualizarea și modificarea datelor - în cazul achitării amenzii contravenționale, anulării documentului prin care a fost aplicată;

c) scoaterea de la evidență a datelor - în momentul stingerii sumei;

2) cu privire la obiectul informațional „persoana fizică”:

a) înregistrarea primară - în momentul înscrierii informației cu privire la amenda contravențională aplicată;;

b) actualizarea și modificarea datelor - la modificarea datelor înregistrate despre persoana fizică;

3) cu privire la obiectul informațional „persoana juridică”:

a) înregistrarea primară - înscrierii informației cu privire la amenda contravențională aplicată;

b) actualizarea și modificarea datelor - la modificarea datelor înregistrate despre persoana juridică sau în cazul reorganizării persoanei juridice;

4) cu privire la obiectul informațional „raport”, scenariul de bază este:

a) înregistrarea primară - în momentul adresării de a genera un raport (operativ, statistic, de sistem).

1. **Datele sistemului**

 Datele SIA „RAC” reprezintă totalitatea atributelor obiectelor informaționale, după cum urmează:

1) atributele (caracteristicile) obiectului informațional „persoană fizică”:

a) număr de identificare de stat (IDNP);

b) nume;

c) prenume;

d) data naşterii;

e) numărul de identificare de stat;

f) seria și numărul actului de identitate;

g) oficiul și data eliberării actului de identitate;

h) adresa poștală și, opțional, cea electronică a persoanei fizice;

2) atributele (caracteristicile) obiectului informațional „persoana juridică”:

a) denumirea;

b) numărul de identificare de stat (IDNO);

c) adresa poștală și, opțional, cea electronică a persoanei juridice sau a întreprinzătorului individual;

3) atributele (caracteristicile) obiectului informațional „dosarul electronic al cauzei contravenționale”:

a) număr unic de identificare;

b) denumirea și descrierea dosarului;

c) tipul acțiunii întreprinse;

d) termen de executare a documentului/sistem de alertă;

e) termen limită de păstrare/ de valabilitate;

f) acte de confirmare cu privire la dosar;

g) date de identificare;

h) altă informaţie conform legislației în vigoare.

**31. Clasificatoarele (nomenclatoarele) sistemului**

În scopul asigurării veridicității și reducerii volumului informației stocate în SIA „RAC”, precum şi al clasificării corecte a obiectelor sistemului, se utilizează următoarele nomenclatoare:

1) Locale (proprii sistemului):

a) nomenclatorul stărilor dosarelor cauzei contravenționale;

b) nomenclatorul documentelor executorii;

c) nomenclatorul stărilor documentelor;

d) nomenclatorul tipurilor de documente;

e) nomenclatorul tipurilor de obiecte (acțiuni) ale executării;

f) nomenclatorul birourilor executorilor judecătorești;

g) nomenclatorul perioadelor de raportare;

h) alte nomenclatoare și clasificatoare relevante;

2) Naționale:

a) CUATM - nomenclatorul unităţilor administrativ-teritoriale ale Republicii Moldova;

b) CFOJ - nomenclatorul formelor organizatorico-juridice;

c) CAEM - nomenclatorul activităţilor din economia Moldovei;

d) CFP - nomenclatorul formelor de proprietate;

3) Internaționale:

a) CS - nomenclatorul statelor;

b) CV- nomenclatorul valutelor.

1. **Fluxurile informaționale**

 În derularea activității specifice, Serviciul Fiscal de Stat interacționează cu o serie de persoane, instituții, autorități, conturându-se astfel o serie de fluxuri informaționale.

**Capitolul VII. Spațiul tehnologic al sistemului**

 **33.** Spaţiul tehnologic al SIA „RAC” reprezintă un complex informaţional de telecomunicaţii centralizat. Toate datele se depozitează într-un stoc de date centralizat.

 Prezenţa componentelor produselor software şi mijloacelor tehnologice în complexul informaţional de telecomunicaţii este stabilită la etapa elaborării sarcinii tehnice şi proiectului tehnic.

1. **Platforma tehnologică**

 Platforma tehnologică utilizează standarde deschise şi este compatibilă cu serverele care respectă specificaţiile non-proprietare și cu standardele existente.

 Pentru schimbul de date cu alte sisteme se solicită utilizarea de standarde deschise.

 Sistemul expune o interfaţă bazată pe servicii web prin care aplicaţiile instituţiilor pot transmite informaţie folosind un canal de comunicare de tip sistem la sistem.

**35.** Platformă tehnologică trebuie:

a) să optimizeze soluțiile gata de utilizat (COTS), atunci când acestea satisfac cerințele funcționale esențiale și utilizează capabilitățile esențiale de integrare a informațiilor, de management al documentelor și înregistrărilor, de fluxuri de lucru și reguli funcționale și de management al datelor cât mai mult posibil. Totodată, trebuie să minimizeze dezvoltarea customizată;

b) să se bazeze pe standarde comune în domeniile care pot fi aplicate în cadrul Serviciului Fiscal de Stat;

c) să fie o arhitectura orientată pe servicii - SOA. O astfel de abordare trebuie să faciliteze satisfacerea necesităților funcționale, fiind mai ușor de administrat cu un număr limitat de personal IT;

d) aplicațiile și infrastructura software trebuie să se bazeze pe licențe perpetue pentru toate produsele software incluse în sistem și să asigure suportul de la producători;

e) să fie conform cu standardele care promovează interoperabilitatea pentru date, aplicații și tehnologie;

f) să fie astfel conceput încât sistemele IT să fie operaționale în cazul unor perturbări (defecțiuni hardware, coruperi de date) sau să permită extensii ulterioare pentru un centru alternativ folosit în cazul unor dezastre naturale;

g) să asigure că datele confidențiale sunt protejate corespunzător, iar accesul la informațiile din sistemul de producție să fie limitat conform unei matrice de drepturi în funcție de roluri și să fie monitorizat astfel încât să prevină divulgarea sau utilizarea neautorizată a datelor din sistem.

 **36.** Sistemul informațional trebuie să ofere următoarele funcționalități generale:

a) partajarea eficientă a informaţiei în cadrul Serviciului Fiscal de Stat;

b) crearea de fluxuri de proces automatizate suportate de aplicaţii;

c) oferirea unui suport de decizie la nivelul Serviciului Fiscal de Stat;

d) accesul „online”, pe bază de servicii web, la informațiile utile angajaților și clienților;

e) flexibilitate în a suporta diversele obiective ale evidenței amenzilor contravenționale;

f) integrabilitate şi deschidere;

g) suport tehnologic sigur şi scalabil;

h) administrarea identității utilizatorilor şi controlul accesului la toate resursele sistemului;

i) asigurarea unei disponibilități ridicate (24 ore x 7 zile ) a aplicaţiilor;

j) administrarea şi operarea la costuri reduse a infrastructurii şi componentelor soluţiei.

 **37.** Sistemul informațional trebuie să implementeze următoarele caracteristici generice:

a) principiile standard ale industriei de profil pentru utilizarea prietenoasă;

b) facilități de securitate și administrare de sistem;

c) facilități de management al datelor (informațiilor), cu atribute de protecție corespunzătoare;

d) Sistem coerent de indicatori de performanță.

 **38.** În calitate de platformă tehnologică, SIA „RAC” este găzduit pe Platforma Tehnologică Guvernamentală Comună M-Cloud.

 M-Cloud funcționează în baza tehnologiei de „cloud computing”, care este reprezentată schematic în figura de mai jos.

 

 Tehnologia „cloud computing” („nor informațional”) reprezintă un model de furnizare a serviciilor IT care permite accesul, la cerere, pe bază de reţea, la totalitatea configurabilă a resurselor de calcul virtualizabile (de exemplu reţele, servere, echipamente de stocare, aplicaţii şi servicii) și care pot fi puse rapid la dispoziţie cu un efort minim de administrare sau interacţiune cu furnizorul acestor servicii.

 M-Cloud urmează să satisfacă următoarele cerinţe:

a) posibilitatea stocării unor volume mari de informaţie;

b) posibilitatea extinderii funcţionale şi a puterii de calcul (extensibilitate şi scalabilitate);

c) asigurarea unei fiabilități înalte.

1. **Standardele tehnologice**

 Tipurile principale de standarde utilizate sunt:

a) standardele datelor;

b) standardul metadatelor (ISO 11179);

c) standardele schimburilor de informaţii;

d) standardele căutării informaţiilor;

e) standardele de calitate;

f) standardele de securitate;

g) standardele de multilingvism.

 **40.** Conformitatea cu aceste standarde constă în:

a) susţinerea interfeţei browserului public pentru accesare;

b) XML ca mijloc principal pentru integrarea datelor;

c) utilizarea standardelor Internet şi WWW - HTML, TCP/IP, SMTP;

d) utilizarea standardelor naţionale şi internaţionale privind calitatea şi securitatea.

**Capitolul VIII. Asigurarea securității informației**

 **41.** Sistemul complex al securităţii informaţionale reprezintă totalitatea măsurilor legislative, organizatorice şi economice, precum şi a mijloacelor software-hardware, care sunt orientate spre asigurarea unui nivel necesar al integrităţii, confidenţialităţii şi accesibilităţii resurselor informaţionale ale SIA „RAC” pentru minimalizarea prejudiciilor care ar putea fi suportate de utilizator şi proprietar.

 **42.** Pentru asigurarea îndeplinirii cerinţelor de securitate legate de constrângerile privind lucrul cu date cu caracter personal, vor fi respectate următoarele reguli aferente SIA „RAC”:

1) Înregistrarea și accesul utilizatorilor - sistemul este capabil de a determina univoc dacă utilizatorul este cel care pretinde că este. Procesul de înregistrare cuprinde informații relevante privind utilizatorul: nume utilizator, parola și/sau certificatul și drepturile pe care le deține în sistem. Sunt prevăzute reguli parametrizate privind politica de securitate, precum complexitatea parolei, perioada de valabilitate, număr de încercări eșuate, informații privind datele în care sistemul a fost accesat.

2) Autentificare⁄ identificare - utilizatorii care accesează informațiile și funcționalitățile sistemului sunt autentificați înainte de a li se permite accesul.

3) Autorizare bazată pe roluri - sistemul restricționează drepturile de acces ale utilizatorului la funcționalitățile sistemului pe baza rolului desemnat acestuia. Fiecare utilizator are asociat unul sau mai multe roluri. Fiecare rol are asociat un set de drepturi. Drepturile reprezintă prerogativele acordate unui utilizator de a efectua anumite activități în cadrul unui sistem informatic. Sistemul poate limita sau permite accesul unui utilizator la anumite date și funcționalități pe baza apartenenței la un rol.

4) Control acces (autorizare) - sistemul include mecanisme de prevenire a utilizării neautorizate sau de manieră neautorizată a resurselor. Fiecărui utilizator autorizat i se asociază o autorizare. Controlul accesului constă în restricționarea capacității unui subiect de a folosi un sistem sau un obiect în acel sistem, precum și jurnalizarea activităților efectuate.

5) Auditare - activitățile derulate în sistem sunt înregistrate, fiind posibilă auditarea ulterioară. Sistemul trebuie să aibă capacitatea de a înregistra toate tranzacțiile și incidentele din sistem, fiind posibilă analiza acestor înregistrări în scopul identificării modului de funcționare al sistemului și activităților derulate de utilizatori.

6) Integritatea datelor - datele stocate și procesate în sistem urmează a fi corecte și complete. Sistemul permite implementarea unor mecanisme care să verifice și să valideze datele din punctul de vedere al corectitudinii și completitudinii.

7) Administrare (configurare) - sistemul permite aplicarea politicilor de securitate încorporate în arhitectura și funcționalitățile lui. Definirea utilizatorilor și grupurilor sau rolurilor, precum și atribuirea de drepturi se realizează de către utilizatori cu drepturi de administrator. Sistemul permite delegarea administrării drepturilor complet sau limitat la anumite operații (de exemplu, adăugare utilizator, schimbare parola) către alți utilizatori dintr-o organizație. Sistemul oferă posibilitatea ca administratorul să poată configura restricții legate de adresele de IP sau domeniile de la care conectarea va fi permisă, pentru fiecare utilizator/grupuri de utilizatori în parte.

8) Securitatea împotriva accesului neautorizat - sistemul informatic este protejat împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le stochează. Sistemul include următoarele facilități: controlul accesului utilizatorilor la sistemele de aplicații și fișierele de date; ierarhizarea în clase a utilizatorilor finali; facilități de administrare parole; permiterea accesului direct la bazele de date numai administratorilor de baze de date autorizați; asigurarea securității tuturor interfețelor sistemului informatic, prevenind accesul utilizatorilor neautorizați la sistem; raportarea pe baze periodice a detaliilor privitoare la accesul în sistem al utilizatorilor.

9) Integritate - asigurarea protecţiei, exactităţii şi completitudinii datelor şi a soluţiilor furnizate pentru stocarea şi gestionarea acestora, dar şi asigurarea împotriva manipulării frauduloase a datelor/informaţiilor. Protecţia împotriva dezastrelor este realizată prin crearea copiilor de rezervă incrementale şi depline. SIA „RAC” este găzduită pe infrastructura hardware şi software guvernamentală M-Cloud, care nu permite coruperea datelor sistemului.

10) Disponibilitate - sistemul asigură un proces de redundanţă pentru a asigura utilizatorii de eventualele defecţiuni care pot surveni în timpul funcţionării precum şi asigurarea datelor, componentelor funcţionale şi serviciilor asociate către utilizatorii autorizaţi la momentul solicitării.

 **43.** Asigurarea securităţii informaţiei se realizează de Agenția Resurse Informaționale Juridice în conformitate cu cerinţele standardelor internaţionale SM ISO/CEI 15408-1:2014, SM ISO/CEI 15408-2:2014, SM ISO/CEI 15408-3:2014, SM SR ISO/CEI 27001:2016, SM ISO/CEI 27002:2014 şi subliniază faptul că SIA „RAC” este un produs hard&soft, care corespunde în totalitate cerinţelor utilizatorilor, inclusiv şi în ceea ce priveşte securitatea informaţională.

 **44.** Pentru gestiunea riscurilor de securitate va fi implementată o politică generală de securitate. Angajații Serviciului Fiscal de Stat urmează a fi instruiți în ceea ce priveşte riscurile de securitate la care pot fi expuşi. Politica de securitate va include prevederi referitoare la organizarea auditurilor periodice de securitate pentru a verifica politica şi conformitatea cu regulile de securitate, precum şi a stabili domeniile care necesită îmbunătăţiri.

 **45.** Procesul de gestionare a securităţii informaţionale trebuie să corespundă următoarelor cerinţe:

a) să asigure confidenţialitatea informaţiei importante;

b) să asigure integritatea informaţiei şi a proceselor legate de aceasta (crearea, introducerea, extragerea, păstrarea, transmiterea);

c) să asigure accesibilitatea la timp a informaţiei;

d) să asigure funcţionarea fără deficienţe în procesul realizării unor operaţii concrete;

e) să asigure monitorizarea în vederea asigurării capacităţii proceselor IT de a fixa orice activitate a utilizatorilor sau a proceselor;

f) să ţină evidenţa tuturor proceselor şi evenimentelor legate de informaţie.

 **46.** Pentru asigurarea securității sistemului sunt implementate următoarele măsuri:

a) Separarea drepturilor de acces la date. Asigurarea controlului centralizat al tuturor aspectelor legate de securitate (autentificare, autorizare, auditare), bazate pe separarea clară a dreptului de acces la date, conform rolurilor de securitate în sistem.

b) Funcţionalitatea de acces unic. SIA „RAC” utilizează funcţionalitatea de autorizare doar prin intermediul Serviciului guvernamental de autentificare şi control al accesului pentru serviciile electronice M-Pass.

c) Permisiunile utilizatorilor şi semnătura electronică. Semnătura electronică şi permisiunile utilizatorilor sunt modalităţi de securitate care asigură autorizarea, confidenţialitatea, autenticitatea şi non-repudierea. Aceste servicii se bazează pe infrastructura de semnătură electronică M-Sign şi pe directoarele de sistem pentru a gestiona permisiunile utilizatorilor şi autorizarea la nivelul blocurilor funcţionale.

d) Managementul utilizatorilor şi a grupurilor de utilizatori. Utilizatorii SIA „RAC” sunt autorizaţi să lucreze doar asupra documentelor, actelor sau a altor elemente informaţionale pentru care au permisiunile necesare. Din acest motiv, administratorul SIA „RAC” gestionează grupele de utilizatori într-un director. Un grup este caracterizat de un nume şi de un set de permisiuni (desemnând rolurile acelui grup), care definesc accesul la funcţionalităţile sistemului. Fiecare grup trebuie să conţină o listă de utilizatori, care preiau permisiunile de la grupul din care fac parte. La autentificare, sistemul verifică datele de acces ale utilizatorilor şi le dă acces la informaţia disponibilă.

 Cererea de motivare a accesului este realizată în cadrul unui sistem de control al accesului la resursele SIA „RAC” (de exemplu, documente, informaţii), în care este stabilit: cine, cui, în conformitate cu care împuterniciri, care documente, pentru care acţiuni sau care tip de acces poate fi permis şi în care condiţii, şi care presupune determinarea pentru toţi utilizatorii SIA „RAC”, a resurselor informaţionale şi program la care au acces pentru operaţii concrete de accesare (citire, scriere, modificare, ştergere, execuţie) folosind resursele tehnice şi program de accesare.

e) Infrastructura de semnătură electronică. SIA „RAC” operează un sistem de semnătură electronică ce permite utilizatorilor să semneze documente cu putere juridică. În calitate de mecanism de implementare a semnăturii electronice în cadrul SIA „RAC” este folosit serviciul guvernamental MSign. Semnătura electronică şi controlul accesului constituie măsurile de control de securitate, care asigură integritatea, confidenţialitatea, disponibilitatea, autenticitatea şi non-repudierea.

f) Înregistrările de audit. O necesitate importantă legată de securitate este necesitatea păstrării înregistrărilor de audit pentru analiza integrităţii sistemului şi pentru monitorizarea activităţii utilizatorilor. SIA „RAC” se bazează pe un mecanism de înregistrări de audit ce urmează practicile mondiale curente. Pentru garantarea securităţii la nivelul infrastructurii tehnico-logice este implementat auditul activ al securităţii informaţionale. Cele mai importante evenimente din cadrul sistemului sunt înregistrate în paralel prin intermediul serviciului MLog.

g) Disponibilitatea sistemului. Utilizatorii SIA „RAC” depind într-o măsură considerabilă de disponibilitatea sistemului pentru a-şi putea îndeplini sarcinile. Acest lucru ridică cerinţe semnificative faţă de infrastructura sistemului informațional pentru ca aceasta să fie rezistentă la erori de hardware şi software. Pentru a preveni aceste probleme, infrastructura include un set de circuite redundante care consistă din noduri de rezervă ce vor prelua încărcătura sistemului pe timpul cât sistemul principal se află în proces de mentenanţă sau restaurare.

h) Criptarea informaţiei. La transmiterea informaţiei confidenţiale, metoda de protecţie a informaţiei transmise prin toate tipurile de canale de comunicaţie, contra interceptării, alterării sau a falsificării informaţiei, este criptarea informaţiei, iar la distanţe mici - utilizarea fibrelor optice protejate în calitate de canale de comunicaţie. Sunt folosite mijloace de securizare criptografică a datelor cu rezistenţă garantată pentru nivelul necesar de confidenţialitate şi sistemul de chei electronice, ce asigură autentificarea mesajelor şi schimb sigur de informaţie.

 **47.** În procesul de gestionare a SIA „RAC” se va asigura securitatea datelor cu caracter personal, în conformitate cu Legea nr. 133 din 8 iulie 2011 privind protecţia datelor cu caracter personal, Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, conform Politicii de securitate a datelor cu caracter personal în cadrul Serviciului Fiscal de Stat, aprobate prin Ordinul Serviciului Fiscal de Stat nr. 715 din 28 decembrie 2018.

 Securitatea informaţională se menţine pe parcursul întregului ciclu de viaţă SIA „RAC” şi se perfecţionează continuu pentru prevenirea noilor pericole.

**Capitolul IX. Impactul general al sistemului**

**48.Impactul general**

 Impactul SIA „RAC” va consta în implementarea unei soluţii moderne de colaborare, gestiune şi automatizare a fluxurilor de lucru şi a circulaţiei de documente, crearea unei arhive electronice a tuturor documentelor ce vizează o amendă contravențională, îmbunătăţirea calităţii informaţiilor, inclusiv a relevanţei, integrităţii, oportunităţii, exactităţii, accesibilităţii, comparabilităţii, coerenţei acestora, pentru a oferi un serviciu mai calitativ, a face mai transparent şi mai rapid procesul de luare deciziilor.

 Implementarea SIA „RAC” va determina scăderea cheltuielilor generale deoarece va creşte fluxul de lucru în format electronic, fapt ce va duce la reducerea considerabilă a folosirii hârtiei şi a rechizitelor de birou şi la îmbunătăţirea calităţii şi sporirea diversităţii mijloacelor de comunicare interinstituţională.

 Implementarea SIA „RAC” va aduce următoarele beneficii:

a) creșterea transparenței activităților desfășurate de către autoritățile competente să soluționeze cauzele contravenționale, scurtarea timpului procedurilor de rutină și reducerea timpului de așteptare și acces la informație;

b) securizarea accesului la aplicaţii/date/sisteme/infrastructură, cu aplicarea politicilor de securitate, profilurilor de identitate şi a soluţiilor de gestiune a accesului;

c) oferirea de informaţii autentice, veridice, curente şi consistente tuturor actorilor implicaţi;

d) reducerea timpului de răspuns şi suport decizional;

e) acces rapid, garantat la date şi informaţii indiferent de locaţie;

f) sporirea calităţii informaţiilor, inclusiv a relevanţei, integrităţii, oportunităţii, exactităţii, accesibilităţii, comparabilităţii, coerenţei acesteia;

g) perfecționarea modului de păstrare şi diseminare a informaţiilor prin asigurarea protecţiei informaţiilor confidenţiale, acces nediscriminatoriu tuturor utilizatorilor la informaţii şi servicii, obiectivitate şi imparţialitate în diseminarea informaţilor;

h) consolidarea unei arhive digitale a dosarelor cauzei contravenționale și protejarea datelor în timp prin proceduri automatizate de salvare și restaurare.

1. **Cerințe privind dezvoltarea sistemului**

 Implementarea sistemului se va face în conformitate cu Reglementarea tehnică „Procesele ciclului de viață al software-lui” RT 38370656-002:2006 și va avea următoarele activități obligatorii:

a) Analiza, proiectarea, dezvoltarea, implementarea şi testarea tuturor componentelor informatice;

b) Livrarea şi instalarea bunurilor constitutive ale sistemului, precum şi efectuarea tuturor lucrărilor aferente punerii în funcţiune a acestuia;

c) Acceptanţa, punerea în funcţiune, garanţie şi suportul operaţional pentru componentele sistemului şi pentru sistemul integrat;

d) Managementul implementării proiectului, inclusiv pregătirea şi livrarea documentației aferente proiectului, în conformitate cu specificaţiile tehnice;

e) Trainingul şi transferul de know-how corespunzător, atât pentru operarea sistemului, cât şi pentru înregistrarea în sistem a procedurilor administrative;

f) Mentenanţa activă a sistemului este perioada în care dezvoltatorul sistemului îşi asumă obligaţiunea faţă de Serviciul Fiscal de Stat de a-l asista în menţinerea capacităţii SIA „RAC” de a presta servicii, precum şi de a modifica produsul software, păstrând integritatea lui.