

REGULAMENT
cu privire la modul de ținere a Registrului de stat al persoanelor care
au interdicție de a ocupa o funcție publică sau de demnitate publică

Capitolul I
Dispoziții generale

1. Regulamentul cu privire la modul de ținere a Registrului de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică (în continuare – *Regulament*) stabilește modul de organizare și mecanismul de funcționare a resursei informatice destinate pentru automatizarea proceselor de lucru aferente înregistrării interdicțiilor de ocupare a funcțiilor publice și funcțiilor de demnitate publică sau, după caz, a funcției electorale.

2. Registrul de stat al persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică (în continuare - RSI) este o parte componentă a SIA „e-Integritate”, care asigură automatizarea procesului de înregistrare a interdicțiilor aplicate persoanelor pentru ocuparea funcțiilor publice sau a funcțiilor de demnitate publică sau, după caz, a funcției electorale, precum și gestiunea ulterioară a acestor înregistrări.

3. În sensul prezentului Regulament, următoarele noțiuni semnifică:
autentificare – procedeu folosit de sistemele informaționale de recunoaștere la distanță a identității unei persoane sau sistem prin tehnici și mijloace de identificare electronică, pentru obținerea anumitor drepturi în cadrul sistemelor informaționale în baza identității acesteia;

declarație – declarație de avere și interese personale depusă (sub formă de document electronic) pe propria răspundere de către subiectul declarării prevăzut la art. 3 din Legea nr. 133/2016 *privind declararea averii și intereselor personale*;

dosar de control – totalitate a documentelor acumulate conform legislației de către Autoritatea Națională de Integritate (în continuare – Autoritate) în procesul de control al declarațiilor sau în procesul de control privind respectarea regimului juridic al averii, al conflictelor de interese și al incompatibilităților;

registrator – persoane autorizate ale Autorității, persoane responsabile din cadrul organizațiilor publice în care activează subiecții declarării;

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

SIA „e-Integritate” – sistem informațional destinat depunerii, arhivării, verificării și analizării automate a declarațiilor, înregistrării interdicțiilor de ocupare a funcțiilor publice sau funcțiilor de demnitate publică sau, după caz, a funcției electorale și gestiunii ulterioare a acestor înregistrări, precum și facilitării accesului electronic al persoanelor și instituțiilor interesate la informațiile de interes public;

utilizator al RSI – persoană care interacționează cu sistemul în scopul utilizării acestuia și al întreprinderii altor acțiuni necesare gestionării RSI;

profil (cont de utilizator) – compartiment al RSI, care include date generale despre un utilizator al acestuia.

4. RSI creează un spațiu informațional integrat și constituie sursa oficială de informații privind lista persoanelor care au interdicție de a ocupa o funcție publică sau de demnitate publică sau, după caz, a funcției electorale.

5. Regulamentul formulează sarcinile de bază ale RSI, subiecții raporturilor juridice în domeniul creării și funcționării RSI, drepturile și obligațiile posesorului, deținătorului și ale participanților la RSI, obiectele informaționale și lista datelor incluse în RSI, procedurile de colectare și gestiune a datelor, interoperabilitatea cu alte registre și sisteme informaționale, precum și metodele de protecție a datelor RSI.

6. Sarcinile de bază ale RSI constau în formarea bazei de date (colectarea, introducerea și stocarea datelor), actualizarea pe parcursul formării resursei informaționale și exploatarea (procesarea, sistematizarea, generalizarea, furnizarea și analiza datelor).

Capitolul II

Structura și funcțiile RSI

7. RSI include următoarele contururi funcționale de bază:

1) conturul Autorității:

a) înregistrarea interdicțiilor de a ocupa funcții publice sau de demnitate publică sau, după caz, a funcției electorale, ca urmare a constatării încălcărilor în procesul de control privind respectarea regimului juridic al averii, al conflictelor de interese și al incompatibilităților;

b) rectificarea și radierea interdicțiilor din RSI;

c) importul datelor în format tipizat privind interdicțiile de ocupare a funcțiilor publice și de demnitate publică emise de alte instituții abilitate (opțional);

d) administrarea RSI.

2) portalul public al RSI:

a) publicarea datelor detaliate cu privire la persoanele care au interdicție de a ocupa o funcție publică sau de demnitate publică sau, după caz, a funcției electorale;

b) căutarea interdicțiilor în baza unor criterii de filtrare prestabilite;

3) audit, rapoarte și statistici.

8. RSI va avea următoarele componente asociate funcționalităților de bază:

1) Gestionarea RSI:

a) Înregistrarea interdicției de ocupare a funcției publice sau de demnitate publică, sau, după caz, a funcției electorale, ca urmare a unui control și a prevederilor actului de constatare (conține toate etapele de la perfectarea actului de constatare care prevede interdicție până la marcarea actului de constatare ca definitiv și sincronizarea datelor despre interdicții pe pagina oficială a ANI);

b) procesarea solicitărilor de rectificare/radiere a interdicțiilor (angajatul ANI accesează și completează formularul de adăugare a unei solicitări de rectificare/radiere a interdicției, cu mecanism de atașare a documentelor justificative);

c) aprobarea/respingerea solicitării de rectificare/radiere a interdicțiilor – totalitatea funcționalităților necesare gestiunii procesului de coordonare a solicitării de rectificare/radiere a interdicției cu persoana decidentă din cadrul ANI;

d) importul interdicțiilor din fișiere cu format tipizat – funcționalitate accesibilă administratorului de sistem, care permite preluarea datelor în format tipizat privind interdicțiile de ocuparea a funcțiilor publice și de demnitate publică sau, după caz, a funcției electorale, emise de alte instituții abilitate și importarea acestora (opțional);

e) căutarea și vizualizarea autorizată a datelor despre interdicții – totalitatea funcționalităților necesare utilizatorilor autorizați ai ANI pentru căutarea informației relevante,

prin completarea formularelor speciale de căutare după o secvență de text, cu opțiuni avansate de căutare în baza regulilor de reducere a arealului de căutare utilizând valorile metadatelor RSI.

2) Publicarea datelor despre interdicții, statistici și indicatorilor cheie de performanță – livrează totalitatea funcționalităților necesare generării, exportării și publicării informației statistice cu caracter public privind activitatea RSI:

a) rapoarte statistice furnizate automatizat de sistem pentru a fi publicate pe pagina web oficială a ANI;

b) date publice detaliate despre interdicții;

c) valori ale indicatorilor de performanță ale ANI.

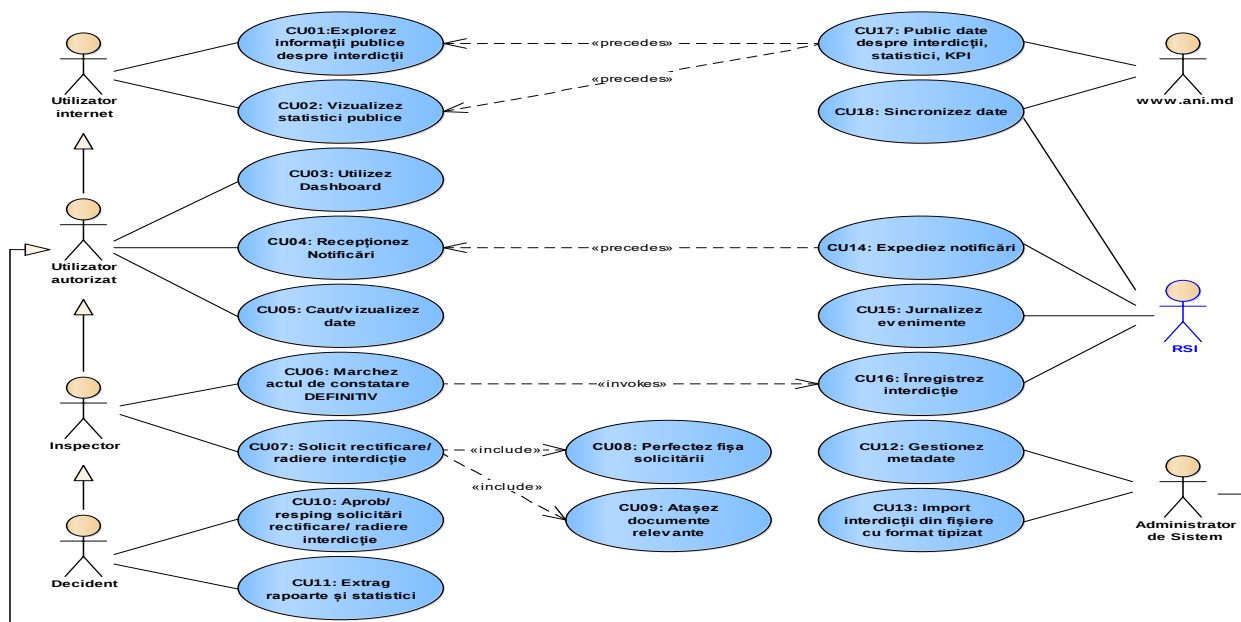
3) Sincronizarea datelor despre interdicții pe pagina oficială a ANI – funcționalitate automatizată prin intermediul căreia RSI comunică cu pagina web oficială a ANI cu scopul de a publica date privind interdicțiile de ocupare a funcțiilor publice sau de demnitate publică sau, după caz, a funcției electorale.

4) Rapoarte și statistici – funcționalitate accesibilă persoanelor cu rol decident din cadrul ANI, care permite generarea rapoartelor predefinite și ad-hoc privind conținutul informațional al RSI.

5) Administrarea sistemului – totalitatea funcționalităților de gestiune a clasificatoarelor, nomenclatoarelor, constantelor, variabilelor de sistem necesare pentru buna funcționare a RSI.

6) Jurnalizarea evenimentelor, care include totalitatea funcționalităților de configurare a principiilor de funcționare și generare a evenimentelor care vor fi jurnalizate și de definire a strategiilor de colectare a evenimentelor jurnalizate. Funcționalitatea include atât mecanismul de jurnalizare internă (integrate în cadrul SIA „e-Integritate”), cât și integrarea mecanismelor externe de jurnalizare a evenimentelor de business critice (MLog).

8. Funcționalitățile livrate de RSI actorilor care beneficiază de ele sunt redată în figura de mai jos:



Capitolul III

Subiecții raporturilor juridice în domeniul creării și exploatării RSI

9. Posesorul RSI este Autoritatea. Rolul de posesor al sistemului informatic reflectă aspectul administrativ ce ține de competențele totale deținute de ANI, necesare creării,

administrării și dezvoltării continue a sistemului informatic. În această calitate, ANI asigură achiziționarea sistemului din sursele bugetare disponibile pentru astfel de activități. ANI, în calitate de implementator, asigură suportul organizațional și metodologic întru automatizarea funcțiilor business necesare atingerii obiectivelor sistemului informatic.

10. Deținătorul RSI din punct de vedere informațional este Autoritatea, care asigură crearea și exploatarea RSI. Administratorul tehnic al soluției informatice este IP „STISC”, care furnizează infrastructura tehnică care va găzdui RSI în conformitate cu cerințele față de sistemele informatice de importanță statală.

11. Administratorul de sistem este angajatul Autorității sau o organizație – persoană subcontractată de Autoritate, care acordă suportul tehnic de administrare a RSI.

12. Registratorii RSI sunt totalitatea inspectorilor de integritate ai ANI, care vor crea înregistrările în RSI în cadrul proceselor de business de examinare a sesizărilor parvenite în adresa ANI și perfectarea actelor de constatare în urma verificărilor efectuate.

13. Furnizorii RSI sunt instituțiile abilitate cu atribuții de evidență a persoanelor condamnate penal sau sancționate contravențional prin hotărâre judecătorească, pedeapsa cărora include interdicții de ocupare a funcțiilor publice sau funcțiilor de demnitate publică sau, după caz, a funcției electorale.

14. Utilizatorii RSI sânt:

1) *utilizator internet* - actor uman care dispune de acces la funcționalitățile specifice de afișare a informațiilor cu caracter public furnizate de RSI prin intermediul paginii WEB a ANI (ww.ani.md). Categoria dată de actori dispune de acces la următoarele funcționalități:

- accesarea paginii web oficiale a ANI pentru vizualizarea statisticilor și coeficienților de performanță cu caracter public furnizate de RSI;

- accesarea paginii web oficiale a ANI pentru vizualizarea conținutului actelor de constatare și stabilire a interdicțiilor de exercitare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale;

- formarea interpelărilor și vizualizarea informației cu caracter public conținută în RSI.

2) *inspector de integritate* – actor uman, angajat al ANI cu atribuții de perfectare a formularelor destinate modificării conținutului RSI. Acești utilizatori vor perfectă cea mai mare parte a datelor aferente interdicțiilor de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale. Actorii în cauză dispun de acces la următoarele funcționalități:

- utilizarea Dashboard-ului pentru recepționarea și accesarea notificărilor privind evenimentele de business care-l vizează;

- formularea interogărilor de căutare în conținutul BD a RSI;

- perfectarea formularelor electronice de rectificare/anulare a înregistrărilor de interdicție de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale;

- generarea și extragerea rapoartelor/statisticilor relevante drepturilor sale de acces la date;

- recepționarea notificărilor de sistem;

3) *decident ANI* – actor uman, angajat al ANI cu acces absolut la conținutul informațional și avansat la funcționalitățile furnizate de RSI, care dispune de rol de decident în fluxurile de lucru aferente înregistrării/modificării datelor privind statutul angajatului organizației publice. Această categorie de actori are acces la următoarele funcționalități:

- dispune de acces la toate funcționalitățile disponibile inspectorului de integritate;

- dispune de rol de decizie (aprobare/respingere) în cadrul verigilor fluxului de lucru destinat rectificării/anulării interdicțiilor de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale;

4) administrator de sistem – actor uman, abilitat cu administrarea RSI. Dacă mediul tehnologic include capacități suficiente pentru îndeplinirea lucrărilor de administrare apoi implementarea acestora în sistem este opțională. Această categorie de actori are acces la următoarele funcționalități:

- folosește necondiționat toate funcționalitățile sistemului informatic, cu excepția modificării fișierelor de evenimente;
- vizualizează orice înregistrare din baza de date;
- administrează profilurile utilizatorilor;
- generează rapoarte aferente auditului RSI și conținutului informațional al bazei de date;
- administrează sistemul de nomenclatoare;
- recepționează notificări de sistem.

5) administrator tehnic - actor uman, care monitorizează infrastructura tehnică ce găzduiește RSI, asigură mentenanța și securitatea informațională a RSI. Această categorie de actori are acces la următoarele funcționalități:

- folosește necondiționat toate funcționalitățile sistemului informatic, cu excepția modificării fișierelor de evenimente;
- vizualizează orice înregistrare din baza de date;
- administrează serverul de aplicații ;
- administrează baza de date în producție;
- generează rapoarte aferente auditului RSI și conținutului informațional al bazei de date;
- administrează sistemul de nomenclatoare;
- recepționează notificări de sistem;
- efectuează copii de rezervă a bazei de date.

15. Destinatari ai datelor din RSI este Autoritatea și orice persoană fizică sau juridică, care pot accesa pe portalul public datele din RSI, pentru informare, conform prevederilor legislației.

16. Posesorul are următoarele atribuții:

- 1) asigură condițiile organizatorice și financiare pentru funcționarea RSI;
- 2) stabilește scopurile și sarcinile funcționale ale RSI;
- 3) determină obiectele informaționale supuse înregistrării în RSI și conținutul acestora;
- 4) monitorizează procesul de înregistrare și prelucrare a datelor în RSI;
- 5) gestionează activitatea de exploatare și ținere a conținutului informațional al RSI;
- 6) asigură securitatea și protecția datelor din RSI ca parte componentă a SIA „e-Integritate” prin intermediul structurilor de stat specializate;

7) aprobă și coordonează cu administratorul tehnic executarea modificărilor/rectificărilor solicitate în cererile privind erorile de sistem, erorile cauzate de factorul uman, incidentele de infrastructură care afectează funcționarea normală a RSI;

8) autorizează, suspendă și revocă dreptul de acces în RSI;

9) stabilește măsurile tehnice și organizatorice de protecție și securitate a RSI parte componentă a SIA „e-Integritate”;

10) monitorizează și, după caz, ajustează cerințele de securitate și conformitate a RSI parte componentă a SIA „e-Integritate” la domeniul protecției datelor cu caracter personal;

11) adoptă măsurile tehnice și organizatorice necesare pentru a proteja datele cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite în conformitate cu Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123/2010;

12) prelucrează datele cu caracter personal care sunt strict necesare, adecvate, relevante și care nu sunt excesive în raport cu scopurile pentru care sunt colectate sau prelucrate ulterior;

13) generează și păstrează înregistrările de audit ale securității pentru operațiunile de prelucrare a datelor cu caracter personal în conformitate cu Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123/2010;

14) exercită alte atribuții necesare asigurării bunei funcționări a RSI ca parte componentă a SIA „e-Integritate”..

17. Posesorul asigură păstrarea RSI ca parte componentă a SIA „e-Integritate” până la adoptarea deciziei despre lichidarea acestuia. În cazul lichidării, datele și documentele conținute în acesta se transmit în arhivă, conform legislației.

18. Deținătorul RSI din punct de vedere informațional este Autoritatea, care asigură crearea și exploatarea RSI și are dreptul de gestionare și de utilizare a datelor și a resurselor acestuia.

19. Administratorul RSI este angajatul Autorității sau o organizație – persoană contractată de Autoritate, care acordă suportul tehnic de administrare a acestuia.

20. Administratorul RSI are următoarele atribuții:

- 1) crearea, modificarea, suspendarea/activarea contului de utilizator;
- 2) atribuirea unui rol utilizatorului și/sau unui grup de utilizatori;
- 3) atribuirea nivelului de acces și aplicarea restricțiilor de acces (după adresă IP);
- 4) managementul formularelor electronice;
- 5) managementul șabloanelor de rapoarte și statistici;
- 6) monitorizarea jurnalizării evenimentelor;
- 7) asigurarea suportului Centrului Național pentru Protecția Datelor cu Caracter Personal în cadrul investigațiilor efectuate în contextul RSI;

8) întocmește lista nominală a angajaților cu drepturi în sistem și datele de contact la fiecare modificare a datelor;

9) alte atribuții necesare asigurării bunei funcționări a RSI.

21. Administratorul de sistem are posibilitatea să creeze șabloane predefinite, iar în baza acestora RSI generează rapoarte cu posibilitatea selectării formatelor descrise.

22. Administratorul de sistem are funcții de creare, adăugare/ștergere a câmpurilor informaționale, redenumire a casetelor informaționale în cadrul formularelor electronice.

23. Administratorul tehnic al RSI ca parte componentă a SIA „e-Integritate” este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, care asigură mentenanța, securitatea și dezvoltarea SIA „e-Integritate”.

24. Administratorul tehnic are următoarele atribuții:

1) asigură administrarea tehnică a RSI ca parte componentă a SIA „e-Integritate”, inclusiv funcționalitatea și securitatea logică și cibernetică în conformitate cu actele normative în domeniu;

2) asigură funcționarea RSI;

3) execută modificările/rectificările solicitate în demersurile primite referitoare la erorile de sistem ale RSI, erorile cauzate de factorul uman în RSI, incidentele de infrastructură care afectează funcționarea normală a RSI ca parte componentă a SIA „e-Integritate”, cu condiția primirii în prealabil a aprobării posesorului, în urma verificării de către posesor a corespunderii solicitării cu prevederile legislației;

4) acordă suport posesorului la elaborarea Planului de continuitate al RSI ca parte componentă a SIA „e-Integritate” și instituie activități de control menite să diminueze riscurile privind integritatea datelor RSI;

5) alte atribuții necesare asigurării bunei funcționări a RSI.

25. Administrarea tehnică a SIA „e-Integritate” include asigurarea funcționalității, disponibilității și continuității SIA „e-Integritate” în conformitate cu Planul de continuitate al SIA „e-Integritate”, precum și procedurile operaționale ale administratorului tehnic.

26. Activitatea administratorului tehnic se supune auditului extern.

27. Registratorii RSI sunt inspectorii de integritate ai ANI, care creează înregistrări în RSI în cadrul activității de examinare a sesizărilor parvenite în adresa ANI și emiterii actelor de constatare în urma verificărilor efectuate.

28. Furnizorul datelor din cadrul instituțiilor abilitate cu atribuții de evidență a persoanelor condamnate penal sau sancționate contravențional are următoarele atribuții:

1) asigură corectitudinea și autenticitatea datelor introduse sau prezentate pentru a fi introduse în RSI;

2) actualizează informația prezentată cu privire la subiecții aplicării interdicțiilor în modul stabilit de actele normative;

3) asigură confidențialitatea datelor accesate ce vizează viața privată a subiecților aplicării interdicțiilor;

4) raportează posesorului problemele de funcționalitate ale RSI.

29. Utilizatorii din cadrul Autorității au următoarele atribuții:

1) asigură colectarea, introducerea și prelucrarea informației relevante în baza de date a RSI, în termenele și condițiile stabilite;

2) asigură autenticitatea, plenitudinea, integritatea datelor din RSI;

3) asigură securitatea și confidențialitatea informației introduse în RSI;

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 RSI;

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

8) raportează posesorului sau administratorului tehnic problemele de sistem în utilizarea RSI;

9) înaintează demersuri privind necesitatea de dezvoltare și îmbunătățire a RSI;

10) participă în grupurile de lucru organizate în scopul dezvoltării și îmbunătățirii RSI.

30. RSI va ține cont de subiecții vizați în dosarele de control aflate în gestiunea inspectorului de integritate și va restricționa accesul privind depunerea solicitării de rectificare sau radiere a datelor despre interdicție.

Capitolul IV

Spațiul informațional al sistemului informatic

31. Totalitatea obiectelor informaționale, care reprezintă resursa informațională a RSI, este determinată de destinația sistemului și include următoarele obiecte:

1) interdicție;

2) act de constatare;

3) solicitare de rectificare/radiere interdicție;

4) eveniment de gestiune a înregistrării.

32. Identificarea obiectelor în cadrul RSI se efectuează prin utilizarea numărului de identificare unic.

1) pentru „interdicții” – numărul de identificare unic generat de sistem;

2) pentru „acte de constatare” – numărul de identificare unic furnizat de SIA „e-Management”;

3) pentru „solicitare de rectificare/radiere interdicție” – numărul de identificare unic furnizat de SIA „e-Management”;

4) pentru „Eveniment de gestiune a înregistrării (eveniment)” - numărul de identificare unic generat de sistem.

33. Datele Sistemului informatic. Datele prezentului Sistem reprezintă totalitatea de atribute ale obiectelor informaționale și includ:

- 1) Interdicție:**
 - a)** Numărul unic de identificare a interdicției în RSI;
 - b)** Date despre actul de constatare:
 - numărul unic de identificare a actului de constatare;
 - data emiterii actului de constatare;
 - mențiuni despre statutul actului de constatare (în termen (pasibil) de contestare, contestat, definitiv, anulat);
 - c)** Date despre subiectul declarării:
 - IDNP subiectului;
 - numele, prenumele subiectului;
 - denumirea organizației, IDNO;
 - funcția deținută.
 - d)** Date despre perioada pentru care este aplicată interdicția:
 - statutul interdicției, determinat de statutul actului de constatare (preventivă, definitivă, contestată, anulată);
 - termenul de aplicare a interdicției (luni);
 - data intrării în vigoare a interdicției;
 - data încetării interdicției;
 - e)** Alte mențiuni speciale:
 - publicată pe pagina WEB a ANI (da/nu).
- 2) Act de constatare:**
 - numărul unic de identificare a actului de constatare;
 - data emiterii actului de constatare;
 - tipul actului de constatare (de încetare, de constatare a încălcării);
- d)** date despre tipul încălcării (01- avere; 02 - conflict de interese; 03-incompatibilități).
- e)** date despre operatorul inspector care a elaborat actul de constatare:
 - identificatorul unic al inspectorului ANI în SIA „e-Integritate”;
- f)** date despre subiectul declarării pentru care a fost examinat cazul de încălcare;
 - IDNP subiectului;
 - numele, prenumele subiectului;
 - denumirea organizației, IDNO;
 - funcția deținută;
- g)** date despre interdicție:
 - numărul unic de identificare a interdicției în RSI;
 - termenul de aplicare a interdicției (luni).
- 3) Solicitare de rectificare/radiere interdicție:**
 - numărul unic de identificare a solicitării de rectificare;
 - numărul unic de identificare a interdicției în RSI;
 - numele, prenumele, IDNP al subiectului declarării pentru care a fost adăugată interdicția;
 - nota informativă despre datele care trebuie rectificate.
- 4) Eveniment de gestiune a înregistrării:**
 - numărul unic de identificare al evenimentului;
 - tipul evenimentului;
 - data și ora evenimentului.

5) Scenarii de bază. Scenariul de bază include o listă a evenimentelor ce se produc cu obiectul informațional și se țin la evidență în Sistem. În RSI sânt ținute la evidență următoarele evenimente:

a) Stabilirea inițială a interdicției. În urma sesizărilor recepționate de la cetățeni sau organizații, de către ANI este identificat subiectul declarării și inițiat un dosar de control, examinarea căruia finalizează cu emiterea unui act de constatare. Actul de constatare poate avea prevederi cu privire la aplicarea interdicțiilor de ocupare a funcției publice și de demnitate publică sau, după caz, a funcției electorale.

Odată cu publicarea actului de constatare, dacă acesta prevede aplicarea de interdicție, SIA „e-Integritate” va adăuga o înregistrare preventivă aferentă interdicției.

După expirarea perioadei legale de contestare a actului de constatare, SIA „e-Integritate” verifică interdicțiile preventive și expediază inspectorului de integritate notificări referitor la expirarea termenului legal de contestare a actelor de constatare.

După recepționarea notificării referitor la expirarea termenului legal de contestare a actelor de constatare, inspectorul de integritate verifică, dacă actul de constatare a rămas definitiv.

În cazul rămânerii actului definitiv, inspectorul de integritate va activa în RSI interdicția de ocupare a funcției publice sau funcției de demnitate publică, sau, după caz, a funcției electorale, cu respectarea normelor prevăzute de art. 23 alin. (6) și alin. (7) din Legea nr. 133/2016.

După activarea interdicției SIA „e-Integritate” va sincroniza datele cu pagina web oficială a ANI.

Dacă actul de constatare sau prevederile aplicării interdicției au fost anulate de instanța de judecată în urma contestării, atunci inspectorul de integritate anulează înregistrarea preventivă a interdicției.

b) Rectificarea sau radierea interdicției. Odată înscrisă în RSI, informația despre interdicție nu poate fi modificată direct, dar numai prin intermediul unor documente specifice care argumentează necesitatea rectificării sau radierii interdicției.

Când apare necesitatea de rectificare/radiere a interdicției, inspectorul de integritate perfectează în RSI un formular electronic de rectificare/radiere a interdicției, pe care îl expediază spre aprobare decidentului ANI.

Decidentul ANI, după recepționarea solicitării, o examinează și decide dacă permite sau nu rectificarea/radierea interdicției.

Dacă decidentul ANI aprobă solicitarea, inspectorul de integritate aplică modificările necesare pentru rectificarea/radierea interdicției. După efectuarea tuturor modificărilor necesare, SIA „e-Integritate” va sincroniza datele cu pagina web oficială a ANI.

În cazul, în care decidentul ANI anulează solicitarea, rectificarea/radierea interdicției nu este aplicată în RSI.

6) Clasificatoarele și nomenclatoarele sistemului informatic.

În scopul asigurării veridicității și asigurării interoperabilității RSI cu sisteme informatice terțe, reducerii volumului de informație stocată, se vor utiliza clasificatoare și nomenclatoare care pot fi divizate în 4 grupuri:

- internaționale (valorile cărora sunt standardizate și acceptate la nivel internațional);
- naționale (CUATM, FOJ, CFP etc.);
- de interoperabilitate (valorile cărora sunt utilizate la interacțiune cu sisteme informatice terțe);
- intrasistemice (variabile de system, parametri ai interfeței de utilizator, parametri de configurare a sistemului informatic, roluri, categoriile de documente, tipuri de încălcări, funcții publice).

Clasificatoarele intrasistemice se elaborează și se utilizează în cadrul RSI doar în lipsa clasificatoarelor/nomenclatoarelor internaționale și naționale aprobate.

7) Interacțiunea cu alte sisteme informatice.

Pentru asigurarea funcționalității în condiții optime a RSI, este necesară realizarea interacțiunii cu alte sisteme informatice.

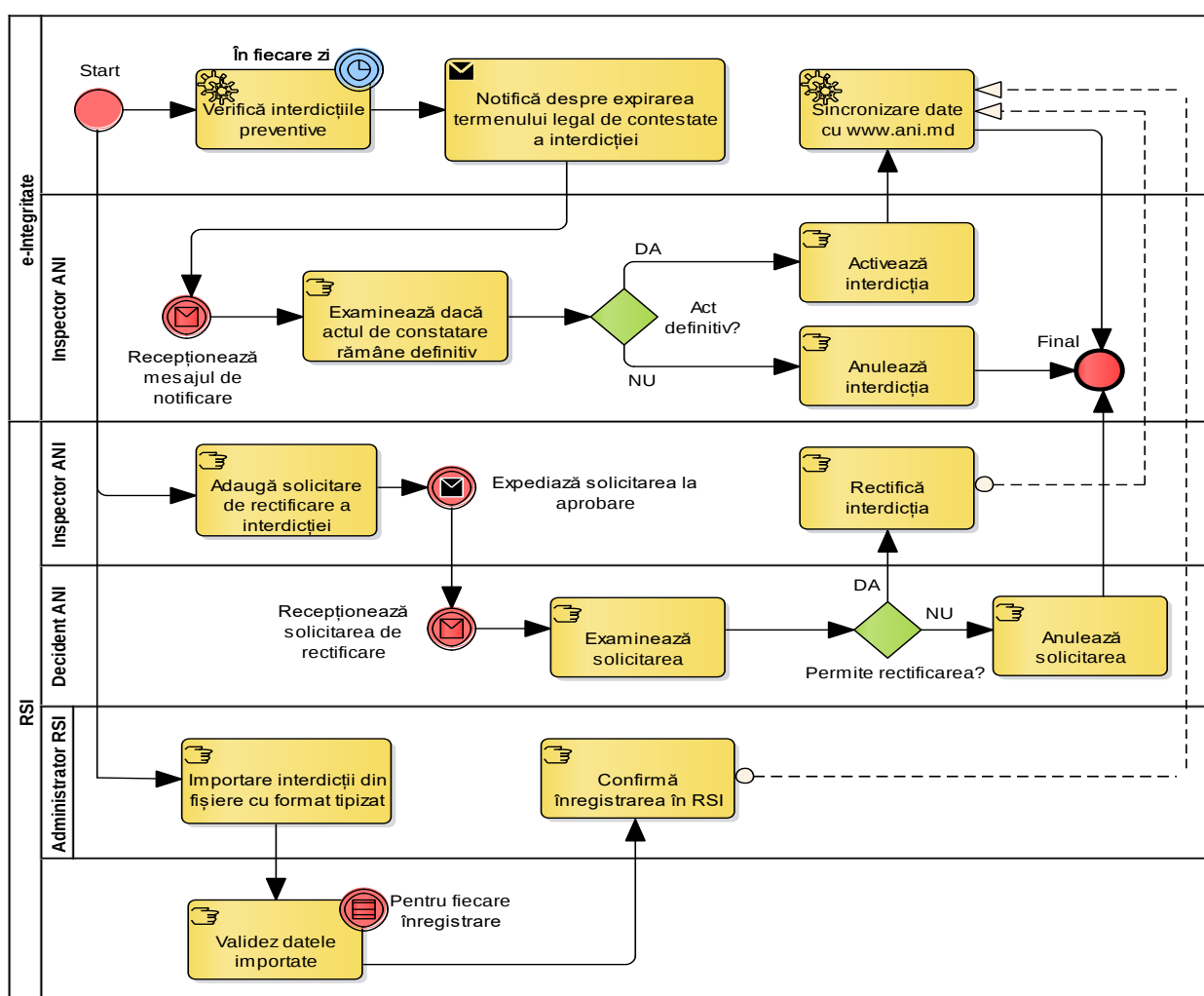
În special, este prioritară integrarea cu următoarele servicii de platformă MCloud:

- MPass - pentru autentificarea și controlul accesului;
- MSign – pentru aplicarea și validarea semnăturii electronice;
- MLog – pentru jurnalizarea evenimentelor de business critice;
- MNotify – pentru notificarea utilizatorilor.

34. Interacțiunea cu platforma de interoperabilitate MConnect va fi utilizată pentru interacțiunea RSI cu alte sisteme informatice, care aparțin autorităților publice ale Republicii Moldova (Registrul de stat al populației, Registrul de stat al unităților de drept). În perspectivă, în condițiile în care sistemele informatice ale instituțiilor terțe, care conțin date privind interdicțiile de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale, vor fi funcționale și interoperabile (spre exemplu: SIA „e-Probațiune”), integrarea cu acestea se va efectua prin platforma de interoperabilitate MConnect.

35. Interacțiunea cu Portalul public al SIA „e-Integritate” este utilizată pentru a asigura accesul cetățenilor la datele cu caracter public furnizate de RSI.

36. Pentru asigurarea funcționalității în bune condiții a RSI e necesară implementarea fluxului generic descris în figura de mai jos:



Capitolul V

Interoperabilitatea cu alte sisteme informaționale

37. Pentru asigurarea funcționalității în condiții optime a RSI, este realizată interacțiunea cu alte sisteme informatice. În special, este realizată integrarea cu următoarele servicii de platformă MCloud:

- MPass - pentru autentificarea și controlul accesului;
- MSign – pentru aplicarea și validarea semnăturii electronice;
- MLog – pentru jurnalizarea evenimentelor de business critice;
- MNotify – pentru notificarea utilizatorilor.

38. Interacțiunea cu platforma de interoperabilitate MConnect este utilizată pentru interacțiunea RSI cu alte sisteme informatice, care aparțin autorităților publice ale Republicii Moldova:

- 1)** “Registrul de stat al unităților de drept” pentru accesul la datele aferente tuturor unităților de drept din Republica Moldova;
- 2)** “Registrul de stat al populației” pentru accesul la datele aferente tuturor persoanele fizice rezidente și documentate în Republica Moldova.

39. În condițiile în care sistemele informatice ale instituțiilor terțe – furnizori de date, care conțin date privind interdicțiile de ocupare a funcțiilor publice și funcțiilor de demnitate publică, sau, după caz, a funcției electorale, vor fi funcționale și interoperabile (spre exemplu: SIA „e-Probațiune”), integrarea cu acestea se va efectua prin platforma de interoperabilitate MConnect.

40. Interacțiunea cu Portalul public al SIA „e-Integritate” este utilizată pentru a asigura accesul cetățenilor la datele cu caracter public furnizate de RSI.

41. Pentru asigurarea interoperabilității cu alte sisteme informaționale departamentale se utilizează serviciile web furnizate de RSI.

Capitolul VI

Ținerea și asigurarea funcționării RSI

42. RSI este ținut în formă electronică, în limba de stat.

43. În procesul de exploatare a RSI se formează resursa informațională, care reprezintă totalitatea informației sistematizate despre interdicțiile aplicate persoanelor pentru ocuparea funcțiilor publice sau a funcțiilor de demnitate publică sau, după caz, a funcției electorale.

44. Accesul la resursele RSI este asigurat prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass), cu utilizarea semnăturii electronice. La începutul sesiunii de lucru fiecare utilizator trece procedura de autentificare în sistem prin utilizarea semnăturii electronice. În caz de neconfirmare a autenticității utilizatorului conectarea la RSI nu se permite.

45. Datele din RSI fac parte din categoria datelor cu caracter personal.

46. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul RSI se efectuează cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale, aprobate prin legislație.

47. Introducerea informației în RSI se efectuează de către registratorii ANI în baza conținutului dosarelor de control în cadrul proceselor de examinare a sesizărilor parvenite în

adresa ANI și emiterii actelor de constatare în urma controalelor efectuate.

48. Evidența obiectelor informaționale se ține conform Ghidului de utilizare a RSI, care conține instrucțiuni clare de introducere, modificare și vizualizare a datelor în baza de date, elaborat în cadrul procesului de dezvoltare a RSI și pus la dispoziția participanților la RSI.

49. Conturile de acces pentru toți utilizatorii RSI se creează de către administratorul sistemului la necesitate. Fiecărui utilizator i se atribuie un identificator/nume de utilizator și o parolă pentru a avea acces la RSI.

50. Pentru asigurarea funcționării eficiente și neîntrerupte a RSI, schimbul informațional de date între participanții la RSI și baza de date este asigurat în regim nonstop.

51. Funcționarea RSI este suspendată de către administratorul de sistem sau de administratorul tehnic al RSI în următoarele cazuri:

- 1)** în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware ale RSI;
- 2)** la apariția circumstanțelor de forță majoră;
- 3)** la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea RSI.

52. Lucrările profilactice în complexul de mijloace software și hardware se efectuează după notificarea în scris a participanților cu cel puțin 2 zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora.

53. În cazul apariției circumstanțelor de forță majoră, precum și a dificultăților tehnice în funcționarea complexului de mijloace software și hardware a RSI din vina terțelor persoane, este posibilă suspendarea funcționării RSI cu notificarea ulterioară a participanților conectați.

54. Revocarea dreptului de acces la RSI pentru utilizatorii participanților se efectuează în una dintre următoarele situații:

- 1)** în temeiul cererii (demersului) conducătorului acestuia;
- 2)** la încetarea raporturilor de serviciu/ de muncă ale utilizatorului;
- 3)** la intervenirea modificărilor raporturilor serviciu/ de muncă când noile atribuții nu impun accesul la datele din RSI;
- 4)** la constatarea încălcării de către utilizatorul participantului a sistemului securității informaționale a RSI.

Capitolul VII

Asigurarea protecției și securității informației

55. Datele din RSI fac parte din categoria datelor care necesită a fi protejate. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul RSI se efectuează de către subiecții cu drepturi de acces la sistem, cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

56. Măsurile de protecție și securitate a datelor din RSI, ca parte componentă a SIA „e-Integritate”, reprezintă un compartiment al lucrărilor de creare, dezvoltare și exploatare a SIA „e-Integritate” și se actualizează de către toți subiecții acestuia.

57. Securitatea informațională a RSI se efectuează prin aplicarea metodelor și efectuarea acțiunilor descrise în Planul de continuitate al SIA „e-Integritate” și, după caz, a procedurilor operaționale.

58. Schimbul informațional se efectuează cu utilizarea mijloacelor software și hardware, doar prin canale securizate, asigurând integritatea și securitatea datelor.

- 59.** Implementarea și monitorizarea respectării prevederilor normelor de securitate informațională este asigurată de persoana subordonată nemijlocit conducătorului instituției.
- 60.** 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.
- 61.** Conducătorul instituției asigură instruirea utilizatorii interni privind metodele și procedeele de contracarare a pericolelor informaționale.

Capitolul VIII

Controlul și răspunderea

- 62.** Ținerea RSI, ca parte componentă a SIA „e-Integritate”, este supusă controlului intern și extern. Controlul intern privind organizarea și funcționarea RSI se efectuează de către posesor. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea RSI se efectuează de către instituții abilitate și certificate în domeniul auditului.
- 63.** Responsabilitatea pentru organizarea funcționării RSI aparține posesorului și deținătorului acestuia.
- 64.** Utilizatorii în atribuțiile cărora intră ținerea RSI, introducerea datelor, furnizarea informațiilor și asigurarea funcționării RSI poartă răspundere personală, în conformitate cu legislația, pentru completitudinea, autenticitatea, veridicitatea, integritatea informației, precum și pentru păstrarea și utilizarea ei.
- 65.** Toți subiecții RSI și solicitantul informațiilor ce conțin date cu caracter personal poartă răspundere, conform legislației, pentru prelucrarea, divulgarea, transmiterea informației din sistem persoanelor terțe, contrar prevederilor legislației.
- 66.** Pentru asigurarea funcționalității eficiente și neîntrerupte a RSI, schimbul informațional de date RSI este asigurat în regim non-stop.
- 67.** Funcționarea RSI, ca parte componentă a SIA „e-Integritate”, se suspendă de către administratorul tehnic, 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 SIA „e-Integritate”;
 - 2)** la apariția unui impediment în afara controlului persoanei în cauză;
 - 3)** la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea SIA „e-Integritate”;
 - 4)** în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SIA „e-Integritate”;
 - 5)** la cererea scrisă a posesorului.
- 68.** În cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SIA „e-Integritate” din vina terțelor persoane, este posibilă suspendarea funcționării SIA „e-Integritate”, cu informarea subiecților SIA „e-Integritate” prin mijloacele tehnice disponibile.