Anexa nr. 2
la ordinul ANI nr. 80 din 26.08.2020

REGULAMENT
cu privire la modul de ținere a Registrului electronic al subiecților declarării averii și a intereselor personale

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul cu privire la modul de ținere a Registrului electronic al subiecților declarării averii și a intereselor personale (în continuare – *Regulament*) stabileşte modul de organizare şi mecanismul de funcţionare a resursei informatice destinate gestiunii resurselor umane din cadrul organizațiilor publice în care activează subiecții declarării.

2. Registrul electronic al subiecților declarării averii și a intereselor personale (în continuare - RSD) este o parte componentă a SIA „e-Integritate", care asigură funcționalitatea de management al resurselor umane din cadrul organizațiilor publice în care activează subiecții declarării, monitorizarea termenelor specificate în legislație de depunere a declarațiilor și notificarea subiecților declarării prin intermediul serviciului electronic guvernamental de notificare (MNotify).

3. În sensul prezentului Regulament, se definesc următoarele noțiuni:

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 de avere și interese personale sau în procesul de control privind respectarea regimului juridic al conflictelor de interese, incompatibilităților și restricțiilor;

registrator – persoane autorizate ale Autorității, persoane responsabile (operator resurse umane) 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 de avere și interese personale, înregistrării interdicțiilor de ocupare a funcțiilor publice sau funcțiilor de demnitate publică și gestiunii ulterioare a acestor înregistrări, precum și facilitării accesului electronic al persoanelor și instituțiilor interesate la informațiile de interes public;

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

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

4. RSD creează un spaţiu informaţional integrat şi constituie sursa oficială de informaţii privind lista subiecților declarării din cadrul organizațiilor publice, evenimentele de angajare/numire/alegere în funcție, precum și de demisie/eliberare din funcție a subiecților declarării și obligațiile apărute privind depunerea declarației de avere și interese personale.

5. Regulamentul formulează sarcinile de bază ale Registrului, subiecţii raporturilor juridice în domeniul creării şi funcţionării Registrului, drepturile şi obligaţiile posesorului, deţinătorului şi ale participanţilor la Registru, obiectele informaţionale şi lista datelor incluse în Registru, procedurile de colectare şi gestiune a datelor, interoperabilitatea cu alte registre şi sisteme informaţionale, precum şi metodele de protecţie a datelor Registrului.

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

Capitolul II
STRUCTURA ȘI FUNCȚIILE RSD

7. RSD „e-Integritate” include următoarele contururi funcționale de bază:

1) conturul organizațiilor publice:

a) înregistrarea subiecților declarării în Registrul electronic al subiecților declarării averii și a intereselor personale;

b) modificarea statutului subiecților declarării în Registrul electronic al subiecților declarării averii și a intereselor personale;

2) conturul Autorității:

a) gestionarea utilizatorilor;

b) gestionarea Registrului electronic al subiecților declarării averii și a intereselor personale;

3) audit, rapoarte și statistici.

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

1) Gestionarea Registrului electronic al subiecților declarării averii și a intereselor personale:

a) Înregistrarea subiectului declarării la angajare/numire/alegere în funcție;

b) Modificarea statutului subiectului declarării la demisie/transfer;

2) monitorizarea evenimentelor de angajare/numire/alegere în funcție, precum și de demisie/eliberare din funcție a subiecților declarării și obligațiilor apărute privind depunerea declarației:

a) notificarea subiecților declarării, expedierea notificărilor utilizând serviciul electronic guvernamental de notificare (MNotify) cu privire la obligațiile apărute privind depunerea declarației;

b) furnizarea automatizată a datelor către SIA „e-Integritate", în caz de nedepunere a declarației în termenul stabilit, spre includere în lista subiecților declarării pasibili de declanșarea din oficiu a procedurii de control;

3) Audit, rapoarte și statistici:

a) generarea rapoartelor;

b) exportul rapoartelor;

c) jurnalizarea evenimentelor din sistem.

Capitolul III
SUBIEȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII ȘI EXPLOATĂRII RSD

9. Posesorul RSD 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.

10. Deținătorul RSD din punct de vedere informațional este Autoritatea, care asigură crearea și exploatarea RSD. Administratorul tehnic al soluției informatice este IP „STISC", care furnizează infrastructura tehnică care va găzdui RSD 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 RSD.

12. Registratorii RSD sânt persoanele responsabile (operator resurse umane) din cadrul organizațiilor publice în care activează subiecții declarării. La angajarea în câmpul muncii a subiecților declarațiilor, persoana responsabilă din cadrul direcției/secției resurse

umane al organizației va înregistra/modifica (în cazul când persoana se regăsește în baza de date) statutul angajatului organizației publice.

13. Utilizatorii RSD sânt:

1) *operator resurse umane* - persoane responsabile din cadrul organizațiilor publice în care activează subiecții declarării, care completează RSD (IDNP/IDNO, nume, prenume, funcția, actul juridic, data emiterii acestuia, adresa etc.) în modul stabilit de legislație.

2) *inspector de integritate* – angajat al ANI cu atribuții de vizualizare a datelor din RSD, în cadrul procedurilor/dosarelor de control atribuite în gestiune, generare de rapoarte specifice și perfectare a formularelor electronice privind actele de constatare emise în privința subiecților declarării.

3) *administrator de sistem* – angajatul Autorității sau o organizație – persoană contractată de Autoritate, care acordă suportul tehnic de administrare a acestuia;

4) *administrator tehnic* - Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, care asigură mentenanța, securitatea și dezvoltarea RSD ca parte componentă a SIA „e-Integritate”.

14. Registratorii Registrului sânt subdiviziunile resurse umane sau persoanele responsabile de evidenţa resurselor umane (în cazul lipsei subdiviziunii respective în autoritate) ale participanţilor la Registru. Fiecare registrator asigură introducerea în Registru a datelor relevante autorităţii pentru care efectuează evidenţa personalului (IDNP/IDNO, nume, prenume, funcția, actul juridic, data emiterii acestuia, adresa etc.) în conformitate cu metodologia/manualul prezentat de către posesorul Registrului. Angajaţii subdiviziunilor resurse umane au acces la informaţia aferentă autorităţii sale şi autorităţilor administartive din subordine.

15. Furnizor al datelor Registrului este persoana fizică sau persoana juridică de drept public, care livrează date despre obiectele informaţionale ale Registrului (cum ar fi: structura scriptică a autorităţilor administraţiei publice, funcţiile publice şi posturile existente în autoritate şi despre titularii acestora) în modul stabilit de lege sau acord. Furnizori ai datelor pentru Registru sânt autorităţile publice participante la Registru şi angajaţii acestor autorităţi.

16. Destinatar al datelor din Registru este persoana fizică sau juridică mandatată cu dreptul de a primi datele din Registru, conform legii sau acordului.

17. Posesorul are următoarele atribuții:

1) asigură condițiile organizatorice și financiare pentru funcționarea RSD;

2) stabilește scopurile și sarcinile funcționale ale RSD;

3) determină obiectele informaționale supuse înregistrării în RSD și conținutul acestora;

4) monitorizează procesul de înregistrare și prelucrare a datelor în RSD;

5) gestionează activitatea de exploatare și ținere a conținutului informațional al RSD;

6) asigură securitatea și protecția datelor din RSD 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 RSD;

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

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

10) monitorizează și, după caz, ajustează cerințele de securitate și conformitate a RSD 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 RSD ca parte componentă a SIA „e-Integritate".

18. Drepturile și obligațiile posesorului sunt stabilite în conformitate cu Legea nr. 467/2003 *cu privire la informatizare și la resursele informaționale de stat* și Legea nr. 132/2016 *cu privire la Autoritatea Națională de Integritate*.

19. Posesorul asigură păstrarea RSD 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.

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

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

22. Administratorul RSD 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 RSD ca parte componentă a SIA „e-Integritate";

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 RSD.

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

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

25. Administratorul tehnic al RSD 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".

26. Administratorul tehnic are următoarele atribuții:

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

2) asigură funcționarea RSD;

3) execută modificările/rectificările solicitate în demersurile primite referitoare la erorile de sistem ale RSD, erorile cauzate de factorul uman în RSD, incidentele de infrastructură care afectează funcționarea normală a RSD 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 RSD ca parte componentă a SIA „e-Integritate" și instituie activități de control menite să diminueze riscurile privind integritatea datelor RSD;

5) alte atribuții necesare asigurării bunei funcționări a RSD.

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

28. Activitatea administratorului tehnic se supune auditului extern.

29. Registratori ai RSD sunt persoanele autorizate ale Autorității, precum și persoanele responsabile (operator resurse umane) din cadrul organizațiilor publice în care activează subiecții declarării, precum și subiecții declarării.

30. Furnizorii datelor în RSD sunt organizațiile publice, care, prin intermediul operatorilor resurse umane, completează Registrul electronic al subiecților declarării averilor și a intereselor personale (IDNP/IDNO, nume, prenume, funcția, actul juridic, data emiterii acestuia, adresa etc.) în modul stabilit de legislație, precum și subiecții declarării, care completează declarația și o semnează electronic. Furnizorii datelor RSD sunt obligați să asigure corectitudinea și autenticitatea datelor prezentate pentru a fi introduse în sistem și actualizarea acestora în modul stabilit de legislație.

31. Furnizorul datelor din cadrul organizației publice are următoarele atribuții:

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

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

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

4) raportează posesorului problemele de funcționalitate ale RSD.

32. În calitate de furnizor de date în RSD, subiectul declarării are următoarele obligații:

1) să utilizeze RSD în conformitate cu Ghidul de utilizare pentru depunerea on-line a declarațiilor de avere și interese personale;

2) să nu permită accesul terților la contul său de utilizator și să nu divulge altor persoane neautorizate datele sale de acces;

3) să nu utilizeze sistemul în numele altor subiecți;

4) să asigure confidențialitatea datelor și a informațiilor de care ia cunoștință prin utilizarea RSD.

33. Destinatari ai datelor din RSD este Autoritatea și organizațiile publice, care, prin intermediul operatorilor resurse umane, care pot accesa datele din RSD, conform prevederilor legislației.

34. Utilizatorii din cadrul Autorității au următoarele atribuții:

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

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

3) asigură securitatea și confidențialitatea informației introduse în RSD;

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 RSD;

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

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

9) înaintează demersuri privind necesitatea de dezvoltare și îmbunătățire a SIA „e-Integritate”;

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

35. Furnizorii datelor din cadrul organizației publice vor completa câmpurile informaționale ale obiectelor informaționale vizând profilul persoanei – subiect al declarării și activitatea angajatului.

36. Câmpurile informaționale ale obiectelor vizând profilul persoanei și activitatea angajatului, de regulă, vor fi introduse și, respectiv, pre-populate în baza cheilor predefinite (IDNP și IDNO) din registrele de stat pertinente utilizând platforma de interoperabilitate MConnect.

37. Organizațiile publice desemnează în mod oficial utilizatori autorizați cu rol de operator resurse umane, să exercite funcții de înscriere, utilizare și procesare inclusiv de control intern al calității datelor înscrise în Registrul electronic al subiecților averii și intereselor personale. În cazul survenirii unor schimbări cu privire la utilizatorii autorizați desemnați, organizațiile publice sunt responsabile să informeze ANI oficial, în scris, despre numele și funcția persoane nou desemnate.

38. Persoana responsabilă de resursele umane din cadrul organizațiilor publice are drepturi de:

1) adăugare a noi subiecți în registru (doar cu privire la persoanele din cadrul organizației în care activează);

2) vizualizare a subiecților din registru (doar cu privire la persoanele din cadrul organizației în care activează);

3) modificare a informațiilor despre subiecți (doar cu privire la persoanele din cadrul organizației în care activează).

39. Persoana responsabilă de resursele umane din cadrul organizațiilor publice, sub sancțiunea răspunderii disciplinare, contravenționale sau, după caz, penale, are obligația de:

1) introducere doar a informației veridice în baza datelor obținute în procesul de lucru;

2) neadmitere a modificării, distrugerii şi/sau utilizării ilegale a datelor din sistem.

40. Sistemul ”E-Integritate” va ține cont de organizația din care face parte persoana responsabilă de resursele umane și va restricționa accesul la restul informațiilor din registru.

Capitolul IV
SPAȚIUL INFORMAȚIONAL AL SISTEMULUI INFORMATIC

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

1) Profilul persoanei (subiect al declarării);
2) Organizația;
3) Subdiviziunea organizației;
4) Activitatea angajatului;
5) Eveniment de gestiune a înregistrării.

42. Identificarea obiectelor în cadrul RSD se efectuează prin utilizarea numărului de identificare unic:

1) pentru „subiecții declarării averii și intereselor personale” – cheia combinată „denumirea organizației publice și IDNO-ul organizației publice”, „numele/prenumele și IDNP-ul persoanei fizice”;

2) pentru organizații – cheia combinată „denumirea organizației publice și IDNO-ul organizației publice”;

3) pentru subdiviziunile organizației – cheia combinată „denumirea organizației publice și IDNO-ul organizației publice”+„denumirea subdiviziunii”;

4) activitatea angajatului – „numele/prenumele și IDNP-ul persoanei fizice”+„denumirea funcției”+„actul ce atestă numirea în funcție”;

5) Eveniment de gestiune a înregistrării (eveniment) - cheia combinată „numele/prenumele și IDNP-ul persoanei fizice”+ „tipul evenimentului” +„data evenimentului”.

43. Datele Sistemului informatic reprezintă totalitatea de atribute ale obiectelor informaţionale şi includ:

1) date privind obiectul informaţional „profilul persoanei”:

a) Numele și prenumele
b) IDNP persoana
c) Seria, nr. buletinului de identitate
d) Viza de reședință
e) Starea civilă
f) Soț/Soție:
- Numele și prenumele
- IDNP
g) Copii minori
- Numele și prenumele
- Data și anul nașterii
- IDNP
h) Persoane aflate la întreținere
- Numele și prenumele
- Data și anul nașterii
- IDNP
i) Sex
j) Telefon fix
k) Telefon mobil
l) Email
m) Data creării
n) Data actualizării

2) date privind obiectul informaţional „Organizația”:

a) IDNO Organizației;
b) Denumirea Organizației;
c) Descrierea organizației
d) Date de contact;
e) Adresa;
f) Rechizite bancare;
g) Data creării;
h) Data actualizării.

3) date privind obiectul informaţional „Subdiviziunea Organizației”:

a) IDNO Organizației;
b) Denumirea Organizației;
c) Descrierea organizației
d) Denumirea Subdiviziunii;
e) Filiala;
f) Date de contact;
g) Adresa;
h) Rechizite bancare;
i) Data creării;
j) Data actualizării.

4) date privind obiectul informaţional „activitatea angajatului”:

a) Numele și prenumele
b) IDNP
c) Data angajării
d) IDNO Organizației;
e) Denumirea Organizației;
f) Subdiviziunea Organizației;
g) Funcția
h) Actul ce atestă numirea în funcție
i) Modificarea raportului de muncă
j) Data eliberării
k) Actul ce atestă eliberarea din funcție
l) Statutul angajatului în organizație
m) Transferat de la (IDNO Organizației)

5) date privind obiectul informaţional „eveniment”:

a) Evenimentul angajare/numire/alegere în funcție:
   - IDNP al subiectului declarațiilor
   - Data angajării
   - Funcția
   - Organizația
   - Ordinul de angajare

b) Evenimentul demisie/eliberare din funcție:
   - IDNP al subiectului declarațiilor
   - Data eliberării din funcție
   - Funcția
   - Organizația
   - Ordinul de eliberare

Capitolul V
INTEROPERABILITATEA CU ALTE SISTEME INFORMAȚIONALE

44. Pentru asigurarea actualizării operative şi automate a conţinutului informaţional al Registrului cu informaţie veridică este realizată interacţiunea şi sincronizarea datelor cu următoarele sisteme informaţionale automatizate de importanţă statală:

1) "Registrul de stat al unităţilor de drept" pentru accesul la datele aferente tuturor unităţilor de drept din Republica Moldova;

2) "Registrul de stat al populaţiei" pentru accesul la datele aferente tuturor persoanele fizice rezidente şi documentate în Republica Moldova.

45. În baza numărului de identificare de stat al autorităţii publice (IDNO) din "Registrul de stat al unităţilor de drept" se importă automat date despre autoritatea publică (denumirea, data creării, adresa juridică, data lichidării).

46. Datele despre profilul persoanei indicate în punctul 39, lit.a) a prezentului Regulament sunt preluate automat din „Registrul de Stat al Populaţiei".

47. Pentru asigurarea corectitudinii datelor importate din Registrele de Stat a Populaţiei şi a Unităţilor de Drept periodic se efectuează reînnoirea acestor date.

48. Pentru asigurarea interoperabilităţii cu alte sisteme informaţionale departamentale se utilizează serviciile WEB furnizate de Registru.

Capitolul VI
ŢINEREA ȘI ASIGURAREA FUNCȚIONĂRII RSD

49. Registrul este ţinut în formă electronică.

50. Registrul se implementează de către autorităţile publice, în care activează subiecți ai declarării care cad sub incidenţa art.3 alin.(1) din Legea nr.133/2016 privind declararea averii și a intereselor personale.

51. În procesul de exploatare a Registrului se formează resursa informaţională, care reprezintă totalitatea informaţiei sistematizate despre angajații organizațiilor publice, subiecți ai declarării averii și intereselor personale.

52. Sistemul elaborat permite ţinerea Registrul în limba de stat.

53. Fiecare autoritate publică participantă la Registru desemnează şi coordonează cu deţinătorul registratorii - persoanele cu atribuţii de introducere nemijlocită a datelor în baza de date. Aceste persoane sânt angajaţii subdiviziunii resurse umane sau persoane responsabile de evidenţa personalului care au acces la dosarele personale ale angajaţilor.

54. Introducerea informației în Registru se efectuează de către registratori în baza conţinutului dosarelor personale ale angajaţilor şi altor documente relevante ale participanţilor la Registru.

55. Pentru a putea înregistra date în Registru toţi registratorii care sânt angajaţi a subdiviziunilor resurse umane trebuie să fie înregistraţi de către administratorul sistemului primind un nume şi o parolă iniţială pentru a avea acces la Registru. Parola poate fi schimbată de registrator. În caz de angajare a persoanelor noi în serviciul resurse umane, aceste persoane la fel se înregistrează de către administratorul central al sistemului.

56. Evidenţa obiectelor informaţionale se ţine conform Ghidului de utilizare a Registrului, care conţine instrucţiuni clare de introducere, modificare şi vizualizare a datelor în baza de date, elaborat în cadrul procesului de dezvoltare a Registrului şi pus la dispoziţia participanţilor la Registru.

57. Conturile de acces pentru toţi utilizatorii Registrului se creează de către administratorul sistemului la necesitate. Fiecărui utilizator i se atribuie un identificator/nume de utilizator şi o parolă pentru a avea acces la Registru.

58. Accesul la resursele Registrului 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 autenticităţii utilizatorului conectarea la Registru nu se permite.

59. Datele din Registru fac parte din categoria datelor cu caracter personal. Asigurarea securităţii, confidenţialităţii şi integrităţii datelor prelucrate în cadrul Registrului se efectuează cu respectarea strictă a cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale, aprobate prin legislaţie.

60. Pentru asigurarea funcţionării eficiente şi neîntrerupte a Registrului, schimbul

informaţional de date între participanţii la Registru şi baza de date este asigurat în regim nonstop.

61. Funcţionarea Registrului este suspendată de către administratorul de sistem sau de administratorul tehnic al Registrului în următoarele cazuri:

1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software şi hardware ale Registrului;

2) la apariţia circumstanţelor de forţă majoră;

3) la încălcarea cerinţelor sistemului securităţii informaţiei, dacă aceasta prezintă pericol pentru funcţionarea Registrului.

62. Lucrările profilactice în complexul de mijloace software şi hardware se efectuează după notificarea în scris a participanţilor cu cel puţin 2 zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora.

63. În cazul apariţiei circumstanţelor de forţă majoră, precum şi a dificultăţilor tehnice în funcţionarea complexului de mijloace software şi hardware a Registrului din vina terţelor persoane, este posibilă suspendarea funcţionării Registrului cu notificarea ulterioară a participanţilor conectaţi.

64. Revocarea dreptului de acces la Registru pentru utilizatorii participanţilor se efectuează în una dintre următoarele situaţii:

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 atribuţii nu impun accesul la datele din Registru;

4) la constatarea încălcării de către utilizatorul participantului a sistemului securităţii informaţionale a Registrului.

Capitolul VII
ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI

65. Datele din RSD fac parte din categoria datelor care necesită a fi protejate. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul RSD 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.

66. Măsurile de protecție și securitate a datelor din RSD, 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.

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

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

69. Utilizatorii interni desemnează o persoană, subordonată nemijlocit conducătorului instituției, responsabilă de implementarea și monitorizarea respectării prevederilor normelor de securitate informațională.

70. 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.

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

Capitolul VIII
CONTROLUL ȘI RESPONSABILITATEA

72. Ținerea RSD, ca parte componentă a SIA „e-Integritate”, este supusă controlului intern și extern. Controlul intern privind organizarea și funcționarea RSD se efectuează de către posesor. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea RSD se efectuează de către instituții abilitate și certificate în domeniul auditului.

73. Responsabilitatea pentru organizarea funcționării RSD aparține posesorului și deținătorului acestuia.

74. Utilizatorii în atribuțiile cărora intră ținerea RSD, introducerea datelor, furnizarea informațiilor și asigurarea funcționării RSD poartă răspundere personală, în conformitate cu legislația, pentru completitudinea, autenticitatea, veridicitatea, integritatea informației, precum și pentru păstrarea și utilizarea ei.

75. Toți subiecții RSD 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.

76. Pentru asigurarea funcționalității eficiente și neîntrerupte a RSD, schimbul informațional de date RSD este asigurat în regim non-stop.

77. Funcționarea RSD, 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 RSD sau 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.

78. În cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SIA „e-Integritate” din vina terților persoane, este posibilă suspendarea funcționării RSD ca parte componentă a SIA „e-Integritate”, cu informarea subiecților RSD prin mijloacele tehnice disponibile.