*Proiect*

#### **GUVERNUL REPUBLICII MOLDOVA**

#### **HOTĂRÂRE nr. \_\_\_\_\_\_\_**

#### **din \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024**

#### **pentru aprobarea** **Conceptului Sistemului informațional integrat automatizat al Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului și a Regulamentului privind modul de ținere a resursei** **informaționale formată de Sistemul informațional integrat automatizat al Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului**

În conformitate cu prevederile art. 2, alin. (1) și art. 16, alin. (1) din Legea nr. 71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314), art. 22, lit. c) și d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), Guvernul

**HOTĂRĂŞTE**:

1. Se instituie Sistemul informațional integrat automatizat al Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului.
2. Se aprobă:
3. Conceptul Sistemului informațional integrat automatizat al Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului, conform anexei nr. 1;
4. Regulamentul privind modul de ținere a resursei informaționale formată de Sistemul informațional integrat automatizat al Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului, conform anexei nr. 2.
5. Se desemnează Instituția Publică Organizația pentru Dezvoltarea Antreprenoriatului în calitate de posesor și deținător al Sistemului informațional integrat automatizat al Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului.
6. Instituirea, dezvoltarea, întreținerea și asigurarea funcționării Sistemului informațional integrat automatizat al Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului se realizează din contul și în limita mijloacelor financiare aprobate anual în bugetul Ministerului Dezvoltării Economice și Digitalizării, precum și din alte surse prevăzute de legislație.
7. Realizarea prevederilor prezentei hotărâri se va efectua din contul și în limitele mijloacelor financiare prevăzute în bugetul de stat și altor mijloace, precum și din contul asistenței externe.
8. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Dezvoltării Economice și Digitalizării.

**PRIM-MINISTRU** **DORIN RECEAN**

**Contrasemnează:**

**Viceprim-ministru,**

**ministrul dezvoltării**

**economice și digitalizării Dumitru ALAIBA**

Anexa nr. 1 la Hotărârea Guvernului

nr.\_\_\_\_ 2024

**Conceptul**

**Sistemului informațional integrat automatizat al Instituției Publice**

**Organizația pentru Dezvoltarea Antreprenoriatului**

**Capitolul I**

**INTRODUCERE**

Instituția Publică Organizația pentru Dezvoltarea Antreprenoriatului (IP ODA) are misiunea de a implementa politica statului privind susținerea dezvoltării afacerilor, inclusiv a întreprinderilor mici și mijlocii, conform strategiilor și programelor aprobate de Guvern. În acest sens, IP ODA implementează o serie de programe care urmăresc: (i) oferirea de consultanță, instruire și mentorat pentru îmbunătățirea capacităților de administrare a afacerilor; (ii) acordarea de suport financiar nerambursabil pentru anumite categorii de antreprenori sau anumite proiecte investiționale; și (iii) facilitarea accesului la finanțare prin emiterea de garanții la credite, compensarea ratei dobânzii sau acordarea de finanțări pe termen lung.

Pentru a spori eficiența și calitatea, precum și pentru a facilita procesul de interacțiune dintre părțile implicate în implementarea programelor de stat, este necesară crearea, adaptarea și implementarea unui sistem informațional de management al proceselor interne ale IP ODA. Implementarea unui sistem informațional în activitatea aferentă acestor procese va contribui pe de o parte la optimizarea procedurilor administrative aferente acordării suportului, iar pe de altă parte va permite efectuarea monitorizării, evidența, raportarea statistică și analitică cu o mai mare eficacitate și eficiență.

În acest context, reieșind atât din situația de fapt, cât din prevederile cadrului normativ privind întreprinderile mici și mijlocii, se prefigurează necesitatea adoptării unei decizii privind crearea și implementarea Sistemului informațional integrat automatizat al Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului (în continuare – SIIA ODA).

**Capitolul II**

**DISPOZIȚII GENERALE**

1. Conceptul SIIA ODA (în continuare – Concept) stabilește scopurile, sarcinile și funcțiile sistemului, structura organizațională și cadrul normativ necesare creării și exploatării lui, obiectele informaționale și lista datelor care se păstrează în sistem, infrastructura tehnologică și măsurile de asigurare a securității și protecției informației, precum și măsurile legate de crearea, implementarea, exploatarea și menținerea sistemului.
2. SIIA ODA reprezintă totalitate de resurse şi tehnologii informaționale interdependente, de metode și de personal, destinat optimizării proceselor operaționale, sporirii eficienței instituționale și consolidării capacității de asigurare a înregistrării, păstrării, prelucrării, furnizării și utilizării informației și formării resursei informaționale în scopul facilitării accesului la finanțare.
3. Noțiunile utilizate în prezentul Concept, dacă nu este definit altfel, au semnificațiile prevăzute în Legea nr.179/2016, cu privire la întreprinderile mici și mijlocii și Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat.
4. Obiectivele SIIA ODA sunt:
5. crearea resursei informaționale în vederea generării, procesării, păstrării și securizării datelor precum și schimbului de date în limita sarcinilor IP ODA;
6. eficientizarea procesului solicitării resurselor și informațiilor de către solicitanții și beneficiari a asistenței IP ODA, inclusiv referitor la etapele de examinarea acestora;
7. diminuarea erorilor umane în introducerea și prelucrarea datelor;
8. facilitarea și eficientizarea controlului informației primare introduse de Solicitanți;
9. crearea unui cadru de interoperabilitate între SIIA ODA și sistemele informatice externe furnizoare și consumatoare de date.
10. Principiile de creare a SIIA ODA sunt următoarele:
    * 1. Principiul legalității - presupune crearea și exploatarea sistemului în conformitate cu legislația națională, a normelor și standardelor internaționale recunoscute în domeniu;
      2. Principiul divizării arhitecturii pe nivele - proiectarea independentă a componentelor sistemului în conformitate cu standardele de interfață dintre nivele;
      3. Principiul datelor sigure - introducerea datelor în sistem doar prin canalele autorizate și autentificate;
      4. Principiul securității informaționale - asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și de acces nesancționat;
      5. Principiul modularității - proiectarea și dezvoltarea sistemului fără modificarea componentelor create anterior, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicații;
      6. Principiul expansibilității - posibilitatea extinderii și completării sistemului informatic cu noi funcții sau îmbunătățirea celor existente;
      7. Principiul scalabilității - asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării SIIA ODA;
      8. Principiul simplității și comodității utilizării - proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor sistemului, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție;
      9. Principiul integrității, plenitudinii și veridicității datelor - implementarea mecanismelor care permit păstrarea conținutului și interpretării univoce a datelor în condițiile unor influențe accidentale și eliminării fenomenelor de denaturare sau lichidare accidentală a acestora, furnizarea unui volum de date suficient executării funcțiilor de business al sistemului informatic și asigurarea unui grad înalt de corespundere a datelor cu starea reală a obiectelor pe care le reprezintă și care fac parte dintr-un sector concret al sistemului informatic.
11. Sarcinile de bază ale SIIA ODA sunt:
    * 1. automatizarea și digitalizarea proceselor;
      2. asigurarea interopabilității și schimbului de date între sistemele existente;
      3. formarea bazei de date, inclusiv prin importul datelor istorice;
      4. înregistrarea, actualizarea, controlul şi analiza informației cu privire la obiectele și subiecții suportului oferit de IP ODA;
      5. colectarea și formarea informației statistice
      6. colectarea și procesarea indicatorilor de impact.

**Capitolul III**

**CADRUL NORMATIV-JURIDIC**

1. Cadrul normativ-juridic aferent SIIA ODA este constituit din legislația națională, tratatele şi convențiile internaționale la care Republica Moldova este parte, precum şi de prevederile prezentului Concept.
2. Crearea și funcționarea SIIA ODA este reglementată de următoarele acte legislative și normative:
3. Legea nr. 845/1992 cu privire la antreprenoriat și întreprinderi;
4. Legea nr. 548/1995 cu privire la Banca Națională a Moldovei;
5. Legea nr. 1069/2000 cu privire la informatică;
6. Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;
7. Legea nr. 71/2007 cu privire la registre;
8. Legea nr. 133/2011 privind protecția datelor cu caracter personal;
9. Legea nr.124/2022 privind identificarea electronică și serviciile de încredere;
10. Legea nr. 179/2016 cu privire la întreprinderile mici și mijlocii;
11. Legea nr.202/2017 privind activitatea băncilor;
12. Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;
13. Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;
14. Hotărârea Guvernului nr. 487/2022 cu privire la organizarea și funcționarea Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului;
15. Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;
16. Hotărârea Guvernului nr. 546/2011 privind aprobarea Regulamentului cu privire la acordarea serviciilor Sistemului de telecomunicații al autorităților administrației publice și operarea modificărilor în unele hotărâri ale Guvernului;
17. Hotărârea Guvernului nr. 710/2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare) ;
18. Hotărârea Guvernului nr.329/2012 cu privire la Serviciul Guvernamental de Plăți Electronice (MPay);
19. Hotărârea Guvernului nr. 656/2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate;
20. 20) Hotărârea Guvernului nr.712/2020 cu privire la serviciul guvernamental de plăți electronice (MPay);
21. Hotărârea Guvernului nr.1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
22. Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
23. Hotărârea Guvernului nr. 404/2014 cu privire la pilotarea platformei de interoperabilitate;
24. Hotărârea Guvernului nr.405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
25. Hotărârea Guvernului nr. 700/2014 pentru aprobarea Concepției privind principiile datelor guvernamentale deschise ;
26. Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog) ;
27. Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;
28. Hotărârea Guvernului nr. 1141/2017 pentru aprobarea Regulamentului privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcționarii persoanelor juridice de drept public în cadrul circulației electronice a acestora;
29. Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;
30. Hotărârea Guvernului 211/2019 privind platforma de interoperabilitate (Mconnect);
31. Hotărârea Guvernului 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);
32. Hotărârea Guvernului nr.375/2020 pentru aprobarea Conceptului Sistemului informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) și a Regulamentului privind modul de ținere a Registrului împuternicirilor de reprezentare în baza semnăturii electronice;
33. Hotărârea Guvernului nr. 712/2020 cu privire la serviciul guvernamental de plăți electronice (MPay);
34. Hotărârea Guvernului nr.153/2021 pentru aprobarea Conceptului Sistemului informațional „Registrul resurselor și sistemelor informaționale de stat” și a Regulamentului privind modul de ținere a Registrului resurselor și sistemelor informaționale de stat;
35. Hotărârea Guvernului nr. 491/2022 cu privire la aprobarea modului de recunoaștere a semnăturilor electronice calificate create utilizând un certificat calificat al cheii publice eliberat de un prestator de servicii de încredere dintr-un stat membru al Uniunii Europene;
36. Hotărârea Guvernului nr. 184/2023 pentru aprobarea Regulamentului privind activitatea prestatorilor de servicii de încredere calificați;
37. Reglementarea tehnică Procesele ciclului de viață al software-lui RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78 din 1 iunie 2006.
38. Programele de stat privind susținerea dezvoltării întreprinderilor mici și mijlocii;
39. Manualele operaționale aprobate de IP ODA, care prevăd mecanismul de primire, procesare, evaluare, aprobare, implementare, monitorizare și analiză de impact.
40. Standardele TIC și standardele relevante pentru SIIA ODA sunt următoarele:

SM ISO/CEI 12207:2014 – ,,Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului”;

SM SR ISO 15489-1:2012 – Informare și documentare. Managementul înregistrărilor. Partea 1: Generalități;

SM ISO/CEI/IEEE 15288:2015 – „Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului”;

SM ISO/IEC 27001:2023 – Securitatea informației, securitatea cibernetică și protecția confidențialității. Sisteme de management al securității informației. Cerințe;

SM EN ISO/IEC 27002:2022 – Securitatea informației, securitatea cibernetică și protecția vieții private. Mijloace de control al securității informației;

SM ISO 14641:2018 – Managementul documentelor electronice. Proiectarea și exploatarea sistemului informațional de stocare a documentelor electronice. Specificații;

SM EN ISO/IEC 15408-1:2022 – Securitatea informației, securitatea cibernetică și protecția datelor personale. Criterii de evaluare a securității IT. Partea 1: Introducere și model general;

SM EN ISO/IEC 15408-2:2022 – Securitatea informației, securitatea cibernetică și protecția datelor personale. Criterii de evaluare a securității IT. Partea 2: Componente funcționale de securitate;

SM ISO/IEC 15408-3:2022 – Securitatea informației, securitatea cibernetică și protecția datelor personale. Criterii de Evaluare a securității IT. Partea 3: Componente de asigurare a securității;

Recomandările W3C (http://validator.w3.org) privind testarea paginilor WEB;

Standardul SDMX (Statistical data and metadata exchange standard –[http://sdmx.org](http://sdmx.org/));

SM ISO/IEC 11179-1:2023 Tehnologia informației. Registre de metadate (MDR). Partea 1: Structura”.

**Capitolul IV**

**SPAȚIUL FUNCȚIONAL AL SIIA ODA**

1. Funcțiile de bază ale SIIA ODA sunt formarea spațiului informațional în baza atribuțiilor si sarcinilor IP ODA precum urmează:
2. procesul de formare a bazei de date a SIIA ODA constă în înregistrarea, stocarea și procesarea datelor informaționale;
3. asigurarea nivelul de acces în corespundere cu criteriile setate;
4. asigurarea securității și protecției datelor;
5. asigurarea calității informației;
6. asigurarea interoperabilității și a schimbului de date cu alte sisteme și resurse informaționale de stat, private precum și cu alte sisteme informaționale;
7. alte funcționalități de administrare.
8. formarea și actualizarea bazei de date;
9. asigurarea informațională a autorităților abilitate cu verificarea și controlul resurselor financiare.
10. În cadrul funcționării SIIA ODA se realizează funcții specifice, grupate în următoarele contururi funcționale:
11. Conturul destinat persoanelor fizice și persoanelor juridice, care va include următoarele funcționalități:
    1. perfectare și depunere online a cererilor individuale de suport pentru instruiri, acces la finanțare și alte tipuri de suport oferite prin intermediul IP ODA;
    2. istoricul depunerilor online;
    3. componenta de prezentare a actelor justificative privind valorificarea suportului acordat.
    4. componenta de autoevaluare a față de criteriile de eligibilitate față de programele de stat;
    5. componenta de interopabilitate cu datele din alte resurse informaționale de stat pentru autocompletarea cu informațiile relevante;
    6. componenta de procesare și evaluare a dosarelor cererilor individuale;
    7. componenta de generare a rapoartelor implementarea programelor de stat;
    8. cabinetul personal al utilizatorului autorizat;
    9. interacțiunea online cu entitățile financiare partenere;
    10. componenta de notificare și interacțiune.
12. Conturul destinat angajaților IP ODA, care va include următoarele funcționalități:
    1. componenta destinată gestiunii profilurilor prin intermediul căreia va fi posibilă crearea profilurilor, vizualizarea și gestiunea lor;
    2. componenta destinată configurării tipurilor de suport oferit de IP ODA;
    3. componenta destinată gestiunii și evidenței resurselor financiare a IP ODA;
    4. componenta destinată înregistrării și repartizării spre aprobare a cererilor conform domeniilor de activitate IP ODA;
    5. componenta destinată analizei cererilor de acces la finanțare;
    6. componenta de interopabilitate cu alte resurse informaționale de stat pentru extragerea automatizată a datelor despre solicitanți.
    7. componenta destinată convocării comisiilor/grupurilor de lucru interne ale I.P.ODA, care se expun asupra oportunității emiterii deciziilor de finanțare;
    8. componenta de comunicare cu persoanelor fizice, persoanelor juridice și entităților financiare partenere de suport antreprenorial;
    9. componenta de completare a informațiilor, conținutul datelor corespund cerințelor stabilite, după caz codificate, doar câmpurile relevante pentru tipul de raportare sunt incluse în obiectele informaționale;
    10. afișarea statutului procesării datelor, ce reprezintă posibilitatea de a vizualiza în timp real etapele procesării datelor;
    11. componenta de generare și configurare a rapoartelor privind domeniile de activitate;
    12. elaborarea documentelor de planificare;
    13. componenta de căutare, actualizarea, reutilizarea, salvarea, anularea și radierea obiectelor informaționale;
    14. cabinetul personal al funcționarului IP ODA;
    15. componenta de generare a raportului de impact privind implementarea programelor de stat.
13. Conturul destinat entităților financiare partenere, care va include următoarele funcționalități:
    1. perfectare și depunere online a cererilor individuale de suport oferite beneficiarilor prin intermediul IP ODA;
    2. istoricul depunerilor online;
    3. componenta de prezentare a actelor justificative privind valorificarea suportului acordat;
    4. componenta de autoevaluare a față de criteriile de eligibilitate față de programele de stat.
    5. componenta de procesare și evaluare a dosarelor cererilor individuale;
    6. componenta de generare a rapoartelor privind implementarea programelor de stat;
    7. componenta de raportare de către entitățile financiare partenere;
    8. cabinetul personal al utilizatorului autorizat;
    9. componenta de notificare și interacțiune.
14. Conturul de evidență automatizată a dosarelor obiectelor și subiecților impunerii, cu următoarele funcții:
    1. evidența obiectelor impunerii;
    2. evidența subiecților impunerii;
    3. evidența plăților efectuate;
    4. evidența stingerii obligațiunilor;
    5. componenta de generare a raportului de impact privind implementarea programelor de stat.
15. Conturul de prezentare a informației privind obiectele și subiecții impunerii, autorităților abilitate pentru efectuarea verificării și controlului programului de stat cu următoarele funcții:
    1. prezentarea informației în mod electronic în regim automatizat;
    2. prezentarea informației în mod electronic, la solicitare;
    3. gestionarea interfeței programatice pentru prezentarea automatizată a informației;
    4. gestionarea interfeței web pentru accesarea informației de utilizatori autorizați.
16. Conturul de administrare a sistemului, care asigură următoarele funcții specifice:
    1. administrarea sistemului;
    2. jurnalizarea evenimentelor de sistem;
    3. gestionarea copiilor de rezervă;
    4. gestionarea șabloanelor de documente ale sistemului;
    5. gestionarea clasificatoarelor și nomenclatoarelor sistemului;
    6. monitorizarea performanței sistemului;
    7. asigurarea integrității datelor;
    8. gestionarea utilizatorilor;
    9. asigurarea securității şi protecției informației în sistem.
17. Conturul destinat Ministerului Dezvoltării Economice și Digitalizării, care va include următoarele funcționalități:
    1. prezentarea informației în mod electronic în regim automatizat;
    2. prezentarea informației în mod electronic, la solicitare;
    3. gestionarea interfeței programatice pentru prezentarea automatizată a informației;
    4. gestionarea interfeței web pentru accesarea informației de utilizatori autorizați;
    5. extragerea automatizată a analizelor de impact;
18. În vederea realizării funcțiilor SIIA ODA, acesta va interacționa cu sistemele și resursele informaționale indicate la pct. 46.
19. Ca rezultat a implementării SIIA ODA va fi optimizat procesul de interacțiune dintre părțile implicate în solicitare, examinare, emitere, monitorizare, executare și recuperare de către IP ODA a tuturor tipurilor de suport destinat mediului antreprenorial. Implementarea acestor procese va contribui pe de o parte la optimizarea procedurilor administrative aferente implementării programelor de stat, iar pe de altă parte va permite efectuarea monitorizării, evidența, raportarea statistică și analitică cu o mai mare eficacitate și eficiență.

**Capitolul V**

**STRUCTURA ORGANIZAȚIONALĂ A SIIA ODA**

1. Proprietarul SIIA ODA este statul.
2. Posesor și deținător al SIIA ODA este IP ODA.
3. Registratorii datelor în SIIA ODA sunt IP ODA, entitățile financiare partenere, întreprinderi, asociații și alte entități la necesitate.
4. Furnizorul de date este persoana fizică sau persoana juridică de drept public sau de drept privat furnizoare de date aferente obiectelor informaționale ale SIIA ODA.
5. Furnizorii datelor SIIA ODA externi sunt:

Registrul de stat al populației și Registrul de stat al unităților de drept conțin date despre persoanele fizice și juridice, iar accesul la acestea este oferit in următoarele cazuri:

pentru verificarea IDNO sau IDNP la momentul înregistrării și verificarea statutului curent al acestora;

pentru verificarea afilierii solicitanților de proiecte investiționale;

datele privind istoricul modificărilor fondatorilor și administratorilor;

datele privind rudele de gradul I (soț/ soție, părinți / copii) și ce afaceri dețin;

datele privind persoana juridică și dacă este plătitor de accize;

1. Registrul fiscal de stat despre:

sumele accizelor și impozitelor calculate și achitate de agenții economici;

conturile bancare ale persoanei juridice;

restanțele persoanei juridice față de Bugetul Public Național, vânzările lunare ale companiei;

Impozite și taxe achitate detaliate pe tipuri;

Contribuțiile sociale ale angajatorului;

Datele cu referire la plățile achitate salariaților și altor persoane fizice;

1. Registrul bunurilor imobile (e-cadastru) conține înscrieri privind fiecare bun imobil, dreptul de proprietate și alte drepturi patrimoniale, titularii de drepturi, documentele ce confirma drepturile, tranzacțiile cu bunuri imobile și alte temeiuri ale nașterii, modificării, grevării și stingerii drepturilor.
2. Date despre procesele de judecată de pe Portalul Național al Instanțelor de Judecată;
3. Date de la Biroul Național de Statistică (rapoartele financiare și cele statistice pe care le prezintă compania, preponderent sunt necesare cele legate de câștigurile salariale);
4. Acte permisive eliberate companiei și perioada de valabilitate;
5. Mărci comerciale înregistrate și perioada de valabilitate;
6. Alte date relevante procesului de evaluare, aprobare și monitorizare a solicitanților.
7. Destinatarul datelor din SIIA ODA sunt angajații IP ODA, persoanele fizice și juridice care sunt mandatate conform legislației, să primească datele conținute în SIIA ODA.
8. Administratorul tehnic al SIIA ODA este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică” care își exercită atribuțiile în conformitate cu cadrul normativ care reglementează domeniul administrării tehnice și menținerii sistemelor informaționale de stat.

**Capitolul VI**

**DOCUMENTELE SISTEMULUI**

1. Documentele utilizate de sistem sunt clasificate în următoarele grupuri:

documente de intrare, care constau din:

* 1. șabloane de date;
  2. documente generate de sistem;
  3. documente scanate în format PDF.

documente de ieșire, care constau din:

a) decizii de acceptare/respingere a datelor transmise;

b) notificări adresate furnizorilor de date.

c) rapoartele, statisticile și indicatorii de performanță agregate privind utilizarea sistemului, vizualizarea utilizatorilor conectați la SIIA ODA, precum și a utilizatorilor activi sau inactivi.

3) documente tehnologice, care constau din:

a) notificări ale sistemului privind solicitarea procesării datelor;

b) notificări ale sistemului privind finalizarea procesării datelor;

c) notificări ale sistemului privind modificarea statutelor datelor transmise;

d) documentele ce conțin înregistrări de audit privind acțiunile utilizatorilor;

e) rapoartele.

4) documente interne, care constau din:

a) șabloane de date;

b) documente scanate în format PDF;

c) documente interne generate de sistem;

d) notificări ale sistemului modificarea datelor în sistem.

**Capitolul VII**

**SPAŢIUL INFORMAŢIONAL AL SISTEMULUI**

**Secțiunea 1**

**Obiectele informaționale gestionate de sistem**

1. Resursa informațională a SIIA ODA este reprezentată de un ansamblu de obiecte informaționale de bază. Obiectele informaționale reprezintă totalitatea de date care le caracterizează și sunt determinate în funcție de destinația acestora, incluzând următoarele:
2. profilul solicitantului, beneficiarului sau a reprezentantului legal;
3. utilizator autorizat;
4. sursă de finanțare;
5. conținutul și structura planului de acțiuni;
6. indicator;
7. raportare a progresului planului de acțiuni;
8. document;
9. sarcină;
10. proiectul de finanțare a beneficiarului.
11. Profilul solicitantului, beneficiarului sau a reprezentantului legal – obiect informațional cu următoarele atribute:
12. denumirea solicitantului, beneficiarului sau a reprezentantului legal (date împrumutate din Registrul de stat al unităților de drept (în continuare – RSUD);
13. codul unic de identificare a solicitantului, beneficiarului sau a reprezentantului legal (IDNO) (date împrumutate din RSUD);
14. Cod CAEM;
15. nume, prenume, IDNP a administratorului și asociaților solicitantului, beneficiarului sau a reprezentantului legal, sexul și anul nașterii a acestora (date împrumutate din Registrul de stat al populației (în continuare – RSP);
16. date de contact (număr de telefon și adresa de Email);
17. adresa (raionul/municipiul, localitatea, strada, casa, blocul, apartamentul, cod poștal).
18. Utilizator – obiect informațional cu următoarele atribute:
19. nume, prenume, IDNP;
20. date de contact (număr de telefon și adresa de Email);
21. rolurile atribuite în SIIA ODA;
22. subdiviziunea/entitatea juridică pe care o reprezintă;
23. drepturi de acces la datele SIIA ODA;
24. statutul curent al profilului (activ/inactiv);
25. alte date relevante.
26. Sursă de finanțare – obiect informațional cu următoarele atribute:
27. identificatorul sursei de finanțare;
28. tipul sursei de finanțare;
29. denumirea categoriei de sursă de finanțare;
30. bugetul sursei de finanțare;
31. referința la clasificația sursei de finanțare (conform clasificației bugetare);
32. perioada de accesibilitate a sursei de finanțare.
33. Conținutul și structura Planului de acțiuni (obiective generale, obiective specifice, acțiuni etc.) – obiect informațional cu următoarele atribute:
34. identificatorul categoriei de structură;
35. tipul categoriei de structură;
36. titlul categoriei de structură;
37. descrierea categorie de structură;
38. sursa de finanțare;
39. riscurile de implementare;
40. impactul planificat;
41. perioada de implementare a categoriei de structură;
42. indicatorul de raportare progres/șablon de raportare progres ce urmează a fi utilizat;
43. periodicitatea de raportare a progresului de implementare;
44. costul total de implementare planificat;
45. costul efectiv;
46. progresul implementat;
47. documente atașate categoriei de structură;
48. notă;
49. statutul;
50. referință la categoria ierarhic superioară;
51. alte tipuri de date, după caz.
52. Indicator – obiect informațional cu următoarele atribute:
53. identificatorul indicatorului;
54. denumirea indicatorului;
55. tipul indicatorului;
56. valoarea țintă finală a indicatorului;
57. valorile țintă intermediare ale indicatorului;
58. valoarea de referință a indicatorului;
59. unitatea de măsură a indicatorului;
60. sursa/modalitatea de calculare a datelor despre valoarea indicatorului;
61. statutul indicatorului.
62. Raportarea progresului acțiunii – obiect informațional cu următoarele atribute:
63. identificatorul raportului de progres;
64. data expedierii raportului de progres;
65. formularul electronic de raportare completat (completat conform indicatorului);
66. semnătura electronică a raportorului;
67. autoritatea publică raportoare;
68. utilizatorul autorizat raportor;
69. statutul raportului de progres.
70. Document – obiect informațional cu următoarele atribute:
71. identificatorul documentului;
72. tipul documentului;
73. formatul documentului;
74. emitentul documentului;
75. conținutul documentului;
76. semnătura electronică a emitentului documentului;
77. referință către obiectul informațional la care se referă (plan de acțiuni, tabel de concordanță, act normativ, angajament);
78. statutul documentului.
79. Sarcină - obiect informațional cu următoarele atribute:
80. identificatorul sarcinii;
81. executantul sarcinii;
82. termenul limită de executare a sarcinii;
83. detalii despre sarcină (în contextul fluxurilor de lucru de gestiune a planurilor de acțiuni sau armonizare a legislației);
84. statutul sarcinii.
85. Proiectul de finanțare a solicitantului, beneficiarului sau a reprezentantului legal- obiect informațional cu următoarele atribute:
86. codul de identificare a proiectului de finanțare a solicitantului, beneficiarului sau a reprezentantului legal;
87. IDNO al solicitantului, beneficiarului sau a reprezentantului legal;
88. IDNP al solicitantului, beneficiarului sau a reprezentantului legal;
89. denumirea solicitantului, beneficiarului sau a reprezentantului legal;
90. datele de contact ale solicitantului, beneficiarului sau a reprezentantului legal;
91. planificarea bugetului;
92. tipul de finanțare solicitat;
93. valoarea finanțării solicitată;
94. contribuția solicitantului, beneficiarului sau a reprezentantului legal;
95. valoarea finanțării aprobate;
96. perioada/termenul de finanțare;
97. termenul debursării finanțării;
98. valoarea finanțării achitate;
99. valoarea angajamentului de finanțare;
100. condiții de finanțare;
101. măsurile din cadrul programelor de suport;
102. datele bancare (IBAN, BIC, denumirea băncii).
103. statutul dosarului (depus/în procesare/în evaluare/spre aprobare/în implementare/în monitorizare/arhivat).

**Secțiunea a 2-a**

**Scenariile de bază aferente obiectelor informaționale**

1. Scenariile referitoare la profilul solicitantului, beneficiarului sau a reprezentantului legal:

Punerea la evidență inițială:

* 1. extragerea informației despre solicitant prin intermediul platformei de interoperabilitate (Mconnect) din RSUD și RSP;
  2. completarea profilului cu identificatoarele obiectului.

1. Actualizarea la necesitate a datelor obiectului;
2. Radierea din evidență.
3. Scenariile referitoare la obiectul informațional „Utilizator autorizat”:
4. înregistrarea primară – de către administratorul de sistem, de către utilizatorul autorizat al autorității publice cu rol de gestiune a conturilor utilizatorilor autorității publice sau, în mod automat, de către SIIA ODA în cazul autentificării în interfața publică. O parte din valorile atributelor se preiau, în mod automat, din (MPass);
5. actualizarea datelor – de către administratorul de sistem, la modificarea datelor despre utilizator sau rolul acestuia în cadrul SIIA ODA, de către utilizatorul autorizat al autorității publice cu rol de gestiune a conturilor utilizatorilor autorității publice sau de către SIIA ODA în cazul recepționării datelor actualizate din (MPass);
6. scoaterea din evidență – de către administratorul de sistem sau de către utilizatorul autorizat al autorității publice cu rol de gestiune a conturilor utilizatorilor autorității publice (scoaterea din evidență presupune dezactivarea contului utilizatorului).
7. Scenariile referitoare la obiectul informațional „Sursă de finanțare”:
8. înregistrarea primară – de către IP ODA (în cazul recepționării a datelor privind sursele noi de finanțare );
9. actualizarea datelor – de către IP ODA ca urmare a actualizării datelor în cadrul planificării bugetare;
10. scoaterea din evidență –de către IP ODA în cazul expirării perioadei de accesibilitate a sursei de finanțare (scoaterea din evidență presupune stabilirea unui statut specific de dezactivare a sursei de finanțare).
11. Scenariile referitoare la obiectul informațional „Conținut de structură al Planului de acțiuni”:
12. înregistrarea primară – de către de către IP ODA în funcție de tipul planului de acțiuni;
13. actualizarea datelor – de către de către IP ODA la modificarea planului de acțiuni sau la elaborarea unei noi versiuni a planului de acțiuni;
14. scoaterea din evidență – de către IP ODA în cazul în care categoria de structură nu mai este relevantă.
15. Scenariile referitoare la obiectul informațional „Indicator”:
16. înregistrarea primară – de către IP ODA în cazul necesității elaborării unui indicator de raportare a progresului de implementare pentru tipuri de categorii de structură noi ale planului de acțiuni sau schimbarea metodologie de raportare a progresului.
17. actualizarea datelor – de către utilizatorul cu rol de administrator de sistem în cazul necesității eliminării unor erori de configurare a indicatorilor de raportare a progresului;
18. scoaterea din evidență – de către utilizatorul cu rol de administrator de sistem în cazul schimbării metodologiei de raportare progres și renunțare la indicator (scoaterea din evidență presupune stabilirea unui statut specific de dezactivare a indicatorului de raportare a progresului).
19. Scenariile referitoare la obiectul informațional „Raportare progres acțiune”:
20. înregistrarea primară – de către IP ODA în cazul elaborării unui raport de progres și aprobării din partea utilizatorilor cu rol decident a instituțiilor raportoare;
21. actualizarea datelor – de către IP ODA în cazul necesității eliminării unor constrângeri semnalate de utilizatori cu rol decident în cadrul instituțiilor raportoare (până la aprobarea raportului de către utilizatorul cu rol decident);
22. scoaterea din evidență – de către IP ODA în cazul depistării erorilor în rapoartele de progres aprobate (scoaterea din evidență presupune stabilirea unui statut specific de dezactivare a raportului de progres).
23. Scenariile referitoare la obiectul informațional „Document”:
24. înregistrarea primară – de către orice utilizator autorizat al SIIA ODA cu drept de elaborare sau atașare a documentelor specifice fluxurilor de lucru ale sistemului informațional (document de politici publice, raport de evaluare a conformității documentului de politici publice, plan de acțiuni, comentariu, aviz, notă informativă, act normativ, analiză ex-ante/ex-post, tabel de concordanță, eveniment aprobare/ respingere);
25. actualizarea datelor – de către utilizatorii autorizați cu drept de elaborare sau atașare a documentelor specifice fluxurilor de lucru ale sistemului informațional în cazul modificării înregistrărilor în baza cărora sunt generate documentele sau necesității actualizării conținutului documentelor care nu sunt generate de SIIA ODA;
26. scoaterea din evidență – de către utilizatorii autorizați cu drept de elaborare sau atașare a documentelor specifice fluxurilor de lucru ale sistemului informațional sau automat de SIIA ODA în cazul scoaterii din evidență a obiectelor informaționale în baza cărora sunt generate documentele (scoaterea din evidență presupune stabilirea unui statut specific de document anulat).
27. Scenariile referitoare la obiectul informațional „Sarcină”:
28. înregistrarea primară – de către utilizatori cu rol decident în cazul atribuirii explicite a unei sarcini noi sau de către SIIA ODA în cazul atribuirii automate a sarcinilor ca urmare a producerii unor evenimente specifice în cadrul fluxurilor de lucru;
29. actualizarea datelor – de către utilizatori cu rol decident în cazul modificării termenului de executare a sarcinii sau atribuirea sarcinii altui utilizator;
30. scoaterea din evidență – de către utilizatori cu rol decident în cazul irelevanței sarcinii sau de către SIIA ODA în cazul depășirii semnificative a termenului de implementare a sarcinii (scoaterea din evidență presupune stabilirea unui statut specific sarcinii).
31. Scenariile referitoare la proiectul de finanțare a solicitantului, beneficiarului sau a reprezentantului legal:
32. înregistrarea primară a unui proiect de finanțare se realizează în baza cererii depuse de solicitant, beneficiar sau a reprezentantului legal;
33. actualizarea datelor se realizează la solicitarea aplicantului, prin depunerea unei cereri online;
34. scoaterea din evidență (inclusiv arhivarea datelor) se realizează de posesor conform perioadei de păstrare a actelor oficiale stabilite. Arhivarea datelor se efectuează în mod automat în intervalele stabilite de deținător.

**Secțiunea a 3-a**

**Fluxurile informaționale**

1. Fluxul de gestiune a resurselor include date despre efectuarea tranzacțiilor pentru evidența fondurilor. Gestionarea fondurilor se va efectua prin tranzacții, prin intermediul a două tipuri de tranzacții posibile:
2. tranzacții manuale - reprezintă totalitatea operațiunilor de debitare sau creditare a fondurilor IP ODA efectuate de către persoanele autorizate din partea IP ODA;
3. tranzacții automate - reprezintă totalitatea operațiunilor de debitare sau creditare a fondurilor FGC și FACEM ca rezultat al gestiunii programelor implementate de IP ODA, urmare a modificării statutelor proiectului investițional.
4. Fluxul de gestiune a Programelor de suport antreprenorial este realizat prin adăugarea sau eliminarea setului de criterii specifice Programului și atribuitele definite pentru acesta, elaborate și aprobate de către IP ODA. Programele vor conține minim următoarele criterii și informații:
5. Denumirea programului de suport antreprenorial;
6. Valoarea maximă a suportului financiar (lei);
7. Cota maximă disponibilă (%);
8. Perioada maximă și minimă de finanțare (luni);
9. Categoriile de clasificare a Solicitantului/Beneficiarului;
10. Destinațiile suportului eligibil;
11. Domenii de activitate neeligibile;
12. Valoarea maximă și minimă a proiectului investițional (lei);
13. Criterii de eligibilitate specifice Programului, aprobate de IP ODA;
14. Documentele obligatorii ce urmează a fi atașate în format PDF.
15. SIIA ODA va oferi posibilitatea creării, ajustării și eliminării Programelor de suport antreprenorial, păstrând și jurnalizând toate evenimentele de modificare a acestora.
16. Fluxul privind solicitarea, emiterea, monitorizarea și recuperarea resurselor financiare alocate individual includ următoarele acțiuni:
17. Cererea de finanțare este generată automatizat de către SIIA ODA urmare a introducerii de către solicitant, beneficiar, reprezentantului legal sau entitatea financiară parteneră a tuturor informațiilor în corespundere cu cerințele programului solicitat și atașarea tuturor documentelor necesare procesului de examinare a dosarului;
18. Evidența cererilor este ținută de către sistem, fiind generat un identificator unic pentru fiecare cerere;
19. SIIA ODA va oferi posibilitatea semnării cererii și a tuturor documentelor încărcate în sistem (după caz), folosind serviciul guvernamental MSIGN;
20. Înainte de transmiterea cererii către IP ODA, aceasta va fi semnată cu semnătura electronică de către reprezentantul Solicitantului;
21. SIIA ODA va asigura circulația și evidența tuturor fluxurilor interne de analiză a cererii în corespundere cu limitele de competență și plafoanele aprobate de IP ODA;
22. SIIA ODA va asigura generarea automatizată a documentelor de lucru, precum și posibilitatea semnării acestora cu semnătura electronică;
23. Dacă în perioada când proiectul investițional este activ, intervin anumite modificări a condițiilor de implementare, beneficiarul va avea posibilitatea să solicite modificările prin intermediul SIIA ODA, cererea fiind generată automatizat și semnată electronic;
24. Procesul de analiză a solicitărilor de modificare a condițiilor de finanțare va fi asigurat de către SIIA ODA, iar documentele interne ale IP ODA vor fi generate automatizat și vor putea fi semnate cu semnătura electronică;
25. SIIA ODA va asigura circulația și evidența tuturor fluxurilor interne de analiză a cererii în corespundere cu limitele de competență și plafoanele aprobate de IP ODA;
26. SIIA ODA va ține evidența proiectelor investițional implementate.
27. Fluxul de generare a rapoartelor privind informațiile colectate de obiectele informaționale se va realiza automatizat sau la cerere. Sistemul va permite configurarea rapoartelor după informațiile necesare de a fi prezentate/exportate.
28. SIIA ODA va interacționa cu următoarele sisteme și resurse informaționale:

Registrul de stat al unităților de drept;

Registrul de stat al populației;

Registrul bunurilor imobile;

Registrul de stat al unităților administrativ-teritoriale și al adreselor;

Portalul de participare (www.particip.gov.md);

Registrul de stat al actelor locale (www.rsal.gov.md);

Registru fiscal de stat;

Registrul ajutoarelor de stat;

Sistemul informațional automatizat de gestionare și eliberare a actelor permisive ( SIA GEAP);

Sistemul Informațional de Gestionare a Finanțelor Publice;

platforma de interoperabilitate (MConnect);

serviciul electronic guvernamental de autentificare şi control al accesului (MPass);

serviciul electronic guvernamental integrat de semnătură electronică (MSign);

serviciul guvernamental de plăţi electronice (MPay);

serviciul guvernamental de notificare electronică (MNotify);

serviciul electronic guvernamental de jurnalizare (MLog);

Sistemul informaţional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower);

Portalul guvernamental unic de date deschise (www.date.gov.md);

Portalul serviciilor publice (www.servicii.gov.md);

Portalul guvernamental al cetățeanului;

Portalul guvernamental al antreprenorului;

platforma tehnologică guvernamentală comună (MCloud) – pentru găzduirea sistemului;

Sistemului informațional de gestiune a garanțiilor financiare pentru credite;

Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower);

alte sisteme informaționale care vor implementa interfețe program necesare pentru realizarea comunicării și schimbului de date cu e-APL în vederea realizării funcțiilor APL.

**Capitolul VIII**

**SPAȚIUL TEHNOLOGIC AL SISTEMULUI**

1. SIIA ODA va fi proiectat ca un sistem modular, care va asigura posibilitatea dezvoltării sale fără a afecta continuitatea funcționării. Arhitectura acestuia trebuie concepută după schema-tip a infrastructurii informaționale a sistemului informațional automatizat, în conformitate cu cerințele legale.
2. La nivel conceptual, arhitectura SIIA ODA este definită pe 3 nivele:
3. nivelul de interfață – serverul pentru paginile web, cu formularele utilizatorilor și informațiile din baza de date pentru vizualizare și utilizare prin intermediul browserului (navigatorului web);
4. produsul program al nivelului de mijloc – serverul aplicațiilor care va susține partea client, ce deservește interfața bazei de date cu utilizatorii, va transforma cererile utilizatorilor în interpelări SQL și va primi informația de la baza de date și o va prezenta în formă comodă pentru percepție;
5. nivelul de jos – serverul bazei de date.
6. Componenta Centrală a infrastructurii SIIA ODA este găzduită de către administratorul tehnic şi asigură procesarea şi stocarea centralizată a datelor. Componentele distribuite reprezintă punctele de acces către componenta centrală prin canale securizate, asigurate de către administratorul tehnic.
7. Arhitectura complexului software-hardware, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale se determină de către dezvoltatorul SIIA ODA, în comun cu posesorul și deținătorul, la etapele inițiale și ulterioare de elaborare și implementare a SIIA ODA.
8. Pentru comunicarea dintre nivelurile SIIA ODA se utilizează rețelele de comunicații electronice securizate.
9. Platforma tehnologică a SIIA ODA va:
10. asigura formate unice de prezentare a datelor și protocoale comune de schimb de date;
11. oferi mecanisme de asigurare a concordanței bazelor de date ale SIIA ODA cu cele ale sistemelor informaționale ale altor autorități publice. Concordanța trebuie să fie respectată între clasificatoare, nomenclatoare, completitudine;
12. pune la dispoziția dezvoltatorilor de software un cadru formal și metodologic propice creării și implementării sistemului de management al securității informaționale.
13. Produsele program și echipamentele SIIA ODA trebuie să satisfacă următoarele cerințe:
14. să asigure posibilitatea stocării unor volume mari de informații;
15. să asigure posibilitatea extinderii funcționale și a puterii de calcul (extensibilitate și scalabilitate);
16. să susțină prelucrarea distribuită a datelor, accesul la resurse atît în rețeaua locală, cît și în Internet;
17. să utilizeze un sistem unic de clasificare și codare (unificare);
18. să funcționeze pe diferite platforme hardware;
19. să asigure fiabilitate înaltă;
20. să asigure consistența și completitudinea informației;
21. să susțină posibilitatea de modernizare în timpul procesului de exploatare.
22. Posesorul și deținătorul SIIA ODA vor asigura găzduirea acestuia pe platforma tehnologică guvernamentală comună MCloud.

**Capitolul IX**

**ASIGURAREA SECURITĂȚII INFORMAȚIONALE A SIIA ODA**

1. Securitatea informațională presupune protecția SIIA ODA la toate etapele proceselor de creare, procesare, stocare și transmitere a datelor de acțiuni accidentale sau intenționate cu caracter artificial sau natural, care au ca rezultat cauzarea prejudiciului posesorului și utilizatorilor resurselor și infrastructurii informaționale.
2. Asigurarea securității informaționale va fi realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărîrea Guvernului nr.201/2017. Pentru gestiunea riscurilor de securitate va fi implementată o politică generală de securitate. Personalul implicat în utilizarea și administrarea SIIA ODA va fi instruit în ceea ce privește riscurile de securitate la care poate fi expus. Politica de securitate va include prevederi referitoare la organizarea auditurilor periodice de securitate pentru a verifica politica și conformitatea cu regulile de securitate, precum și pentru a stabili domeniile care necesită îmbunătățiri.
3. Posesorul, deținătorul și registratorii vor proteja SIIA ODA de pericolul cauzării prejudiciilor resurselor sau infrastructurii informaționale. Principalele pericole pentru securitatea informațională a SIIA ODA sunt:
4. colectarea și utilizarea ilegală a datelor;
5. încălcarea tehnologiei de prelucrare a datelor;
6. implementarea în produsele software și hardware a componentelor care realizează funcții neprevăzute în documentația care însoțește aceste produse;
7. elaborarea și răspândirea programelor ce pot afecta funcționarea normală a sistemelor informaționale și de comunicații, precum și a sistemelor de protecție a informației;
8. nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor hardware și/sau software de prelucrare a informației;
9. influențarea sistemelor cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a datelor;
10. compromiterea cheilor și a mijloacelor de protecție criptografică a informației;
11. scurgerea de informație prin canale tehnice;
12. implementarea dispozitivelor electronice de interceptare a informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor prin canalele de comunicații, precum și în încăperile de serviciu ale registratorilor SIIA ODA;
13. nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;
14. tentativele de interceptare a datelor în rețelele locale ale registratorilor și în liniile de comunicații, decodificarea ei și impunerea informației false;
15. utilizarea tehnologiilor informaționale necertificate, a mijloacelor de protecție a datelor, a mijloacelor de informatizare și comunicații la crearea și dezvoltarea infrastructurii informaționale;
16. accesul neautorizat la resursele informaționale care se află în băncile și bazele de date;
17. încălcarea restricțiilor legale ce țin de răspândirea informației;
18. încălcarea prevederilor Legii nr.133/2011 privind protecția datelor cu caracter personal.
19. În contextul asigurării protecției datelor cu caracter personal:
20. în condițiile prezentului Concept, posesorul, deținătorul și registratorii vor prelucra doar datele cu caracter personal strict necesare, neexcesive scopului prestabilit, conform competențelor atribuite, respectînd principiile stabilite de actele normative din domeniul protecției datelor cu caracter personal;
21. la prelucrarea datelor cu caracter personal, posesorul și deținătorul vor asigura măsuri organizatorice și tehnice necesare pentru protecția datelor cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate;
22. în cazul incidentelor de securitate, posesorul deținătorul și administratorul tehnic vor întreprinde măsuri necesare pentru depistarea sursei de producere a incidentului, vor efectua analiza acestuia și vor înlătura cauzele incidentului de securitate cu informarea Centrului Național pentru Protecția Datelor cu Caracter Personal;
23. în cadrul operațiunilor de prelucrare a datelor cu caracter personal efectuate conform prezentului Concept, posesorul, deținătorul și registratorii în limitele responsabilităților vor asigura respectarea drepturilor subiecților de date cu caracter personal.
24. SIIA ODA asigură realizarea următoarelor obiective de securitate:
25. autentificarea – garantează că zonele restricționate ale SIIA ODA vor fi accesibile doar utilizatorilor cu o identitate verificată prin serviciul electronic guvernamental de autentificare şi control al accesului (MPass);
26. autorizarea – garantează că utilizatorii autentificați prin serviciul electronic guvernamental de autentificare şi control al accesului (MPass) pot accesa serviciile şi datele care corespund drepturilor lor de acces:
27. confidențialitatea – garantează că datele înregistrate în SIIA ODA nu pot fi accesate de o parte terță neautorizată;
28. integritatea – garantează că datele înregistrate în SIIA ODA nu au fost modificate sau alterate de o parte terță neautorizată;
29. non repudierea – garantează că datele înregistrate în SIIA ODA nu pot fi negate mai târziu.
30. Pentru atingerea obiectivelor de securitate, SIIA ODA trebuie să dispună de mai multe mecanisme de securitate:
31. semnătura electronică – mecanism ce asigură integritatea şi nonrepudierea datelor înregistrate în SIIA ODA;
32. firewall – filtrul firewall face parte din arhitectura tehnică a platformei tehnologice (MCloud) pentru a asigura un mecanism de apărare împotriva utilizatorilor externi neautorizați;
33. antivirus/antispam – soluțiile hardware şi/sau software asigură protecția antivirus şi antispam pentru toate serverele. Fișierele se scanează la încărcare în SIIA ODA. În cazul detectării unui fișier infectat, procedura de încărcare este oprită şi fișierul – respins;
34. sistem de detectare a intruziunilor – sistem de detectare a accesului neautorizat la nivelul componentelor de sistem al SIIA ODA;
35. comunicare sigură (transferuri de date) între serverele web și utilizatori – schimbul de informații confidențiale este securizat;
36. backup sistematic al datelor păstrate – permite recuperarea rapidă și fiabilă a datelor în caz de incident care a dus la pierderea sau deteriorarea datelor;
37. instrument de înregistrare a evenimentelor de audit – toate activitățile desfășurate de către utilizatori, indiferent dacă au succes sau nu (cum ar fi conectările încercate, dar nereușite), sunt monitorizate și înregistrate în jurnalele SIIA ODA, cu acces limitat pentru utilizatorii neautorizați.
38. În cadrul SIIA ODA trebuie să se asigure generarea şi păstrarea înregistrărilor de audit ale securității pentru operațiile de prelucrare a datelor cu caracter personal în condițiile cadrului normativ în materie de protecție a datelor cu caracter personal. Înregistrările de audit ale operațiilor şi rezultatele acestora pot fi accesate de către Centrul Național pentru Protecția Datelor cu Caracter Personal și puse la dispoziția acestuia în scopul investigării potențialelor încălcări ale regimului de prelucrare/protecție a datelor cu caracter personal. SIIA ODA va utiliza funcționalitatea de autentificare doar prin intermediul serviciului MPass.
39. Utilizatorii SIIA ODA vor fi autorizați să acceseze doar blocurile funcționale şi datele pentru care au permisiunile necesare, conform rolurilor fiecăruia. Utilizatorii şi rolurile acestora vor fi gestionate prin intermediul serviciului MPass. SIIA ODA va prelua rolurile utilizatorilor din serviciul MPass.
40. SIIA ODA se va baza pe un mecanism de înregistrări de audit, cu utilizarea serviciului MLog.

**Capitolul X**

**DISPOZIȚII FINALE**

1. Prezentul Concept conține descrierea principalelor aspecte organizaționale, metodologice și tehnologice în conformitate cu care este concepută și implementată soluția tehnică necesară să asigure evidența resurselor și sistemelor informaționale de stat.
2. IP ODA în calitate de deținător al sistemului, poate asigura mentenanța sistemului din resursele programelor de suport antreprenorial, resursele proprii, programelor de asistență externă, pentru suport tehnic, inclusiv ajustarea sistemului informațional în caz de necesitate.

Anexa nr. 2 la

Hotărârea Guvernului nr.\_\_\_/2024

**REGULAMENTUL**

**privind modul de ținere a resursei informaționale formată de Sistemul informațional integrat automatizat al Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului**

**Capitolul I**

**DISPOZIȚII GENERALE**

1. Regulamentul stabilește reguli privind modul de ținere a resursei informaționale formată de Sistemul informațional integrat automatizat al Instituției Publice Organizația pentru Dezvoltarea Antreprenoriatului (în continuare - Regulament) în procesul de implementare a programelor de dezvoltare a antreprenoriatului.
2. SIIA ODA este parte componentă a resurselor informaționale de stat ale Republicii Moldova.
3. Formarea SIIA ODA se realizează prin intermediul funcționării SIIA ODA, care este destinat să ofere persoanelor fizice și persoanelor juridice de drept public și privat un mecanism eficient, fiabil și modern în procesul de solicitare, acordare, monitorizare, executare și recuperare.
4. SIIA ODA este organizat astfel încât să asigure ca procesele de înregistrare și acces să fie simple, eficiente, accesibile și transparente.
5. SIIA ODA conține date privind solicitantul, beneficiarul, reprezentantului legal sau entitatea financiară parteneră de suport prin programele destinate dezvoltării antreprenoriatului.
6. Noțiunile utilizate în prezentul Regulament au semnificația dată de definițiile acestora prevăzute în Legea nr.71/2007 cu privire la registre, Legea nr. 467/2004 cu privire la informatizare și resursele informaționale de stat și Legea nr 179/2016 cu privire la întreprinderile mici și mijlocii.

**Capitolul II**

**SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL**

**CREĂRII, EXPLOATĂRII ȘI UTILIZĂRII SIIA ODA**

1. Subiecții din domeniul creării, exploatării și utilizării SIIA ODA sunt:
2. proprietarul;
3. posesorul;
4. deținătorul;
5. registratorul;
6. furnizorul de date;
7. destinatarul datelor.
8. Proprietarul SIIA ODA este statul. Resursele financiare pentru dezvoltarea, mentenanța și exploatarea Registrului sunt asigurate din bugetul de stat și din alte mijloace financiare, conform legislației.
9. Posesorul al SIIA ODA este IP ODA care are următoarele atribuții:
10. asigură condițiile juridice, organizatorice și financiare pentru crearea și ținerea SIIA ODA;
11. aprobă proceduri, reguli și instrucțiuni privind introducerea, acumularea, păstrarea, completarea, corectarea, sistematizarea și utilizarea datelor, precum și funcționarea SIIA ODA;
12. reglementează nivelul agreat de servicii;
13. alte atribuții care decurg din prevederile cadrului normativ și întreprinderea cărora este necesară pentru asigurarea funcționării SIIA ODA.
14. Deținătorul SIIA ODA este IP ODA care are următoarele atribuții:
15. asigură crearea și exploatarea SIIA ODA;
16. asigură ținerea SIIA ODA în conformitate cu prevederile legislației inclusiv ale prezentului Regulament, precum și cu actele normative aprobate de posesor;
17. asigură funcționarea, administrarea și dezvoltarea continuă a SIIA ODA, în conformitate cu nivelul agreat de servicii și în limitele bugetului alocat;
18. intervine, conform nivelului agreat de servicii, pentru investigarea, soluționarea, îndepărtarea erorilor identificate sau comunicate de utilizatorii SIIA ODA;
19. asigură înregistrarea obiectelor supuse înregistrării;
20. asigură autenticitatea, plenitudinea și integritatea datelor din SIIA ODA;
21. stabilește scopurile și sarcinile funcționale ale SIIA ODA;
22. monitorizează procesul de înregistrare și prelucrare a datelor în SIIA ODA;
23. asigură accesul registratorilor, furnizorilor, destinatarilor în conformitate cu drepturile de acces stabilite și atribuțiile delegate;
24. asigură securitatea și protecția datelor din SIIA ODA;
25. stabilește măsurile tehnice și organizatorice de protecție și securitate a SIIA ODA;
26. monitorizează și ajustează cerințele de securitate și conformitate a SIIA ODA în domeniul protecției datelor cu caracter personal;
27. exercită alte atribuții necesare asigurării bunei funcționări a SIIA ODA.
28. Deținătorul asigură păstrarea SIIA ODA până la adoptarea deciziei despre lichidarea acestuia. În cazul lichidării, datele și documentele conținute în acesta se transmit în arhivă, conform legislației.
29. Registratorii datelor în SIIA ODA sunt IP ODA, solicitantul, beneficiarul, reprezentantului legal sau entitatea financiară parteneră, care în conformitate cu prevederile legislației, inclusiv ale prezentului Regulament, înregistrează, completează sau modifică datele privind obiectele informaționale ale SIIA ODA în funcție și în limitele rolurilor și drepturilor de acces cu care sunt învestite.
30. Furnizorul de date este persoana fizică sau persoana juridică de drept public sau de drept privat care livrează date aferente obiectelor informaționale ale SIIA ODA.
31. Destinatarul datelor din SIIA ODA sunt persoanele fizice și juridice care sunt mandatate conform legislației, să primească datele conținute în SIIA ODA.
32. Administratorul tehnic al SIIA ODA este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică” care își exercită atribuțiile în conformitate cu cadrul normativ care reglementează domeniul administrării tehnice și menținerii sistemelor informaționale de stat.

**Capitolul III**

**DREPTURILE ȘI OBLIGAȚIILE SUBIECȚILOR RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII, EXPLOATĂRII ȘI UTILIZĂRII SIIA ODA**

**Secțiunea 1**

**Drepturile și obligațiile posesorului**

1. Posesorul SIIA ODA are dreptul:
2. să înainteze propuneri de modificare a cadrului normativ care reglementează modul de ținere a SIIA ODA și de organizare, funcționare și exploatare a SIIA ODA;
3. să perfecționeze, în funcție de competența sa, cadrul normativ cu privire la SIIA ODA;
4. Posesorul SIIA ODA este obligat:
5. să adopte actele necesare punerii în aplicare a prevederilor prezentului Regulament și care asigură funcționarea în condiții de legalitate a SIIA ODA;
6. să asigure controlul executării prevederilor cadrului normativ care reglementează organizarea și funcționarea SIIA ODA.

**Secțiunea a 2-a**

**Drepturile și obligațiile deținătorului**

1. Deținătorul SIIA ODA are dreptul:
2. să propună soluții pentru perfecționarea și eficientizarea procesului de funcționare a SIIA ODA, precum și să le pună în aplicare;
3. să supravegheze respectarea cerințelor de securitate a informației de către utilizatorii SIIA ODA, să fixeze cazurile și tentativele de încălcare a acestora;
4. să inițieze procedura de revocare a drepturilor de acces la SIIA ODA pentru utilizatorii care nu respectă regulile, standardele și normele general acceptate în domeniul securității informaționale.
5. Deținătorul SIIA ODA este obligat:
6. să asigure atribuirea rolurilor și drepturilor de acces la interfața și datele SIIA ODA;
7. să efectueze monitorizarea și supravegherea accesărilor informației din SIIA ODA;
8. să identifice încălcările comise și să întocmească un raport privind datele accesate;
9. să asigure funcționarea și ținerea SIIA ODA în conformitate cu prevederile cadrului normativ;
10. să asigure funcționarea neîntreruptă a SIIA ODA;
11. să acorde suportul necesar utilizatorilor care au acces la SIIA ODA, privind folosirea complexului de mijloace software aferente acestuia;
12. să stabilească condițiile tehnice de funcționare a SIIA ODA;
13. să efectueze măsurile organizatorico-tehnice necesare asigurării protecției și confidențialității informației stocate în SIIA ODA, inclusiv împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate;
14. să asigure implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu legislația în materie de protecție a datelor cu caracter personal;
15. să asigure accesul securizat la informația conținută în SIIA ODA, respectarea condițiilor de securitate și a regulilor de exploatare a acestuia;
16. să utilizeze informația obținută din baza de date a SIIA ODA doar în scopurile stabilite de legislație.

**Secțiunea a 3-a**

**Drepturile și obligațiile registratorului**

1. Registratorul are dreptul:
2. să vizualizeze și să editeze informațiile din SIIA ODA, conform rolului atribuit;
3. să acceseze spațiul informațional al SIIA ODA, în limitele rolului atribuit;
4. să acceseze informațiile care se conțin în SIIA ODA și care au fost prezentate de către acesta;
5. să înainteze posesorului propuneri privind modificarea actelor normative care reglementează funcționarea SIIA ODA;
6. să solicite și să primească de la deținător susținere metodologică și practică privind funcționarea SIIA ODA;
7. să solicite și să primească de la posesor și deținător informații referitoare la nivelul agreat al serviciilor conform indicatorilor stabiliți în anexele tehnice;
8. să înainteze posesorului și deținătorului propuneri privind îmbunătățirea și sporirea eficacității funcționării SIIA ODA.
9. Registratorul este obligat:
10. să asigure corectitudinea, autenticitatea și veridicitatea datelor introduse în SIIA ODA;
11. să asigure actualizarea datelor introduse în SIIA ODA;
12. să întreprindă măsuri pentru evitarea accesului neautorizat al persoanelor terțe;
13. să utilizeze funcționalitățile SIIA ODA în exclusivitate conform destinației acestora și în strictă conformitate cu legislația;
14. să utilizeze informația obținută din SIIA ODA doar în scopurile stabilite de legislație.

**Secțiunea a 4-a**

**Drepturile și obligațiile altor categorii de subiecți**

1. Fiecare subiect are dreptul:
   1. să participe la implementarea și dezvoltarea SIIA ODA;
   2. să înainteze posesorului SIIA ODA propuneri privind modificarea actelor normative care reglementează funcționarea SIIA ODA;
   3. să solicite și să primească de la deținătorul SIIA ODA ajutor metodologic și practic privind funcționarea acestuia;
   4. să solicite și să primească de la posesor și deținător informații referitoare la nivelul agreat al serviciilor conform indicatorilor stabiliți în anexele tehnice;
   5. să solicite și să primească de la deținător accesul la datele/informațiile din SIIA ODA în conformitate cu scopul prelucrării și rolul atribuit;
   6. să vizualizeze datele/informațiile/documentele din SIIA ODA în conformitate cu drepturile de acces stabilite, pornind de la atribuțiile și funcțiile deținute, fără dreptul de a modifica aceste date/informații/documente;
   7. să prezinte posesorului și/sau deținătorului SIIA ODA propuneri privind perfecționarea și eficientizarea funcționării acestuia.
2. În funcție de rolurile atribuite, subiecții sunt obligați:
   1. să asigure corectitudinea, autenticitatea și confidențialitatea datelor, a informațiilor sau documentelor prezentate;
   2. să asigure actualizarea datelor, a informațiilor sau a documentelor prezentate;
   3. să asigure accesarea și utilizarea datelor, informațiilor și/sau documentelor din SIIA ODA în conformitate cu rolurile atribuite și scopul legitim de utilizare a acestora;
   4. să efectueze acțiunile de asigurare a securității informației, să documenteze cazurile și tentativele de încălcare a acesteia, precum și să întreprindă măsurile ce se impun pentru prevenirea și lichidarea consecințelor;
   5. să asigure accesul securizat la informația conținută în SIIA ODA, respectarea condițiilor de securitate și a regulilor de exploatare a acestuia;
   6. să ia măsurile organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu instrucțiunile aprobate de posesorului SIIA ODA;
   7. să utilizeze informația obținută din baza de date a SIIA ODA doar în scopurile stabilite de legislație;
   8. să aducă la cunoștința posesorului și deținătorului SIIA ODA, în termen de o zi, orice situație (incidente aflate în afara ariei de competență a subiectului) care ar putea influența în mod negativ exercitarea funcțiilor subiectului.

**Capitolul IV**

**ȚINEREA, ASIGURAREA FUNCȚIONĂRII ȘI ÎNREGISTRAREA DATELOR ÎN SIIA ODA**

1. SIIA ODA se ține în format electronic prin SIIA ODA, în limba română.
2. Deținătorul SIIA ODA efectuează administrarea acestuia cu ajutorul complexului de mijloace software și hardware, în corespundere cu prezentul Regulament.

**Capitolul V**

**MODIFICAREA, COMPLETAREA ȘI RADIEREA DATELOR DIN**

**SIIA ODA**

1. Modificarea şi/sau completarea datelor din cadrul SIIA ODA se efectuează de către registratorii SIIA ODA.
2. Modificarea și/sau completarea datelor din cadrul SIIA ODA pot fi realizate de către registratorii care le-au prezentat.
3. SIIA ODA asigură posibilitatea accesării și vizualizării informației la orice etapă de modificare și/sau completare a datelor, precum și evidența tuturor modificărilor și completărilor. Toate modificările operate în SIIA ODA se păstrează în ordine cronologică.
4. Din momentul acordării suportului până la executarea acesteia, dosarul se păstrează în SIIA ODA în vederea vizualizării și verificării statutului.
5. Dosarul inclusiv datele cu caracter personal ce se conțin în acesta se păstrează în SIIA ODA conform termenelor prevăzute de cadrul normativ ce reglementează modul de administrare a programelor de dezvoltare pentru întreprinderile mici și mijlocii, ulterior urmând a fi arhivată conform legislației.
6. La expirarea termenului de păstrare în SIIA ODA, dosarul de finanțare este radiat din SIIA ODA, inclusiv datele cu caracter personal ce se conțin în acesta cu înregistrarea evenimentelor respective în modul corespunzător.

**Capitolul VII**

**REGIMUL JURIDIC DE UTILIZARE**

**A DATELOR DIN SIIA ODA**

1. Accesul la datele din SIIA ODA este condiționat de rolul utilizatorului. Astfel, registratorul are acces tehnic la datele din SIIA ODA, ceea ce presupune introducerea, modificarea și radierea datelor înregistrate de acesta. Ceilalți utilizatori au acces informațional la datele din SIIA ODA, ceea ce presupune vizualizarea datelor numai în formatul individual permis pentru fiecare utilizator în parte. În unele cazuri registratorul poate avea rol de utilizator cu acces limitat informațional la date.
2. Se interzice utilizarea datelor din SIIA ODA în scopuri contrare legii.
3. Datele cu caracter personal ale persoanelor fizice se utilizează în temeiul legislației privind protecția datelor cu caracter personal.
4. Destinatarul datelor din SIIA ODA nu este în drept să modifice datele obținute din SIIA ODA, iar la utilizarea acestora este obligat să indice sursa lor.
5. Datele recepționate din SIIA ODA nu pot fi transmise persoanelor terțe, dacă legislația sau tratatele internaționale la care Republica Moldova este parte nu prevăd altfel.

**Capitolul VIII**

**INTERACȚIUNEA CU FURNIZORII DE INFORMAȚII**

1. Datele din cadrul SIIA ODA se actualizează și se sincronizează operativ cu datele din cadrul registrelor și sistemelor informaționale de stat.
2. SIIA ODA accesează, în limitele competenței, registrele și sistemele informaționale de stat prevăzute în pct. 37 din Conceptul SIIA ODA.
3. Accesul la informațiile din registrele și sistemele informaționale de stat este asigurat prin intermediul platformei de interoperabilitate (Mconnect).

**Capitolul IX**

**MANAGEMENTUL UTILIZATORILOR ÎN CADRUL SIIA ODA ȘI PROCESELE DE ADMINISTRARE**

1. Managementul utilizatorilor va fi efectuat prin intermediul modulului de gestiune a rolurilor și utilizatorilor din cadrul SIIA ODA de către administratorii desemnați.
2. Atât pentru asigurarea posibilității de intervenție operativă, cât și pentru descentralizarea gestionării utilizatorilor și a drepturilor de acces se va realiza distribuirea drepturilor conform proceselor de administrare:

1) administrare de sistem/infrastructură;

2) administrare de conținut;

3) administrare de utilizatori;

4) administrare de securitate.

1. Administratorul de sistem gestionează sistemele operaționale (administrare de sistem) și sistemul informațional. De asemenea, administratorul de sistem realizează configurările de bază ale proceselor, redactările de formă și administrarea utilizatorilor. Funcțiile administratorului de sistem i se atribuie deținătorului SIIA ODA.
2. Administratorul tehnic al SIIA ODA este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică , care își exercită atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a sistemelor informaționale de stat.
3. La prima autentificare prin intermediul serviciului guvernamental de autentificare și control al accesului (MPass) în cadrul sistemului, fiecărui utilizator i se atribuie un identificator unic și rolul de care depinde dreptul de acces la obiectele informaționale.
4. SIIA ODA atribuie sau suspendă rolul, de care depinde nivelul de acces la funcționalitățile sistemului, pentru utilizatorii cu funcții de conducere, care dispune de dreptul de desemnare ulterioară a persoanelor responsabile.
5. Persoanele responsabile, angajați ai IP ODA și/sau ai solicitantului, beneficiarului, reprezentantului legal și a entităților financiare partenere, în baza dispozițiilor interne, atribuie rolul, de care depinde nivelul de acces la funcționalitățile SIIA ODA, pentru angajații persoanelor juridice respective.
6. Dreptul de acces la SIIA ODA nu este unul permanent, acesta poate fi revocat în circumstanțele prevăzute în pct.51. Introducerea și/sau modificarea datelor în SIIA ODA de pe un nume sau profil de utilizator străin este strict interzisă, urmând a fi considerată ca acces neautorizat. Utilizatorii urmează să se asigure de faptul că nu au fost încălcate confidențialitatea cheii private, precum și a profilului de utilizator.
7. Dreptul de acces al utilizatorilor la sistem se revocă în următoarele cazuri:
   1. în baza cererii/solicitării conducătorilor persoanelor juridice, în cazul utilizatorilor angajați;
   2. la încetarea raporturilor de muncă ale utilizatorilor;
   3. la modificarea raporturilor de muncă, când noile responsabilități nu presupun accesul la datele SIIA ODA;
   4. la încălcarea regulilor de utilizare a sistemului;
   5. la constatarea încălcării securității informaționale de către utilizatorul sistemului.
8. Autorizarea utilizatorilor se produce în conformitate cu nivelul de acces stabilit și utilizatorii au posibilitatea să acceseze funcționalitățile sau informațiile disponibile potrivit nivelului de acces.
9. Mecanismul de autentificare în cadrul SIIA ODA este serviciul guvernamental de autentificare și control al accesului (MPass).
10. Accesul la SIIA ODA ai solicitantului, beneficiarului, reprezentantului legal entităților financiare partenere se efectuează în baza condițiilor prevăzute în programele de granturi, manualele operaționale sau a contractelor între părți.

**Capitolul X**

**ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI SIIA ODA**

1. Datele din SIIA ODA fac parte din categoria datelor care necesită a fi protejate. Asigurarea securității, confidențialității și a integrității datelor prelucrate în cadrul SIIA ODA 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.
2. Măsurile de protecție și securitate a informației cu caracter personal din SIIA ODA reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a SIIA ODA și se efectuează neîntrerupt de către toți subiecții SIIA ODA.
3. Obiecte ale asigurării protecției și securității informației din SIIA ODA se consideră tot complexul de mijloace software și hardware care asigură realizarea proceselor informaționale:
   1. baza de date, sistemele informaționale, sistemele operaționale, sistemele de gestiune a bazelor de date și alte aplicații care asigură funcționarea SIIA ODA;
   2. sistemele de telecomunicații, rețelele, serverele, calculatoarele și alte mijloace tehnice de prelucrare a informației.
4. Protecția informației din SIIA ODA, la nivel de deținător, se efectuează prin următoarele metode:
5. asigurarea măsurilor de protecție a datelor prin folosirea metodelor criptografice de transmitere a informației prin rețelele de transport de date guvernamentale;
6. excluderea accesului neautorizat la datele din SIIA ODA prin utilizarea funcționalităților de autentificare ale serviciului guvernamental de autentificare și control al accesului (MPass);
7. prevenirea acțiunilor speciale tehnice și de program care duc la distrugerea, denaturarea datelor sau care cauzează defecțiuni în funcționarea complexului tehnic și de program;
8. efectuarea periodică planificată a copiilor de siguranță a datelor și fișierelor mijloacelor de program;
9. efectuarea tuturor măsurilor aferente asigurării restabilirii și continuității funcționării SIIA ODA în cazul incidentelor.
10. Protecția informației cu caracter personal din SIIA ODA la nivel de utilizatori SIIA ODA se efectuează prin următoarele metode:
11. prevenirea acțiunilor intenționate și/sau neintenționate care pot duce la distrugerea sau denaturarea datelor din SIIA ODA;
12. monitorizarea procesului de exploatare a SIIA ODA prin intermediul mecanismului de jurnalizare efectuat de deținătorul acestuia.
13. Utilizatorii SIIA ODA sunt autorizați să acceseze doar blocurile funcționale și datele pentru care au permisiunile necesare, conform rolurilor fiecăruia.
14. Semnătura electronică avansată calificată este modalitatea de securitate care asigură autenticitatea și nonrepudierea.
15. Subiecții SIIA ODA, elaborează și implementează politica de securitate informațională pentru asigurarea respectării regulilor, standardelor și normelor general acceptate în domeniul securității informaționale, incluzând:
    1. identitatea persoanei responsabile de politica de securitate;
    2. principalele măsuri tehnico-organizatorice necesare asigurării funcționării SIIA ODA;
    3. procedurile interne ce exclud cazurile de modificare nesancționată a mijloacelor software și/sau a informației din SIIA ODA;
    4. responsabilitățile personalului subiectului SIIA ODA privind asigurarea securității informaționale;
    5. procedurile de control intern al subiectului SIIA ODA privind respectarea condițiilor de securitate informațională.
16. Fiecare subiect al SIIA ODA, cu excepția beneficiarului desemnează o persoană subordonată nemijlocit conducătorului persoanei juridice, responsabilă de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate informațională.
17. Fiecare subiect al SIIA ODA, cu excepția beneficiarului, asigură informarea și instruirea utilizatorilor privind metodele și procedeele de contracarare a pericolelor informaționale.
18. Schimbul informațional se efectuează cu utilizarea mijloacelor software și hardware, doar prin canale securizate, asigurând integritatea și securitatea datelor.

**Capitolul XI**

**CONTROLUL ȘI RESPONSABILITATEA**

1. SIIA ODA este supus unui control intern și extern. Controlul intern este efectuat de posesor și deținător, iar controlul extern este efectuat anual de către autoritățile administrației publice autorizate.
2. Responsabilitatea pentru organizarea funcționării SIIA ODA aparține posesorului și deținătorului în limitele competențelor acestora stabilite de cadrul normativ.
3. Angajații responsabili de asigurarea funcționării sistemului și înregistrării datelor poartă răspundere civilă, contravențională sau penală, după caz, conform legislației, pentru autenticitatea, fiabilitatea, integritatea informației, precum și pentru păstrarea/stocarea și utilizarea acesteia.
4. Toți subiecții SIIA ODA poartă răspundere civilă, contravențională sau penală, după caz, conform cadrului normativ, pentru prelucrarea, divulgarea și transmiterea informației din sistem ce conține date cu caracter personal persoanelor terțe, contrar prevederilor legislației.
5. Păstrarea SIIA ODA este asigurată de deținător până la adoptarea deciziei despre lichidarea acestuia. În cazul lichidării, datele și documentele conținute în acesta se transmit în arhivă conform legislației.
6. Pentru asigurarea funcționalității eficiente și neîntrerupte a SIIA ODA, schimbul informațional de date SIIA ODA este asigurat în regim non-stop.
7. Funcționarea SIIA ODA se suspendă de către administratorul tehnic, după coordonarea prealabilă cu posesorul și deținătorul, în caz de apariție a uneia dintre următoarele situații:
   1. în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al SIIA ODA;
   2. la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea SIIA ODA;
   3. în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SIIA ODA;
   4. la cererea scrisă a posesorului și/sau a deținătorului.
8. În cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SIIA ODA din vina terțelor persoane, este posibilă suspendarea funcționării SIIA ODA, cu informarea subiecților prin mijloacele tehnice disponibile**.**