

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. _____

din _____
Chișinău

Cu privire la aprobarea Conceptului sistemului informațional „Registrul fiduciilor și construcțiilor juridice similare” și a Regulamentului „Registrului fiduciilor și construcțiilor juridice similare”

În temeiul art. 14 alin. (21) din Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului (Monitorul Oficial al Republicii Moldova, 2018, nr. 58-66, art. 133), cu modificările ulterioare, art. 2074 din Codul civil nr. 1107/2002 (Monitorul Oficial al Republicii Moldova, 2019, nr. 66-75, art. 132), cu modificările ulterioare, 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), cu modificările ulterioare, art. 16 alin. (1) din Legea nr. 71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314), cu modificările ulterioare, Guvernul Republicii Moldova

HOTĂRĂȘTE:

1. Se instituie Sistemul și Resursa Informațională „Registrul fiduciilor și construcțiilor juridice similare”.
2. Se aprobă:
 - 1) Conceptul sistemului informațional „Registrul fiduciilor și construcțiilor juridice similare” conform Anexei nr.1;
 - 2) Regulamentul „Registrului fiduciilor și construcțiilor juridice similare”, conform Anexei nr. 2.
3. În scopul implementării prezentei hotărâri, Ministerul Finanțelor în conformitate cu prevederile Legii finanțelor publice și responsabilități bugetar-fiscale nr.181/2014, va prevedea alocarea în Legea bugetului de stat pentru anul corespunzător a mijloacelor bugetare necesare pentru finanțarea centralizată a asigurării serviciilor de administrare tehnică și dezvoltare a Sistemului informațional „Registrul fiduciilor și construcțiilor juridice similare”.
4. În termen de 3 luni de la data intrării în vigoare a prezentei hotărâri, fiduciarul/fiduciarii vor depune la Serviciul Fiscal de Stat, cerere de înregistrare a fiduciilor sau construcțiilor juridice similare constituite/înființate până la intrarea în vigoare a prezentei hotărâri.

Prim-ministru

DORIN RECEAN

Contrasemnează:

Ministrul finanțelor

Victoria Belous

CONCEPT
al sistemului informațional „Registrul Fiduciilor și construcțiilor juridice similare”

INTRODUCERE

Capitolul I
DISPOZIȚII GENERALE

1. Sistemul informațional „Registrul fiduciilor și construcțiilor juridice similare” (*în continuare – SI RF*) este un sistem informațional de evidență a fiduciilor sau construcțiilor juridice similare (în continuare fiducie), care au fost constituite/înființate, în temeiul contractelor de fiducie, declarațiilor unilaterale de constituire a fiduciei, prin testament, iar în cazurile expres prevăzute de lege, prin act administrativ sau hotărâre judecătorească.
2. SI RF este o totalitate de resurse și tehnologii informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informații cu privire la fiducii.
3. Prezentul Concept utilizează noțiunile prevăzute în Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, în Legea nr. 71/2007 cu privire la registre și în Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate, precum și următoarele noțiuni:
 - 1) *certificat privind înregistrarea fiduciei* – documentul ce conține date din Registrul fiduciilor și construcțiilor juridice, care confirmă înregistrarea, modificarea fiduciei sau radierea acestuia din Registru, emis fiduciarului sau reprezentantului lui legal de către Serviciul Fiscal de Stat;
 - 2) *eveniment (operație tehnologică)* – unul dintre scenariile comportamentului obiectului informațional, scontat în sistemul informațional. Lista evenimentelor cuprinde tot ciclul de viață al obiectului în resursa informațională, începând cu etapa înregistrării și finalizând cu radierea din evidență. Totodată, evenimentul înregistrat sau produs în alt sistem informațional de stat, care interacționează cu SI RF, poate genera modificări în datele obiectului informațional conținut în SI RF;
 - 3) *document electronic* – astfel cum este definit la art. 2 din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;
 - 4) *protecția informației* – totalitatea activităților privind prevenirea accesului neautorizat la informația documentată protejată;
 - 5) *proces informațional* - proces de colectare, prelucrare, acumulare, păstrare, actualizare și furnizare către utilizator a informației documentate;
 - 6) *securitate cibernetică* – stare de normalitate a sistemului și resursei informaționale, rezultată în urma aplicării unui ansamblu de măsuri prin care este asigurată autenticitatea, integritatea, confidențialitatea, disponibilitatea și nonrepudiarea datelor.
4. Scopurile SI RF sunt:
 - 1) Asigurarea formării resursei informaționale de stat în domeniul fiduciilor;
 - 2) evidența fiduciei aferent contractelor de fiducie, declarațiilor unilaterale de constituire a fiduciilor, fiduciilor constituite prin testament, iar în cazurile expres prevăzute de lege, constituite prin act administrativ sau prin hotărâre judecătorească;
 - 3) eficientizarea procesului de administrare fiscală.
5. Sarcinile de bază realizate de SI RF sunt:

- 1) colectarea, înregistrarea, modificarea și radierea din SI RF a fiduciei;
- 2) stocarea informației aferente fiduciei;
- 3) generarea statisticilor și rapoartelor;
- 4) prelucrarea datelor;
- 5) distribuția informațiilor;
- 6) asigurarea securității și protecției informațiilor la toate etapele de colectare, stocare și utilizare a resurselor informaționale de stat;
- 7) actualizarea datelor.

6. Principiile de bază ale SI RF sunt:

- 1) principiul legalității, care presupune crearea și exploatarea SI RF în conformitate cu legislația națională;
- 2) principiul integrității datelor, care presupune păstrarea conținutului și interpretarea univocă în condițiile unor acțiuni accidentale. Integritatea datelor se consideră a fi păstrată dacă datele nu au fost denaturate sau distruse;
- 3) principiul veridicității datelor, care presupune evidența resurselor și sistemelor informaționale de stat în baza unor date autentice;
- 4) principiul plenitudinii datelor, prin care se are în vedere asigurarea volumului complet al informației gestionate de SI RF, în conformitate cu actele normative;
- 5) principiul confidențialității informației, care se referă la restricționarea accesului persoanelor neautorizate la informația cu accesibilitate limitată;
- 6) principiul securității informaționale, care presupune asigurarea nivelului integrității, exclusivității, accesibilității și eficienței protecției datelor împotriva pierderii, alterării, denaturării, deteriorării, modificării, accesului și utilizării neautorizate. Securitatea SI RF presupune rezistență la atacuri, protecția integrității informației și pregătirea pentru lucru atât la nivel de sistem, cât și la nivel de date prezentate în această informație;
- 7) principiul compatibilității SI RF cu sistemele informaționale publice existente în țară;
- 8) principiul dezvoltării SI RF prin prisma apariției unor obiecte noi;
- 9) principiul modularității și scalabilității, ce reprezintă posibilitatea de a dezvolta SI RF fără modificarea componentelor create anterior;
- 10) principiul neexcesivității și pertinentei prelucrării datelor cu caracter personal, care relevă necesitatea limitării volumului datelor cu caracter personal prelucrate, în așa fel încât să fie prelucrate doar informațiile relevante și necesare în contextul realizării sarcinilor SI RF.

Capitolul II

SPAȚIUL JURIDICO-NORMATIV AL FUNCȚIONĂRII SI RF

7. Elaborarea SI RF este reglementată de următoarele acte normative și documente de politici:
 - 1) Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;
 - 2) Codul civil nr. nr. 1107/2002;
 - 3) Legea nr.133/2011 privind protecția datelor cu caracter personal.
8. Crearea și funcționarea SI RF este reglementată, în particular, de următoarele acte normative și documente de politici:
 - 1) Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat;
 - 2) Legea nr.71/2007 cu privire la registre;
 - 3) Legea nr.142/2018 cu privire la schimbul de date și interoperabilitate;

- 4) Hotărârea Guvernului nr.562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;
- 5) 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;
- 6) Hotărârea Guvernului nr.1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- 7) Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
- 8) Hotărârea Guvernului nr.405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
- 9) Hotărârea Guvernului nr.708/2014 privind serviciul electronic guvernamental de jurnalizare „(MLog)”;
- 10) Hotărârea Guvernului nr.201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;
- 11) Hotărârea Guvernului nr.211/2019 privind platforma de interoperabilitate (MConnect);
- 12) Ordinul ministrului dezvoltării informaționale nr. 78/2006 cu privire la aprobarea reglementării tehnice „Procese ciclului de viață al software-ului” RT 38370656 – 002:2006;
- 13) Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul de date public și de raționalizare a administrării sistemelor informaționale de stat.

Capitolul III

SPAȚIUL FUNCȚIONAL AL SI RF

9. SI RF asigură realizarea funcțiilor de bază ale unui sistem informațional, stipulate conform legislației, precum și a funcțiilor specifice ce reies din destinația sistemului informațional.
10. Funcțiile de bază ale SI RF sunt:
 - 1) formarea bazei de date a SI RF:
 - a) luarea în evidență primară, care constă în atribuirea identificadorului unic obiectului de evidență și introducerea în baza de date a volumului stabilit de date;
 - b) actualizarea datelor;
 - c) radierea, care nu presupune excluderea fizică a datelor din registru, ci doar schimbarea statutului acestora.
 - 2) formarea resursei informaționale. Funcțiile de bază în procesul de formare a bazei de date a SI RF sunt cele de evidență a fiduciilor care au fost constituite/înființate, în temeiul contractelor de fiducie, declarațiilor unilaterale de constituire a fiducie, fiduciilor constituite prin testament, iar în cazurile expres prevăzute de lege, constituite prin act administrativ sau hotărâre judecătorească;
 - 3) jurnalizarea evenimentelor. Orice acțiune a utilizatorilor se documentează în registre electronice speciale, arătând momentul și utilizatorul care a efectuat acțiunea. Pentru fiecare acțiune a utilizatorului se salvează în evenimentul jurnalizat datele care au fost modificate. SI RF jurnalizează evenimentele de business critice prin intermediul serviciului electronic guvernamental de jurnalizare (MLog). Acțiunile care sunt jurnalizate prin intermediul serviciului electronic guvernamental de jurnalizare (MLog) pot fi configurate în opțiunile de administrare. SI RF jurnalizează local evenimentele ce țin de buna funcționare a RF;

- 4) organizarea asigurării informaționale prin oferirea accesului la datele din SI RF utilizatorilor autentificați. Fiecare utilizator urmează să utilizeze datele din SI RF doar în scopuri legale și în conformitate cu drepturile atribuite;
- 5) asigurarea informațională a SI sub toate aspectele;
- 6) asigurarea securității informației;
- 7) asigurarea funcționării SI sub toate aspectele.

11. Având în vedere funcțiile SI RF, acesta va avea următoarele contururi funcționale de bază:

- 1) conturul înregistrarea informației, care asigură următoarele funcții specifice:
 - a) luarea în evidență primară, actualizarea și radierea din SI RF a fiduciei aferent contractelor de fiducie, declarațiilor unilaterale de constituire a fiduciei, fiduciilor constituite prin testament, iar în cazurile expres prevăzute de lege, constituite prin act administrativ sau hotărâre judecătorească;
 - b) evidența fiduciei aferent contractelor de fiducie, declarațiilor unilaterale de constituire a fiduciei, fiduciilor constituite prin testament, iar în cazurile expres prevăzute de lege, constituite prin act administrativ sau hotărâre judecătorească.
- 2) conturul „Generator de rapoarte”, care asigură generarea rapoartelor și a statisticilor;
- 3) conturul „Interoperabilitatea cu alte sisteme informaționale”;
- 4) conturul „Administrare și Control”, care asigură următoarele funcții:
 - a) administrarea bazei de date;
 - b) asigurarea integrității logice a SI RF;
 - c) determinarea nivelului de acces al utilizatorilor;
 - d) asigurarea securității și protecției informației în SI RF;
 - e) jurnalizarea evenimentelor de sistem;
 - f) monitorizarea performanței SI RF;
 - g) suport tehnic și mentenanță.

12. Funcțiile de administrare sunt destinate administrării și configurării Sistemului informațional, printre acestea fiind:

- 1) funcția de gestiune a utilizatorilor, rolurilor, grupurilor și drepturilor;
- 2) funcția de administrare a datelor de referință (nomenclatoare, clasificatoare, indici și alte metadate);
- 3) funcția de administrare a spațiului de lucru;
- 4) grupul de funcții de definire a fluxurilor de lucru;
- 5) funcția de asigurare a calității informației;
- 6) funcția de asigurare a securității și protecției informației.

13. Funcțiile de sistem asigură utilizarea sistemului și susțin realizarea funcțiilor de bază. Dintre funcțiile de sistem sunt relevante, în special, următoarele:

- 1) funcția de autentificare a utilizatorilor;
- 2) funcția de autorizare a utilizatorilor.

Capitolul IV

STRUCTURA ORGANIZAȚIONALĂ AL SI RF

14. Funcțiile de bază privind formarea și exploatarea SI RF sunt distribuite între:

- 1) Proprietarul sistemului;
- 2) Posesorul sistemului;
- 3) Deținătorul sistemului;
- 4) Administratorul tehnic sistemului;
- 5) Registratorul sistemului;
- 6) Furnizorul de date sistemului;

- 7) Destinatarii datelor sistemului.
15. Proprietarul SI RF este statul care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din Registru.
16. Posesorul și deținătorul SI RF este Serviciul Fiscal de Stat (în continuare - SFS), care asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea SI RF, precum și realizarea nemijlocită a competențelor de creare, administrare, mentenanță și dezvoltare a SI RF.
17. Administratorul tehnic al Registrului este Instituția Publică ”Serviciul Tehnologia Informației și Securitate Cibernetică”, care își realizează atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a sistemelor informaționale de stat.
18. Registratorul este SFS care are atribuția de înregistrare, actualizare/modificare a datelor în Registru, în baza informației recepționate de la persoane fizice și juridice.
19. Furnizorii de date sunt persoanele fizice și juridice care dețin calitatea de fiduciar, inclusiv prin intermediul reprezentantului legal al acestora, în condițiile art. 2094 din Codul civil.
20. Furnizorii de date sunt obligați să asigure corectitudinea și autenticitatea datelor prezentate pentru a fi înscrise în Registru.
21. Destinatarii datelor Registrului sunt:
- 1) autoritățile și instituțiile publice;
 - 2) părțile fiduciei aferent contractelor de fiducie, declarațiilor unilaterale de constituire a fiduciei, fiduciilor constituite prin testament, iar în cazurile expres prevăzute de lege, constituite prin act administrativ sau hotărâre judecătorească, în care sunt vizate/parte;
 - 3) persoanelor fizice și juridice menționate la art. 14 alin. (22) din Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;
 - 4) Utilizatorii SI RF.

Capitolul V

DOCUMENTELE SI RF

22. Documentele SI RF reprezintă totalitatea documentelor procedurale necesare înregistrării fiduciilor care au fost constituite/înființate, în temeiul contractelor de fiducie, declarațiilor unilaterale de constituire a fiduciei, fiduciilor constituite prin testament, iar în cazurile expres prevăzute de lege, constituite prin act administrativ sau hotărâre judecătorească.
23. SI RF va utiliza datele până la atingerea scopului, ulterior va permite arhivarea datelor și a documentelor în format electronic, în vederea eficientizării procesului de prelucrare și furnizare către utilizatorul a informației documentate.
24. Procedura de înregistrare, modificare, completare și radiere, precum și termenul de păstrare a datelor cu caracter personal în cadrul modulelor SI RF se reglementează prin anexa nr. 2 la prezenta hotărâre.
25. În cadrul SI RF se folosesc următoarele categorii de documente:
- 1) documente de intrare, care sunt relevante populării cu date SI RF, care pot fi în format electronic sau pe suport de hârtie și care reprezintă cererea privind înregistrarea fiduciei, actul de identitate a fiduciarului, actul de constituire/înființare a fiduciei;
 - 2) documente de ieșire, care se consideră documentul final care poate fi utilizat și care reprezintă certificat privind înregistrarea fiduciei;
 - 3) documente tehnologice, care reprezintă structura registrului fiduciilor.

Capitolul VI

SPAȚIUL INFORMAȚIONAL AL SI RF

Secțiunea 1

Obiectele informaționale

26. SI RF este reprezentată de un ansamblu de obiecte informaționale și interacțiunea acestora, organizate în concordanță cu necesitățile soluției aplicative. Obiectele informaționale principale aferente componentei de gestiune/evidență a datelor sunt:

- a) Cerere;
- b) Fiducia;
- c) Certificat.

Secțiunea 2

Identificatori și datele obiectelor informaționale

27. Identificarea obiectelor SI RF prin utilizarea pentru fiecare dintre ele a numărului de identificare unic generat și atribuit de sistem.

28. Identificatorul obiectului informațional „Cerere” este cheia unică formată din litere și cifre atribuit de SI RF.

29. Identificatorul obiectului informațional „Cod unic de identificare a fiduciei” reprezintă o serie de 5 simboluri alfanumerice aranjate într-o ordine strictă:

XXXXX

Unde:

X - este cifra atribuită de sistem în ordine cronologică la etapa înregistrării fiduciei de către Serviciul Fiscal de Stat.

30. Identificatorul obiectului informațional „Certificat” este cheia unică formată din litere și cifre.

31. În SI RF se utilizează următorii identificatori ai obiectelor informaționale principale aferente componentei de gestiune/evidență a datelor sunt:

1) cerere:

- a) Date de identificare a fiduciarului/fiduciarilor, completate de către fiduciar;
- b) Date de identificare a constitutorului/constitutorilor, completate de către fiduciar;
- c) Datele de identificare a beneficiarului/beneficiarilor, completate de către fiduciar;
- d) Datele de identificare a asistentului fiduciei, completate de către fiduciar;
- e) Datele de identificare a beneficiarului/beneficiarilor efectiv, completate de către fiduciar;
- f) Date despre fiducie, completate de către fiduciar;
- g) Termenul fiduciei, completate de către fiduciar.

2) fiducia:

- a) Cod unic de identificare, generat de Registru la etapa examinării cererii de înregistrare;
- b) Date de identificare a fiduciarului/fiduciarilor, conform datelor completate de către fiduciar;
- c) Date de identificare a constitutorului/constitutorilor, conform datelor completate de către fiduciar;
- d) Datele de identificare a beneficiarului/beneficiarilor, conform datelor completate de către fiduciar;
- e) Datele de identificare a asistentului fiduciei, conform datelor completate de către fiduciar;
- f) Datele de identificare a beneficiarului/beneficiarilor efectiv, conform datelor completate de către fiduciar;
- g) Date despre fiducie, conform datelor completate de către fiduciar;
- h) Termenul fiduciei, conform datelor completate de către fiduciar.

3) certificat:

- a) Cod unic de identificare, generat de Registru la etapa examinării cererii de înregistrare;
- b) Actul de constituire/înființare a fiduciei, prezentat de către fiduciar;
- c) Denumirea fiduciei, conform datelor completate de către fiduciar;
- d) Data încetării fiduciei, conform datelor completate de către fiduciar;
- e) Numele și prenumele/denumirea fiduciarului/fiduciarilor, conform datelor completate de către fiduciar;
- f) Codul fiscal/Codul de identificare fiscală fiduciarului/fiduciarilor, conform datelor completate de către fiduciar;
- g) Rezidența fiscală fiduciarului/fiduciarilor, conform datelor completate de către fiduciar;
- h) Numele și prenumele/denumirea beneficiarului/beneficiarilor, conform datelor completate de către fiduciar;
- i) Codul fiscal/Codul de identificare fiscală beneficiarului/beneficiarilor, conform datelor completate de către fiduciar;
- j) Cetățenia beneficiarului/beneficiarilor, conform datelor completate de către fiduciar;
- k) Rezidența fiscală beneficiarului/beneficiarilor, conform datelor completate de către fiduciar.

Secțiunea 3

Scenariile de bază utilizate

32. Scenariile de bază din cadrul SI RF sunt dezvoltate și relaționate obiectelor informaționale ale sistemului, având la bază necesitățile de colectare de date necesare pentru asigurarea îndeplinirii consecvente a funcționalităților scontate.

33. Scenariile de bază aferente componentei de gestiune/evidență a datelor sunt:

- 1) Recepționarea obiectului informațional Cerere:
 - a) înregistrarea, care constă în recepționarea cererii privind înregistrarea/modificarea fiduciei;
 - b) analiza, care constă în verificarea datelor incluse în cerere;
 - c) arhivarea, care constă în modificarea statutului obiectului informațional și transmiterea acestuia în arhivă, urmare terminării procesului.
- 2) Înregistrarea obiectului informațional Fiducia:
 - a) înregistrarea, care constă în popularea cu date a Registrului conform datelor completate în cerere;
 - b) actualizarea datelor, care constă în modificarea datelor introduce în Registru conform datelor completate în cererea de modificare/încetare;
 - c) arhivarea, care constă în modificarea statutului obiectului informațional și transmiterea acestuia în arhivă, urmare terminării procesului.
- 3) Eliberarea obiectului informațional Certificat:
 - a) completarea, care constă în completarea automata sau manuală cu date confirmative aferente fiduciilor care au fost constituite/înființate conform prevederilor Republicii Moldova, în temeiul contractelor de fiducie, declarațiilor unilaterale de constituire a fiducie, fiduciilor constituite prin testament, iar în cazurile expres prevăzute de lege, constituite prin act administrativ sau hotărâre judecătorească;

- b) generarea, care constă în afișarea/imprimarea certificatului și prezentarea/expedierea în adresa fiduciarului;
- c) arhivarea, care constă în modificarea statutului obiectului informațional și transmiterea acestuia în arhivă, urmare terminării procesului.

Secțiunea 4

Interacțiunea cu alte sisteme informaționale

34. SI RF se integrează și interacționează cu următoarele sisteme informaționale:

- 1) Sistemul informațional automatizat „Registrul de stat al populației” – pentru schimbul automatizat de date despre persoane fizice;
- 2) Sistemul informațional „Registrul de stat al unităților de drept” – date despre toate categoriile de unități de drept, constituite în bază legală, adresa juridică;
- 3) Sistemul informațional automatizat „Registrul fiscal de stat” – date despre înregistrarea nerezidenților;
- 4) Platforma de interoperabilitate (MConnect) – soluție tehnică, destinată asigurării schimbului de date dintre sistemele informaționale deținute de către participanții la schimbul de date;
- 5) Serviciul electronic guvernamental de autentificare și control al accesului (MPass) – serviciu reutilizabil, care are scopul de a oferi un mecanism integrator, securizat și flexibil de autentificare și control al accesului utilizatorilor în sistemele informaționale, inclusiv serviciile electronice;
- 6) Serviciul electronic guvernamental integrat de semnătură electronică (MSign) – serviciu reutilizabil, care are scopul de a oferi un mecanism integrator, securizat și flexibil al diferitelor soluții de aplicare și verificare a autenticității semnăturii electronice de către utilizatori (inclusiv în contextul utilizării sistemelor informaționale și a serviciilor electronice), oferite de către furnizorii de semnătură electronică în conformitate cu legislația;
- 7) Serviciul electronic guvernamental de notificare (MNotify) – soluție informațională din categoria Guvern către Cetățean (G2C) și Guvern către Business (G2B), și are ca obiectiv principal asigurarea necesităților informatice și informaționale pentru realizarea procesului de notificare;
- 8) Serviciul electronic guvernamental de jurnalizare (MLog) – serviciu centralizat, reutilizabil, care are scopul de a oferi un mecanism securizat și flexibil de jurnalizare și audit, asigurând evidența evenimentelor, în contextul utilizării sistemelor informaționale;
- 9) Sistemul informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) – sistem informațional constituit dintr-un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii, aflate în interconexiune, destinate consemnării împuternicirilor de reprezentare în baza semnăturii electronice, acordate de către persoane fizice sau persoane juridice altor persoane fizice sau persoane juridice.

Capitolul VII

SPAȚIUL TEHNOLOGIC AL SI RF

35. SI RF va utiliza standarde deschise și va fi compatibil cu sistemele care, la fel, utilizează atât standarde nonproprietary, cât și standarde deja existente.

- 36.** Arhitectura complexului resurselor TI, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale se determină de către posesor în etapele ulterioare de dezvoltare a SI RF, ținând cont de:
- 1) implementarea unei soluții bazate pe SOA (Service-Oriented Architecture – arhitectură software bazată pe servicii), care oferă posibilitatea reutilizării unor funcții ale SI RF cu noi funcționalități, fără a afecta funcționarea SI RF;
 - 2) implementarea funcționalităților de arhivare (backup) și restabilire a datelor în caz de incidente.
- 37.** SI RF va putea fi ușor extins pe verticală, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori atât în regim normal de lucru, cât și în perioadele de vârf.
- 38.** Sistemul de comunicații se va baza pe infrastructură și echipamentul rețelelor guvernamentale, care includ posibilitatea conectării la Internet. Infrastructura existentă va fi planificată în mod corespunzător, pentru a oferi nivelurile adecvate de performanță și capacitate.
- 39.** Interfața de utilizare a SI RF se va adapta automat la diverse rezoluții de afișare.
- 40.** SI RF este găzduit pe platforma tehnologică guvernamentală comună (Mcloud) și este compatibil cu platforma de găzduire bazată pe tehnologii de tip container.

Capitolul VIII

ASIGURAREA SECURITĂȚII INFORMAȚIONALE

- 41.** Securitatea informațională presupune protecția SI RF 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.
- 42.** Asigurarea securității informației va fi realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr.201/2017. Personalul implicat în utilizarea și administrarea SI RF 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.
- 43.** SI RF asigură realizarea următoarelor obiective de securitate:
- 1) autentificarea – garantează că zonele restricționate ale SI RF vor fi accesibile doar utilizatorilor cu o identitate verificată;
 - 2) autorizarea – garantează că utilizatorii autentificați pot accesa serviciile și datele care corespund drepturilor lor de acces;
 - 3) confidențialitatea – garantează că datele înregistrate în RF nu pot fi accesate de o parte terță neautorizată;
 - 4) integritatea – garantează că datele înregistrate în RF nu au fost modificate sau alterate de o parte terță neautorizată.
 - 5) non-repudierea: măsură prin care se asigură faptul că, după emiterea/recepționarea unei informații, expeditorul/destinatarul nu poate nega, în mod fals, că a expedit/primit informații;
 - 6) mentenanță: SI RF trebuie asigurat în permanență cu suportul și mentenanța necesară conform nivelului agreat de servicii.
- 44.** Pentru atingerea obiectivelor de securitate, SI RF dispune de mai multe mecanisme de securitate:
- 1) antivirus/antispam – soluțiile TI asigură protecția antivirus și antispam pentru toate serverele. Fișierele se scanează la încărcare în SI RF. În cazul detectării unui fișier infectat, procedura de încărcare este oprită și fișierul – respins;

- 2) backup sistematic al datelor păstrate – permite recuperarea rapidă și fiabilă a datelor în caz de incident care a dus la pierderea sau deteriorarea datelor;
 - 3) 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 SI RF, cu acces limitat pentru utilizatorii neautorizați.
45. În cadrul SI RF se asigură generarea și 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 operațiunilor și rezultatele acestora pot fi solicitate de către organele competente în investigarea potențialelor încălcări ale regimului de prelucrare/protecție a datelor cu caracter personal. SI RF va utiliza funcționalitatea de autentificare doar prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass).
46. Utilizatorii SI RF vor fi autorizați să acceseze doar blocurile funcționale și datele pentru care au permisiunile necesare, conform rolurilor fiecăruia. Utilizatorii și rolurile acestora vor fi gestionate prin intermediul serviciului MPass. SI RF va prelua rolurile utilizatorilor din serviciul electronic guvernamental de autentificare și control al accesului (MPass).
47. O necesitate importantă legată de securitate este necesitatea păstrării înregistrărilor de audit pentru analiza integrității SI RF și pentru monitorizarea activității utilizatorilor. SI RF se va baza pe un mecanism de înregistrări de audit dublu (intern și cu utilizarea serviciului electronic guvernamental de jurnalizare (MLog), ce urmează practicile internaționale.

Capitolul X

ÎNCHEIERE

48. Prezentul Concept conține descrierea principalelor aspecte organizaționale, metodologice și tehnologice în conformitate cu care este concepută și implementată soluția tehnică necesară să asigure evidența fiduciilor care au fost constituite/înființate, în temeiul contractelor de fiducie, declarațiilor unilaterale de constituire a fiducie, fiduciilor constituite prin testament, iar în cazurile expres prevăzute de lege, constituite prin act administrativ sau hotărâre judecătorească.
49. Implementarea SI RF va permite angajaților SFS să realizeze înregistrarea, actualizarea și radierea acestora, precum și a informațiilor aferente într-un mod autonom, fără intervenția altor entități.
50. În scopul asigurării interoperabilității și a schimbului de date a SI RF cu alte sisteme și resurse informaționale de stat, Serviciul Fiscal de Stat înregistrează activele semantice utilizate în Sistemul informațional „Catalogul semantic”.

REGULAMENTUL

Registrului fiduciilor și construcțiilor juridice similare

Capitolul I

Dispoziții generale

1. Registrul reprezintă registrul de evidență a fiduciilor sau construcțiilor juridice similare (în continuare fiducie) care au fost constituite/înființate conform prevederilor cadrului normativ al Republicii Moldova, în temeiul contractelor de fiducie, declarațiilor unilaterale de constituire a fiduciei, fiduciilor constituite prin testament, iar în cazurile expres prevăzute de lege, constituite prin act administrativ sau hotărâre judecătorească.
2. Regulamentul Registrului fiduciilor și construcțiilor juridice similare (în continuare - Regulament) cuprinde reglementări privind drepturile și obligațiile subiecților raporturilor juridice aferente creării și ținerii Registrului fiduciilor și construcțiilor juridice similare; modalitatea de ținere a Registrului; procedura de înregistrare, modificare, completare și radiere a datelor; procedura de interacțiune cu furnizorii de date; măsuri privind asigurarea securității resursei informaționale.

Capitolul II

SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII, GESTIONĂRII ȘI ACTUALIZĂRII REGISTRULUI

3. Subiecții din domeniul creării, gestionării și actualizării Registrului sunt:
 - 1) Proprietarul;
 - 2) Posesorul;
 - 3) Deținătorul;
 - 4) Registratorul;
 - 5) Furnizorul de date;
 - 6) Destinatarul datelor.
4. Proprietarul Registrului este statul, care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din Registru.
5. Posesorul și deținătorul SI RF este Serviciul Fiscal de Stat (în continuare - SFS), care asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea SI RF, ținerea registrului în conformitate cu regulile de ținere a registrului, asigură autenticitatea, plenitudinea și integritatea datelor din registru, securitatea și protecția datelor din registru, cât și asigură tuturor destinatarilor acces la datele din registru în conformitate cu legea și cu regulile de ținere a registrilor.
6. Furnizorii de date sunt persoanele fizice și juridice care dețin calitatea de fiduciar. Persoana juridică este obligată să desemneze o singură persoană fizică care va exercita permanent funcțiile sale.

7. Furnizorii de date sunt obligați să asigure corectitudinea și autenticitatea datelor prezentate pentru a fi înscrise în Registru;
8. Destinatarii datelor Registrului sunt:
 - 1) autoritățile și instituțiile publice;
 - 2) părțile fiduciei, aferent contractelor de fiducie, declarațiilor unilaterale de constituire a fiduciei, fiduciilor constituite prin testament, iar în cazurile expres prevăzute de lege, constituite prin act administrativ sau hotărâre judecătorească, în care sunt vizate/parte;
 - 3) Entitățile raportoare prevăzute la art. 4 alin. (1) din Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;
 - 4) Utilizatorii SI RF.
9. Administratorul tehnic al Registrului este Instituția Publică ”Serviciul Tehnologia Informației și Securitate Cibernetică”, care își realizează atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a sistemelor informaționale de stat.

Capitolul III

DREPTURILE ȘI OBLIGAȚIILE PARTICIPANȚILOR LA REGISTRU

10. Posesorul, Deținătorul și Registratorul au următoarele drepturi:

- 1) Să propună, în baza competențelor sale, îmbunătățiri ale cadrului normativ cu privire la Registrul fiduciilor;
- 2) Să propună soluții de perfecționare și eficientizare a procesului de funcționare a Registrului;
- 3) Să inițieze procedura de suspendare sau revocare a accesului la Registrul fiduciilor pentru participanții care nu respectă regulile, standardele și normele în domeniul securității informaționale;
- 4) Să verifice autenticitatea și veridicitatea datelor introduse de către Registratori în Registrul fiduciilor;
- 5) Să vizualizeze și să editeze informațiile din Registrul fiduciilor conform rolului atribuit;
- 6) Să acceseze spațiul informațional și informațiile care se conțin în Registrul fiduciilor.

11. Posesorul, Deținătorul și Registratorul au următoarele obligații:

- 1) Să asigure ținerea RF în conformitate cu regulile de ținere a registrului, aprobate prin prezenta hotărâre;
- 2) Să asigure funcționalitatea neîntreruptă a Registrului și ținerea acestuia în conformitate cu cadrul normativ;
- 3) Să acorde suportul necesar persoanelor autorizate care au acces la RF privind utilizarea complexului de mijloace software aferente acestuia;
- 4) Să informeze participanții la RF despre modificările condițiilor tehnice de funcționare a acestuia;
- 5) Să asigure implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitatea informației și a datelor cu caracter personal;
- 6) Să utilizeze informația din RF doar în scopurile stabilite de prezentul Regulament;
- 7) Să asigure actualizarea datelor introduse în RF, inclusiv corectitudinea, autenticitatea și veridicitatea datelor introduse în RF.
- 8) Să monitorizeze și să supravegheze accesările datelor din SI RF și identifică încălcările comise;
- 9) Să asigure ținerea auditului operațiunilor de prelucrare a datelor cu caracter personal în SI RF în funcție de criterii și indicatori specifici.

12. Furnizorii de date au următoarele drepturi:

- 1) să solicite și să primească de la posesorul SI RF ajutor metodologic și practic privind funcționarea acestuia;
- 2) să prezinte propuneri posesorului SI RF privind perfecționarea și eficientizarea funcționării acestuia;
- 3) să colaboreze cu deținătorul SI RF pentru asigurarea securității accesului la SI RF și să informeze despre orice acțiune suspicioasă de care are cunoștință și care ar putea să reprezinte un atentat la securitatea accesului la SI RF.

13. Furnizorii de date au obligația să asigure corectitudinea și autenticitatea datelor prezentate pentru a fi înscrise în Registru.**14. Destinatarii datelor au următoarele drepturi:**

- 1) să solicite și să primească de la posesorul SI RF ajutor metodologic și practic privind funcționarea acestuia;
- 2) să prezinte propuneri posesorului SI RF privind perfecționarea și eficientizarea funcționării acestuia;
- 3) să înainteze posesorului SI RF propuneri privind modificarea și/sau completarea actelor normative care reglementează funcționarea SI RF.

15. Destinatarii datelor au următoarele obligații:

- 1) să utilizeze informația obținută din baza de date a SI RF doar în scopurile stabilite de legislație;
- 2) să întreprindă toate măsurile necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu instrucțiunile deținătorului SI RF și cu prevederile Legii nr. 133/2011 privind protecția datelor cu caracter personal;
- 3) să raporteze imediat, în formă verbală sau scrisă, posesorului SI RF și/sau administratorului tehnic despre incidentele de securitate;
- 4) să nu întreprindă anumite acțiuni în vederea obținerii accesului neautorizat la informații, indiferent de metodă.

Capitolul IV

CONȚINUTUL REGISTRULUI

16. Registrul este ținut în formă electronică.

17. Forma și conținutul Registrului fiduciilor este stabilită în anexa nr. 1 al Regulamentului.

18. Înregistrarea datelor cu privire la fiducie în Registrul fiduciilor se efectuează de către Serviciul Fiscal de Stat.

19. Înscrierile se efectuează în ordine cronologică, fiecărei fiduciei fiindu-i atribuit cod unic de identificare generat de Registrul la etapa înregistrării de către Serviciul Fiscal de Stat.

20. Codul unic de identificare este unic, invariabil și nu poate fi atribuit altor fiducii, inclusiv după radierea acestuia din Registru.

21. Codul unic de identificare, atribuit fiduciei la înregistrarea în Registru, se indică de către fiduciar la depunerea cererilor de modificare sau încetare a fiduciei.

Capitolul V

ÎNREGISTRAREA FIDUCIILOR SAU CONSTRUCȚIILOR JURIDICE SIMILARE

22. Pentru înregistrarea fiduciei, fiduciarul și/sau reprezentantul legal al acestuia depune la Serviciul Fiscal de Stat, în termen de 30 de zile calendaristice de la data constituirii/înființării fiduciei,

cererea privind înregistrarea fiduciei, prevăzută în anexa nr. 2 al Regulamentului, denumită în continuare cerere, care va fi însoțită de următoarele documente:

- 1) Actul de identitate/identificare a fiduciarului sau copia autentificată a acestuia;
 - 2) Actul de constituire/înființare a fiduciei sau copia autentificată a acestuia.
23. Cererea se depune pe suport de hârtie semnată olograf sau în format electronic semnată cu semnătură electronică calificată.
24. În termen de 3 zile lucrătoare de la depunerea cererii prevăzute la pct. 23, Serviciul Fiscal de Stat va emite un Certificat de înregistrare a fiduciei, prevăzută în anexa nr. 3 al Regulamentului.
25. Data înregistrării la Serviciul Fiscal de Stat a fiduciei este data emiterii Certificatului de înregistrare a fiduciei.
26. Mențiunile privind modificarea sau radierea fiduciei se declară prin completarea și depunerea cererii, prevăzute la pct. 23, în termen de 30 de zile calendaristice din momentul survenirii modificării sau încetării fiduciei, având bifată în formular căsuța „Modificare” sau „Încetare”, însoțită de următoarele documente:
- 1) Actul de identitate a fiduciarului sau copia autentificată a acestuia;
 - 2) Actul de modificare sau radiere a fiduciei sau copia autentificată a acestuia.
27. Actele prevăzute la pct. 22 și 26 se vor autentifica în modul prevăzut de legislație.
28. În cazul modificării sau încetării fiduciei, în termen de 3 zile lucrătoare de la depunerea cererii prevăzute la pct. 26, Serviciul Fiscal de Stat va emite un Certificat de înregistrare a fiduciei cu datele actualizate.
29. În cazul pierderii/distrugerii Certificatului de înregistrare a fiduciei, Serviciul Fiscal de Stat va elibera fiduciarului un duplicat al certificatului, conform procedurii, în termen de trei zile lucrătoare din data depunerii cererii. În cazul pierderii certificatului de atribuire a codului fiscal, la cerere se va anexa dovada de publicare a pierderii/distrugerii în Monitorul Oficial al Republicii Moldova.
30. Înregistrarea fiduciei va fi realizată la prezentarea informației menționate în Anexa nr. 2.

Capitolul VI

REGIMUL JURIDIC DE UTILIZARE A DATELOR DIN SI RF

31. Datele din „RF” au un caracter public, cu excepția datelor cu acces limitat din domeniul datelor cu caracter personal și a celor care asigură securitatea sistemului informațional, în privința cărora se aplică cadrul normativ ce reglementează domeniile respective.
32. Accesul la datele cu acces limitat din „RF” este condiționat de rolul utilizatorului. Astfel registratorul care are acces tehnic la datele din „RF”, ceea ce presupune introducerea, modificarea datelor înscrise de acesta. Ceilalți utilizatori au acces la introducerea informației și acces informațional, ceea ce presupune introducerea datelor conform nivelului de acces, vizualizarea datelor numai în formatul individual permis. Totodată registratorul în unele cazuri poate avea rolul de utilizator cu acces limitat informațional la date.
33. SFS asigură înregistrarea „RF” prin intermediul Sistemului informațional „Registrul resurselor și sistemelor informaționale de stat”.
34. Punerea la dispoziție de către Posesorul, Deținătorul și Participanți a datelor din „RF” se realizează prin:
- 1) acordarea accesului autorizat la SI „RA”;
 - 2) acordarea informației prin intermediul poștei electronice sau altor mijloace de comunicații electronice/aplicații web, conform prevederilor normative.
35. Acordarea accesului la datele din „RF” se va efectua prin intermediul platformei de interoperabilitate (Mconnect).
36. Datele cu caracter personal ale persoanelor fizice se utilizează în conformitate cu actele normative privind protecția datelor cu caracter personal.

Capitolul VII

ASIGURAREA SECURITĂȚII INFORMAȚIONALE

- 37.** Securitatea informațională presupune protecția Registrului 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.
- 38.** Asigurarea securității informației va fi realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr.201/2017. Personalul implicat în utilizarea și administrarea Registrului 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.
- 39.** Registrului asigură realizarea următoarelor obiective de securitate:
- 1) autentificarea – garantează că zonele restricționate ale Registrului vor fi accesibile doar utilizatorilor cu o identitate verificată;
 - 2) autorizarea – garantează că utilizatorii autentificați pot accesa serviciile și datele care corespund drepturilor lor de acces;
 - 3) confidențialitatea – garantează că datele înregistrate în Registru nu pot fi accesate de o parte terță neautorizată;
 - 4) integritatea – garantează că datele înregistrate în Registru nu au fost modificate sau alterate de o parte terță neautorizată.
- 40.** Pentru atingerea obiectivelor de securitate, Registrul dispune de mai multe mecanisme de securitate:
- 1) antivirus/antispam – soluțiile TI asigură protecția antivirus și antispam pentru toate serverele. Fișierele se scanează la încărcare în Registru. În cazul detectării unui fișier infectat, procedura de încărcare este oprită și fișierul – respins;
 - 2) backup sistematic al datelor păstrate – permite recuperarea rapidă și fiabilă a datelor în caz de incident care a dus la pierderea sau deteriorarea datelor;
 - 3) 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 Registrului, cu acces limitat pentru utilizatorii neautorizați.
- 41.** În cadrul Registrului se asigură generarea și 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 operațiunilor și rezultatele acestora pot fi solicitate de către organele competente în investigarea potențialelor încălcări ale regimului de prelucrare/protecție a datelor cu caracter personal. Registrul va utiliza funcționalitatea de autentificare doar prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass).
- 42.** Utilizatorii Registrului vor fi autorizați să acceseze doar blocurile funcționale și datele pentru care au permisiunile necesare, conform rolurilor fiecăruia. Utilizatorii și rolurile acestora vor fi gestionate prin intermediul serviciului MPass. SI RRSIS va prelua rolurile utilizatorilor din serviciul electronic guvernamental de autentificare și control al accesului (MPass).
- 43.** O necesitate importantă legată de securitate este necesitatea păstrării înregistrărilor de audit pentru analiza integrității SI RF și pentru monitorizarea activității utilizatorilor. Registrul se va baza pe un mecanism de înregistrări de audit dublu (intern și cu utilizarea serviciului electronic guvernamental de jurnalizare (MLog), ce urmează practicile internaționale.

Capitolul VIII

CONTROLUL ȘI RESPONSABILITATEA

- 44.** SI RF este supus unui control intern. Controlul intern privind organizarea și funcționarea SI RF se efectuează de către SFS.
- 45.** Responsabilitatea pentru organizarea funcționării SI RF aparține posesorului acestuia.
- 46.** Subiecții, în atribuțiile cărora intră ținerea SI RF înscrierea datelor, furnizarea informațiilor din SI RF precum și asigurarea funcționării SI RF poartă responsabilitatea, pentru autenticitatea, fiabilitatea, integritatea informației, precum și pentru păstrarea/stocarea și utilizarea acesteia.
- 47.** Toți subiecții SI RF poartă răspundere conform legislației, pentru prelucrarea, divulgarea și transmiterea informației din SI RF ce conține date cu caracter personal persoanelor terțe, contrar prevederilor legislației.
- 48.** Păstrarea SI RF este asigurată de posesor până la adoptarea deciziei despre scoaterea din exploatare a acestuia. În cazul scoaterii din exploatare, datele și documentele conținute în acesta se transmit în arhivă conform legislației.
- 49.** Pentru asigurarea funcționalității eficiente și neîntrerupte a SI RF, schimbul informațional dintre participanții la SI RF și baza de date este asigurat în regim nonstop.

Anexa nr. 1
la Regulamentul Registrul fiduciilor și construcțiilor juridice similare

REGISTRUL FIDUCIILOR SAU CONSTRUCȚIILOR JURIDICE SIMILARE

[illegible]

CERERE
din _____

Înregistrare

Actualizare

Radiere

1. Date de identificare a fiduciarului/fiduciarilor

1.1.Numele și prenumele/denumirea:

1.2. Data nașterii:

1.3.Codul fiscal/numărul de identificare personal
(IDNP)

1.4.Domiciliul:

1.5.Date de contact (telefon, e-mail):

1.6.Rezidența fiscală/țara de reședință:

1.7. Cetățenia:

2. Date de identificare a constitutorului/constitutorilor

2.1.Numele și prenumele/denumirea:

2.2. Data nașterii:

2.3.Codul fiscal/numărul de identificare personal
(IDNP)

2.4.Domiciliul:

2.5.Date de contact (telefon, e-mail):

2.6.Rezidența fiscală/țara de reședință:

2.7.Cetățenia:

3. Datele de identificare a beneficiarului/beneficiarilor

3.1.Numele și prenumele/denumirea:

3.2.Data nașterii:

3.3.Codul fiscal/numărul de identificare personal
(IDNP):

3.4.Domiciliul:

3.5.Date de contact (telefon, e-mail):

3.6.Rezidența fiscală:

3.7.Cetățenia:

4. Datele de identificare a asistentului fiduciei

4.1.Numele și prenumele/denumirea:

4.2. Data nașterii:

4.3.Codul fiscal/numărul de identificare personal
(INDP):

4.4.Domiciliul:

4.5.Date de contact (telefon, e-mail):

4.6.Rezidența fiscală/țara de reședință:

4.7.Cetățenia:

5. Datele de identificare a beneficiarului/beneficiarilor efectiv/efectivi

5.1.Numele și prenumele

5.2.Data nașterii

5.3.Codul fiscal

5.4.Cetățenia

5.5.Domiciliul:

5.6.Date de contact (telefon, e-mail):

5.7.Rezidența fiscală:

6. Datele de identificare a reprezentantului legal al fiduciarului

6.1.Numele și prenumele

6.2.Codul fiscal

6.3.Cetățenia

6.4.Domiciliul:

6.5.Date de contact (telefon, e-mail):

6.6.Rezidența fiscală:

7. Date despre fiducie sau construcției juridice similare

7.1.Actul de constituire/înființare a fiduciei

7.2.Numărul

7.3.Data

7.4.Actul de modificare a fiduciei

7.5.Numărul

7.6.Data

7.7.Actul de încetare a fiduciei

7.8.Numărul

7.9.Data

7.10. Denumirea fiduciei

7.11. Cod unic de identificare*
(se completează pentru cererile de actualizare sau
radiere)

8. Termenul fiduciei

8.1.Data instituirii

8.2.Data radierii

La cerere sunt anexate următoarele documente:

1.

2.

(semnătura depunătorului)

Mențiunea Serviciului Fiscal de Stat despre recepționarea cererii
--

/Antetul Serviciului Fiscal de Stat/

CERTIFICAT
privind înregistrarea fiduciei sau construcției juridice similare
Nr. ____ din _____

1. Codul unic de identificare, generat de
Registru la etapa examinării cererii de
înregistrare:
2. Numele, prenumele, numărul de
identificare personal (IDNP) a
fiduciarului/fiduciarilor:
3. Denumirea fiduciei/construcției juridice
similare:
4. Numele, prenumele, numărul de
identificare personal (IDNP) a
constituitorului/constituitorilor:
5. Numele, prenumele, numărul de
identificare personal (IDNP) a asistenului
fiduciei:
6. Numele, prenumele, data nașterii, numărul
de identificare personal (IDNP) a
beneficiarului/beneficiarilor efectivi.

_____	L.Ș.	_____	_____
(funcția deținută)	(semnătura)		(funcția numele, prenumele)