

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÎRE nr. _____

din _____
Chișinău

**Cu privire la aprobarea Conceptului Sistemului informațional
„Registrul de stat al serviciilor publice” și a Regulamentului
privind modul de ținere a Registrului de stat al serviciilor publice**

În temeiul art.2 alin.(1), 6 alin.(1) și 16 alin.(1) și (3) din Legea nr.71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314), cu modificările ulterioare, art.22 lit.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, Guvernul HOTĂRĂȘTE:

1. Se instituie Registrul de stat al serviciilor publice, format de Sistemul informațional „Registrul de stat al serviciilor publice”.

2. Se aprobă:

1) Conceptul Sistemului informațional „Registrul de stat al serviciilor publice”, conform anexei nr. 1;

2) Regulamentul privind modul de ținere a Registrului de stat al serviciilor publice, conform anexei nr. 2;

3) Regulamentul-cadru privind organizarea și prestarea serviciului public, conform anexei nr. 3.

3. Se desemnează Instituția publică „Agenția de Guvernare Electronică” în calitate de posesor și deținător al Registrului de stat al serviciilor publice.

4. Autoritățile și instituțiile publice, care, în limitele competențelor atribuite în conformitate cu actele normative, prestează servicii publice, vor utiliza Sistemul informațional „Registrul de stat al serviciilor publice” pentru înregistrarea serviciilor publice și a informațiilor aferente acestora.

5. În termen de 6 luni din momentul intrării în vigoare a prezentei hotărâri, autoritățile și instituțiile publice vor asigura înregistrarea în Registrul de stat al serviciilor publice a serviciilor publice incluse în Nomenclatorul integrat al serviciilor publice administrative, aprobat prin Hotărârea Guvernului nr.670/2020.

6. Proiecte de acte normative care propun instituirea unor servicii publice noi, ce urmează a fi înaintate spre examinare Guvernului, trebuie să prevadă în mod obligatoriu:

1) completarea Nomenclatorului, aprobat prin Hotărârea Guvernului nr.670/2020;

2) aprobarea Regulamentului privind organizarea și prestarea serviciului public respectiv, care va fi elaborat în baza Regulamentului-cadru privind organizarea și prestarea serviciului public, aprobat prin prezenta hotărâre.

7. Odată cu instituirea unui serviciu public nou, prestatorul acestuia asigură înregistrarea obligatorie a serviciului respectiv în Registrul de stat al serviciilor publice.

8. Instituția publică „Agenția de Guvernare Electronică” înregistrează în Sistemul informațional „Registrul de stat al serviciilor publice”, evenimentele de viață incluse în anexa nr.2 la Hotărârea Guvernului nr.670/2020, precum și alte evenimente de viață, identificate ca fiind necesare pentru corelarea cu serviciile publice.

9. În scopul implementării prezentei hotărâri, Cancelaria de Stat, în comun cu Instituția publică „Agenția de Guvernare Electronică”, vor evalua anual costurile necesare administrării și dezvoltării continue a Sistemului informațional „Registrul de stat al serviciilor publice” și vor înainta propuneri de solicitare a mijloacelor financiare necesare Ministerului Finanțelor în conformitate cu prevederile Legii finanțelor publice și responsabilității bugetar-fiscale nr.181/2014, pentru a fi incluse în legea bugetului de stat pe anul respectiv.

10. Prezenta hotărâre intră în vigoare la data publicării.

PRIM-MINISTRU

ION CHICU

Contrasemnează:

Ministrul economiei și infrastructurii

Anatol USATÎI

CONCEPTUL Sistemului informațional „Registrul de stat al serviciilor publice”

Capitolul I DISPOZIȚII GENERALE

1. Sistemul informațional „Registrul de stat al serviciilor publice” (în continuare - *SI RSSP*) este sistemul unic integrat de evidență automatizată a serviciilor publice prestate de autoritățile publice din Republica Moldova.

2. SI RSSP este parte componentă a sistemelor informaționale de stat ale Republicii Moldova și reprezintă un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii.

3. În sensul prezentului concept vor fi utilizate următoarele noțiuni de bază:

serviciu public (în continuare - servicii publice) – totalitatea activităților administrative cu caracter necomercial, instituite și reglementate normativ la nivel național în vederea executării cadrului normativ, organizate și desfășurate în regim de putere publică de către prestatorii de servicii publice, în beneficiul direct al persoanelor fizice sau juridice ori în scopul îndeplinirii de către aceștia a unor obligații prevăzute în cadrul normativ și/sau rezultatul acestor activități;

prestator al serviciului public (în continuare – prestatori de servicii):

- ministerul, altă autoritate administrativă centrală, Cancelaria de Stat sau structura organizațională din sfera lor de competență (autoritate administrativă din subordine, serviciul public desconcentrat și cel aflat în subordine, instituție publică sau întreprinderea de stat în care ministerul, altă autoritate administrativă centrală subordonată Guvernului sau Cancelaria de Stat are calitatea de fondator);

- persoană juridică de drept privat care prestează servicii publice, în limitele competențelor prevăzute de lege;

- autoritate publică autonomă față de Guvern și responsabilă față de Parlament;

- autoritate executivă a administrației publice locale, care prestează servicii publice în domeniile proprii de activitate ale autorităților publice locale și servicii publice descentralizate, transferate ei, în condițiile legii;

beneficiar al serviciului public – persoană fizică sau juridică de drept privat, la solicitarea și/sau în interesul căreia este prestat un serviciu public, inclusiv prin reprezentare sau solicitare asistată a prestării unui serviciu public;

eveniment de viață – denumirea generică a unui grup de servicii publice asociate unui fapt de importanță deosebită pentru o persoană fizică sau persoană juridică de drept privat;

regulamentul privind organizarea și prestarea serviciului public – act normativ aprobat de către autoritatea publică care instituie serviciul public și care stabilește cerințele pentru prestarea serviciului public și reflectă un sistem de prescripții ce descrie ordinea acțiunilor prestatorului, a subdiviziunilor și a angajaților acestuia, precum și condițiile, criteriile și alte elemente pentru realizarea ordinii de executare a acestor acțiuni și de luare a deciziilor, standardele

și criteriile de calitate ale procesului de prestare a serviciilor, inclusiv ordinea de interacțiune cu alți prestatori de servicii și de utilizare a sistemelor informaționale în procesul de prestare a serviciilor.

4. Scopul SI RSSP este de a oferi autorităților și instituțiilor publice, un mecanism eficient, fiabil și modern de evidență a serviciilor publice prestate de aceste autorități și instituții publice.

5. Obiective de bază specifice stabilite pentru SI RSSP:

- 1) evidența serviciilor publice prestate de autoritățile publice din Republica Moldova;
- 2) publicarea informațiilor privind serviciile publice înregistrate în SI RSSP;
- 3) sporirea calității informațiilor cu privire la serviciile publice și facilitarea accesului la acestea;
- 4) eficientizarea procesului de prestare a serviciilor publice ;
- 5) îmbunătățirea calității prestării serviciilor publice în baza sugestiilor și propunerilor din partea beneficiarilor de servicii publice .

6. Sarcinile de bază realizate de SI RSSP:

- 1) înregistrarea, actualizarea și radierea din SI RSSP a serviciilor publice;
- 2) înregistrarea, actualizarea și radierea din SI RSSP a evenimentelor de viață;
- 3) publicarea informațiilor actualizate despre prestatorii serviciilor publice, serviciile publice prestate de către aceștia și evenimentele de viață;
- 4) facilitarea interacțiunii dintre prestatorii de servicii publice și beneficiarii acestora;
- 5) ținerea evidenței informațiilor aferente prestatorilor de servicii publice;
- 6) ținerea evidenței informațiilor aferente serviciilor publice;
- 7) generarea de statistici și rapoarte;
- 8) asigurarea interconexiunii cu alte sisteme informaționale de stat.

7. Principiile de bază ale SI RSSP sunt:

- 1) principiul legalității, care presupune crearea și exploatarea SI RSSP în conformitate cu legislația națională;
- 2) principiul respectării drepturilor omului, care presupune exploatarea SI RSSP în strictă conformitate cu legislația națională, tratatele și acordurile internaționale din domeniul drepturilor omului la care Republica Moldova este parte;
- 3) 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;
- 4) principiul veridicității datelor, care presupune evidența serviciilor publice în baza unor date autentice;
- 5) principiul plenitudinii datelor, prin care se are în vedere asigurarea volumului complet al informației gestionate de SI RSSP, în conformitate cu actele normative;
- 6) principiul confidențialității informației, care se referă la restricționarea accesului persoanelor neautorizate la informația cu accesibilitate limitată;

7) principiul îndrumării procesului de utilizare a SI RSSP, care reprezintă o totalitate de măsuri organizatorice și tehnice de program, asigurând calitatea înaltă a resurselor informaționale de stat formate, fiabilitatea stocării lor și corectitudinea utilizării în corespundere cu legislația, garantând accesul operativ la informație pentru utilizator, în limitele competenței stabilite prin actele normative și nivelul de acces;

8) 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 RSSP presupune rezistența la atacuri, protecția integrității informației și pregătirea pentru lucru atât la nivel de sistem, cât și la nivel de date prezentate în această informație;

9) principiul compatibilității SI RSSP cu sistemele informaționale publice existente în țară;

10) principiul dezvoltării SI RSSP prin prisma apariției unor obiecte noi;

11) principiul modularității și scalabilității, ce reprezintă posibilitatea de a dezvolta SI RSSP fără modificarea componentelor create anterior;

12) principiul neexcesivității și pertinentei, care relevă necesitatea limitării volumului de informații cu accesibilitate limitată prelucrate, în așa fel încât să fie prelucrate doar informațiile relevante și necesare în contextul realizării sarcinilor SI RSSP.

Capitolul II

CADRUL NORMATIV-JURIDIC AL SI RSSP

8. Crearea și funcționarea SI RSSP este reglementată, în particular, de următoarele acte normative și documente de politici:

1) Legea nr. 982/2000 privind accesul la informație (Monitorul Oficial al Republicii Moldova, 2000, nr. 88-90, art. 664);

2) 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);

3) Legea nr. 71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314);

4) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate (Monitorul Oficial al Republicii Moldova, 2018, nr. 295-308, art. 452);

5) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat (Monitorul Oficial al Republicii Moldova, 2006, nr. 79-82, art. 591);

6) Concepția guvernării electronice, aprobată prin Hotărârea Guvernului nr. 733/2006 (Monitorul Oficial al Republicii Moldova, 2006, nr. 106-111, art. 799);

7) Hotărârea Guvernului nr. 709/2011 cu privire la unele măsuri în domeniul e-Transformare a guvernării (Monitorul Oficial al Republicii Moldova, 2011, nr. 156-159, art. 779);

8) Programul strategic de modernizare tehnologică a guvernării (e-Transformare), aprobat prin Hotărârea Guvernului nr. 710/2011 (Monitorul Oficial al Republicii Moldova, 2011, nr. 156-159, art. 780);

9) Programul privind Cadrul de Interoperabilitate, aprobat prin Hotărârea Guvernului nr. 656/2012 (Monitorul Oficial al Republicii, 2012, nr. 186-189, art. 708);

10) Strategia națională de dezvoltare a societății informaționale „Moldova Digitală 2020”, aprobată prin Hotărârea Guvernului nr. 857/2013 (Monitorul Oficial al Republicii Moldova, 2013, nr. 252-257, art. 963);

11) Hotărârea Guvernului nr. 760/2010 cu privire la Instituția publică „Agenția de Guvernare Electronică” (Monitorul Oficial al Republicii Moldova, 2010, nr. 150-152 art. 832);

12) Concepția Portalului guvernamental, aprobată prin Hotărârea Guvernului nr. 916/2007 (Monitorul Oficial al Republicii Moldova, 2007, nr. 127-130 art. 952);

13) Hotărârea Guvernului nr. 330/2012 cu privire la crearea și administrarea portalului guvernamental unic al serviciilor publice (Monitorul Oficial al Republicii Moldova, 2012, nr. 104-108 art. 370);

14) Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017 (Monitorul Oficial al Republicii Moldova, 2017, nr. 109-118, art. 277);

15) Regulamentul privind utilizarea, administrarea și dezvoltarea platformei tehnologice comune (MCloud), aprobat prin Hotărârea Guvernului nr. 128/2014 (Monitorul Oficial al Republicii Moldova, 2014, nr. 47-48, art. 145);

16) Regulamentul privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), aprobat prin Hotărârea Guvernului nr. 1090/2013 (Monitorul Oficial al Republicii Moldova, 2014, nr. 4-8, art. 02);

17) Regulamentul privind serviciul electronic guvernamental de jurnalizare (MLog), aprobat prin Hotărârea Guvernului nr. 708/2014 (Monitorul Oficial al Republicii Moldova, 2014, nr. 261-267, art. 756);

18) Regulamentul privind modul de utilizare a platformei de interoperabilitate (MConnect), aprobat prin Hotărârea Guvernului nr. 211/2019 (Monitorul Oficial al Republicii Moldova, 2019, nr. 132-138, art. 254);

19) Reglementarea tehnică „Procese ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006 (Monitorul Oficial al Republicii Moldova, 2006, nr. 95-97, art. 335);

20) Ordinul ministrului dezvoltării informaționale nr. 94/2009 cu privire la aprobarea unor reglementări tehnice (Monitorul Oficial al Republicii Moldova, 2010, nr. 58-60, art. 232).

Capitolul III

SPAȚIUL FUNCȚIONAL AL SI RSSP

9. Funcțiile de bază ale sistemului sunt:

1) Formarea resursei informaționale (Registrul de stat al serviciilor publice). Funcțiile de bază în procesul de formare a bazei de date a SI RSSP sunt funcțiile de înregistrare, actualizare a datelor și scoaterea din evidență a obiectelor informaționale (schimbarea statutului obiectului, de exemplu arhivare);

2) organizarea accesului la date. Datele conținute în banca de date a SI RSSP sunt puse la dispoziția utilizatorilor pentru organizarea procesului de schimb

informațional. Fiecare utilizator de date al SI RSSP va accesa și utiliza aceste date numai în scopuri legale în conformitate cu drepturile de utilizator atribuite. SI RSSP va asigura accesul automatizat la sistem pentru utilizatori, în urma autentificării prin intermediul serviciului guvernamental de autentificare și control al accesului (MPass). Totodată, SI RSSP va realiza identificarea automatizată a administratorului persoanei juridice conform datelor din Registrul de stat al unităților de drept;

3) asigurarea multilaterală a funcționării SI RSSP. Funcția respectivă presupune o interacțiune și integrare cu alte sisteme informaționale de stat sau servicii electronice guvernamentale;

4) interoperabilitatea. Schimbul de date este asigurat prin platforma de interoperabilitate (MConnect) cu toate registrele de stat cu care autoritățile publice interacționează;

5) auditul utilizatorilor. SI RSSP conține un mecanism propriu de jurnalizare a tuturor evenimentelor de business aferente utilizării sale. Orice acțiune a utilizatorilor se documentează în registre electronice speciale, arătând momentul și utilizatorul care a efectuat acțiunea. Pentru fiecare acțiune a utilizatorului se salvează în evenimentul jurnalizat datele care au fost modificate. SI RSSP jurnalizează în paralel prin intermediul serviciului electronic guvernamental de jurnalizare (MLog) evenimentele de business critice. Toate acțiunile care sunt jurnalizate în paralel prin intermediul serviciului electronic guvernamental de jurnalizare (MLog) pot fi configurate în opțiunile de administrare;

6) asigurarea calității informației se realizează prin crearea și menținerea componentelor sistemului de calitate, bazate pe principiul abordării de proces.

10. SI RSSP este creat pentru înregistrarea și evidența într-o listă clasificată a serviciilor publice și a prestatorilor acestora. Acesta este sursa principală de informații despre serviciile publice, autoritățile publice prestatoare, Regulamentul administrativ de prestare a serviciului public, locurile de prestare, lista documentelor necesare pentru a beneficia de un serviciu, modele de cereri și formulate care trebuie completate la solicitarea unui serviciu, informații cu referire la actele juridice care reglementează prestarea serviciilor, precum și alte informații de referință.

11. Serviciile publice instituite în modul stabilit de cadrul normativ aplicabil se înregistrează obligatoriu în Registrul de stat al serviciilor publice (în continuare – RSSP), format de SI RSSP.

12. Având în vedere funcțiile SI RSSP, sistemul va avea următoarele contururi funcționale de bază:

1) Conturul „Evidența prestatorilor de servicii” care asigură următoarele funcții specifice:

- a) înregistrarea, actualizarea și radierea prestatorilor de servicii;
- b) evidența datelor de contact ale prestatorilor de servicii;
- c) evidența punctelor de prestare a serviciilor aferente prestatorilor de servicii;
- d) evidența orarului de prestare a serviciilor publice;
- e) generarea rapoartelor, statisticilor.

2) Conturul „Evidența serviciilor publice” care asigură următoarele funcții specifice:

- a) înregistrarea, actualizarea și radierea serviciilor publice atribuite unui prestator de servicii;
- b) descrierea și publicarea fișelor serviciilor publice;
- c) evidența serviciilor publice și a informațiilor aferente acestora.

3) Conturul „Evidența evenimentelor de viață” care asigură următoarele funcții specifice:

- a) înregistrarea, actualizarea și radierea evenimentelor de viață;
- b) descrierea și publicarea etapelor evenimentului de viață;
- c) evidența evenimentelor de viață și a serviciilor publice conexe acestora.

4) Conturul „Administrare și Control”, care asigură următoarele funcții:

- a) generarea rapoartelor, statisticilor și indicatorilor de performanță;
- b) gestionarea utilizatorilor și drepturilor acestora;
- c) gestionarea copiilor de rezervă;
- d) jurnalizarea evenimentelor de sistem;
- e) monitorizarea performanței sistemului;
- f) suportul tehnic și mentenanța.

Capitolul IV

STRUCTURA ORGANIZAȚIONALĂ A SI RSSP

13. Proprietarul SI RSSP este statul.

14. Posesorul și deținătorul RSSP este Instituția publică „Agenția de Guvernare Electronică” (în continuare - *posesor*), care asigură crearea și exploatarea SI RSSP.

15. Administratorul de sistem al SI RSSP este angajatul posesorului responsabil de administrarea SI RSSP. Administratorul de sistem deține acces avansat la funcționalitățile sistemului, administrează prestatorii de servicii, clasificatoarele sistemului, dispune de instrumente de configurare și ajustare a sistemului și funcționalităților acestuia și monitorizează activitatea registratorilor.

16. Administratorul tehnic al SI RSSP 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.

17. Registratorii datelor în RSSP sunt:

- 1) prestatorii de servicii, care vor asigura înregistrarea, actualizarea și radierea serviciilor publice pe care le prestează și a informațiilor aferente acestora;
- 2) posesorul, care va asigura înregistrarea, actualizarea și radierea evenimentelor de viață.

18. Furnizorii de date sunt persoanele juridice de drept public sau de drept privat care livrează date aferente obiectelor informaționale ale RSSP.

19. Destinatari ai datelor din RSSP sunt beneficiarii de servicii publice, prin intermediul Portalului guvernamental unic al serviciilor publice, aplicațiile web (mobile) ale serviciilor publice, paginile web ale prestatorilor de servicii și alte resurse informaționale.

Capitolul V

DOCUMENTELE SI RSSP

- 20.** Documentele de bază ale SI RSSP se clasifică, după cum urmează:
- 1) documente de intrare;
 - 2) documente de ieșire;
 - 3) documente tehnologice.
- 21.** Documentele de intrare ale SI RSSP sunt considerate:
- 1) solicitare de înregistrare a prestatorului de servicii;
 - 2) solicitări privind înregistrarea, actualizarea sau radierea unui serviciu public și a informațiilor aferente acestuia;
 - 3) solicitări privind înregistrarea, actualizarea sau radierea unui eveniment de viață.
- 22.** Documentele de ieșire ale SI RSSP sunt considerate:
- 1) fișa serviciului public;
 - 2) fișa evenimentului de viață;
 - 3) profilul prestatorului de servicii publice.
- 23.** Documentele tehnologice ale SI RSSP sunt considerate:
- 1) șabloanele fișelor serviciului public și evenimentului de viață;
 - 2) documentele tehnologice privind parametrii de sistem;
 - 3) documentele ce conțin înregistrări de audit privind acțiunile registratorilor în cadrul SI RSSP;
 - 4) rapoarte, statistici și indicatori de performanță agregate privind utilizarea sistemului.

Capitolul VI

SPAȚIUL INFORMAȚIONAL AL SI RSSP

Secțiunea 1

Obiectele informaționale gestionate

- 24.** Obiectele informaționale de bază, care reprezintă resursa informațională a SI RSSP, sunt:
- 1) „Serviciul public” cu următoarele caracteristici:
 - a) identificatorul serviciului, generat de către SI RSSP;
 - b) codul serviciului conform clasificatorului de produse (bunuri și servicii) al Republicii Moldova, rev.2;
 - c) denumirea serviciului;
 - d) beneficiarii serviciului (persoane fizice/juridice);
 - e) data înregistrării serviciului;
 - f) statutul serviciului;
 - g) descrierea serviciului;
 - h) modul de prestare a serviciului (electronic/hârtie);
 - i) etapele de obținere a serviciului;
 - j) tarifele prestării serviciului/ serviciu gratuit;
 - k) termenul prestării serviciului;
 - l) lista actelor necesare pentru solicitarea serviciului;
 - m) descrierea rezultatului prestării serviciului;
 - n) prestatorul serviciului (IDNO și denumirea instituției);

o) alte autorități publice și prestatori de servicii, implicate în prestarea serviciului;

p) harta tehnologică a interacțiunii interdepartamentale (dacă sunt mai multe instituții implicate în prestarea serviciului);

q) informații de referință:

- modelele formularelor de cereri pentru prestarea serviciului și altor documente, a căror completare de către solicitant sunt necesare pentru a i se presta un serviciu;

- lista actelor normative care reglementează nemijlocit prestarea serviciului, inclusiv a Regulamentului privind organizarea și prestarea serviciului, cu indicarea datelor de identificare și a surselor de publicare oficială ale acestora;

- temeiurile pentru refuzarea prestării serviciului public, stabilite de legile Republicii Moldova;

- ordinea de contestare a deciziilor, acțiunilor/inacțiunilor organelor autorităților publice care participă la prestarea serviciului, precum și ale prestatorilor de servicii și/sau ale angajaților acestora în chestiunile ce țin de prestarea serviciilor publice;

- răspunderea prestatorului serviciului și a personalului acestuia pentru neexecutarea sau executarea necorespunzătoare a activității administrative în legătură cu prestarea serviciilor;

- adresa poștală și adresa locației autorității publice care prestează servicii, precum și ale instituțiilor care prestează servicii din numele acestor autorități;

- numerele telefoanelor de informare, ale fax-urilor, adresele site-urilor oficiale din rețeaua Internet, adrese de e-mail, programele de lucru ale organelor care prestează servicii, inclusiv ale organelor lor teritoriale, precum și ale instituțiilor care prestează servicii din numele acestor organe;

- date despre sistemele de plată utilizate la prestarea serviciilor cu plată și despre ordinea de plată a serviciului.

2) „Prestatorul de servicii” cu următoarele caracteristici:

a) identificatorul prestatorului (IDNO);

b) denumirea prestatorului;

c) date referitoare la administrator (numărul de identificare de stat (IDNP), numele și prenumele);

d) date referitoare la persoanele responsabile de înregistrarea datelor în RSSP (numărul de identificare de stat (IDNP), numele și prenumele)

e) datele de contact ale prestatorului;

f) punctele de livrare a serviciilor;

g) datele de contact (număr de telefon, e-mail, etc.);

3) „Evenimentul de viață” cu următoarele caracteristici:

a) identificatorul/, generat de către SI RSSP;

b) etapele evenimentului de viață;

c) lista serviciilor publice conexe.

25. Informațiile privind numele/prenumele și numărul de identificare de stat al persoanei fizice (IDNP) și denumirea și numărul de identificare de stat al persoanei juridice (IDNO) sunt inițial înregistrate și identificate în alte sisteme, respectiv Registrul de stat al populației și Registrul de stat al unităților de drept. În SI RSSP se mențin numai numerele de identificare de stat (IDNP sau IDNO) – în acest caz nu se admite modificarea identificatorului. Toate datele suplimentare necesare sunt accesibile în Registrul de stat al populației sau Registrul de stat al unităților de drept, iar în caz de necesitate, pot fi completate sau accesate din alte sisteme informaționale de stat.

26. Administratorul de sistem cu următoarele caracteristici:

- a) identificator (IDNP) preluat din serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- b) nume prenume preluat din serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- c) adresă de poștă electronică preluat din serviciul electronic guvernamental de autentificare și control al accesului (MPass).

27. Registratorul cu următoarele caracteristici:

- a) identificatorul registratorului (IDNP);
- b) denumirea registratorului;
- c) datele de contact ale registratorului.

28. Serviciului public i se atribuie un număr unic de înregistrare, alcătuit din opt cifre sub formă de cod numeric, care se formează din codurile clasificatorului de servicii utilizat în registru.

Numărul de înregistrare are următoarea structură:

A YYYY NNN K unde,

A – codul care indică nivelul de prestare a serviciului public (1 - serviciul este prestat de autoritatea publică centrală; 2 - serviciul este prestat de autoritatea publică locală);

YYYY – codul prestatorului;

NNN – este alcătuit din 3 cifre și indică numărul de ordine al serviciului public;

K – suma de control (se calculează conform unui algoritm special).

Numărul de înregistrare se generează de sistemul informațional și automat se atribuie serviciului public la înregistrarea primară a acestuia în registru.

Secțiunea a 2-a

Scenariile de bază aferente obiectelor informaționale

29. Scenariul de bază reprezintă lista evenimentelor aferente obiectelor informaționale.

30. Scenarii referitoare la obiectul informațional „Serviciu public”:

- 1) înregistrarea primară – realizată de către registrator;
- 2) actualizarea datelor – realizată de către registrator, la necesitatea modificării sau completării informației despre serviciul public;
- 3) scoaterea din evidență – de către registrator, în cazul desființării serviciului public.

31. Scenarii referitoare la obiectul informațional „Prestator de servicii”:

1) înregistrarea primară – de către administratorul de sistem, la momentul solicitării;

2) actualizarea datelor – de către registrator la necesitatea modificării sau completării informației despre prestatorul de servicii;

3) scoaterea din evidență – de către administratorul de sistem, în momentul lichidării persoanei juridice sau la solicitare.

32. Scenarii referitoare la obiectul informațional „Eveniment de viață”:

1) înregistrarea primară – de către registrator;

2) actualizarea datelor – de către registrator, la necesitatea modificării sau completării informației despre evenimentul de viață;

3) scoaterea din evidență – de către registrator, în situația dispariției evenimentului de viață.

33. Scenarii referitoare la obiectul informațional „Registrator”:

a) înregistrarea primară – de către administratorul de sistem, la momentul solicitării;

b) actualizarea datelor – de către administratorul de sistem la necesitatea modificării sau completării informației despre registrator sau la solicitare;

c) scoaterea din evidență – de către administratorul de sistem.

Secțiunea a 3-a

Interacțiunea cu alte sisteme și platforme electronice guvernamentale

34. SI RSSP va fi găzduit pe platforma tehnologică guvernamentală comună (MCloud) care funcționează în baza tehnologiei de „cloud computing”, utilizată pentru găzduirea sistemelor informaționale guvernamentale.

35. SI RSSP va interacționa cu următoarele platforme și servicii electronice guvernamentale:

1) platforma de interoperabilitate (MConnect) – pentru schimbul de date cu alte sisteme informaționale și registre de stat;

2) serviciul electronic guvernamental de autentificare și control al accesului (MPass) - pentru autentificarea și controlul accesului în cadrul sistemului;

3) serviciul electronic guvernamental de jurnalizare (MLog) - pentru asigurarea evidenței operațiunilor (evenimentelor) produse în cadrul SI RSSP;

4) serviciul electronic guvernamental de notificare (MNotify) – pentru notificarea registratorilor;

5) portalul guvernamental unic al serviciilor publice - pentru căutarea și vizualizarea informațiilor privind serviciile publice de către utilizatori.

36. Informația din RSSP se furnizează gratuit autorităților/instituțiilor publice, persoanelor fizice și juridice, prin publicarea diverselor date despre serviciile publice înregistrate în RSSP pe Portalul guvernamental unic al serviciilor publice.

Capitolul VII

SPAȚIUL TEHNOLOGIC AL SI RSSP

37. La dezvoltarea SI RSSP se va aplica arhitectura multi-nivel (având cel puțin următoarele nivele - baza de date, logica de aplicație și interfața cu utilizatorul) și principiile agile. Utilizarea unei astfel de arhitecturi și principii va permite o cuplare redusă între componente, în care responsabilitățile fiecărei componente sunt specializate, precum și implementarea iterativă, operarea modificărilor și flexibilitate în implementare.

38. SI RSSP va utiliza standarde deschise și va fi compatibilă cu sisteme care, la fel, utilizează standarde non-proprietare, cât și cu standardele deja existente.

39. Arhitectura complexului software-hardware, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale se determină de posesor la etapele ulterioare de dezvoltare a sistemului, 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 sistemului cu noi funcționalități fără a afecta funcționarea sistemului;

2) implementarea funcționalităților de arhivare (backup) și restabilire a datelor în caz de incidente.

40. Platforma MCloud, pe care este găzduit SI RSSP, permite accesul, la cerere, pe bază de rețea la totalitatea configurabilă a resurselor de calcul virtualizabile (de exemplu rețele, servere, echipamente de stocare, aplicații și servicii) și care pot fi puse rapid la dispoziție cu un efort minim de administrare sau interacțiune cu furnizorul acestor servicii. În acest fel, SI RSSP 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.

41. Sistemul de comunicații se va baza pe infrastructura și echipamentul rețelelor guvernamentale, care includ posibilitatea conectării la internet. Infrastructura existentă va fi planificată în mod corespunzător, pentru a oferi nivelele adecvate de performanță și capacitate.

42. Interfața de utilizare a SI RSSP se va adapta automat la diverse rezoluții de afișare și va fi disponibilă în limbile română și rusă.

43. Interfața de utilizare a SI RSSP va fi implementată folosind tehnologii progresive pentru aplicații web și va fi funcțională pe dispozitivele mobile.

44. Având în vedere locul SI RSSP în cadrul resurselor informaționale de stat ale Republicii Moldova, este necesară o disponibilitate înaltă și accesul neîntrerupt la sistem. Din acest motiv, întreaga soluție va fi construită în regim de înaltă disponibilitate (24 de ore pe zi, 7 zile pe săptămână).

Capitolul VIII

ASIGURAREA SECURITĂȚII INFORMAȚIONALE

45. Securitatea informațională presupune protecția SI RSSP, 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 informaționale și infrastructurii informaționale.

46. Asigurarea securității informației va fi realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017. Pentru gestiunea riscurilor de securitate va fi implementată o politică generală de securitate. Personalul implicat în utilizarea și administrarea SI RSSP 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 a stabili domeniile, care necesită îmbunătățiri.

47. Pericolele securității informaționale sunt:

- 1) colectarea și utilizarea ilegală a datelor;
- 2) încălcarea tehnologiei de prelucrare a datelor;
- 3) implementarea în produsele software și hardware a componentelor care îndeplinesc funcții neprevăzute în documentația aferentă acestor produse;
- 4) elaborarea și răspândirea programelor ce afectează funcționarea normală a sistemelor informaționale și de telecomunicații, precum și a sistemelor securității informaționale;
- 5) nimicirea, deteriorarea, suprimarea radioelectronică sau distrugerea mijloacelor și sistemelor de prelucrare a datelor, de telecomunicații și comunicații;
- 6) influențarea sistemelor cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a datelor;
- 7) compromiterea cheilor și mijloacelor de protecție criptografică a informației;
- 8) scurgerea informației prin canale tehnice;
- 9) implementarea dispozitivelor electronice pentru interceptarea informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor utilizând sistemele de comunicații, precum și în încăperile de serviciu ale autorităților administrației publice;
- 10) nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;
- 11) interceptarea datelor în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acestei informații și impunerea unei informații false;
- 12) utilizarea tehnologiilor informaționale naționale și internaționale necertificate, a mijloacelor de protecție a informației, a mijloacelor de informatizare, de telecomunicații și comunicații la crearea și dezvoltarea infrastructurii informaționale de telecomunicații;
- 13) accesul nesanționat la resursele informaționale din băncile și bazele de date;
- 14) încălcarea restricțiilor legale privind răspândirea informației;
- 15) încălcarea prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal.

48. SI RSSP asigură următoarele obiective de securitate:

- 1) autentificarea – garantează că zonele restricționate ale SI RSSP vor fi accesibile doar utilizatorilor cu o identitate verificată prin serviciul electronic guvernamental de autentificare și control al accesului (MPass);

2) autorizarea – garantează că utilizatorii autentificați prin serviciul electronic guvernamental de autentificare și control al accesului (MPass) pot accesa serviciile și datele care corespund drepturilor lor de acces;

3) confidențialitatea – garantează că datele înregistrate în SI RSSP nu pot fi accesate de o parte terță neautorizată;

4) integritatea – garantează că datele înregistrate în SI RSSP nu au fost modificate sau alterate de o parte terță neautorizată;

5) nonrepudierea - garantează că datele înregistrate în RSSP nu pot fi negate mai târziu.

49. Pentru atingerea obiectivelor de securitate, SI RSSP dispune de mai multe mecanisme de securitate:

1) firewall – filtrul firewall face parte din arhitectura tehnică a platformei tehnologice (MCloud) pentru a asigura un mecanism de apărare împotriva utilizatorilor externi neautorizați;

2) antivirus/anti-spam – soluțiile hardware și/sau software asigură protecția antivirus și anti-spam pentru toate serverele. Fișierele se scanează la încărcare în sistem. În cazul detectării unui fișier infectat, procedura de încărcare este oprită și fișierul – respins;

3) sistem de detectare a intruziunilor – sistem de detectare a intruziunilor care include toți utilizatorii de pe toate serverele;

4) comunicare sigură (transferuri de date) între serverele web și utilizatori – schimbul de informații confidențiale este securizat;

5) backup sistematic al datelor păstrate – permite recuperarea rapidă și fiabilă a datelor în caz de incident care a dus la pierderea sau deteriorarea datelor;

6) 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 RSSP cu acces limitat pentru utilizatorii neautorizați.

50. În cadrul SI RSSP se asigură generarea și păstrarea înregistrărilor de audit ale securității pentru operațiunile 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 accesate de 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.

51. SI RSSP va minimiza cantitatea de informații de identificare personală stocate.

52. SI RSSP va utiliza funcționalitatea de autentificare doar prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass).

53. Utilizatorii SI RSSP 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. Sistemul va prelua rolurile utilizatorilor din serviciul electronic guvernamental de autentificare și control al accesului (MPass).

54. O necesitate importantă legată de securitate este necesitatea păstrării înregistrărilor de audit pentru analiza integrității sistemului și pentru monitorizarea

activității utilizatorilor. SI RSSP 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.

55. Dat fiind necesitatea disponibilității înalte a SI RSSP pentru asigurarea accesului continuu a utilizatorilor la SI RSSP, infrastructura SI RSSP va include circuite cu noduri de rezervă ce vor prelua încărcătura sistemului pe perioada cât sistemul principal se află în proces de mentenanță sau restaurare.

Încheiere

56. Implementarea SI RSSP va accelera și va simplifica procesul de evidență a serviciilor publice, ceea ce va avea un impact pozitiv asupra interacțiunii dintre prestatorii de servicii publice și beneficiarii acestora.

REGULAMENT

privind modul de ținere a Registrului de stat al serviciilor publice

Capitolul I

DISPOZIȚII GENERALE

1. Prezentul Regulament stabilește modul de utilizare, administrare și mentenanță a Registrului de stat al serviciilor publice (în continuare – *RSSP*), format de Sistemul informațional „Registrul de stat al serviciilor publice” (în continuare – *SI RSSP*), inclusiv atribuțiile participanților la raporturile aferente utilizării și operării registrului în cauză.

2. Noțiunile utilizate în prezentul Regulament sunt corespunzătoare definițiilor de la pct. 3 al Anexei nr. 1 din prezenta hotărâre.

Capitolul II

SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL EXPLOATĂRII ȘI UTILIZĂRII RSSP

3. Subiecții din domeniul exploatării și al utilizării RSSP (participanții la RSSP) sunt:

- 1) proprietarul;
- 2) posesorul;
- 3) deținătorul;
- 4) administratorul de sistem;
- 5) administratorul tehnic;
- 6) furnizorii datelor;
- 7) registratorii;
- 8) destinatarii.

4. Proprietarul RSSP este statul, care își realizează dreptul de proprietate, de gestionare și de utilizare a datelor din registru. Resursele financiare pentru dezvoltarea, mentenanța și exploatarea registrului sunt asigurate din bugetul de stat și alte mijloace financiare, conform legislației.

5. Posesorul și deținătorul RSSP este Instituția publică „Agenția de Guvernare Electronică” (în continuare – *AGE*), cu drept de gestionare și de utilizare a datelor și resurselor acestuia.

6. Furnizorii de date sunt persoanele juridice de drept public sau de drept privat care livrează date aferente obiectelor informaționale ale RSSP..

7. Furnizorii de date în SI RSSP sunt obligați să asigure corectitudinea și autenticitatea datelor introduse, precum și actualizarea lor prin solicitările transmise registratorului.

8. Registratorii datelor în RSSP sunt:

- 1) prestatorilor de servicii, care vor asigura înregistrarea, actualizarea și radierea serviciilor publice pe care le prestează și a informațiilor aferente acestora;
- 2) posesorului, care va asigura înregistrarea, actualizarea și radierea evenimentelor de viață.

9. Registratorii vor asigura plenitudinea și integritatea datelor introduse în RSSP.
10. Destinatari ai datelor din RSSP sunt beneficiarii de servicii publice.

Capitolul III

DREPTURILE, ATRIBUȚIILE ȘI OBLIGAȚIILE PARTICIPANȚILOR LA RSSP

Secțiunea 1

Drepturile, atribuțiile și obligațiile posesorului și administratorului de sistem

11. Posesorul are următoarele drepturi:
 - 1) să elaboreze și să dezvolte, prin intermediul Cancelariei de Stat, în baza competențelor sale, cadrul normativ cu privire la RSSP;
 - 2) să propună soluții de perfecționare și eficientizare a procesului de funcționare a RSSP, precum și să le pună în aplicare;
 - 3) să supravegheze respectarea cerințelor de securitate a informației de către participanții la registru, să fixeze cazurile și tentativele de încălcare a acestora;
 - 4) să solicite de la participanți actualizarea sau corectarea datelor introduse în SI RSSP, în caz de depistare a omiterilor și erorilor.
12. Posesorul are următoarele atribuții:
 - 1) asigură condițiile organizatorice și financiare pentru crearea și funcționarea RSSP;
 - 2) stabilește scopurile și funcționalitățile SI RSSP, în conformitate cu prezenta hotărâre;
 - 3) determină, în comun cu deținătorul, obiectele informaționale supuse înregistrării în SI RSSP și conținutul acestora;
 - 4) aprobă, prin ordin al directorului, modelul contractului cu privire la utilizarea gratuită a SI RSSP;
 - 5) semnează contracte cu privire la utilizarea gratuită a SI RSSP;
 - 6) aprobă și coordonează cu administratorul tehnic executarea modificărilor/rectificărilor solicitate în cererile privind erorile de sistem ale SI RSSP, erorile cauzate de factorul uman, incidentele de infrastructură care afectează funcționarea normală a acestuia;
 - 7) asigură dezvoltarea continuă a RSSP prin adăugarea de noi componente ce pot fi utilizate de participanți;
 - 8) autorizează, suspendă și revocă dreptul de acces în SI RSSP în condițiile prezentului Regulament;
 - 9) stabilește măsurile tehnice și organizatorice de protecție și securitate a SI RSSP;
 - 10) monitorizează conformitatea cerințelor de securitate a SI RSSP la cerințele cadrului normativ în domeniul protecției datelor cu caracter personal;
 - 11) organizează seminare și instruirii de promovare și utilizare a SI RSSP pentru furnizori și beneficiari;
 - 12) exercită alte atribuții necesare asigurării bunei funcționări a SI RSSP.
13. Posesorul are următoarele obligații:

1) să asigure ținerea RSSP în conformitate cu regulile de ținere a registrului, aprobate prin prezenta hotărâre;

2) să asigure funcționarea neîntreruptă și ținerea RSSP în conformitate cu cadrul normativ;

3) să acorde suportul necesar persoanelor autorizate, care au acces la registru, privind utilizarea complexului de mijloace software aferente acestuia;

4) să informeze participanții la RSSP despre modificările condițiilor tehnice de funcționare a acestuia;

5) să asigure implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a informației și a datelor cu caracter personal;

6) să utilizeze informația obținută din RSSP doar în scopurile stabilite de prezentul Regulament și cadrul normativ.

14. Drepturile și obligațiile posesorului RSSP sunt stabilite în conformitate cu Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat și Legea nr. 71/2007 cu privire la registre.

15. Deținătorul are următoarele drepturi:

1) să supravegheze respectarea cerințelor de securitate a informației de către participanții la registru, să fixeze cazurile și tentativele de încălcare a acestora;

2) să inițieze procedura de revocare a accesului la RSSP pentru participanții care nu respectă regulile, standardele și normele în domeniul securității informaționale;

3) să verifice autenticitatea și veridicitatea datelor introduse de participanții la RSSP;

4) să solicite de la participanți actualizarea sau corectarea datelor introduse în RSSP, în caz de depistare a omiterilor și erorilor.

16. Deținătorul are următoarele atribuții:

1) determină obiectele informaționale supuse înregistrării în SI RSSP și conținutul acestora;

2) asigură securitatea și protecția datelor din registru;

3) aprobă solicitările furnizorilor de date de înregistrare în sistem a serviciilor publice;

4) desemnează persoana responsabilă de înregistrarea în RSSP a datelor privind evenimentele de viață;

5) asigură măsurile tehnice și organizatorice de protecție și securitate a SI RSSP;

6) ajustează cerințele de securitate și conformitate a RSSP la cerințele cadrului normativ în domeniul protecției datelor cu caracter personal;

7) asigură păstrarea informațiilor conținute în Registru și imposibilitatea modificării neautorizate a acestora;

8) participă la organizarea de seminare și instruiți de promovare și utilizare a SI RSSP;

9) asigură acordarea suportului metodologic și tehnic furnizorilor de date în procesul de gestionare a datelor din registru;

10) asigură elaborarea și menținerea ghidului metodologic privind introducerea, acumularea, păstrarea, completarea, corectarea, sistematizarea și utilizarea datelor din RSSP, precum și funcționarea sa;

11) monitorizează și supraveghează accesările informației din RSSP și identifică încălcările comise;

12) exercită alte atribuții necesare asigurării bunei funcționări a RSSP.

17. Deținătorul are următoarele obligații:

1) să asigure ținerea RSSP în conformitate cu regulile de ținere a registrului, aprobate prin prezenta hotărâre;

2) să acorde suportul necesar persoanelor autorizate, care au acces la registru, privind utilizarea complexului de mijloace software aferente acestuia;

3) să informeze participanții la SI RSSP despre modificările condițiilor tehnice de funcționare a acestuia;

4) să asigure implementarea măsurilor necesare pentru asigurarea regimului de confidențialitate și securitate a informației și a datelor cu caracter personal;

5) să utilizeze informația obținută din RSSP doar în scopurile stabilite de prezentul Regulament și cadrul normativ.

18. Drepturile și obligațiile deținătorului RSSP sunt stabilite în conformitate cu Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat și Legea nr. 71/2007 cu privire la registre.

19. Administratorul de sistem este angajatul posesorului care are următoarele atribuții:

1) atribuirea nivelului de acces și aplicarea restricțiilor de acces la datele SI RSSP;

2) managementul șabloanelor de rapoarte și statistici;

3) monitorizarea jurnalizării evenimentelor produse în registru.

Secțiunea a 2-a

Drepturile, atribuțiile și obligațiile furnizorului de date

20. Furnizorul de date are următoarele drepturi:

1) să primească de la posesor toate datele despre obiectele informaționale din SI RSSP și care sunt prezentate de către furnizor;

2) să fie informat cu privire la modificările operate de către posesor la SI RSSP;

3) să ofere sugestii de îmbunătățire și contribuie la dezvoltarea continuă a SI RSSP prin adăugarea de noi componente ce pot fi reutilizate de participanți.

21. Furnizorul de date are următoarele atribuții:

1) dezvoltă, plasează și deține date în SI RSSP referitoare la obiectele informaționale „Prestator de servicii publice” și „Serviciu public” pe care le prestează;

2) raportează posesorului problemele de funcționalitate ale SI RSSP;

3) alte atribuții aferente furnizării de date în RSSP.

22. Furnizorul de date are următoarele obligații:

1) să asigure corectitudinea, confidențialitatea și autenticitatea datelor introduse sau prezentate pentru a fi introduse în SI RSSP;

2) să asigure actualizarea datelor introduse în SI RSSP, în conformitate cu prevederile prezentului Regulament.

Secțiunea a 3-a **Drepturile și obligațiile registratorului**

23. Registratorul are dreptul:

- 1) să vizualizeze și să editeze informațiile din RSSP, conform rolului atribuit;
- 2) să acceseze spațiul informațional al SI RSSP, în limitele rolului atribuit;
- 3) să acceseze informațiile care se conțin în RSSP și care au fost prezentate de către acesta;
- 4) să înainteze posesorului propuneri privind modificarea actelor normative care reglementează funcționarea RSSP;
- 5) să solicite și să primească de la posesor susținere metodologică și practică privind funcționarea RSSP;
- 6) să înainteze posesorului propuneri privind îmbunătățirea și sporirea eficacității funcționării SI RSSP.

24. Registratorul este obligat:

- 25.** să înregistreze în RSSP serviciile publice pe care le prestează și informațiilor aferente acestora;
- 26.** să desemneze persoane responsabile de înregistrarea serviciilor publice și informațiilor aferente acestora;
- 27.** să asigure corectitudinea, autenticitatea și veridicitatea datelor introduse în RSSP;
- 28.** să asigure actualizarea datelor introduse în RSSP;
- 29.** să întreprindă măsuri pentru evitarea accesului neautorizat al persoanelor terțe;
- 30.** să utilizeze funcționalitățile SI RSSP în exclusivitate conform destinației acestora și în strictă conformitate cu legislația.

Capitolul IV **ȚINEREA ȘI ASIGURAREA FUNCȚIONĂRII RSSP**

31. RSSP se ține în format electronic, în limba română.

32. Toate înregistrările și modificările operate în RSSP se păstrează în ordine cronologică.

33. Posesorul RSSP efectuează administrarea acestuia cu ajutorul complexului de mijloace software și hardware, în corespundere cu prezentul Regulament.

Capitolul V **ÎNREGISTRAREA DATELOR ÎN RSSP**

34. Registratorii înregistrează în RSSP serviciile publice și datele aferente acestora.

35. Informațiile înregistrate în RSSP se semnează de către registratori, la transmitere, prin intermediul certificatelor cheii publice, în scopul asigurării integrității și nonrepudierii datelor.

Capitolul VI

MODIFICAREA ȘI COMPLETAREA DATELOR DIN RSSP

36. Modificarea și/sau completarea datelor din RSSP se efectuează de către registratori prin adăugarea unor noi înscrieri privind anularea și substituirea datelor înregistrate anterior.

37. Modificarea și/sau completarea datelor din RSSP se pot realiza de către registratorii care le-au înregistrat.

38. RSSP 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 RSSP se păstrează în ordine cronologică.

Capitolul VII

REGIMUL JURIDIC DE UTILIZARE A DATELOR DIN RSSP

39. Datele disponibile în RSSP sunt publice și pot fi accesate fără necesitatea autentificării prealabile.

40. Accesul la datele din RSSP se realizează prin accesarea aplicației web a SI RSSP sau prin intermediul altor sisteme informaționale de stat care expun date din RSSP.

41. Se interzice utilizarea datelor din RSSP în scopuri contrare legii.

42. Destinatarii datelor din RSSP nu sunt în drept să modifice datele obținute din RSSP, iar la utilizarea acestora sunt obligați să indice sursa lor.

Capitolul IV

GESTIONAREA ȘI ASIGURAREA FUNCȚIONĂRII SI RSSP

Secțiunea 1

Solicitarea serviciilor SI RSSP

43. Solicitarea serviciilor SI RSSP de către furnizorii de date se efectuează în baza contractului de utilizare gratuită a SI RSSP semnată cu posesorul, modelul căruia se aprobă prin ordinul directorului Agenției de Guvernare Electronică.

44. Posesorul examinează cererea furnizorului de date în termen de 10 zile lucrătoare.

45. După acceptarea cererii, posesorul pune la dispoziția furnizorului de date, în termen de 10 zile lucrătoare, informația de acces la SI RSSP.

46. Posesorul poate respinge cererea de solicitare a serviciilor în cazul în care scopurile indicate în cerere contravin prezentului Regulament și cadrului normativ aferent, informând furnizorul de date despre motivele respingerii.

Furnizorul de date este în drept să conteste respingerea cererii în condițiile prevăzute de legislație.

Secțiunea a 2-a

Furnizarea datelor și înregistrarea serviciilor SI RSSP

47. Pentru orice serviciu public, concomitent, în actul normativ de instituire a acestuia se aprobă regulamentul privind organizarea și prestarea serviciului public.

48. Autoritatea/instituția publică desemnată să presteze serviciul public este obligată să furnizeze pentru înregistrarea în RSSP de către registrator a datelor aferente serviciului public. Dacă la prestarea serviciului public sunt implicate mai multe autorități/instituții publice, atunci responsabil pentru furnizarea informațiilor în RSSP cu privire la serviciul public este prestatorul care oferă solicitantului rezultatul final al serviciului public.

49. Este interzisă prestarea serviciilor publice care nu sunt înregistrate în SI RSSP sau pentru care nu este aprobat Regulamentul cu privire la organizarea și prestarea serviciului public.

50. După aprobarea actului normativ de instituire a serviciului public și de aprobare a Regulamentului acestuia, prestatorul, prin intermediul contului său din SI RSSP, furnizează datele pentru înregistrarea serviciului public.

51. Procedura de înregistrare a serviciului public, introducerea modificărilor, formei de prezentare a datelor statistice, a procedurii de completare a acestora, se stabilesc în recomandările metodologice privind evidența serviciilor în RSSP, elaborate de posesor.

52. Formele electronice care conțin date despre servicii sunt supuse verificării formale și logice automatizate, ceea ce presupune verificarea corectitudinii completării acestor forme electronice cu date despre serviciile publice, conform recomandărilor metodologice despre ordinea de completare a formularelor electronice ale registrului. Dacă, urmare a verificării se vor identifica erori, atunci formularele completate incorect se returnează solicitantului, cu indicarea erorilor identificate.

53. Solicitantul elimină erorile și prezintă formele corectate spre examinare repetată.

54. Datele despre serviciile publice sunt supuse modificărilor în cazul: modificării regulamentului cu privire la organizarea și prestarea serviciului public și a altor modificări ale datelor din partea prestatorului de servicii.

55. Temei pentru excluderea serviciilor (modificarea statutului) din lista serviciilor înregistrate în registru este adoptarea legilor și a altor acte normative prin care se anulează prestarea serviciului public. În acest caz, deținătorul registrului asigură păstrarea în registru a informațiilor privind denumirea serviciului public, numărul de înregistrare și statutul acestui serviciu. Restul informațiilor care caracterizează serviciul se plasează în arhivă. Datele despre serviciile plasate în arhivă se păstrează permanent.

56. Datele statistice despre serviciile prestate sunt înregistrate în registru prin interacțiunea SI RSSP cu sistemele informaționale ale prestatorilor de servicii. În cazul în care prestatorii de servicii nu dispun de sisteme informaționale în care sunt

prelevate date statistice despre prestarea de către aceștia a serviciilor, atunci prestatorii de servicii trimit trimestrial către deținător forme electronice speciale cu privire la datele statistice ale serviciului public.

Secțiunea a 3-a

Condițiile de furnizare și utilizare a serviciilor SI RSSP

57. Furnizarea și utilizarea serviciilor SI RSSP se efectuează numai în scopuri ce rezultă din necesitățile de activitate ale furnizorului de date.

58. Acordarea accesului registratorilor la SI RSSP se realizează doar prin intermediul administratorilor de sistem.

59. Serviciile SI RSSP nu vor fi utilizate:

- 1) în scopuri ce contravin legislației naționale;
- 2) în scopuri ce pot periclita imaginea participanților la SI RSSP;
- 3) pentru crearea, stocarea sau transmiterea informației ofensatoare, defăimătoare sau discriminării, cum ar fi informația cu privire la rasă, naționalitate, sex, religie, dizabilități, orientare sexuală, convingeri religioase, opțiuni politice, precum și a materialelor pornografice și cu conținut erotic etc.;
- 4) prin modalități care implică riscuri de securitate a informației;
- 5) pentru introducerea altor tipuri de date decât cele stabilite în prezentul Regulament;
- 6) pentru folosirea neconformă a spațiului alocat.

Capitolul V

REGIMUL JURIDIC DE UTILIZARE A SI RSSP

Secțiunea 1

Acordarea dreptului de acces la SI RSSP

60. Participanții au drept de acces la informația din SI RSSP conform atribuțiilor și funcțiilor deținute și regimului juridic al informației accesate. Nivelul de acces la informație pentru fiecare participant corespunde funcției de serviciu și/sau profilului de acces.

61. La înregistrarea în cadrul sistemului, fiecărui participant i se atribuie și rolul de care depinde dreptul de acces la obiectele informaționale. Autorizarea participanților se produce în conformitate cu nivelul de acces stabilit și aceștia au posibilitatea să acceseze funcționalitățile sau informațiile disponibile potrivit nivelului de acces.

62. La baza mecanismului de autentificare în cadrul SI RSSP se află serviciul electronic guvernamental de autentificare și control al accesului (MPass).

63. Destinatarii SI RSSP pot accesa informațiile publice plasate în registru fără a fi necesară autentificarea, prin intermediul portalului guvernamental unic al serviciilor publice.

64. Dreptul de acces la resursele informaționale ale SI RSSP este segmentat pe unități de conținut, atribuind prerogative partajate, și anume: vizualizare, adăugare, redactare și ștergere.

65. Accesul la resursele informaționale ale SI RSSP este segmentat pentru utilizatorii interni și utilizatorii externi.

66. Utilizatori interni ai SI RSSP sunt posesorul/deținătorul, registratorii și administratorul de sistem, ale căror drepturi de acces sunt definite în prezentul Regulament și alte acte normative.

67. Posesorul și deținătorul au acces cu drept de vizualizare a datelor din SI RSSP, în limita scopului și atribuțiilor acordate prin prezentul Regulament și cadrul normativ.

68. Utilizatorii externi ai SI RSSP sunt furnizorii de date și destinatarii SI RSSP.

69. Furnizorii de date pot modifica și radia datele introduse de aceștia în SI RSSP, prin intermediul registratorilor. Furnizorii de date au acces de vizualizare a informației potrivit drepturilor acordate de posesor.

70. Exploatarea SI RSSP fără autorizare nominală este strict interzisă și urmează a fi considerată ca acces neautorizat la un sistem informațional public, cu excepția utilizării datelor cu caracter public plasate în registru.

Secțiunea a 2-a

Revocarea dreptului de acces la SI RSSP

71. Dreptul de acces la SI RSSP nu este unul permanent și poate fi revocat în circumstanțele prevăzute de prezentul Regulament. Introducerea și/sau modificarea datelor din registru de pe un nume sau profil de utilizator străin este strict interzisă, urmând a fi considerată ca acces neautorizat. Participanții la SI RSSP urmează să se asigure că profilul de utilizator, precum și semnătura electronică sunt confidențiale.

72. Revocarea dreptului de acces la SI RSSP se efectuează de către posesor, în una din următoarele situații:

1) la intervenirea modificărilor raporturilor de serviciu/de muncă ale angajaților furnizorului de date, când noile atribuții nu impun accesul la datele SI RSSP, în urma informării de către furnizorul de date;

2) la încetarea/suspendarea raporturilor de serviciu/de muncă ale angajaților posesorului/deținătorului;

3) la intervenirea modificărilor raporturilor de serviciu/de muncă ale angajaților posesorului/deținătorului, când noile atribuții nu impun accesul la datele registrului;

1) la încălcarea regulilor de utilizare a sistemului sau la constatarea încălcării securității informaționale de către utilizatori;

2) la suspendarea/expirarea/rezilierea sau revocarea acordului cu privire la utilizarea SI RSSP, încheiat între posesor și furnizorul de date;

3) la cererea expresă a furnizorului de date, pentru sine.

Capitolul VI

ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI SI RSSP

Secțiunea 1

Securitatea informației SI RSSP

73. Serviciile furnizate de SI RSSP se conformează cerințelor minime de securitate corespunzătoare cerințelor de securitate a aplicațiilor livrate din platforma MCloud.

74. Măsurile de protecție și securitate a informației cu caracter personal din SI RSSP reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a registrului și se efectuează neîntrerupt de către toți participanții.

75. Obiecte ale asigurării protecției și securității informației din SI RSSP se consideră tot complexul de mijloace software și hardware care asigură realizarea proceselor informaționale.

76. Protecția informației cu caracter personal din SI RSSP la nivel de posesor se efectuează prin următoarele metode:

- 1) prevenirea conexiunilor neautorizate la rețelele de transport date guvernamentale și interceptării cu ajutorul mijloacelor tehnice specifice a datelor din registru transmise prin aceste rețele;

- 2) asigurarea măsurilor de protecție a datelor prin folosirea metodelor criptografice de transmitere a informației prin rețelele de transport date guvernamentale;

- 3) excluderea accesului neautorizat la datele din registru prin utilizarea funcționalităților de autorizare ale serviciului guvernamental MPass;

- 4) prevenirea acțiunilor speciale tehnice și de program care duc la distrugerea, denaturarea datelor sau cauzează defecțiuni în funcționarea complexului tehnic și de program;

- 5) efectuarea periodică planificată a copiilor de siguranță a datelor și fișierelor mijloacelor de program;

- 6) efectuarea tuturor măsurilor aferente asigurării restabilirii și continuității funcționării registrului în cazul incidentelor.

77. Protecția informației cu caracter personal la nivel de participant la SIRSSP se efectuează prin următoarele metode:

- 1) prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor din registru;

- 2) monitorizarea procesului de exploatare a registrului prin intermediul mecanismului de jurnalizare efectuat de posesorul acesteia.

78. Participanții la SI RSSP elaborează și implementează politica de securitate informațională pentru asigurarea respectării regulilor, standardelor și normelor în domeniul securității informaționale, incluzând:

- 1) identitatea persoanei responsabile de politica de securitate;

- 2) principalele măsuri tehnico-organizatorice necesare asigurării funcționării SI RSSP;

- 3) procedurile interne ce exclud cazurile de modificare nesancționată a mijloacelor software și/sau a informației din registru;

- 4) responsabilitățile personalului participantului la registru privind asigurarea securității informaționale;

- 5) procedurile de control intern al participantului la SI RSSP privind respectarea condițiilor de securitate informațională.

79. Fiecare participant la SI RSSP asigură informarea sau, după caz, instruirea utilizatorilor privind metodele și procedeele de contracarare a pericolelor informaționale.

Secțiunea a 2-a

Protecția datelor cu caracter personal din SI RSSP

80. Datele de autentificare din SI RSSP fac parte din categoria datelor cu caracter personal. Asigurarea securității, confidențialității și a integrității datelor prelucrate în cadrul SI RSSP 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.

81. Dreptul de informare a subiectului datelor cu caracter personal, dreptul de acces la datele cu caracter personal, dreptul de intervenție asupra datelor cu caracter personal, dreptul de opoziție al subiectului datelor cu caracter personal și alte aspecte ce țin de domeniul protecției datelor cu caracter personal se vor realiza în corespundere cu cadrul normativ ce reglementează domeniul dat.

82. Prelucrarea de date elaborate pe baza SI RSSP trebuie să garanteze respectarea următoarelor principii privind protecția datelor cu caracter personal:

- 1) specificarea și limitarea scopului;
- 2) adoptarea de măsuri tehnice și organizaționale în scopul asigurării unui nivel adecvat de protecție a datelor cu caracter personal, în conformitate cu legislația.

83. În cazul incidentelor de securitate, posesorul va 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.

Capitolul VII

SUSPENDAREA FUNCȚIONĂRII SI RSSP

84. Pentru asigurarea funcționalității eficiente și neîntrerupte, schimbul informațional de date în SI RSSP este asigurat în regim non-stop.

85. Funcționarea SI RSSP se suspendă de către administratorul tehnic, după coordonarea prealabilă cu posesorul, în cazul apariției uneia dintre următoarele situații:

- 1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al SI RSSP;
- 2) la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea SI RSSP;
- 3) în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SI RSSP;
- 4) la cererea scrisă a posesorului.

86. Lucrările profilactice planificate în complexul de mijloace software și hardware se efectuează după notificarea, în scris sau prin e-mail, a furnizorilor de date de către posesor, în baza planului coordonat cu administratorul tehnic, cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă este posibil. Lucrările profilactice neplanificate se efectuează la solicitarea furnizorilor de date și coordonarea prealabilă cu posesorul, în situația nefuncționării sau funcționării necorespunzătoare a complexului de mijloace software și hardware. Dacă lucrările profilactice durează mai mult de 5 de zile, la expirarea fiecărei perioade de 5 de zile de efectuare a lucrărilor, se notifică furnizorii de date.

87. Furnizarea serviciilor oferite de SI RSSP poate fi suspendată de către administratorul tehnic fără consimțământul posesorului, cu notificarea ulterioară a acestuia, în următoarele situații:

- 1) situații de incidente la scară;
- 2) la apariția situațiilor de imposibilitate fortuită de executare.

88. Suspendarea serviciilor se efectuează asigurându-se un impact minim asupra calității serviciilor livrate furnizorilor de date și destinatarilor SI RSSP.

Capitolul VIII MONITORIZARE ȘI CONTROL

Secțiunea 1

Controlul extern

89. SI RSSP este supus unui control intern și extern. Controlul intern este efectuat de posesor, iar cel extern de către instituțiile abilitate și certificate în domeniul tehnologiei informației.

90. Controlul legalității operațiunilor de prelucrare a datelor cu caracter personal desfășurate în SI RSSP se efectuează de către Centrul Național pentru Protecția Datelor cu Caracter Personal.

91. La efectuarea controlului extern, organul de control alcătuiește un raport privind controlul extern. Posesorul este obligat să ia măsuri pentru lichidarea încălcărilor identificate și să informeze despre aceasta organul de control.

92. Pentru organizarea controlului de funcționare a SI RSSP este responsabil posesorul acestuia, care este obligat să asigure dreptul de acces la registru și mijloacele de ținere a acestuia, iar administratorul tehnic în încăperile în care se află mijloacele hardware utilizate în acest scop.

93. Participanții responsabili de asigurarea funcționării sistemului și înregistrării datelor poartă răspundere personală, în conformitate cu prevederile Legii privind protecția datelor cu caracter personal, pentru autenticitatea, fiabilitatea, integritatea informației, precum și pentru păstrarea/stocarea și utilizarea acesteia.

94. Toți participanții la SI RSSP și destinatarii informațiilor ce conțin date cu caracter personal poartă răspundere pentru prelucrarea neconformă a datelor cu caracter personal în conformitate cu prevederile Legii privind protecția datelor cu caracter personal.

95. SI RSSP se înregistrează în Registrul resurselor și sistemelor informaționale de stat și în Registrul de evidență al operatorilor de date cu caracter personal.

96. Funcționarea SI RSSP este asigurată de posesor până la adoptarea deciziei de lichidare a acestuia. În cazul lichidării, datele și documentele conținute în acesta se transmit în arhivă conform legislației.

Secțiunea a 2-a

Monitorizarea și controlul intern

97. În vederea asigurării funcționării eficiente a SI RSSP, acordul cu privire la utilizarea gratuită a registrului, încheiat între posesor și furnizorul de date, va conține, după caz, clauze referitoare la:

- 1) monitorizarea constantă a operării SI RSSP;

2) controlul permanent asupra executării de către participanții la registru a atribuțiilor prevăzute în prezentul Regulament, precum și a celor specificate în acordurile încheiate;

3) gestionarea riscurilor aferente operării SI RSSP, identificate prin implementarea activităților de prevenire, gestionare, combatere etc.;

4) evaluarea cu regularitate a performanței activității participanților implicați în asigurarea calității necesare operării SI RSSP și prestării serviciilor aferente acestora.

98. În scopul monitorizării și controlului asupra executării Regulamentului, cooperarea dintre posesorul SI RSSP și furnizorul de date va fi asigurată prin schimb de informație, raportare periodică, ședințe comune de evaluare, replanificare, audit etc.

99. Concluziile generate de eforturile de monitorizare, control și evaluare sistematică vor servi drept bază în luarea deciziilor corective pe parcursul implementării SI RSSP, planificarea activităților la diferite etape de operare a acestuia, evaluarea performanței participanților la utilizarea registrului, supravegherea procesului de implementare și operare a resurselor informaționale elaborate pe baza SI RSSP etc.

Regulamentul-cadru cu privire la organizarea și prestarea serviciului public

1. Dispoziții generale

Prestarea fiecărui serviciu public se realizează în conformitate cu regulamentul aprobat. Serviciul public poate fi prestat doar după intrarea în vigoare a regulamentului de organizare și prestare a acestuia.

Proiectul regulamentului de organizare și prestare a serviciului public se elaborează și se promovează în conformitate cu prevederile Legii nr. 100/2017 cu privire la actele normative, de către prestatorul acestuia, și se prezintă spre aprobare concomitent cu proiectul de act normativ care prevede instituirea acestuia. În cazul implicării în procesul de prestare a serviciului public a mai multor autorități/instituții publice, proiectul regulamentului se elaborează de către autoritatea/instituția publică care este abilitată cu realizarea funcției de gestionare a serviciului public și se coordonează obligatoriu cu toți participanții procesului de prestare a serviciului public.

Regulamentul de organizare și prestare a serviciului public în domeniile de activitate ale Guvernului se aprobă de către Guvern. Cu titlul de recomandare, regulamentul de organizare și prestare a serviciului public în domeniile de activitate ale administrației publice locale se aprobă de către administrația publică locală abilitată.

Regulamentul de prestare a serviciului public poate să conțină descrierea mai multor servicii publice grupate într-un eveniment de viață comun.

Regulamentul de prestare a serviciului public determină condițiile de prestare a serviciilor publice, stabilește regulile și procesele operaționale pentru prestarea serviciilor, drepturile și obligațiile prestatorului și beneficiarului serviciului, precum și condițiile de asigurare a securității informaționale și prelucrării datelor cu caracter personal.

2. Structura-tip a regulamentului

Regulamentul este format din următoarele elemente constitutive de bază:

Capitolul I. Dispoziții generale

Secțiunea 1. Cadrul juridic

Secțiunea 2. Domeniul de aplicare

Secțiunea 3. Principiile prestării serviciului/serviciilor

Secțiunea 4. Noțiuni principale

Secțiunea 5. Prelucrarea informației la prestarea serviciilor publice

Capitolul II. Raporturile juridice în domeniul prestării serviciilor publice

Secțiunea 1. Subiecții raporturilor juridice în domeniul prestării serviciilor publice

Secțiunea 2. Drepturile și obligațiile prestatorului serviciului public

Secțiunea 3. Drepturile și obligațiile beneficiarului serviciului public

Capitolul III. Modul de prestare a serviciilor publice

Secțiunea 1. Organizarea și funcționarea serviciului

Secțiunea 2. Cazurile de prestare a serviciului

Secțiunea 3. Condițiile și locul prestării serviciului

Secțiunea 4. Procesul de prestare a serviciului

Secțiunea 5. (opțională) Aspecte specifice de funcționare/furnizare /prestare a serviciului după caz

Secțiunea 6. Refuzul în prestarea serviciilor publice

Secțiunea 7. Informarea beneficiarilor serviciilor publice

Capitolul IV. Managementul serviciului public

Secțiunea 1. Managementul resurselor umane

Secțiunea 2. Managementul serviciului și procedura de raportare

Secțiunea 3. Stabilirea obiectivelor și măsurarea performanței serviciului

Secțiunea 4. Reclamațiile cu privire la prestarea serviciilor publice

Secțiunea 5. Procedura de contestare

Capitolul V. Patrimoniul și finanțarea serviciului

Capitolul VI. Dispoziții finale

La regulament se anexează cererile-tip de solicitare a serviciului, în cazul eliberării rezultatului serviciului pe suport de hârtie – modelele de documente, sau se va face trimitere la act normativ prin care acestea au fost aprobate și puse în aplicare, formularul refuzului de a presta serviciul public, forma de depunere a petiției și alte formulare tipizate.

Structura poate fi completată cu compartimente suplimentare în dependență de complexitatea serviciului. În cazul comasării într-un regulament a mai multor servicii publice, informația privind procedura și condițiile de prestare a serviciilor publice va fi expusă prin capitole separate.

3. Conținutul de bază al regulamentului

3.1. Capitolul I. Dispoziții generale reprezintă un capitol introductiv, care va stabili că regulamentul constituie cadrul normativ ce asigură realizarea raporturilor juridice dintre persoanele fizice, persoanele juridice și instituțiile statului în prestarea unui serviciului public sau a mai multor servicii grupate pe un domeniu.

În regulament se va face referire la baza normativă conform căreia este prestat serviciu public, domeniul de aplicare, denumirea serviciului/serviciilor publice, precum și vor fi stipulate principiile de bază pentru prestarea serviciilor publice precum:

- accesul egal al beneficiarilor la servicii, fără nici o discriminare pe motive de origine, statut social, oficial și de proprietate, sex, rasă, naționalitate, limbă, religie, credințe, loc de reședință sau pentru orice alte circumstanțe;
- inadmisibilitatea barierelor birocratice în prestarea serviciilor publice;
- responsabilitatea și transparența în prestarea serviciilor publice;
- calitatea și accesibilitatea serviciilor publice;
- îmbunătățirea continuă a procesului de prestare a serviciilor publice;
- economie și eficiență în prestarea serviciilor publice.

În sensul regulamentelor de organizare și prestare a serviciilor publice se presupune prelucrarea datelor cu caracter personal. În regulament se va face mențiune la modalitatea procesării datelor cu caracter personal, care urmează a fi efectuată în conformitate cu prevederile Legii nr. 133/2011 privind protecția datelor cu caracter personal și actelor normative aferente sistemelor informaționale utilizate în procesul prestării serviciului public. În cazul în care în procesul prestării serviciului public se procesează informația ce constituie secret de stat sau comercial, acest aspect va fi menționat, inclusiv prin trimitere la acte normative corespunzătoare.

Fiecare Regulament de organizare și prestare a serviciilor publice va conține un set de noțiuni specifice (*după cele generale*), relevante serviciului prestat. Totodată, Regulamentul urmează să conțină și un set minim de noțiuni generale/comune pentru toate serviciile publice.

3.2. În Capitolul II. Raporturile juridice în domeniul prestării serviciilor publice vor fi stipulați subiecții raporturilor juridice în domeniul prestării serviciilor publice, cu descrierea clară drepturilor și obligațiilor prestatorului și beneficiarului serviciului în procesul prestării serviciului public.

3.3. Capitolul III. Modul de prestare a serviciilor publice reprezintă o descriere generală privind modul de acordare a serviciului, proceselor derulate și formelor de prestare a serviciului public. În cazul comasării mai multor servicii într-un regulament, acestea se descriu separat, structurate în sub-compartimente.

Conform standardelor pentru furnizarea de servicii este necesară respectarea a unei serii de cerințe, în special, să conțină informații cu privire la rezultatul prestării serviciului, calendarul prestării acestuia, motive legale pentru prestare, o listă exhaustivă de documente necesare pentru obținerea unui serviciu, o listă exhaustivă de motive pentru care este acceptată și refuzată acceptarea documentelor și prestarea serviciilor, legalitatea încasării taxelor de stat și a tarifelor pentru prestarea serviciilor, cu referire la actul normativ ce stabilește cuantumul tarifului și taxei percepute pentru prestarea serviciilor, timpul de așteptare maximă la depunerea unei cereri și primirea rezultatului prestării serviciului, termenul limită pentru înregistrarea cererii solicitantului și primirea rezultatului serviciului, cerințe pentru spațiile în care serviciile sunt prestate, inclusiv sala de așteptare, locuri pentru depunerea cererilor, standuri de informare și altor modalități de difuzare a informațiilor despre serviciu public.

În cazul posibilității de a primi servicii în formă electronică, dacă acest lucru nu este interzis de lege, precum și în alte forme prevăzute de legislație, la opțiunea

solicitantului se descrie modalitatea de comandă și primirea rezultatului serviciului public.

Totodată compartimentul dat conține descrierea succintă a funcțiilor care îi revin prestatorului, inclusiv cu referire la atribuțiile persoanelor împuternicite de prestator (*operator/registrator etc.*) și solicitantului serviciului. Aici poate fi prezentat schematic (*Forma grafică*) procesul de prestare a serviciului public.

3.4. Capitolul IV. Managementul serviciului public cuprinde prevederi standardizate referitoare la gestionarea serviciului din partea autorității prestatoare în scopul monitorizării continue a procesului de prestare a serviciului pentru atingerea impactului juridic și social-economic, cum ar fi:

- îmbunătățirea calității serviciilor publice;
- îmbunătățirea accesibilității și confortului serviciilor publice;
- extinderea listei serviciilor publice prestate și a variabilității modalităților de obținere a serviciilor publice;
- sensibilizarea prestatorilor și beneficiarilor serviciilor publice;
- eficientizarea proceselor operaționale de prestare a serviciilor publice de către prestatorii acestora;
- optimizarea proceselor de furnizare a serviciilor publice;
- reducerea riscurilor de corupție în furnizarea de servicii;
- creșterea responsabilității instituționale și individuale pentru încălcări în prestarea serviciilor publice.

Capitolul conține prevederi privind statutul necesar a persoanei împuternicite de prestator (*funcționar public/operator/registrator etc.*) și prevederi referitoare la calificarea acestuia pentru primirea cererii și luarea deciziei privind posibilitatea prestării serviciului și eliberarea rezultatului serviciului.

Prestatorul fiind responsabil de calitatea serviciului, trebuie să asigure evaluarea anuală a acestuia conform standardelor minime de calitate. În capitolul dat trebuie să fie stabilită procedura de asigurare a monitorizării și evaluării serviciului, întocmirea rapoartelor periodice, precum și planificarea activităților în baza rezultatelor obținute, stabilirea obiectivelor, măsurarea indicilor de performanță și întocmirea propunerilor de ridicare a eficienței.

Totodată compartimentul cuprinde prevederi referitoare la indicatorii de calitate a serviciului cum ar fi:

- *Indicatorii de eficiență* care măsoară relațiile dintre rezultatele obținute și resursele alocate pentru obținerea lor. Indicatorii de eficiență au în vedere atât costurile, cât și productivitatea necesară obținerii rezultatului.
- *Indicatori de eficacitate* care măsoară gradul în care instituția publică a reușit, prin rezultatele politicilor sale, să își atingă obiectivele stabilite, răspunzând la principalele provocări impuse de societate și la nevoile cetățenilor. Indicatorii de eficacitate permit analiza relației dintre rezultatele politicilor publice, scopurile politicilor și nevoile cetățenilor.
- *Indicatorii de calitate* care măsoară calitatea serviciilor, fiind un tip de evaluare/apreciere ce descrie serviciile furnizate către cetățeni și instituții din punctul de vedere al rapidității, disponibilității, ratei, continuității, cantității și al satisfacției clienților. Acest tip de indicatori măsoară calitatea produselor și a serviciilor în comparație cu standardele de calitate stabilite. Aceasta înseamnă că

standardele pentru servicii trebuie stabilite și aprobate dinainte, în vederea realizării unor măsurători adecvate.

Prestatorul de serviciu stabilește procedura de depunere și examinare a plângerilor privind calitatea serviciului prestat și asigură informarea Solicitantului despre procedura de depunere și examinare a plângerilor. Prestatorul de serviciu dispune de un registru de înregistrare a plângerilor, care include atât informațiile privind modul de examinare a plângerilor, cât și măsurile întreprinse în acest sens.

Totodată va fi menționată procedura de contestare, stipulată în conformitate cu prevederile Codului administrativ al Republicii Moldova nr.116/2018, privind refuzul prestatorului de a presta serviciul public sau actul administrativ individual emis în rezultatul prestării serviciului public.

3.5. În Capitolul V. Patrimoniul și finanțarea serviciului se vor menționa sursele de finanțare a cheltuielilor necesare pentru a iniția prestarea serviciului și a asigura prestarea serviciului public în condițiile cadrului normativ, inclusiv prin dezvoltarea procedurilor și proceselor aferente serviciului. În estimarea bugetului de venituri și cheltuieli, prestatorul de servicii are în vedere asigurarea resurselor necesare acordării serviciului cel puțin la nivelul standardelor minime de calitate aplicabile.

3.6. Capitolul VI. Dispoziții finale cuprinde prevederi standardizate referitoare la răspunderea pentru încălcarea legislației în domeniul prestării serviciilor publice, acțiuni de introducere, modificare și anularea serviciilor publice, precum și condițiile în care serviciul este suspendat sau sistat.