

**GUVERNUL REPUBLICII MOLDOVA**

**HOTĂRÂRE**

nr. \_\_\_\_ din \_\_\_\_\_

**cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat „Registrul unic al procurilor”**

În temeiul art. 3, art. 4 alin. din Legea nr. 1453-XV din 08 noiembrie 2002 cu privire la notariat (publicată în Monitorul Oficial al Republicii Moldova, 2002, nr. 154-157, art. 1209), cu modificările ulterioare și art. 252 din Codul Civil al Republicii Moldova (publicat în Monitorul Oficial al Republicii Moldova, 2002, nr. 82-86, art. 661), cu modificările ulterioare,

**Guvernul HOTĂRĂȘTE:**

1. Se aprobă Conceptul tehnic al Sistemului informațional automatizat „Registrul unic al procurilor” (se anexează).
2. Ministerul Justiției va asigura realizarea prevederilor Conceptului tehnic al Sistemului informațional automatizat „Registrul unic al procurilor”.
3. Sistemul informațional automatizat „Registrul unic al procurilor” este ținut de Ministerul Justiției prin intermediul Centrului de Informații Juridice.
4. Asigurarea funcționării Sistemului informațional automatizat „Registrul unic al procurilor” se efectuează din contul și în limita alocațiilor aprobate Ministerului Justiției prin legea bugetară anuală.

**PRIM-MINISTRU**

**Contrasemnează:**

**Ministrul justiției**

**Ministrul finanțelor**

**Ministrul tehnologiei informației  
și comunicațiilor**

## **Conceptul tehnic al Sistemului informațional automatizat ”Registrul unic al procurilor”**

### **I. INTRODUCERE**

Întru sporirea eficienței organizării, desfășurării și a monitorizării proceselor de eliberare și management a procurilor notariale, Ministerul Justiției al Republicii Moldova este necesară implementarea unui sistem informatic nou, care va permite gestiunea eficientă a totalității informației aferente procurilor eliberate de notarii publici. Implementarea sistemului informatic destinat gestiunii procurilor (Registrul unic al procurilor) va servi în calitate de instrument eficient pentru organizarea și desfășurarea proceselor de recepție și procesare a cererilor și de eliberare a procurilor conform legislației în vigoare.

Crearea unui sistem informatic cu capacitate de automatizare a proceselor de gestiune a informației privind procurile va avea ca efect alinierea tehnologiilor implementate de Ministerul Justiției la standardele europene.

Datorită utilizării SIA e-Procura se va reduce timpul necesar eliberării, gestiunii procurii și regăsirii informației aferente procurilor.

Sistemul va asigura securitatea și integritatea informației prin implementarea unui mediu unic și centralizat de păstrare a datelor (Registrul unic al procurilor), cu politici de securitate strict reglementate conform legislației în vigoare.

Sistemul va servi drept instrument-cheie de extragere operativă a datelor și rapoartelor privind activitatea notarială, precum și va îndeplini cerințele Centrului de Guvernare Electronică de migrare a sistemelor informaționale pe platforma MCloud și integrarea lor cu sistemele MSign, MPass, MPay, etc.

### **II. GENERALITĂȚI**

1. Denumirea deplină a sistemului informațional automatizat este Sistem informațional automatizat ”Registrul unic al procurilor”. Denumirea prescurtată a sistemului este SIA e-Procura.

2. SIA e-Procura reprezintă o soluție informatică, obiectivul principal al căreia constă în automatizarea proceselor de eliberare, gestiune, monitorizare și evidență a procurilor.

3. SIA „e-Procura” este destinat ca platformă unică de înregistrare în format electronic, stocare și verificare a oricăror tipuri de procuri notariale a căror înregistrare este solicitată prin lege. Toate procedurile urmează a fi efectuate doar prin intermediul acestui registru, cu excluderea totală a fluxurilor funcționale pe suport de hârtie (fluxurile opționale pot fi dublate pe suport de hârtie, spre exemplu, informarea, la solicitare, pe suport de hârtie).

4. Prin intermediul SIA e-Procura vor fi realizate următoarele scopuri:

- 1) automatizarea proceselor de depunere a cererilor de autentificare notarială a procurilor;
- 2) tranziția la procesarea digitală a documentelor;
- 3) crearea unui mecanism de conexiune cu subsistemele informatice relevante activității notariale;
- 4) monitorizarea respectării legii privind procedura de autentificare notarială;
- 5) prevenirea abuzurilor, ilegalităților sau încălcărilor în procesul de autentificare notarială a procurilor;

- 6) asigurarea de către Ministerul Justiției a procesului de monitorizare a activității notariale;
- 7) colectarea și analiza informației necesare pentru a asigura aplicarea principiilor și mecanismelor prevăzute în Legea privind organizarea activității notarilor.

5. În sensul prezentului Concept, noțiunile de bază utilizate semnifică:

*Reprezentat* – persoană care acordă unei alte persoane împuternicirea de a încheia unul sau mai multe acte juridice în numele său.

*Reprezentant* – persoană căreia i s-a acordat împuternicirea de a încheia unul sau mai multe acte juridice în numele persoanei reprezentate.

*Procură* – înscrisul întocmit pentru atestarea împuternicirilor conferite de reprezentat unui sau mai multor reprezentanți.

*Notar* – exponentul puterii de stat împuternicit în modul stabilit de lege, în bază de licență și a ordinului de investire cu împuterniciri, să desfășoare activitatea notarială.

6. La proiectarea, realizarea și implementarea sistemului informatic trebuie să se țină cont de următoarele principii generale:

- 1) Principiul legalității: care presupune crearea și exploatarea sistemului informatic în conformitate cu legislația națională în vigoare și a normelor și standardelor internaționale recunoscute în domeniu;
- 2) Principiul divizării arhitecturii pe nivele: constă în proiectarea independentă a subsistemelor e-Procura în conformitate cu standardele de interfață dintre nivele;
- 3) Principiul arhitecturii bazate pe servicii (SOA): constă în distribuirea funcționalității aplicației în unități mai mici, distincte - numite servicii - care pot fi distribuite într-o rețea și pot fi utilizate împreună pentru a crea aplicații destinate afacerilor;
- 4) Principiul datelor sigure: stipulează introducerea datelor în sistem doar prin canalele autorizate și autentificate;
- 5) Principiul securității informaționale: presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și de acces nesancționat.
- 6) Principiul accesibilității informației cu caracter public: care presupune implementarea procedurilor de asigurare a accesului solicitanților la informația cu caracter public furnizată de soluția informatică.
- 7) Principiul transparenței: presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicații;
- 8) Principiul expansibilității: stipulează posibilitatea extinderii și completării sistemului informatic cu noi funcții sau îmbunătățirea celor existente;
- 9) Principiul scalabilității: presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului informatic;
- 10) Principiul simplității și comodității utilizării: presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor Sistemului, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție.

7. În particular, pentru arhitectura sistemului informatic se insistă asupra respectării următoarelor principii primordiale:

- 1) implementarea unei soluții cu acces autorizat la interfață și date;
- 2) asigurarea unei securități adecvate a sistemului informatic pentru a proteja informația și subsistemele componente împotriva utilizării lor neautorizate sau a divulgării informației cu caracter personal sau a celei cu accesibilitate limitată;
- 3) recunoașterea informației ca patrimoniu și gestionarea ei adecvată;

- 4) dezvoltarea și implementarea sistemului informatic oferind posibilitatea reutilizării lor pentru alte procese sau în perspectiva asigurării posibilității de dezvoltare de noi funcționalități;
  - 5) minimizarea numărului diferitor tehnologii și produse care oferă aceleași funcționalități sau sunt similare după destinație;
  - 6) asigurarea unei viteze performante de procesare a solicitărilor beneficiarilor;
  - 7) pentru soluția informatică livrată trebuie să fie prevăzută capacitatea de restabilire în urma dezastrelor (asigurarea securității fizice a soluției informatice) ca parte componentă a planului de implementare.
8. Sarcinile de bază ale soluției informatice e-Procura sunt:
- 1) Proiectarea și implementarea unor tehnologii moderne de recepție, înregistrare, evidență și monitorizare a documentelor și eliberare a procurilor;
  - 2) Crearea unui repozitoriu centralizat de date, care va fi amplasat în infrastructura MCloud;
  - 3) Implementarea unui registru unic al procurilor și documentelor aferente acestora;
  - 4) asigurarea posibilității de lucru în rețea pentru personalul Ministerului Justiției și a birourilor notariale, pentru exploatarea eficientă a resurselor comune prin implementarea unei arhitecturi client-server multinivel;
  - 5) creșterea vitezei de circulație a informației;
  - 6) controlul accesului la date a utilizatorilor și asigurarea unei veridicități, securități și confidențialități maxime a datelor colectate, care nu sunt publice.

### **III. SPAȚIUL JURIDICO-NORMATIV AL FUNCȚIONĂRII SISTEMULUI**

9. Spațiul juridico-normativ al SIA e-Procura include:
- 1) Legea Nr. 1453-XV din 08.11.2002 cu privire la notariat
  - 2) Legea Nr. 71-XVI din 22.03.2007 cu privire la registre,
  - 3) Legea Nr. 982-XIV din 11.05. 2000 privind accesul la informație.
  - 4) Legea nr. 91 din 29 mai 2014 privind semnătura electronică și documentul electronic.
  - 5) Legea Nr. 467-XV din 21.11.2003 cu privire la informatizare și la resursele informaționale de stat.
  - 6) Legea Nr. 1069-XIV din 22.06.2000 cu privire la informatică.
  - 7) Legea Nr. 231 din 25.11.2011 privind aprobarea Strategiei de reformă a sectorului justiției pentru anii 2011 – 2016.
  - 8) Hotărârea Guvernului Nr. 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.
  - 9) Hotărârea Guvernului Nr. 945 din 05.09.2005 cu privire la centrele de certificare a cheilor publice.
  - 10) Hotărârea Guvernului nr. 320 din 28.03.2006 pentru aprobarea Regulamentului privind modul de aplicare a semnăturii digitale în documentele electronice ale autorităților publice.
  - 11) Hotărârea Guvernului nr. 710 din 20.09.2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare).
  - 12) Standardul Republicii Moldova SMV ISO CEI 15288:2009, „Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului”.
  - 13) Reglementarea tehnică „Procesele ciclului de viață al software-lui” RT 38370656-002:2006.
  - 14) Alte acte normative și standarde în vigoare în domeniul activității notariale, tehnologiei informației și comunicațiilor.

#### **IV. SPAȚIUL FUNCȚIONAL AL SISTEMULUI**

10. SIA e-Procura trebuie să execute următoarele funcții de bază:

- 1) Completarea registrelor electronice – reprezintă un set de funcționalități automate a SIA e-Procura care constau în atribuirea automată a numerelor de înregistrare unice procurilor și documentelor inserate în registrul electronic al procurii, precum și totalitatea funcționalităților de formare a registrelor electronice a procesului de perfectare a procurii.
- 2) Jurnalizarea evenimentelor – Orice eveniment generat în cadrul proceselor implementate în SIA e-Procura vor fi jurnalizate și salvate în tabelele corespunzătoare a Bazei de Date.
- 3) Notificarea utilizatorilor și notarilor – Acest caz de utilizare descrie comportamentul mecanismului de notificare automată a SIA e-Procură. Este un caz de utilizare care conține totalitatea procedurilor automate destinate notificării registratorului, operatorului de eliberare, Ministerului Justiției, etc.

11. SIA e-Procura trebuie să asigure exercitarea funcțiilor specifice determinate de destinația sistemului, grupate în blocuri funcționale specializate:

1) Blocul funcțional "Evidența procurilor" include următoarele funcții:

- a) Evidența reprezentaților;
- b) Evidența reprezentanților;
- c) Evidența momentului înregistrării, modificării, sau revocării procurii;
- d) Evidența imaginilor scanate ale actelor de identitate ale reprezentaților;
- e) Evidența imaginilor scanate ale actelor de identitate ale reprezentanților;
- f) Evidența imaginilor scanate ale procurii perfectate;
- g) Furnizarea informației din SIA „e-Procura” cu privire la valabilitatea procurii.

2) Blocul funcțional „Evidența documentelor SIA „e-Procura” include următoarele funcții:

- a) Generarea documentelor de ieșire;
- b) Evidența documentelor de ieșire;
- c) Evidența documentelor eliberate din SIA „e-Procura”.

12. Descrierea tehnologiei lucrărilor, interacțiunea conturilor și funcțiilor se efectuează la următoarele etape de proiectare și creare a sistemului, în conformitate cu Reglementarea tehnică „Procese ciclului de viață al software-lui" RT 38370656-002:2006

13. SIA e-Procura va fi interconectat cu Registrul de Stat al Populației prin intermediul platformei guvernamentale de interoperabilitate MConnect.

#### **V. STRUCTURA ORGANIZAȚIONALĂ A SIA „e-PROCURA”**

14. Proprietarul SIA e-Procura este statul, care își realizează dreptul de proprietate, de gestionare și utilizare a datelor din sistemul informațional.

15. Posesorul SIA e-Procura este Ministerul Justiției, cu drept de gestionare a registrului și utilizare a datelor din registru și a resurselor în limitele reglementate de proprietar.

16. Deținător al SIA e-Procura este Centrul de Informații Juridice, autoritate administrativă din subordinea Ministerului Justiției, care va asigura crearea și exploatarea acestui sistem.

17. Întreprinderea de Stat „Centrul de Telecomunicații Speciale” va asigura asistența și mijloacele tehnice necesare funcționării SIA e-Procura (infrastructura hardware & software din cadrul MCloud), validare a semnăturii electronice și autentificare prin intermediul certificatului digital sau mobile ID (MPass)).

18. Centrul de Guvernare Electronica va oferi cu titlu gratuit soluția *M-Cloud* și serviciile de platformă MSign, MPass, MPay, MLog, MNotify, MConnect utilizate pentru găzduirea și funcționalitatea SIA e-Procura.

19. Registratori ai SIA e-Procura sunt notarii, administrația publică locală, șefii de spitale și sanatorii, șefii instituțiilor de învățământ militar, comandanții militari, șefii penitenciarelor.

20. Notarii vor înregistra următoarele date:

1) Date despre persoana fizică:

- a) numele și prenumele;
- b) numărul de identificare;
- c) data nașterii;
- d) numărul și seria actului de identitate;
- e) adresa de domiciliu și electronică;

2) Date despre persoana juridică:

- a) denumirea;
- b) numărul de identificare (IDNO);
- c) sediul și adresa electronică;

3) Date despre procură:

- a) numărul de înregistrare a procurii din Registrul actelor notariale;
- b) data autentificării procurii;
- c) numărul procurii revocate, în cazul revocării procurii înregistrate anterior;
- d) data autentificării procurii revocate, în cazul revocării procurii înregistrate anterior;
- e) numele și prenumele notarului care a autentificat procura inițială, în cazul revocării procurii înregistrate anterior;
- f) numărul și data declarației de revocare a procurii din Registrul actelor notariale, în cazul revocării procurii înregistrate anterior;
- g) altă informație conform legislației în vigoare.

21. Administrația publică locală va înregistra următoarele date:

1) Date despre persoana fizică:

- a) numele și prenumele;
- b) numărul de identificare;
- c) data nașterii;
- d) numărul și seria actului de identitate;
- e) adresa de domiciliu și electronică;

2) Date despre persoana juridică:

- a) denumirea;
- b) numărul de identificare (IDNO);
- c) sediul și adresa electronică;

3) Date despre procură:

- a) numărul de înregistrare a procurii din Registrul actelor notariale;
- b) data autentificării procurii;
- c) numărul procurii revocate, în cazul revocării procurii înregistrate anterior;
- d) data autentificării procurii revocate, în cazul revocării procurii înregistrate anterior;
- e) numele și prenumele notarului care a autentificat procura inițială, în cazul revocării procurii înregistrate anterior;
- f) numărul și data declarației de revocare a procurii din Registrul actelor notariale, în cazul revocării procurii înregistrate anterior;
- g) altă informație conform legislației în vigoare.

22. Șefii de spitale și sanatorii vor înregistra următoarele date:

- 1) Date despre persoana fizică:
  - a) numele și prenumele;
  - b) numărul de identificare;
  - c) data nașterii;
  - d) numărul și seria actului de identitate;
  - e) adresa de domiciliu și electronică;
- 2) Date despre persoana juridică:
  - a) denumirea;
  - b) numărul de identificare (IDNO);
  - c) sediul și adresa electronică;
- 3) Date despre procură:
  - a) numărul de înregistrare a procurii din Registrul actelor notariale;
  - b) data autentificării procurii;
  - c) numărul procurii revocate, în cazul revocării procurii înregistrate anterior;
  - d) data autentificării procurii revocate, în cazul revocării procurii înregistrate anterior;
  - e) numele și prenumele notarului care a autentificat procura inițială, în cazul revocării procurii înregistrate anterior;
  - f) numărul și data declarației de revocare a procurii din Registrul actelor notariale, în cazul revocării procurii înregistrate anterior;
  - g) altă informație conform legislației în vigoare.

23. Șefii instituțiilor de învățământ militar vor înregistra următoarele date:

- 1) Date despre persoana fizică:
  - a) numele și prenumele;
  - b) numărul de identificare;
  - c) data nașterii;
  - d) numărul și seria actului de identitate;
  - e) adresa de domiciliu și electronică;
- 2) Date despre persoana juridică:
  - a) denumirea;
  - b) numărul de identificare (IDNO);
  - c) sediul și adresa electronică;
- 3) Date despre procură:
  - a) numărul de înregistrare a procurii din Registrul actelor notariale;
  - b) data autentificării procurii;
  - c) numărul procurii revocate, în cazul revocării procurii înregistrate anterior;
  - d) data autentificării procurii revocate, în cazul revocării procurii înregistrate anterior;
  - e) numele și prenumele notarului care a autentificat procura inițială, în cazul revocării procurii înregistrate anterior;
  - f) numărul și data declarației de revocare a procurii din Registrul actelor notariale, în cazul revocării procurii înregistrate anterior;
  - g) altă informație conform legislației în vigoare.

24. Comandanții militari vor înregistra următoarele date:

- 1) Date despre persoana fizică:
  - a) numele și prenumele;
  - b) numărul de identificare;
  - c) data nașterii;

- d) numărul și seria actului de identitate;
- e) adresa de domiciliu și electronică;
- 2) Date despre persoana juridică:
  - a) denumirea;
  - b) numărul de identificare (IDNO);
  - c) sediul și adresa electronică;
- 3) Date despre procură:
  - a) numărul de înregistrare a procurii din Registrul actelor notariale;
  - b) data autentificării procurii;
  - c) numărul procurii revocate, în cazul revocării procurii înregistrate anterior;
  - d) data autentificării procurii revocate, în cazul revocării procurii înregistrate anterior;
  - e) numele și prenumele notarului care a autentificat procura inițială, în cazul revocării procurii înregistrate anterior;
  - f) numărul și data declarației de revocare a procurii din Registrul actelor notariale, în cazul revocării procurii înregistrate anterior;
  - g) altă informație conform legislației în vigoare.

25. Șefii penitenciarelor vor înregistra următoarele date:

- 1) Date despre persoana fizică:
  - a) numele și prenumele;
  - b) numărul de identificare;
  - c) data nașterii;
  - d) numărul și seria actului de identitate;
  - e) adresa de domiciliu și electronică;
- 2) Date despre persoana juridică:
  - a) denumirea;
  - b) numărul de identificare (IDNO);
  - c) sediul și adresa electronică;
- 3) Date despre procură:
  - a) numărul de înregistrare a procurii din Registrul actelor notariale;
  - b) data autentificării procurii;
  - c) numărul procurii revocate, în cazul revocării procurii înregistrate anterior;
  - d) data autentificării procurii revocate, în cazul revocării procurii înregistrate anterior;
  - e) numele și prenumele notarului care a autentificat procura inițială, în cazul revocării procurii înregistrate anterior;
  - f) numărul și data declarației de revocare a procurii din Registrul actelor notariale, în cazul revocării procurii înregistrate anterior;
  - g) altă informație conform legislației în vigoare.

26. Furnizorii datelor registrului sunt persoanele fizice și juridice care solicită autentificarea sau anularea procurilor.

27. Persoanele fizice și juridice, vor furniza următoarele date:

- 1) Date despre persoana fizică:
  - a) numele și prenumele;
  - b) numărul de identificare (IDNP);
  - c) data nașterii;
  - d) numărul și seria actului de identitate;
  - e) adresa de domiciliu și electronică;
- 2) Date despre persoana juridică:



- d) denumirea;
  - e) numărul de identificare (IDNO);
  - f) sediul și adresa electronică;
- 3) Date despre procură:
- a) scopul procurii;
  - b) numărul procurii;
  - c) data autentificării procurii;
  - d) numele și prenumele notarului care a autentificat procura inițială;
  - e) numărul și data declarației de revocare a procurii din Registrul actelor notariale;
  - f) altă informație conform legislației în vigoare.

## **VI. DOCUMENTELE DE BAZĂ ALE SIA E-PROCURA**

28. Documentele de intrare sunt:
- 1) Cererea privind perfectarea procurii;
  - 2) Cererea privind revocarea procurii.
29. Documentele de ieșire sunt:
- 1) Procura autentificată;
  - 2) Confirmare privind anularea procurii.
30. Documentele tehnologice includ dovada achitării taxei de stat și a plății pentru perfectarea și/sau revocarea procurii autentificate de către notar.

## **VII. SPAȚIUL INFORMAȚIONAL AL SIA E-PROCURA**

31. Totalitatea obiectelor informaționale este determinată de destinația SIA e-Procura și include:
- 1) Persoana fizică, în calitate de reprezentat sau reprezentant;
  - 2) Persoana juridică, în calitate de reprezentat sau reprezentant;
  - 3) Procura:
    - a) Procura autentificată;
    - b) Confirmare privind anularea procurii.
32. Identificator al obiectului informațional ”Procura autentificată” este constituit dintr-un număr de ordine unic și un cod de securitate unic, generate de sistem în momentul înregistrării procurii.
33. Identificator al obiectului informațional ”persoana fizică” este numărul de identificare de stat al persoanei fizice (IDNP).
34. Scenariile de bază reprezintă o listă a evenimentelor aferente obiectului informațional, luate în evidență în SIA e-Procura, după cum urmează:
- 1) Referitor la obiectul informațional ”persoana fizică, în calitate de reprezentat sau reprezentant”:
    - a) înregistrarea primară – în momentul adresării privind desemnarea unei persoane în calitate de reprezentant pentru soluționarea unei anumite probleme;
    - b) scoaterea din evidență – în momentul adresării privind anularea procurii.
  - 2) Referitor la obiectul informațional ”persoana juridică, în calitate de reprezentat sau reprezentant”:
    - a) înregistrarea primară – în momentul adresării privind desemnarea unei persoane în calitate de reprezentant pentru soluționarea unei anumite probleme;
    - b) scoaterea din evidență – în momentul adresării privind anularea procurii.

- 3) Referitor la obiectul informațional „procura”, scenariul de bază este
  - a) înregistrarea primară – în momentul recepționării cererii privind înregistrarea unei procuri
  - b) scoaterea din evidență – în momentul adresării privind anularea procurii în SIA e-Procure.

35. Datele SIA e-Procure reprezintă totalitatea atributelor obiectelor informaționale:

- 1) date despre persoana fizică, în calitate de reprezentat sau reprezentant:
  - a) nume;
  - b) prenume;
  - c) data nașterii;
  - d) numărul de identificare;
  - e) seria și numărul actului de identitate;
  - f) oficiul și data eliberării actului de identitate;
  - g) adresa domiciliului și electronică;
- 2) date despre persoana juridică, în calitate de reprezentat sau reprezentant:
  - g) denumirea;
  - h) numărul de identificare (IDNO);
  - i) sediul și adresa electronică;
- 3) date despre obiectul informațional ”procura”:
  - a) tipul procurii;
  - b) numărul procurii;
  - c) data eliberării procurii;
  - d) numele, prenumele notarului;
  - e) sediul biroului notarului.

36. Informațiile recepționate de la persoana fizică, în calitate de reprezentat sau reprezentant vor fi introduse în sistem de către registratorii SIA e-Procure.

Schema generală a fluxurilor informaționale în cadrul SIA e-Procure este redată în fig.1.

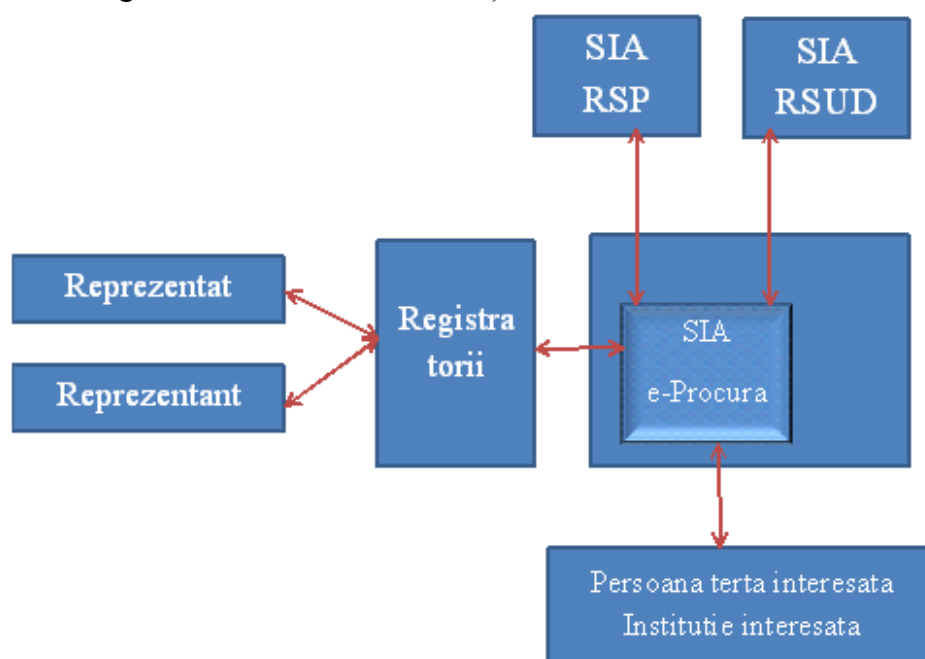


Fig. 1: Schema generală a fluxurilor informaționale în cadrul SIA e-Procure

37. Se va asigura interacțiunea cu:

- a) sistemul informațional de stat SIA "Registrul de stat al populației" pentru verificarea veridicității datelor despre persoana fizică în calitate de reprezentat sau reprezentant,
- b) sistemul informațional de stat SIA "Registrul de stat al unităților de drept" pentru verificarea veridicității datelor despre persoana juridică în calitate de reprezentat sau reprezentant.

Pentru integrarea SIA „e-Procura” cu sistemul informațional de stat, vor fi respectate cerințele Concepției guvernării electronice și anume:

- 1) SOAP-web service (lista metodelor disponibile pentru acțiuni predefinite);
- 2) XML ca mijloc principal pentru integrarea datelor.

38. Interacțiunea cu sistemul informațional al Centrului de telecomunicații speciale va fi utilizată pentru realizarea mecanismelor de semnătură digitală, care oferă posibilitatea verificării identității unui utilizator, stabilește dacă acesta are dreptul să trimită documente, protejează conținutul informației trimise, care nu mai poate fi modificat după ce a fost semnat.

## **VIII. SPAȚIUL TEHNOLOGIC AL SIA E-PROCURA**

39. Spațiul tehnologic al SIA „e-Procura” reprezintă un complex informațional de telecomunicații de un singur nivel, cu sediul în mun. Chișinău. Locurile de muncă automatizate se află la oficiile notarilor.

40. Prezența componentelor produselor software și mijloacelor tehnologice în complexul informațional de telecomunicații este stabilită la etapa elaborării sarcinii tehnice și proiectului tehnic.

41. După necesitate și în corespundere cu procedura stabilită, SIA „e-Procura” poate migra pe platforma tehnologică unică a Guvernului „MCloud”.

## **IX. ASIGURAREA SECURITĂȚII INFORMAȚIEI**

42. Sistemul complex al securității informaționale reprezintă totalitatea măsurilor legislative, organizatorice și economice, precum și a mijloacelor software-hardware, care sînt orientate spre asigurarea unui nivel necesar al integrității, confidențialității și accesibilității resurselor informaționale ale SIA „e-Procura” pentru minimalizarea prejudiciilor care ar putea fi suportate de utilizator și proprietar.

43. Obiectivele principale ale securității sînt:

- 1) asigurarea integrității informației - protecția împotriva modificării și distrugerii datelor;
- 2) asigurarea confidențialității - protecția împotriva accesării neautorizate a datelor;
- 3) asigurarea disponibilității - protecția împotriva blocării accesului utilizatorilor autorizați la resursele informaționale.

44. Cerințele principale ale securității:

- 1) complexitate;
- 2) obiective orientate;
- 3) continuitate;
- 4) fiabilitate, durabilitate;
- 5) gestionare centralizată;
- 6) suficiență rezonabilă.

45. Crearea sistemului complex de securitate informațională include o serie de etape consecutive:

- 1) determinarea profilurilor de securitate;
- 2) clasificarea resurselor protejate;
- 3) analiza riscurilor;
- 4) dezvoltarea politicii de securitate;

- 5) dezvoltarea arhitecturii de securitate;
  - 6) crearea și implementarea sistemului securității informaționale;
  - 7) certificarea sistemului informațional.
46. Componentele de bază ale sistemului securității informaționale sînt:
- 1) protecția informației și a infrastructurii de mentenanță la conectarea la rețelele externe;
  - 2) protecția informației în procesul interacțiunii dintre rețele;
  - 3) protecția fluxurilor de date;
  - 4) protecția serviciilor sistemului informațional;
  - 5) protecția antivirus;
  - 6) asigurarea securității mediului de program;
  - 7) accesul autentificat;
  - 8) protocolarea și auditul.

47. Principalele mecanisme tehnologice de asigurare a protecției și securității informaționale sînt:
- 1) delimitarea accesului utilizatorilor la baza de date în funcție de rolul lor;
  - 2) accesul la date doar prin interfața unică de obiect.

48. În procesul de gestionare a SIA „e-Procura” se va asigura securitatea datelor cu caracter personal, în conformitate cu Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal și conform Politicii de securitate a datelor cu caracter personal în cadrul Centrului de Informații Juridice, aprobate prin Ordinul nr. 13 din 14 mai 2015 al Centrului de Informații Juridice, căruia i se atribuie calitatea de deținător al SIA „e-Procura”.

49. Securitatea informațională se menține pe parcursul întregului ciclu de viață SIA „e-Procura” și se perfecționează continuu pentru prevenirea noilor pericole.