GUVERNUL REPUBLICII MOLDOVA

H O T Ă R Î R E
pentru aprobarea Regulamentului privind modul de ţinere a Registrului de stat al achiziţiilor publice format de Sistemul informaţional automatizat "Registrul de stat al achiziţiilor publice" (MTender)

nr. 986 din 10.10.2018
(în vigoare 12.10.2018)

Monitorul Oficial al R. Moldova nr. 396-397 art. 1042 din 12.10.2018

* * *

În temeiul prevederilor art.16 alin.(3) din Legea nr.71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314), Guvernul

HOTĂRĂŞTE:

1. Se instituie Registrul de stat al achiziţiilor publice format de Sistemul informaţional automatizat "Registrul de stat al achiziţiilor publice" (MTender).

2. Se aprobă Regulamentul privind modul de ţinere a Registrului de stat al achiziţiilor publice format de Sistemul informaţional automatizat "Registrul de stat al achiziţiilor publice" (MTender) (se anexează).

3. Pe tot parcursul textului Hotărîrii Guvernului nr.705/2018 cu privire la aprobarea Conceptului tehnic al Sistemului informaţional automatizat "Registrul de stat al achiziţiilor publice" (MTender), cuvintele "Regulamentul privind funcţionarea Sistemului informaţional automatizat "Registrul de stat al achiziţiilor publice" (MTender)", la orice caz gramatical, se substituie cu cuvintele "Regulamentul privind modul de ţinere a Registrului de stat al achiziţiilor publice format de Sistemul informaţional automatizat "Registrul de stat al achiziţiilor publice" (MTender)", la cazul gramatical corespunzător.

4. Prezenta hotărîre intră în vigoare la data publicării.

PRIM-MINISTRU **Pavel FILIP**

Contrasemnează:
Ministrul finanţelor **Octavian Armaşu**

Nr.986. Chişinău, 10 octombrie 2018.

Aprobat
prin Hotărîrea Guvernului nr.986/2018

REGULAMENT
privind modul de ţinere a Registrului de stat al achiziţiilor publice format de Sistemul informaţional automatizat

“Registrul de stat al achiziţiilor publice”
(MTender)

Capitolul I
DISPOZIŢII GENERALE

Secţiunea 1
Obiectul de reglementare

1. Regulamentul privind modul de ţinere a Registrului de stat al achiziţiilor publice format de Sistemul informaţional automatizat “Registrul de stat al achiziţiilor publice” (MTender) (în continuare – *Regulament*) este elaborat în conformitate cu prevederile Legii nr.71/2007 cu privire la registre, ale Legii nr.131/2015 privind achiziţiile publice şi ale Hotărîrii Guvernului nr.705/2018 cu privire la aprobarea Conceptului tehnic al Sistemului informaţional automatizat “Registrul de stat al achiziţiilor publice” (MTender).

2. Prezentul Regulament stabileşte reguli privind modul de ţinere a Registrului de stat al achiziţiilor publice (în continuare – *Registru*) ca rezultat al funcţionării Sistemului informaţional automatizat “Registrul de stat al achiziţiilor publice” (MTender) (în continuare – *SIA RSAP (MTender)*) în procesul organizării şi desfăşurării procedurilor de achiziţie publică, cerinţele minime faţă de utilizarea mijloacelor de protecţie la introducerea, stocarea, prelucrarea şi accesarea informaţiilor privind procedurile de achiziţie publică şi celei adiacente, precum şi cerinţele minime faţă de echipamentul tehnic, de program şi faţă de utilizatorii SIA RSAP MTender.

3. Deţinător şi operator tehnico-tehnologic al unităţii centrale de date este Instituţia publică “Centrul de Tehnologii Informaţionale în Finanţe”, în conformitate cu Hotărîrea Guvernului nr.705/2018 cu privire la aprobarea Conceptului tehnic al Sistemului informaţional automatizat “Registrul de stat al achiziţiilor publice” (MTender).

4. Deţinător al platformei electronice de achiziţii (în continuare – *PEA*), în conformitate cu legislaţia Republicii Moldova, poate fi persoana juridică care:

1) acceptă principiile SIA RSAP (MTender) şi condiţiile de participare la implementarea SIA RSAP (MTender);

2) întruneşte cerinţele tehnice, funcţionale şi juridice pentru PEA;

3) a susţinut cu succes procesul de acreditare în conformitate cu prevederile Regulamentului privind acreditarea platformelor electronice de achiziţii în cadrul Sistemului informaţional automatizat “Registrul de stat al achiziţiilor publice” (MTender), aprobat prin Hotărîrea Guvernului nr.985/2018.

Secţiunea a 2-a
Noţiuni

5. În sensul prezentului Regulament se aplică următoarele noţiuni:

autentificare – proces de identificare a utilizatorului în cadrul sistemului informaţional prin intermediul certificatului cheii publice sau altor instrumente;

autorizare – proces al sistemului informaţional care determină nivelul de acces atribuit unui utilizator autentificat pentru a accesa resurse securizate controlate de sistem;

cheie de testare – identificator al platformei electronice pentru punerea în aplicare şi testarea funcţionalităţilor pînă la obţinerea acreditării pentru conectarea şi efectuarea schimbului de date în cadrul SIA RSAP (MTender);

cheie de producţie – identificator al platformei electronice acreditate pentru conectarea şi efectuarea schimbului de date în cadrul sistemului de achiziţii electronice în regim de producţie, în conformitate cu nivelul de acreditare primit;

complex de mijloace software şi hardware – totalitatea programelor şi mijloacelor tehnice care asigură realizarea proceselor informaţionale;

operator al PEA **–** persoană juridică, înregistrată în conformitate cu legislaţia Republicii Moldova, deţinător al unei PEA, care are dreptul de a desfăşura/presta serviciile caracteristice unei PEA;

operator SIA RSAP (MTender) – persoană juridică, stabilită prin hotărîre de Guvern, responsabilă de funcţionarea şi administrarea SIA RSAP (MTender);

protecţia informaţiei contra accesului neautorizat – ansamblu de măsuri orientate spre prevenirea, identificarea şi înlăturarea sustragerii informaţiei protejate prin încălcarea regulilor de acces stabilite de actele normative sau de proprietarul (deţinătorul) informaţiei;

rol – set de atribuţii şi sarcini specifice care îi revin utilizatorului în cadrul sistemului informaţional după înregistrarea acestuia;

securitate informaţională – protecţia sistemului informaţional de acţiuni premeditate sau neintenţionate cu caracter natural sau artificial, care au ca rezultat cauzarea prejudiciului participanţilor la schimbul informaţional;

utilizator – persoană sau grup de persoane care foloseşte informaţia din SIA RSAP (MTender) sau interacţionează direct cu acesta.

Capitolul II
SUBIECŢII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII ŞI FUNCŢIONĂRII REGISTRULUI. DREPTURILE ŞI OBLIGAŢIILE LOR

6. Funcţiile subiecţilor raporturilor juridice în cadrul Registrului rezultă din prevederile Legii nr.71/2007 cu privire la registre, ale Legii nr.131/2015 privind achiziţiile publice şi altor acte normative şi sînt următoarele:

1) statul – proprietarul Registrului, care îşi realizează dreptul de proprietate, de gestionare şi utilizare a datelor din Registru;

2) Ministerul Finanţelor – posesorul Registrului, care:

a) asigură condiţiile juridice, organizatorice şi financiare pentru crearea şi ţinerea Registrului;

b) asigură ţinerea Registrului în conformitate cu regulile de ţinere a registrelor;

c) asigură mecanismul de înregistrare a obiectelor supuse înregistrării;

d) asigură autenticitatea, plenitudinea şi integritatea datelor din Registru;

e) asigură securitatea şi protecţia datelor din Registru;

f) asigură accesul la datele din Registru în conformitate cu legislaţia şi regulile de ţinere a registrelor;

g) deleagă funcţii privind ţinerea Registrului deţinătorului şi/sau registratorilor Registrului prin SIA RSAP (MTender);

h) asigură crearea SIA RSAP (MTender) şi dispunerea de codul sursă pentru asigurarea funcţionalităţii SIA RSAP (MTender).

3) Instituţia publică “Centrul de Tehnologii Informaţionale în Finanţe” – deţinătorul Registrului, care îndeplineşte atribuţiile de ţinere a Registrului şi, ca rezultat, a SIA RSAP (MTender) transmise de către posesorul Registrului, şi anume:

a) asigură buna funcţionare a Registrului;

b) asigură ţinerea Registrului în conformitate cu prevederile prezentului Regulament;

c) înregistrează obiectele supuse înregistrării;

d) asigură autenticitatea, plenitudinea şi integritatea datelor în Registru;

e) asigură securitatea şi protecţia datelor din Registru;

f) asigură accesul tuturor destinatarilor la datele din Registru în conformitate cu prezentul Regulament;

4) operatorii PEA – deţinători ai PEA, care îndeplinesc atribuţiile de registratori ai Registrului, transmise de către posesorul Registrului ca rezultat al procedurii de acreditare a PEA deţinute. Registratorii Registrului vor asigura:

a) buna funcţionare a PEA;

b) autenticitatea, plenitudinea şi integritatea datelor transmise;

c) securitatea şi protecţia datelor colectate şi transmise;

d) accesul tuturor destinatarilor la datele din Registru în conformitate cu prezentul Regulament;

e) fluxuri de lucru pentru organizarea procedurilor de achiziţie publică de către autorităţile contractante, entităţile contractante;

f) fluxuri de lucru pentru participarea operatorilor economici la procedura de achiziţie publică;

g) colectarea şi transmiterea către unitatea centrală de date a datelor aferente procesului de organizare şi desfăşurare a procedurilor de achiziţii;

h) sincronizarea datelor între SIA RSAP (MTender) şi PEA;

i) acordarea asistenţei de ordin tehnic autorităţilor contractante şi operatorilor economici în procesul de utilizare a funcţionalităţilor SIA RSAP (MTender) la organizarea procedurilor de achiziţie publică;

5) Agenţia Achiziţii Publice – furnizor şi destinatar al datelor Registrului prin SIA RSAP (MTender), care:

a) coordonează, monitorizează şi evaluează, prin intermediul funcţionalităţilor oferite de sistem, modul în care autorităţile contractante respectă procedurile de achiziţie publică şi de atribuire a contractelor de achiziţii publice;

b) întocmeşte, actualizează şi menţine, prin intermediul funcţionalităţilor oferite de SIA RSAP (MTender), Lista de interdicţie a operatorilor economici;

c) examinează dările de seamă privind procedurile de achiziţie publică;

d) generează şi analizează rapoarte privind procedurile de achiziţie publică;

e) gestionează Buletinul achiziţiilor publice în cadrul SIA RSAP (MTender);

6) Agenţia Naţională pentru Soluţionarea Contestaţiilor – furnizor şi destinatar al datelor Registrului prin SIA RSAP (MTender), care:

a) recepţionează şi înregistrează contestaţiile depuse de participanţii la procedurile de achiziţie publică;

b) înregistrează rezultatele examinării contestaţiilor depuse de participanţii la procedurile de achiziţie publică;

c) intervine în procesele legate de desfăşurarea procedurilor de achiziţie publică, inclusiv prin suspendarea procedurii de achiziţii publice şi anularea procedurii de achiziţii publice;

7) autoritatea contractantă – furnizor şi destinatar al datelor Registrului prin SIA RSAP (MTender), care:

a) elaborează planuri anuale şi trimestriale de efectuare a procedurilor de achiziţii publice;

b) creează grupuri de lucru responsabile de realizarea achiziţiilor publice în cadrul autorităţii contractante;

c) întocmeşte şi publică invitaţiile/anunţurile de participare în cadrul procedurilor de achiziţii publice;

d) elaborează şi publică în cadrul Registrului, prin SIA RSAP (MTender), documentaţia de atribuire şi alte documente aplicabile în cadrul procedurilor de achiziţii publice;

e) iniţiază proceduri de achiziţii publice;

f) examinează, evaluează şi compară ofertele depuse în cadrul procedurilor de achiziţii publice;

g) execută deciziile Agenţiei Naţionale pentru Soluţionarea Contestaţiilor;

h) semnează contractele de achiziţii publice, iar ulterior le transmite spre semnare participanţilor desemnaţi cîştigători;

i) întocmeşte dări de seamă privind rezultatul procedurilor de achiziţii publice şi le publică în SIA RSAP (MTender);

j) transmite contractele semnate către trezorerie pentru înregistrare;

k) menţine corespondenţa electronică cu operatorii economici interesaţi şi participanţii la procedura de achiziţii publice;

l) publică răspunsul la clarificările recepţionate;

m) monitorizează executarea contractului de achiziţii publice;

n) iniţiază, semnează şi transmite spre înregistrare acordurile adiţionale la contractele de achiziţii publice;

8) entitatea contractantă – furnizor şi destinatar al datelor Registrului prin SIA RSAP (MTender), care:

a) elaborează, opţional, planuri anuale şi trimestriale de efectuare a procedurilor de achiziţii;

b) creează grupuri de lucru responsabile de realizarea achiziţiilor în cadrul entităţii;

c) întocmeşte şi publică invitaţiile de participare în cadrul procedurilor de achiziţii;

d) elaborează şi publică în cadrul Registrului, prin SIA RSAP (MTender), documentaţia de atribuire şi alte documente aplicabile în cadrul procedurilor de achiziţii;

e) iniţiază procedurile de achiziţii;

f) examinează, evaluează şi compară ofertele depuse în cadrul procedurilor de achiziţii;

g) semnează contractele de achiziţii, iar ulterior le transmite spre semnare participanţilor desemnaţi cîştigători;

h) menţine corespondenţa electronică cu operatorii economici interesaţi şi participanţii la procedura de achiziţii;

i) publică răspunsul la clarificările recepţionate;

j) monitorizează, opţional, executarea contractului de achiziţii;

k) iniţiază şi semnează acorduri adiţionale la contractele de achiziţii încheiate anterior în cadrul SIA RSAP (MTender);

9) posesorii registrelor şi sistemelor informaţionale de stat – furnizori de date în cadrul Registrului prin SIA RSAP MTender, care oferă informaţii privind:

a) operatorii economici, autorităţile contractante etc. (în baza IDNO);

b) persoanele fizice (în baza IDNP);

c) efectuarea regulată a plăţii impozitelor, contribuţiilor (conform datelor Serviciului Fiscal de Stat);

d) existenţa licenţelor şi altor documente permisive în raport cu participantul la procedura de achiziţii publice;

e) existenţa resurselor financiare şi plăţilor efectuate în cadrul contractului de achiziţie publică;

f) facturile fiscale eliberate în procesul de executare a contractului de achiziţie publică;

g) existenţa/lipsa antecedentelor penale în raport cu participantul la procedura de achiziţie publică;

10) posesorii serviciilor electronice guvernamentale – intermediari de furnizare a datelor în cadrul Registrului prin SIA RSAP (MTender), care:

a) asigură, prin SIA RSAP (MTender), schimbul de date între Registru şi registrele şi sistemele informaţionale de stat;

b) asigură realizarea proceselor interne în cadrul SIA RSAP (MTender), cum ar fi: autentificarea utilizatorilor, semnarea electronică a documentelor, notificarea, înregistrarea evenimentelor etc.;

11) posesorul portalului guvernamental pentru date deschise – destinatar al datelor Registrului prin SIA RSAP (MTender), care asigură publicarea seturilor de date deschise în vederea facilitării accesului cetăţenilor la datele privind procedurile de achiziţii;

12) posesorii sistemelor externe (TED) – destinatari ai datelor Registrului prin SIA RSAP (MTender), care asigură publicarea anunţului de participare şi a notificărilor în cadrul Jurnalului Oficial al Uniunii Europene;

13) administraţia publică – destinatar al datelor Registrului prin SIA RSAP (MTender), care:

a) monitorizează procedurile de achiziţii;

b) vizualizează rapoartele statistice;

c) preia experienţa de desfăşurare a procedurilor de achiziţii;

14) publicul larg – destinatar al datelor Registrului prin SIA RSAP (MTender), care:

a) monitorizează procedurile de achiziţii;

b) vizualizează rapoartele statistice;

c) obţine seturile de date pentru analiza avansată a datelor privind procedurile de achiziţii.

7. Posesorul Registrului este obligat să asigure condiţiile de drept, organizaţionale şi financiare pentru crearea şi funcţionarea Registrului şi a SIA RSAP (MTender). Obligaţiile posesorului Registrului sînt determinate de art.11 din Legea nr.71/2007 cu privire la registre.

8. Deţinătorul Registrului este obligat:

1) să asigure funcţionarea Registrului şi a SIA RSAP (MTender) în corespundere cu baza normativă actuală şi acordul încheiat cu posesorul;

2) să asigure posibilitatea de conectare a participanţilor autorizaţi la Registru;

3) să asigure crearea înscrierilor de evidenţă (conturilor) pentru utilizatorii SIA RSAP (MTender), cu atribuirea/modificarea rolurilor şi drepturilor de acces la interfaţă şi date;

4) să asigure veridicitatea, siguranţa şi integritatea datelor din Registru prin SIA RSAP (MTender);

5) să efectueze monitorizarea şi controlul asupra accesării datelor din Registru prin SIA RSAP (MTender);

6) să asigure suportul metodologic prin elaborarea procedurilor, regulilor şi instrucţiunilor de utilizare a funcţionalităţilor SIA RSAP (MTender), precum şi accesarea şi introducerea datelor;

7) să asigure securitatea Registrului prin SIA RSAP (MTender) şi să aplice măsuri de monitorizare a respectării condiţiilor de securitate şi regulilor de exploatare a Registrului prin SIA RSAP (MTender) prin fixarea cazurilor şi tentativelor de încălcare a măsurilor, precum şi să întreprindă măsurile corespunzătoare pentru prevenirea şi eliminarea consecinţelor lor;

8) să asigure securitatea accesului la informaţia din Registru prin SIA RSAP (MTender) şi să aplice măsuri de monitorizare privind respectarea securităţii accesului la datele sistemului, prin fixarea cazurilor şi tentativelor de încălcare a măsurilor prevăzute, precum şi să întreprindă măsurile corespunzătoare pentru prevenirea şi eliminarea consecinţelor lor;

9) să asigure, să organizeze şi să amenajeze locurile de muncă corespunzătoare pentru persoanele responsabile de deservirea Registrului prin SIA RSAP (MTender);

10) să asigure condiţiile necesare pentru păstrarea securizată a purtătorilor de informaţie şi a copiilor de rezervă, precum şi pentru excluderea accesului persoanelor neautorizate la purtătorii corespunzători de informaţie;

11) să acorde suportul necesar persoanelor autorizate în utilizarea complexului de mijloace software a SIA RSAP (MTender);

12) să informeze participanţii Registrului prin SIA RSAP (MTender) despre schimbările condiţiilor tehnice de funcţionare a acestuia;

13) să asigure protecţia împotriva viruşilor şi spamului;

14) să asigure implementarea măsurilor organizaţionale şi tehnice necesare pentru păstrarea regimului de confidenţialitate şi securitate a datelor personale în corespundere cu legislaţia privind protecţia datelor cu caracter personal;

15) să asigure accesul securizat la informaţia din Registru prin SIA RSAP (MTender), respectarea condiţiilor de securitate şi a regulilor de exploatare;

16) să utilizeze informaţia obţinută în cadrul Registrului prin SIA RSAP (MTender) numai în scopurile stabilite de legislaţie şi acordul cu posesorul sistemului;

17) să asigure confidenţialitatea conţinutului ofertelor pînă la data stabilită pentru deschiderea acestora.

9. Registratorul Registrului prin SIA RSAP (MTender) este obligat:

1) să ofere furnizorilor şi destinatarilor datelor sistemului interfeţe comode şi mecanisme automatizate de înregistrare/ extragere/ vizualizare a informaţiei;

2) să asigure înregistrarea informaţiei în Registru prin SIA RSAP (MTender) în corespundere cu formatul şi regulile stabilite, indicate în instrucţiunile corespunzătoare;

3) să verifice respectarea condiţiilor de înregistrare, evidenţă şi utilizare a datelor cu caracter personal;

4) să asigure corectitudinea, veridicitatea şi autenticitatea datelor din Registru prin SIA RSAP (MTender);

5) să utilizeze informaţia obţinută în cadrul SIA RSAP (MTender) numai în scopurile stabilite de legislaţie, respectînd acordurile semnate şi documentaţia aferentă;

6) să acorde suportul necesar furnizorilor şi destinatarilor de informaţie în utilizarea complexului de mijloace software a SIA RSAP (MTender).

10. Furnizorii şi destinatarii datelor sînt obligaţi:

1) să furnizeze în cadrul Registrului prin SIA RSAP (MTender) doar informaţie corectă şi veridică, în corespundere cu formatul şi regulile stabilite;

2) să utilizeze informaţia obţinută din Registrul prin SIA RSAP (MTender) numai în scopurile stabilite de legislaţia în vigoare şi în conformitate cu atribuţiile ce le revin;

3) să utilizeze funcţionalităţile Registrului prin SIA RSAP (MTender) în exclusivitate conform destinaţiei acestora şi conform atribuţiilor ce le revin, în strictă conformitate cu legislaţia;

4) să asigure protejarea contra compromiterii şi contra utilizării neautorizate a mijloacelor de autentificare şi a credenţialelor utilizate pentru autentificarea în cadrul Registrului prin SIA RSAP (MTender);

5) să anunţe imediat, prin oricare mijloc de comunicare, deţinătorul Registrului despre cazurile de încălcare a securităţii informaţionale a Registrului prin SIA RSAP (MTender);

6) să anunţe imediat deţinătorul Registrului despre apariţia situaţiilor de forţă majoră, care pot compromite îndeplinirea atribuţiilor ce le revin.

11. Posesorul Registrului poate delega o serie de funcţii privind ţinerea Registrului deţinătorului şi/sau registratorului Registrului.

12. Deţinătorul SIA RSAP (MTender) are dreptul:

1) să elaboreze şi să înainteze propuneri de modificare a cadrului normativ privind Registrul;

2) să propună şi să implementeze, cu acordul posesorului, soluţii pentru îmbunătăţirea şi sporirea eficacităţii procesului de funcţionare a Registrului prin SIA RSAP (MTender);

3) să monitorizeze respectarea de către participanţii SIA RSAP (MTender) a cerinţelor de securitate informaţională, să înregistreze cazurile şi încercările de încălcare a acestora;

4) să iniţieze procedura de suspendare a drepturilor de acces la Registru pentru participanţii care nu respectă regulile stabilite, standardele şi normele din domeniul securităţii informaţionale;

5) să verifice autenticitatea şi veridicitatea datelor introduse de participanţii SIA RSAP (MTender);

6) să solicite de la participanţi, în cazul detectării erorilor şi omisiunilor, actualizarea şi corectarea informaţiei din Registru prin SIA RSAP (MTender);

7) să solicite de la participanţi informaţia necesară pentru completarea datelor în SIA RSAP (MTender);

8) să refuze furnizarea informaţiei din Registru prin SIA RSAP (MTender) în cazurile prevăzute de legislaţie;

9) să exercite alte drepturi delegate de către posesorul Registrului.

13. Registratorul Registrului are dreptul:

1) să propună şi să implementeze modificări ale cadrului legal de funcţionare a Registrului;

2) să propună soluţii pentru îmbunătăţirea şi sporirea eficacităţii procesului de funcţionare a Registrului şi a comodităţii de introducere a datelor;

3) să solicite de la furnizorii de informaţie informaţia necesară pentru completarea datelor în Registru prin SIA RSAP (MTender);

4) să solicite de la furnizorii de informaţie, în cazul detectării erorilor şi omisiunilor, actualizarea şi corectarea datelor furnizate;

5) să exercite alte drepturi delegate de către posesorul Registrului prin SIA RSAP (MTender).

14. Furnizorii şi destinatarii datelor au dreptul:

1) să primească informaţie veridică şi actuală în cadrul Registrului prin SIA RSAP (MTender);

2) să solicite şi să acceseze informaţia în cadrul Registrului prin SIA RSAP (MTender) în conformitate cu atribuţiile acestora;

3) să acceseze funcţionalităţile Registrului prin SIA RSAP (MTender) în conformitate cu atribuţiile acestora;

4) să înainteze propuneri de îmbunătăţire a mecanismului de introducere/ extragere/ vizualizare a datelor în cadrul Registrului.

15. Fiecare participant al Registrului prin SIA RSAP (MTender) are dreptul:

1) să participe la implementarea şi dezvoltarea Registrului prin SIA RSAP (MTender);

2) să înainteze posesorului şi deţinătorului propuneri privind modificarea actelor normative care reglementează funcţionarea Registrului prin SIA RSAP (MTender);

3) să solicite şi să primească de la deţinător susţinere metodologică şi practică de funcţionare a Registrului prin SIA RSAP (MTender);

4) să înainteze deţinătorului propuneri privind îmbunătăţirea şi sporirea eficacităţii funcţionării Registrului prin SIA RSAP (MTender).

Capitolul III
GESTIONAREA ŞI ASIGURAREA FUNCŢIONĂRII REGISTRULUI

Secţiunea 1
Modul de ţinere a SIA RSAP (MTender) (Registrului)

16. Registrul se ţine în format electronic prin SIA RSAP (MTender).

17. În procesul de exploatare a Registrului prin SIA RSAP (MTender) se formează resursa unică informaţională de stat – Registrul, care reprezintă o totalitate de informaţie sistematizată, ce cuprinde obiectele informaţionale de bază aferente procesului de achiziţii, şi anume:

1) autoritatea contractantă/entitatea contractantă;

2) operatorul economic;

3) linia de plan;

4) procedura de achiziţie;

5) documentul;

6) criteriul;

7) cerinţa;

8) lotul;
9) poziţia;
10) întrebarea;
11) explicaţia;
12) clarificarea;
13) actul organizatoric;
14) contestaţia;
15) oferta;
16) adjudecarea;
17) contractul;
18) amendamentul;
19) tranzacţia;
20) livrabilul.

18. Scenariile de bază în procesul de formare a Registrului vor corespunde Conceptului tehnic al Sistemului informaţional automatizat "Registrul de stat al achiziţiilor publice" (MTender).

19. Deţinătorul Registrului efectuează administrarea acestuia cu ajutorul complexului de mijloace software şi hardware, în corespundere cu prezentul Regulament.

20. Registrul se ţine în limba de stat, iar produsul de program elaborat se traduce în limbile rusă şi engleză.

21. Accesul la Registru şi schimbul informaţional se realizează prin intermediul reţelei globale Internet, iar comunicarea PEA cu SIA RSAP (MTender) se realizează utilizînd canalele de schimb de date securizate.

22. Accesul la obiectele informaţionale ale Registrului şi funcţiile acestuia se realizează prin nivelurile de acces public şi autorizat.

23. Registrul prin SIA RSAP (MTender) funcţionează zilnic, 24/24, cu excepţia timpului rezervat pentru lucrări de mentenanţă, care sînt programate, cu unele excepţii, în afara orelor de lucru sau în zilele de odihnă ori sărbătoare.

Secţiunea a 2-a
Utilizatorii Registrului prin SIA RSAP (MTender)

24. Utilizatorii Registrului, în conformitate cu principalii participanţi la procesul de achiziţii, se împart în următoarele categorii:

1) utilizatori publici – categorie de utilizatori care nu a trecut procedura de autentificare în Registru prin SIA RSAP (MTender). Această categorie de utilizatori are posibilitatea de a vizualiza obiectele informaţionale, inclusiv Buletinul achiziţiilor publice, fără a le putea modifica;

2) utilizatori ai autorităţii contractante/entităţii contractante – categorie de utilizatori care are acces la funcţionalităţile destinate planificării şi organizării procedurii de achiziţii precum: specificarea planurilor de achiziţii, anunţarea şi desfăşurarea procedurilor de achiziţii, realizarea proceselor de evaluare a ofertelor, selectarea şi desemnarea cîştigătorului, încheierea contractului, gestionarea şi monitorizarea contractului, finalizarea procedurii de achiziţii, generarea documentelor organizatorice, administrarea cataloagelor electronice etc.;

3) utilizatori ai operatorilor economici – categorie de utilizatori care are acces la funcţionalităţile destinate participării la procedurile de achiziţie precum: înaintarea

întrebărilor/clarificărilor, formarea şi depunerea ofertelor, depunerea contestaţiilor, participarea la licitaţia electronică, vizualizarea şi semnarea contractului;

4) utilizatori ai Agenţiei Achiziţii Publice – categorie de utilizatori care are acces la funcţionalităţi specifice precum gestionarea anunţurilor de intenţie, anunţurilor de participare, anunţurilor de modificare a procedurilor de achiziţii publice în vederea editării Buletinului de achiziţii publice, administrarea listelor agenţilor economici interzişi, generarea rapoartelor statistice specifice, conlucrarea în procesul de soluţionare a contestaţiilor etc.;

5) utilizatori ai Agenţiei Naţionale pentru Soluţionarea Contestaţiilor – categorie de utilizatori care are acces la funcţionalităţile specifice destinate lucrului cu contestaţiile depuse de participanţii la procedurile de achiziţii publice precum: înregistrarea, examinarea, soluţionarea contestaţiilor şi accesarea informaţiei statistice privind contestaţiile;

6) utilizatori ai instituţiilor de monitorizare şi control – categorie de utilizatori care are acces la funcţionalităţile specifice destinate generării rapoartelor statistice avansate privind procedurile de achiziţii publice, precum şi alte instrumente de monitorizare şi control, cum ar fi indicatorii-cheie, indicatorii de risc etc.;

7) utilizatori ai organelor pentru achiziţii centralizate – categorie de utilizatori care are acces la funcţionalităţile specifice destinate planificării, organizării şi desfăşurării achiziţiilor centralizate;

8) administrator de sistem – categorie de utilizatori autentificaţi, angajaţi ai deţinătorului, responsabili de administrarea SIA RSAP (MTender). Această categorie de utilizatori deţine acces avansat la funcţionalităţile sistemului, administrează clasificatoarele sistemului, dispune de instrumente de configurare şi ajustare a sistemului şi funcţionalităţilor acestuia, administrează bazele de date şi monitorizează activitatea utilizatorilor şi a sistemului în general.

25. Fiecare categorie de utilizatori deţine un rol de supervizor, care oferă posibilitate de a administra (acordare de roluri, anulare de roluri) tuturor utilizatorilor din această categorie, exclusiv în cadrul unei organizaţii.

26. Un utilizator în cadrul sistemului poate reprezenta mai multe organizaţii. În acest scop, la autentificare utilizatorul va specifica organizaţia în numele căreia va lucra în sesiunea curentă.

27. Utilizatorul nu poate activa concomitent pentru mai multe organizaţii.

Secţiunea a 3-a
Înregistrarea utilizatorilor

28. Procesul de înregistrare a utilizatorilor se efectuează conform regulilor stabilite de deţinător, în corespundere cu condiţiile pct.43 din Hotărîrea Guvernului nr.1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

29. Înregistrarea utilizatorului supervizor al organizaţiei se efectuează de către administratorul de sistem, la cererea semnată de către conducătorul sau persoana autorizată a organizaţiei solicitante.

30. Cererea de solicitare va conţine cel puţin următoarele informaţii:

1) data emiterii documentului;

2) denumirea organizaţiei;

3) codul unic de identificare al organizaţiei;

4) numele, prenumele conducătorului organizaţiei;

5) datele de contact ale organizaţiei (adresa, telefon, e-mail, persoane de contact);

6) solicitarea privind alocarea rolului în cadrul sistemului;

7) numele, prenumele utilizatorului;

8) funcţia în cadrul organizaţiei;

9) codul unic de identificare al utilizatorului;

10) acordul tuturor persoanelor menţionate în cerere privind acceptul de prelucrare a datelor cu caracter personal;

11) semnătura conducătorului organizaţiei şi ştampila umedă, dacă e cazul.

31. Utilizatorul poartă răspundere pentru acţiunile sale şi ale altor persoane care au acţionat în cadrul sistemului folosind datele personale de identificare ale utilizatorului în cadrul sistemului.

32. Utilizatorul poartă răspundere pentru conţinutul informaţiilor publicate în sistem. PEA are dreptul de a efectua controlul informaţiei plasate de către utilizator şi a-l informa pe acesta, precum şi alte organe (posesorul, operatorul SIA RSAP (MTender) ş.a.) despre conţinutul necorespunzător al informaţiei.

33. În cazul plasării în sistem a unei informaţii care aduce atingere onoarei, demnităţii, reputaţiei profesionale sau care încalcă dreptul la respectul vieţii private şi de familie, la secretul comercial, la proprietatea intelectuală, sau care nu este conformă regulilor stabilite în acest sens, posesorul SIA RSAP (MTender) ori organul împuternicit de acesta poate lua decizia de a acorda permisiune operatorului PEA de a refuza publicarea sau retragerea din publicare a acestor informaţii.

34. Înregistrarea/confirmarea utilizatorilor subordonaţi supervizorului se efectuează de către administratorul de sistem la cererea conducătorului organizaţiei sau de către utilizatorul supervizor al organizaţiei respective. Înregistrarea utilizatorului supervizor al organizaţiei se efectuează de către deţinătorul SIA RSAP (MTender), nemijlocit sau prin intermediul PEA, la cererea semnată de către conducătorul sau persoana autorizată a organizaţiei solicitante.

35. La înregistrarea în cadrul sistemului, fiecărui utilizator i se atribuie un identificator unic şi rolul de care depinde dreptul de acces la obiectele informaţionale, iar dacă este cazul – credenţialele temporare, care urmează a fi modificate la prima accesare a sistemului de către utilizator.

36. Dreptul de acces al utilizatorilor la sistem se revocă în următoarele cazuri:

1) în baza cererii/solicitării conducătorului organizaţiei;

2) la încetarea raporturilor de muncă ale utilizatorilor;

3) la modificarea raporturilor de muncă, cînd noile responsabilităţi nu presupun accesul la datele sistemului;

4) la încălcarea obligaţiilor contractuale de utilizare a sistemului;

5) la constatarea încălcării securităţii informaţionale de către utilizatorul sistemului.

Secţiunea a 4-a
Autentificarea şi autorizarea utilizatorilor în cadrul sistemului

37. Autorizarea utilizatorilor se produce în conformitate cu nivelul de acces stabilit şi utilizatorii au posibilitate să acceseze funcţionalităţile sau informaţiile disponibile potrivit nivelului de acces (spre exemplu, utilizatorul care se autorizează în Registru prin SIA

RSAP (MTender) în calitate de operator economic nu are posibilitate să acceseze funcţionalităţile pentru organizarea procedurii de achiziţie).

38. Procesul de autentificare şi autorizare se realizează pe două căi:

1) autentificarea şi autorizarea prin intermediul PEA: PEA asigură autentificarea electronică a utilizatorilor autorităţilor contractante, entităţilor contractante şi operatorilor economici;

2) autentificarea şi autorizarea prin intermediul portalului web mtender.gov.md. În vederea accesării cabinetelor amplasate pe unitatea centrală de date, portalul web mtender.gov.md asigură autentificarea directă a utilizatorilor specifici ai Agenţiei Achiziţii Publice, Agenţiei Naţionale pentru Soluţionarea Contestaţiilor, organelor de supraveghere şi control, centrelor pentru achiziţii centralizate şi a administratorilor SIA RSAP (MTender).

39. La baza mecanismului de autentificare în cadrul SIA RSAP (MTender) se află serviciul guvernamental de autentificare şi control al accesului MPass.

40. În cadrul PEA, pe lîngă autentificarea prin serviciul guvernamental de autentificare şi control al accesului MPass, se asigură minimum un mecanism adiţional de autentificare accesibil pentru utilizatorii nerezidenţi.

41. Procedura de acordare a accesului (conectare) a PEA la unitatea centrală de date se realizează în conformitate cu Regulamentul privind acreditarea platformelor electronice de achiziţii în cadrul Sistemului informaţional automatizat “Registrul de stat al achiziţiilor publice” (MTender), aprobat prin Hotărîrea Guvernului nr.985/2018.

Capitolul IV
INTERACŢIUNEA CU ALTE SISTEME INFORMAŢIONALE

42. Datele din cadrul Registrului se actualizează operativ şi se sincronizează automat cu datele furnizorilor de informaţii.

43. În vederea asigurării formării corecte a resursei informaţionale şi a calităţii datelor, precum şi pentru sporirea eficienţei proceselor de organizare şi desfăşurare a achiziţiilor, se asigură interacţiunea şi schimbul de date cu următoarele resurse informaţionale:

1) Registrul de stat al populaţiei – pentru verificarea informaţiei privind persoana fizică la înregistrarea utilizatorului în cadrul sistemului;

2) Registrul de stat al unităţilor de drept – pentru verificarea informaţiei privind persoana juridică la înregistrarea utilizatorului în cadrul sistemului, precum şi la diferite etape de desfăşurare a procedurii de achiziţie, ţinerea listelor operatorilor economici calificaţi/interzişi, perfectarea contractului de achiziţie etc.;

3) sistemele informaţionale ale Serviciului Fiscal de Stat – pentru verificarea obligaţiilor fiscale ale ofertantului în procesul desfăşurării procedurii de achiziţii publice;

4) Sistemul informaţional trezorerial – pentru schimbul de informaţie privind disponibilitatea alocaţiilor bugetare, datele contractului de achiziţie şi datele referitoare la executarea contractului şi plăţile efectuate;

5) Sistemul informaţional automatizat de gestionare şi eliberare a actelor permisive – pentru verificarea informaţiei privind licenţele şi alte acte permisive solicitate de către autoritatea contractantă/entitatea contractantă în cadrul procedurii de achiziţie;

6) Registrul informaţiei criminalistice şi criminologice – pentru consultarea informaţiei criminalistice a unei persoane fizice sau juridice.

44. Accesul la resursele şi sistemele informaţionale de stat va fi oferit în baza unor acorduri suplimentare cu deţinătorii de registre şi va fi coordonat, în cazul accesului la date cu caracter personal, cu Centrul Naţional pentru Protecţia Datelor cu Caracter Personal.

45. SIA RSAP (MTender) va utiliza următoarele servicii electronice guvernamentale:

1) eFactura – pentru recepţionarea datelor privind facturile electronice emise în cadrul contractelor de achiziţie;

2) MPass – pentru autentificarea şi controlul accesului în cadrul sistemului, utilizînd diferite mecanisme de autentificare, precum: semnătura mobilă, semnătura electronică, buletinul de identitate electronic, numele de utilizator şi parola;

3) MSign – pentru semnarea documentelor electronice; utilizat în special la depunerea ofertelor şi semnarea online a contractelor de achiziţie;

4) MNotify – pentru transmiterea notificărilor în cadrul sistemului, în special pentru expedierea notificărilor către operatorii economici şi autorităţile/entităţile contractante, precum şi alţi utilizatori ai sistemului;

5) MConnect – platforma guvernamentală de schimb de date şi interoperabilitate utilizată pentru organizarea conexiunii cu registrele şi sistemele informaţionale de stat;

6) MCloud – infrastructură informaţională guvernamentală comună, care funcţionează în baza tehnologiei de “cloud computing”, utilizată pentru găzduirea sistemului;

7) MLog – instrument securizat şi flexibil de jurnalizare şi audit, utilizat pentru asigurarea evidenţei operaţiunilor (evenimentelor) produse în SIA RSAP (MTender);

8) MPay – pentru efectuarea plăţilor electronice ale ofertanţilor de aderare la PEA.

Capitolul V
CERINŢE PRIVIND INFORMAŢIA PLASATĂ ÎN REGISTRU

46. Informaţia prezentată în cadrul Registrului prin SIA RSAP (MTender) are caracter oficial şi este rezultatul deciziei instituţiei pe care o reprezintă utilizatorul care a plasat informaţia respectivă.

47. Accesul la informaţia din cadrul SIA RSAP (MTender) va fi asigurat în măsura prevăzută de Legea nr.131/2015 privind achiziţiile publice şi actele legislative secundare care reglementează desfăşurarea procedurilor de achiziţie publică, precum şi de prezentul Regulament.

48. Accesarea şi utilizarea datelor şi a funcţionalităţilor Registrului este gratuită pentru utilizatorii autorităţii contractante.

49. Autoritatea contractantă, participanţii la procedura de achiziţie, precum şi alte instituţii-utilizatori ai sistemului poartă răspundere pentru actualitatea şi corectitudinea informaţiei specificate în cadrul sistemului la momentul plasării acesteia, inclusiv a celei prezentate în cadrul sistemului în formă de fişiere anexate.

50. Deţinătorul Registrului, precum şi operatorii PEA vor fi înregistraţi în Registrul operatorilor de date cu caracter personal, gestionat de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, iar prelucrarea datelor cu caracter personal se va realiza în conformitate cu prevederile Legii nr.133/2011 privind protecţia datelor cu caracter personal şi Hotărîrii Guvernului nr.1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

51. În cazul în care SIA RSAP (MTender) nu oferă un flux de lucru automatizat destinat procesului de pregătire şi coordonare a informaţiei şi documentelor care urmează a fi plasate în cadrul SIA RSAP (MTender), acesta va avea loc în conformitate cu regulile interne ale organizaţiei şi în conformitate cu legislaţia, iar ulterior informaţia va fi plasată în sistem.

52. Persoana responsabilă a autorităţii contractante organizează şi controlează procesul de pregătire a informaţiei în cadrul instituţiei, plasarea şi actualizarea informaţiei în cadrul SIA RSAP (MTender) în conformitate cu prevederile legale.

53. Plasarea informaţiei în SIA RSAP (MTender) se realizează numai cu acordul conducătorului instituţiei sau al persoanei responsabile, dacă nu contravine prevederilor legale.

54. Temei pentru plasarea/actualizarea informaţiei în cadrul SIA RSAP (MTender) poate fi:

1) indicaţia directă a conducătorului instituţiei sau a persoanei responsabile, dacă nu contravine prevederilor legale;

2) necesitatea dictată de normele legale;

3) apariţia unor noi informaţii.

55. Informaţia se consideră plasată în cadrul SIA RSAP (MTender) şi în Registru din momentul publicării acesteia pe portalul mtender.gov.md şi/sau primirea recipisei de recepţionare (de exemplu, în cazul depunerii ofertelor).

56. Autoritatea contractantă/entitatea contractantă nu poate modifica versiunea iniţială a dosarului procedurii de achiziţie sau eventualele anexe după lansarea procedurii de achiziţie. În cazul în care autoritatea trebuie să clarifice vreun aspect al dosarului procedurii de achiziţie, acest lucru se realizează printr-un amendament care defineşte în mod clar ce s-a schimbat, dar nu prin înlocuirea documentelor existente. Totodată, versiunile precedente se păstrează şi fiecare versiune nouă este evidenţiată pentru utilizatori. Operatorii economici înregistraţi primesc notificări privind modificările aplicate dosarului procedurii de achiziţie. Astfel de modificări sînt documentate/publicate pe PEA pentru a asigura transparenţa şi accesul la date al operatorilor economici.

Capitolul VI
CERINŢE MINIME DE SECURITATE ŞI OPERARE

Secţiunea 1
Cerinţe generale

57. Atît operatorul SIA RSAP (MTender), cît şi operatorii PEA aprobă un program de securitate informaţională conceput pentru a proteja confidenţialitatea, integritatea şi disponibilitatea SIA RSAP (MTender). Programul se va baza pe evaluarea riscurilor organizaţiei şi va fi conceput pentru a îndeplini următoarele funcţii principale de securitate informaţională:

1) identificarea şi evaluarea riscurilor de securitate informaţională interne şi externe, care ar putea ameninţa securitatea sau integritatea SIA RSAP (MTender);

2) reglementarea utilizării infrastructurii defensive;

3) implementarea politicilor şi procedurilor pentru protejarea SIA RSAP (MTender) şi a informaţiilor stocate în sistem împotriva accesului neautorizat sau a altor acţiuni de rea intenţie;

4) detectarea incidentelor de securitate informaţională;

5) reacţionarea în cazul incidentelor informaţionale identificate sau detectate pentru a atenua oricare efecte negative;

6) recuperarea de pe urma incidentelor informaţionale şi restabilirea funcţiilor şi serviciilor normale;

7) îndeplinirea obligaţiilor de raportare aplicabile în domeniul securităţii cibernetice;

8) respectarea Cerinţelor minime obligatorii de securitate cibernetică, aprobate prin Hotărîrea Guvernului nr.201/2017.

58. Operatorul SIA RSAP (MTender) şi operatorii PEA vor menţine o politică de securitate cibernetică în formă scrisă, aprobată de conducerea organizaţiei, care stabileşte procedurile de protejare a SIA RSAP (MTender) şi a datelor stocate. Politica privind securitatea informatică se bazează pe evaluarea riscurilor entităţii şi trebuie să abordeze următoarele aspecte:

1) securitatea informaţiilor;

2) administrarea şi clasificarea datelor;

3) inventarierea activelor şi gestionarea dispozitivelor;

4) controlul accesului şi managementul identităţii;

5) asigurarea continuităţii de funcţionare şi planificarea recuperării în caz de dezastru;

6) exploatarea şi disponibilitatea sistemelor;

7) securitatea sistemelor şi a reţelelor;

8) monitorizarea sistemelor şi a reţelelor;

9) dezvoltarea sistemelor şi aplicaţiilor prin prisma asigurării calităţii;

10) asigurarea securităţii fizice;

11) confidenţialitatea datelor clienţilor;

12) utilizarea serviciilor subcontractate;

13) evaluarea riscurilor;

14) intervenţiile în caz de incidente.

59. Operatorii SIA RSAP (MTender) şi ai PEA vor efectua evaluări periodice ale riscurilor legate de SIA RSAP (MTender). Evaluarea riscurilor va fi actualizată cu regularitate pentru a răspunde modificărilor survenite în cadrul SIA RSAP (MTender), datelor stocate sau proceselor de business. Evaluarea riscurilor se va realiza în conformitate cu politicile şi procedurile aprobate şi va fi documentată, specificînd:

1) criteriile de evaluare şi clasificare a riscurilor sau ameninţărilor de securitate cibernetică identificate;

2) criteriile de evaluare a gradului confidenţialităţii, integrităţii, securităţii şi disponibilităţii sistemului de achiziţii electronice, inclusiv nivelul de corespundere a controalelor existente în contextul riscurilor identificate;

3) cerinţele pentru descrierea modului în care riscurile identificate vor fi atenuate sau asumate în baza evaluării riscurilor şi a modului în care programul de securitate cibernetică abordează riscurile.

60. Programul de securitate cibernetică include monitorizarea şi testarea. Avînd la bază rezultatele evaluării riscurilor, monitorizarea şi testarea au drept scop stabilirea eficacităţii programului de securitate cibernetică. Monitorizarea şi testarea includ monitorizarea continuă sau testarea periodică prin teste de penetrare şi depistarea

vulnerabilităţilor. Organizaţiile urmează să prevadă şi să desfăşoare următoarele activităţi:

1) să comande testarea de penetrare a sistemului de achiziţii electronice, înainte de lansarea versiunii noi şi cel puţin o dată la doi ani, de către organizaţii terţe independente specializate în domeniul testărilor sistemelor informaţionale. Testarea urmează să fie bazată pe riscurile relevante identificate;

2) să evalueze anual gradul de vulnerabilitate, inclusiv prin scanări sistematice sau revizuiri ale SIA RSAP (MTender), în vederea depistării şi închiderii vulnerabilităţilor de securitate cunoscute public;

3) să implementeze politici, proceduri şi controale bazate pe risc, menite să monitorizeze activitatea utilizatorilor înregistraţi autorizaţi şi să detecteze accesul neautorizat, utilizarea neconformă sau manipularea datelor de către aceşti utilizatori.

61. Anual operatorii SIA RSAP (MTender) şi ai PEA vor prezenta posesorului sistemului un raport în scris pentru anul calendaristic precedent, care să confirme că sistemele lor au respectat cerinţele stabilite. Fiecare organizaţie trebuie să menţină pentru o perioadă de minimum cinci ani, în scopuri de audit, toate înregistrările şi datele pentru susţinerea acestui raport.

62. Operatorii SIA RSAP (MTender) şi ai PEA vor desemna o persoană calificată cu rolul de responsabil de securitatea informaţională, care va răspunde de punerea în aplicare şi supravegherea programului şi politicii privind securitatea cibernetică.

63. Fiecare organizaţie trebuie să posede personal calificat în domeniul securităţii cibernetice şi să utilizeze furnizorii de servicii sau părţile terţe care participă la procesele legate de exploatarea sistemului de achiziţii electronice, ce corespund cerinţelor de securitate cibernetică expuse în politica de securitate cibernetică a organizaţiei.

64. În baza evaluării riscurilor, operatorii SIA RSAP (MTender) şi ai PEA trebuie să utilizeze instrumente de control al accesului eficiente, care pot include autentificarea multifactorială sau autentificarea bazată pe risc, pentru a proteja sistemul împotriva accesului neautorizat la informaţia din SIA RSAP (MTender).

65. Programul de securitate cibernetică a organizaţiei va include proceduri scrise, instrucţiuni şi standarde destinate să asigure utilizarea practicilor avansate de dezvoltare a aplicaţiilor cu un nivel înalt de securitate, precum şi procedurile de evaluare, apreciere sau testare a securităţii aplicaţiilor dezvoltate de părţi terţe, utilizate în mediul tehnologic al organizaţiei.

66. Organizaţiile urmează să implementeze procese şi proceduri riguroase pentru a asigura o pistă de audit suficient de detaliată a activităţilor desfăşurate în cadrul SIA RSAP (MTender).

67. Atît operatorul SIA RSAP (MTender), cît şi operatorii PEA urmează să implementeze politici şi proceduri riguroase de gestionare a riscurilor de securitate cibernetică de-a lungul întregului ciclu de viaţă al relaţiilor cu părţile terţe. Aceste politici şi proceduri se bazează pe evaluarea riscurilor şi vor include, în măsura aplicabilităţii, următoarele aspecte:

1) identificarea şi evaluarea riscurilor părţilor terţe faţă de organizaţie;

2) practicile minime de securitate cibernetică pe care trebuie să le întrunească furnizorii de servicii terţe pentru ca organizaţia să accepte serviciile;

3) evaluarea periodică a furnizorilor de servicii terţe în baza riscului pe care îl prezintă şi a respectării continue a practicilor de securitate cibernetică solicitate.

68. Operatorul SIA RSAP (MTender) şi operatorii PEA urmează să implementeze planuri şi instrucţiuni eficiente de reacţie la incidente, precum şi mecanisme eficiente de notificare a posesorului sau organului desemnat de acesta privind evenimentele legate de securitatea cibernetică. Programul de securitate cibernetică a organizaţiei va include un plan scris şi aprobat de răspuns la incidentele legate de securitate cibernetică, conceput să reacţioneze prompt şi să restabilească sistemul în urma oricărui incident de securitate cibernetică care afectează confidenţialitatea, integritatea sau disponibilitatea SIA RSAP (MTender). Un astfel de plan de răspuns la incidente va aborda următoarele aspecte:

1) procesele interne de reacţie la un eveniment legat de securitatea cibernetică;

2) obiectivele planului de răspuns la incidente;

3) definirea unor roluri clare, a responsabilităţilor şi a nivelurilor de luare a deciziilor;

4) comunicările interne şi externe, precum şi schimbul de informaţii;

5) identificarea cerinţelor pentru remedierea oricăror deficienţe constatate;

6) documentarea şi raportarea evenimentelor de securitate cibernetică, precum şi a activităţilor legate de intervenţiile în caz de incidente;

7) evaluarea şi revizuirea planului de reacţie la incidente în urma unui eveniment de securitate cibernetică.

Organizaţia notifică posesorul sau organul desemnat de acesta despre un eveniment de securitate cibernetică în cel mai scurt timp posibil, dar nu mai tîrziu de 72 de ore de la stabilirea faptului de producere a unui eveniment de securitate cibernetică.

Secţiunea a 2-a
Cerinţe specifice

69. Operatorii SIA RSAP (MTender) şi PEA vor fi înregistraţi în Registrul operatorilor de date cu caracter personal, gestionat de Centrul Naţional pentru Protecţia Datelor cu Caracter Personal. Organizaţia va prelucra datele cu caracter personal în conformitate cu prevederile Legii nr.133/2011 privind protecţia datelor cu caracter personal şi Hotărîrii Guvernului nr.1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal.

70. Operatorul SIA RSAP (MTender) şi operatorii PEA se angajează să respecte cerinţele cadrului legal al Republicii Moldova privind protecţia tehnică şi criptografică a informaţiilor, precum şi procedura şi cerinţele stabilite în documentaţia sistemului.

71. Operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să adapteze serviciile de securitate utilizate (identificare şi autentificare, control al accesului, jurnalizare, criptare etc.) în conformitate cu cerinţele stabilite în documentaţia sistemului.

72. Operatorul SIA RSAP (MTender) şi operatorii PEA vor acorda asistenţă comprehensivă autorităţilor publice, inclusiv autorităţilor de monitorizare şi control, precum şi reprezentanţilor acestora în cazul investigării cazurilor în ceea ce priveşte securitatea informaţiilor.

73. Mijloacele de protecţie criptografică a informaţiei, inclusiv mijloacele de semnătură electronică utilizate pentru funcţionare, trebuie să respecte pe deplin cerinţele naţionale în domeniul protecţiei criptografice a informaţiei şi utilizării semnăturii electronice.

74. Anual sau în cazul unor incidente legate de securitatea informaţiilor, operatorul unităţii centrale de date şi operatorii PEA vor prezenta posesorului sistemului sau organului abilitat de acesta rapoarte privind securitatea informaţiilor.

75. Operatorul SIA RSAP (MTender) şi operatorii PEA se angajează să protejeze confidenţialitatea utilizatorilor lor. Colectarea oricăror informaţii personale sau de afaceri nu va fi efectuată decît dacă utilizatorul furnizează informaţia către organizaţie în mod voluntar şi conştient în timpul utilizării sistemului.

76. Atunci cînd utilizatorul alege să furnizeze informaţii personale sau de afaceri pentru a efectua o tranzacţie online, informaţia va fi utilizată doar pentru a efectua tranzacţia online specifică solicitată de utilizator. Pentru fiecare tranzacţie online se va solicita doar cantitatea minimă de informaţii personale şi de afaceri necesare procesării tranzacţiei respective.

77. Cînd utilizatorul vizitează sistemul pentru a naviga, citi pagini sau descărca informaţii, vor fi colectate automat şi stocate, fără a fi solicitate direct de la utilizator, doar următoarele informaţii:

1) numele de domeniu Internet şi adresa IP de la care utilizatorul accesează sistemul;

2) data şi ora în care utilizatorul accesează sistemul;

3) paginile vizitate;

4) în cazul accesării de către utilizator a sistemului de pe un alt site web – adresa site-ului respectiv.

78. Informaţiile personale pot fi transmise, partajate, vîndute sau transferate către o parte terţă doar cu acceptul utilizatorului, cu excepţia cazurilor interzise de lege în mod explicit. Revizuirea, actualizarea şi corectarea oricăror informaţii personale sau de afaceri pot fi efectuate direct în sistemul de achiziţii publice electronice de către utilizatorul respectiv.

79. Operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să implementeze măsuri extensive de securitate pentru protejarea împotriva pierderii, utilizării incorecte şi/sau modificării neautorizate a informaţiilor stocate.

80. Sistemele/subsistemele de achiziţii electronice operate vor furniza resurse tehnologice de securitate adecvate pentru a asigura confidenţialitatea şi integritatea datelor prelucrate, astfel încît nicio persoană să nu aibă acces la datele şi informaţiile care nu sînt destinate acesteia, în special la datele incluse în documentele de ofertă prezentate de candidaţi sau ofertanţi înainte de termenele-limită stabilite.

81. Resursele de securitate menţionate în punctele anterioare trebuie să permită detectarea şi înregistrarea promptă a oricăror încălcări ale interdicţiei de acces.

82. Operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să se asigure că documentele electronice care includ oferta sau propunerea pot fi criptate, precum şi să asigure semnarea acestora pe cale electronică.

83. Operatorii SIA RSAP (MTender) şi ai PEA vor asigura verificarea faptului ca pe documentele electronice care constituie oferta şi contractele de achiziţii publice să fie aplicată semnătura electronică validă.

84. Operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să implementeze sisteme de securitate care să permită identificarea codului maliţios ce ar putea accesa şi/sau deteriora datele stocate, sistemele de recepţie, prelucrare şi stocare a datelor sau componente ale acestora.

85. Resursele electronice utilizate de operatorul SIA RSAP (MTender) şi de operatorii PEA vor asigura faptul că autoritatea contractantă şi ceilalţi utilizatori se pot familiariza cu conţinutul ofertelor sau părţi ale acesteia, cererii de participare sau soluţiilor doar după expirarea termenelor-limită pentru depunerea acestora.

86. Operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să opereze un sistem care să permită determinarea sursei de transmitere a datelor, precum şi identificarea entităţii sau a persoanei fizice care le-a transmis, astfel încît transmiţătorul de date să nu poată respinge faptul că a remis informaţia respectivă ori data şi/sau timpul de transmitere al acesteia.

87. Operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să implementeze mecanisme care să asigure că datele remise nu au fost modificate în timpul sau după transmiterea acestora.

88. Data şi ora la care a fost depusă oferta se stabileşte în funcţie de momentul în care ofertantul finalizează transmiterea tuturor documentelor care constituie oferta în termenul stabilit de depunere în cadrul procedurii de achiziţie.

89. "Depunerea ofertei, a cererii sau a soluţiei" semnifică momentul în care ofertantul sau candidatul accesează funcţionalităţile pentru transmiterea setului de documente ce constituie oferta şi, ulterior, confirmă finalizarea depunerii ofertei în sistem.

90. PEA urmează să asigure determinarea exactă a datei şi orei de transmitere a ofertei. Informaţia privind data şi ora transmiterii urmează să fie încorporată în ofertă la momentul acceptării acesteia de către sistem.

91. Informaţia privind recepţionarea ofertei va fi comunicată părţilor interesate imediat după recepţionare.

92. Eşecul recepţionării de către sistem a datelor şi documentelor atrage după sine faptul ca oferta, cererea sau soluţia respectivă să fie considerată ca nefiind prezentată. În acest caz, partea interesată trebuie să fie informată imediat despre acest fapt.

93. Operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să implementeze mecanisme care să asigure confidenţialitatea ofertanţilor sau a candidaţilor pînă la expirarea termenului-limită de depunere a ofertelor, definit de autoritatea contractantă/entitatea contractantă în cadrul procedurii de achiziţie respective.

94. Operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să documenteze (să colecteze informaţie de serviciu) etapele de organizare a unei proceduri de achiziţii publice pe cale electronică, care să permită furnizarea de informaţii fiabile şi care reflectă corect situaţia prezentă sau trecută. Operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să asigure din punct de vedere tehnic şi funcţional respectarea acestei obligaţii, astfel încît documentele să poată fi păstrate în forma lor originală şi stocate în mod corespunzător, precum şi să asigure o înregistrare a tuturor evenimentelor legate de procedura de achiziţie şi accesarea documentelor care ar putea ulterior servi ca dovadă în cazul unui litigiu.

95. Sistemul trebuie să permită identificarea a cel puţin următoarelor informaţii:

1) entitatea şi/sau utilizatorul care a iniţiat operaţia;

2) timpul exact al iniţierii operaţiei;

3) documentele prezentate/accesate în cadrul operaţiei, precum şi entitatea şi/sau persoana care le-a trimis/accesat;

4) rezultatul operaţiei;

5) durata comunicării în cadrul acestor evenimente.

96. Informaţia menţionată urmează să fie actualizată în permanenţă, inclusiv informaţia privind cronologia plasării şi accesării documentaţiei standard şi cea privind atribuirea contractului.

97. Informaţia legată de procedura de achiziţie, inclusiv documentele şi informaţia de serviciu, urmează a fi păstrată în conformitate cu Legea nr.131/2015 privind achiziţiile publice, împreună cu aplicaţiile şi tehnologiile care permit citirea acestei informaţii, pînă la expirarea termenului de păstrare. La expirarea termenului de păstrare, informaţia este arhivată, termenul de păstrare a arhivei fiind nelimitat.

98. Operatorii SIA RSAP (MTender) şi PEA asigură înregistrarea în sistem a tuturor ofertelor, inclusiv a celor plasate incorect, chiar dacă acestea ulterior nu vor fi luate în considerare (vor fi descalificate) în cadrul următoarelor etape ale procedurii de achiziţie.

99. Pentru fiecare procedură de achiziţie, operatorii SIA RSAP (MTender) şi ai PEA asigură accesul tuturor părţilor interesate la: datele şi documentele procedurii de achiziţii electronice, inclusiv versiunile precedente; precizările şi modificările operate de către organizatorul procedurii de achiziţie; deciziile organizatorului de a modifica termenele de desfăşurare a procedurii de achiziţie; erorile şi omisiunile identificate şi raportate de părţile interesate, precum şi faptul despre acceptarea sau respingerea acestora de către organizatorul procedurii de achiziţii; comunicarea care a avut loc înainte de depunerea ofertelor, încheierea contractului sau solicitarea de informaţie suplimentară.

100. Ca urmare a deschiderii ofertelor de către grupul de lucru, operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să asigure ca toate părţile interesate să aibă acces la toate ofertele depuse, clarificările privind ofertele depuse de ofertanţii respectivi, documentele de calificare prezentate de ofertantul descalificat şi cîştigător, precum şi toate celelalte acte sau formalităţi de procedură referitoare la etapa următoare depunerii ofertelor.

101. PEA trebuie să permită părţilor interesate să încarce toată oferta odată sau pe părţi, pînă la data şi ora-limită de depunere a ofertelor, stabilite de autoritatea contractantă.

102. Încărcarea ofertelor menţionate în pct.98 se efectuează în zona rezervată exclusiv ofertantului respectiv în cadrul procedurii de achiziţie în cauză.

103. PEA urmează să pună la dispoziţia ofertantului funcţionalităţile şi/sau aplicaţiile software care îi permit să cripteze şi să semneze digital fişierele ofertei local, pe propriul computer, sau în sistem în momentul încărcării.

104. PEA poate permite părţilor interesate să încarce pe părţi fişierele ofertei fără a fi nevoie de criptare şi semnătura electronică, precum şi să modifice documentele încărcate în orice moment, pînă la depunerea finală a ofertei.

105. Depunerea ofertei finale este precedată în mod obligatoriu de semnarea electronică şi criptarea acesteia.

106. Formularele ofertei, precum şi oricare alte formulare care urmează a fi completate ca parte a procedurii de achiziţie trebuie puse la dispoziţia părţii interesate atît prin oferirea unor formulare online, cît şi prin oferirea spre descărcare pe calculatorul propriu a unui fişier cu conţinut structurat (de exemplu XML), în scopul completării şi încărcării ulterioare în sistem.

107. SIA RSAP (MTender) şi PEA vor asigura faptul că fişierele menţionate în pct.103 pot fi acceptate ulterior doar în cadrul procedurii din care au fost descărcate şi de autoritatea pentru care au fost generate.

108. Ofertantul trebuie să aibă posibilitatea retragerii ofertei după depunerea acesteia, dar pînă la data-limită de depunere a ofertelor, stabilită în anunţul de participare sau în documentaţia de atribuire. Totodată, ofertantul poate modifica conţinutul ofertei sau substitui oferta în întregime şi după depunerea ofertei, dar pînă la data şi ora-limită de depunere a ofertelor.

109. Prezentarea unei oferte este considerată finalizată atunci cînd ofertantul confirmă formal acest fapt, după finalizarea încărcării tuturor fişierelor şi formularelor corespunzătoare, semnate şi criptate în timp util.

110. După depunerea ofertelor, ofertantul primeşte o recipisă electronică, care atestă prezentarea ofertei, înregistrînd identitatea autorităţii contractante, procedura de achiziţii, lotul (dacă este cazul), ofertantul, data şi ora depunerii ofertei.

111. Recipisa trebuie să fie disponibilă în zona rezervată exclusiv ofertantului, dublată printr-o copie trimisă la e-mailul ofertantului.

112. PEA asociază recipisa electronică cu oferta depusă, care devine parte integrantă a acesteia şi, ca atare, este pusă la dispoziţia grupului de lucru pentru organizarea procedurii de achiziţie.

113. PEA va asigura ca ofertanţii să poată consulta în orice moment ofertele depuse la procedura de achiziţie după data deschiderii ofertelor de către grupul de lucru.

114. La expirarea termenului-limită de depunere a ofertelor, unitatea centrală de date şi PEA se angajează să furnizeze grupului de lucru pentru organizarea procedurii de achiziţie toate ofertele depuse pînă la data şi ora stabilite în documentaţia de atribuire şi să ofere instrumente de deschidere a acestora, indiferent de apariţia ulterioară a motivelor respingerii ofertelor.

115. Ofertele transmise în cadrul procedurii de achiziţie prin intermediul PEA nu pot fi făcute publice înainte de expirarea termenului-limită de depunere a ofertelor şi înaintea deschiderii acestora de către grupul de lucru pentru organizarea procedurii de achiziţie în cauză.

116. Accesarea ofertelor de către membrii grupului de lucru în vederea deschiderii acestora se efectuează cu participarea şi acceptul a minimum trei membri ai grupului de lucru.

117. Informaţia transmisă de către o PEA către SIA RSAP (MTender) are destinaţia de a fi stocată într-un format capabil să suporte procesarea automată.

118. Pentru ca procesarea automată să se desfăşoare fără erori, datele transmise urmează a fi codate corespunzător.

119. Codarea utilizată trebuie să fie sincronizată complet cu SIA RSAP (MTender), astfel încît să nu existe rupturi în identificarea corectă a obiectelor informaţionale şi a procedurilor la care se referă informaţiile transmise.

120. Normele şi cerinţele privind interconectarea cu SIA RSAP (MTender) vor fi descrise în documentaţia SIA RSAP (MTender).

121. Toate documentele ofertelor încărcate, precum şi contractele rezultate în urma procedurii de achiziţie urmează a fi semnate digital, utilizînd semnătura electronică avansată calificată.

122. În cazul în care certificatul digital nu poate lega direct semnatarul de poziţia şi autoritatea pe care o reprezintă, partea interesată urmează să prezinte un document electronic oficial care să indice legătura dintre persoana semnatară şi autoritatea pe care o reprezintă.

123. Atît operatorul SIA RSAP (MTender), cît şi operatorii PEA urmează să asigure procesul de autorizare şi controlul accesului utilizatorilor la serviciile pe care le prestează.

124. Orice accesare a serviciilor, aplicaţiilor sau documentelor se va înregistra în jurnalele de evidenţă a accesului.

125. Operatorul SIA RSAP (MTender) şi operatorii PEA vor utiliza mecanisme de protecţie şi recuperare a informaţiilor asociate cu procedurile de achiziţie publică electronică.

126. Operatorul SIA RSAP (MTender) şi operatorii PEA urmează să asigure mecanisme care să protejeze confidenţialitatea informaţiilor şi să prevină accesul neautorizat la acestea.

127. Operatorul SIA RSAP (MTender) şi operatorii PEA trebuie să se asigure că informaţiile sînt disponibile pentru utilizatori exclusiv în funcţie de nivelul de acces al acestora.

128. Operatorul SIA RSAP (MTender) şi operatorii PEA vor pune la dispoziţie tehnologii care să permită efectuarea auditului tehnic şi de conformitate.

129. Operatorul SIA RSAP (MTender) şi operatorii PEA vor garanta mecanisme de securitate fizică şi logică pentru a proteja serviciile şi informaţiile stocate în sistem.

130. Toate serviciile trebuie să fie sincronizate cu NTP (Network Time Protocol), utilizînd standardul de timp UTC (Coordinated Universal Time).

131. Toate informaţiile şi documentele publicate în SIA RSAP (MTender), în conformitate cu legislaţia în vigoare, sînt deschise şi disponibile publicului. Documentele pot fi considerate confidenţiale numai în cazuri excepţionale, la cererea părţii interesate, şi în conformitate cu legislaţia relevantă (Legea nr.171/1994 cu privire la secretul comercial sau alte acte normative relevante).

132. Prelucrarea şi publicarea datelor cu caracter personal se va realiza în conformitate cu prevederile Legii nr.133/2011 privind protecţia datelor cu caracter personal.

Capitolul VII
CONTROLUL ŞI RESPONSABILITATEA

133. Sistemul este supus unui control intern şi extern. Controlul intern este efectuat de posesor, iar controlul extern – de autoritatea administraţiei publice autorizată.

134. La efectuarea controlului intern sau extern, organul de control alcătuieşte actul în două exemplare, din care unul este direcţionat către deţinător, iar celălalt rămîne la organul de control. Deţinătorul este obligat să ia măsuri pentru lichidarea încălcărilor identificate şi să informeze despre aceasta organul de control.

135. Pentru organizarea controlului de funcţionare a sistemului este responsabil deţinătorul, care este obligat să asigure dreptul de acces la Registru şi mijloacele de ţinere a acestuia, precum şi în încăperile în care se află mijloacele hardware utilizate în acest scop.

136. Angajaţii responsabili de asigurarea funcţionării sistemului şi înregistrării datelor poartă răspundere personală în conformitate cu legislaţia în vigoare pentru autenticitatea, fiabilitatea, integritatea informaţiei, precum şi pentru păstrarea/stocarea şi utilizarea acesteia.

137. Toţi subiecţii cu acces la Registru, precum şi destinatarul informaţiei cu conţinut de date personale sînt responsabili pentru dezvăluirea, transferarea către o parte terţă şi utilizarea în scopuri personale a informaţiei, conform legislaţiei în vigoare.

138. Păstrarea Registrului este asigurată de deţinător pînă la luarea deciziei privind lichidarea sau transferul acestuia către un alt deţinător. În cazul lichidării Registrului, toate datele conţinute în acesta sînt stocate în arhivă în conformitate cu legislaţia în vigoare.