|  |
| --- |
| **GUVERNUL REPUBLICII MOLDOVA****H O T Ă R Î R E nr**.**\_\_\_\_\_\_\_** **din** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Chișinău** |

**Pentru** **aprobarea Regulamentului cu privire la utilizarea sistemului informațional** **automatizat “****Registrul de stat al achizițiilor publice” (MTender)**

**------------------------------------------------------------------**

În temeiul prevederilor art. 16 pct (3) al Legii nr. 71-XVI din 22 martie 2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314) și pct.4 alin.(1) din Hotărîrea Guvernului nr. 705 din 11 iulie 2018 cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat „Registrul de stat al achiziíilor publice” (MTender) (Monitorul Oficial al Republicii Moldova, 2018, nr.309-320, art 847), Guvernul

HOTĂRĂȘTE:

1. Se aprobă Regulamentul cu privire la utilizarea sistemului informațional automatizat “MTender” conform anexei.

2. Prezenta hotărîre intră în vigoare la data de 01.10.2018.

**Prim-ministru Pavel FILIP**

**Contrasemnează:**

**Ministrul finanțelor Octavian ARMAȘU**

Anexă

 la Hotărârea Guvernului

 nr. \_\_\_/2018

**REGULAMENT**

**privind funcționarea**

**Sistemului Informațional Automatizat ”** **Registrul de stat al achizițiilor publice” (MTender)**

**Capitolul I**

**Dispoziții generale**

**Secțiunea 1**

**Obiectul de reglementare**

1. Prezentul Regulament stabilește reguli de utilizare al Sistemului MTender în scopul organizării și desfășurării procedurilor de achiziție publică, precum și proceselor aferente acestora, formarea registrului contractelor și procedurilor de achiziție publică, stabilirea cerințelor minime față de utilizarea mijloacelor de protecție la introducerea, stocarea, prelucrarea și accesarea informațiilor privind procedurile de achiziție publică și celei adiacente, cerințelor minime față de echipamentul tehnic și de program față de utilizatorii Sistemului MTender.
2. Sistemul MTender este un sistem informațional și de telecomunicații complex, compus din mai multe platforme electronice de achiziții, portalul web mtender.gov.md, conectate la Unitatea Centrală de Date, care în totalitate asigură accesul către aplicațiile și serviciile informaționale ce se referă la domeniul achizițiilor publice. Sistemul MTender servește drept instrument de susținere a serviciilor de achiziții publice, aplicând schimbul informațional prin intermediul mediului comunicațional.
3. Deținător și operator tehnico-tehnologic al Unității Centrale de Date (în continuare, UCD) este Instituția Publică „Centrul de Tehnologii Informaționale în Finanțe”, în conformitate cu Hotărîrea Guvernului nr. 705 din 11 iulie 2018 cu privire la aprobarea Conceptului tehnic al Sistemului Informațional Automatizat „Registrul de stat al achizițiilor publice” (MTender).
4. Deținător al platformei electronice de achiziții (în continuare, PEA) poate fi orice persoană, înregistrată în calitate de persoană juridică în conformitate cu legislația Republicii Moldova care:
5. acceptă principiile MTender și condițiile de participare la implementarea sistemului MTender;
6. întrunește cerințele tehnice, funcționale și juridice pentru PEA;
7. a susținut cu succes procesul de acreditare în conformitate cu prevederile Regulamentului privind acreditarea PEA.
8. Prevederile prezentului Regulament sunt obligatorii pentru toți utilizatorii sistemului MTender, aplicându-se de asemenea și în cadrul procesului de ținere, prelucrare și utilizare a datelor conținute în cadrul sistemului, precum și în activitățile aferente exploatării acestuia.

#

# Secțiunea 2

# Noțiuni

1. În sensul prezentului Regulament se aplică următoarele noțiuni:

 **Autentificare** – procesul de verificare a identității (digitale) a unui utilizator în cadrul sistemului informațional prin intermediul certificatului cheii publice sau alte instrumente;

 **Autorizare** – mecanism al sistemului informațional care determină ce nivel de acces trebuie de atribuit unui utilizator autentificat pentru a accesa resurse securizate controlate de către sistem;

 **Certificat al cheii publice (certificat digital)** – document electronic conținând cheia publică, semnat cu semnătura digitală a persoanei abilitate a centrului de certificare a cheilor publice, document ce atestă apartenența cheii respective titularului certificatului cheii publice și permite identificarea acestui titular;

 **Cerere de acreditare** – cerere depusă de către operatorul PEA către organul abilitat în vederea inițierii unor proceduri legate de procesul de acreditare în conformitate cu Regulamentul privind acreditarea PEA;

 **Cheie de testare** – identificator al platformei electronice pentru punerea în aplicare și testarea funcționalităților până la obținerea autorizării pentru conectarea și efectuarea schimbului de date în cadrul sistemului de achiziții electronice;

 **Cheie de producție** – identificator al platformei electronice autorizate pentru conectarea și efectuarea schimbului de date în cadrul sistemului de achiziții electronice în regim de producție, în conformitate cu nivelul de acreditare primit;

 **Comisie de acreditare** – organ colectiv cu statut permanent, abilitat cu funcția de luare a deciziilor privind acreditarea PEA, retragerea (temporară sau permanentă) a acreditării ca rezultat a deficiențelor depistate în cadrul verificărilor PEA. Comisia de acreditare este constituită prin ordinul Ministerului Finanțelor și activează în baza Regulamentului privind acreditarea PEA;

 **Complex de mijloace software și hardware** – totalitatea programelor și mijloacelor tehnice, care asigură realizarea proceselor informaționale;

 **Contract de achiziții publice –** contract cu titlu oneros, încheiat în scris între unul sau mai mulți operatori economici și una sau mai multe autorități contractante, care are ca obiect achiziția de bunuri, executarea de lucrări sau prestarea de servicii;

 **Date cu caracter personal** – orice informație referitoare la o persoană fizică identificată sau identificabilă;

 **Document electronic** – document editat, procesat și transmis prin intermediul sistemelor informatice și canalelor de transmisie electronice (INTERNET sau rețele private de date). Un document în format electronic poate fi un fișier în format needitabil (pdf, mdi, jpg, tiff) sau în format editabil –MS Word, MS Excel, MS Power Point (.doc, .xls, .ppt)  etc;

 **Documentație standard sau documentație de atribuire** – document care cuprinde cerințele, criteriile, regulile și alte informații necesare pentru a asigura operatorilor economici o informare completă, corectă și explicită cu privire la cerințele sau elementele achiziției, obiectul contractului și modul de desfășurare a procedurii de atribuire, inclusiv specificațiile tehnice ori documentul descriptiv, condițiile contractuale propuse, formatele de prezentare a documentelor de către ofertanți/candidați, informațiile privind obligațiile generale aplicabile;

 **Entitate Contractantă (EC)** – alte autorități decât autoritățile contractante, care utilizează sistemul MTender în vederea organizării procedurilor de achiziție;

 **Incident** – reprezintă un eveniment, care nu face parte din operarea standard a unui serviciu și cauzează sau poate cauza o perturbare sau o reducere a calității serviciilor și a productivității Sistemului MTender;

 **Ofertant** – operator economic, care a prezentat o ofertă în cadrul procedurii de atribuire a contractului de achiziții publice;

 **Operator economic** – orice persoană fizică sau juridică, orice entitate publică sau asociație a acestor persoane și/sau entități care furnizează bunuri, execută lucrări și/sau prestează servicii pe piață;

 **Operator al PEA –** persoană juridică, înregistrată în conformitate cu legislația Republicii Moldova, deținător al unei platforme electronice de achiziții, care are dreptul de a desfășura/presta serviciile caracteristice unei PEA;

 **Operatorul Sistemului MTender (Operator)** – persoană juridică, stabilită printr-o hotărâre a Guvernului, responsabilă de funcționarea și administrarea Sistemului MTender;

 **Ore de muncă** – perioada de timp de luni până vineri,  de la ora 8.00 până la 18.00, cu excepția zilelor de odihnă și zilelor de sărbătoare;

 **Platformă Electronică de Achiziții (PEA)** – set de resurse informaționale, atât hardware, cât și software, destinate organizării și desfășurării procedurilor de achiziții publice în mod automatizat. Împreună cu UCD, prin aplicarea schimbului de informații în mediul digital, PEA, asigură ciclul electronic de desfășurare a achizițiilor publice. PEA sunt operate de posesorii lor, preventiv autorizați. Rolul unei PEA este de a livra interfața de lucru pentru utilizatorii autorizați ai actorilor participanți la procesul de achiziție publică: autorități contractante, entități contractante și operatori economici;

 **Protecția informației contra accesului neautorizat** – ansamblu de măsuri orientate spre prevenirea, identificarea și înlăturarea sustragerii informației protejate prin încălcarea regulilor de acces stabilite de actele normative sau de proprietarul (deținătorul) informației;

 **Rol** – set de atribuții și sarcini specifice, care îi revin utilizatorului în cadrul sistemului informațional după înregistrarea lui;

 **Securitate informațională** – protecția sistemului informațional de acțiuni premeditate sau neintenționate cu caracter natural sau artificial, care au ca rezultat cauzarea prejudiciului participanților la schimbul informațional;

 **Unitatea Centrală de Date (UCD) –** un set de instrumente hardware și software destinat organizării și stocării datelor privind desfășurarea procedurilor de achiziții publice. UCD asigură sincronizarea datelor cu PEA și furnizează datele stocate către consumatorii de date externi;

 **Utilizator** – orice persoană sau grup de persoane, care folosește informația din Sistemul MTender sau interacționează direct cu acesta.

**Capitolul II**

**Scopul sistemului și domeniul de aplicare**

1. Scopul sistemului MTender este de a spori transparența procesului de achiziții publice în totalitate, de a obține un raport calitate/preț mai bun în cadrul procedurilor de achiziții publice și de a reduce costurile de tranzacționare pentru toate părțile implicate, contribuind astfel la asigurarea unui sistem național de achiziții publice competitiv durabil și accesibil prin:
2. Asigurarea comunicării online ca mod obligatoriu de schimb de date în cadrul procesului de desfășurare a procedurilor de achiziții publice, inclusiv disponibilitatea online a tuturor anunțurilor de participare, a documentației de atribuire și a cererilor de participare. În special, sistemul MTender va aplica comunicarea electronică și schimbul de informații pentru oferirea unor instrumente dedicate exclusiv achizițiilor online: licitațiile electronice, acordurile-cadru, sisteme dinamice de achiziție și cataloage electronice;
3. Aplicarea principiului autentificării unice (single-sign-on) și implementarea proceselor business standardizate și optimizate pentru realizarea achizițiilor publice;
4. Utilizarea Documentului Unic de Achiziții European (în continuare, DUAE) și, după caz, e-CERTIS;
5. Utilizarea semnăturii electronice avansate calificate pentru autentificarea utilizatorilor și semnarea deciziilor sau documentelor produse pe parcursul desfășurării procedurii de achiziții publice;
6. Implementarea criteriilor de interoperabilitate, proporționalitate, transparență, trasabilitate și securitate, conform prevederilor Directivei 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile public;
7. Implementarea funcționalităților care acoperă integral procesele de achiziții publice, de la planificare până la semnarea contractului, evidența plăților în cadrul contractului până la executarea contractului, dar și a unui sistem electronic de realizare a achizițiilor centralizate;
8. oferirea unor instrumente de monitorizare bazate pe datele întregului ciclu de desfășurare a achizițiilor publice și înregistrarea tuturor operațiunilor și tranzacțiilor în timp real.
9. Sistemul MTender este un sistem format din mai multe platforme conectate la UCD, la care sunt conectate mai multe PEA. Rolul UCD este de a colecta și stoca informația transmisă prin intermediul PEA, precum și de a sincroniza în timp real informația între toate platformele conectate, astfel încât, autoritățile contractante, entitățile contractante și operatorii economici să poată utiliza orice PEA pentru a publica sau vizualiza informația despre o anumită procedură de achiziții. Odată publicată de către una din platforme, informația devine accesibilă în timp real și pe toate celelalte platforme conectate. Fiecare utilizator are acces egal, în limita rolului în cadrul sistemului, la informația privind procedura de achiziție și oportunitatea de participare.
10. Domeniul de aplicare a sistemului MTender este cel al proceselor legate de organizarea și desfășurarea procedurilor de achiziție publică în conformitate cu Legea privind achizițiile publice nr. 131 din 03 iulie 2015 și legislația secundară privind achizițiile publice, precum și în conformitate cu acordurile internaționale cu caracter obligatoriu, în special, al Acordului privind achizițiile publice, întocmit la Marrakech la 15 aprilie 1994 (modificat prin Protocolul de modificare, încheiat la Geneva, 30 martie 2012), care a intrat în vigoare la data de 14 iulie 2016 pentru Republica Moldova.

#

**Capitolul III**

# Participanții în cadrul sistemului

1. Funcțiile subiecților Sistemului MTender rezultă din funcțiile atribuite acestora prin Legea nr. 71-XVI din 22 martie 2007 cu privire la registre, Legea nr.131 din 3 iulie 2015 privind achizițiile publice și alte acte normative, și anume:
2. **Ministerul Finanțelor** - posesorul sistemului MTender (registrului), care:
3. asigură condițiile juridice, organizatorice și financiare pentru crearea și ținerea sistemului MTender;
4. asigură ținerea sistemului MTender în conformitate cu regulile de ținere a registrelor;
5. asigură mecanismul de înregistrare a obiectelor supuse înregistrării;
6. asigură autenticitatea, plenitudinea și integritatea datelor din sistemul MTender;
7. asigură securitatea și protecția datelor din registru;
8. asigură accesul la datele din registru în conformitate cu legea și regulile de ținere a registrelor;
9. deleagă funcții privind ținerea registrului deținătorului sistemului MTender și/sau registratorilor sistemului MTender;
10. **Instituția Publică „Centrul de Tehnologii Informaționale în Finanțe”** - deținătorul sistemului MTender (registrului), îndeplinește atribuțiile de ținere a sistemului MTender transmise de către posesorul sistemului MTender;
11. **Operatorii PEA** - deținători ai PEA, îndeplinesc atribuțiile de ținere a PEA (parte a sistemului “MTender”), transmise de către posesorul sistemului MTender ca rezultat al procedurii de acreditare;
12. **Agenția Achiziții Publice** (în continuare, AAP) - furnizor și destinatar al datelor sistemului MTender (registrului), care:
13. coordonează, monitorizează și evaluează prin intermediul funcționalităților oferite de sistem a modului în care autoritățile contractante respectă procedurile de achiziție publică și de atribuire a contractelor de achiziții publice;
14. întocmește, actualizează și menține, prin intermediul funcționalităților oferite de sistemul MTender, Lista de interdicție a operatorilor economici;
15. examinează dările de seamă privind procedurile de achiziție publică;
16. generează și analizează rapoarte privind procedurile de achiziție publică;
17. gestionează Buletinul Achizițiilor Publice în cadrul sistemului MTender;
18. **Agenția Națională pentru Soluționarea Contestațiilor** (în continuare, ANSC**)** - furnizor și destinatar al datelor sistemului MTender, care:
19. recepționează și înregistrează contestațiile depuse de participanții la procedurile de achiziție publică;
20. înregistrează rezultatele examinării contestațiilor depuse de participanții la procedurile de achiziție publică;
21. intervine în procesele legate de desfășurarea procedurilor de achiziție publică, inclusiv prin suspendarea procedurii de achiziții publice și anularea procedurii de achiziții publice;
22. **Autoritatea contractantă** - furnizor și destinatar al datelor sistemului MTender (registrului), care:
23. elaborează planuri anuale și trimestriale de efectuare a procedurilor de achiziții publice;
24. creează grupuri de lucru responsabile de realizarea achizițiilor publice în cadrul autorității contractante;
25. întocmește și publică invitațiile/anunțurile de participare în cadrul procedurilor de achiziții publice;
26. elaborează și publică în cadrul sistemului MTender documentația de atribuire și alte documente aplicabile în cadrul procedurilor de achiziții publice;
27. inițiază proceduri de achiziții publice;
28. examinează, evaluează și compară ofertele depuse în cadrul procedurilor de achiziție publică;
29. aplică deciziile Agenției Naționale pentru Soluționarea Contestațiilor;
30. semnează contractele de achiziții publice, iar, ulterior, le transmite spre semnare participanților desemnați câștigători;
31. întocmește dări de seamă privind rezultatul procedurilor de achiziții publice și le publică în Sistemul MTender;
32. transmite contractele semnate către trezorerie spre înregistrare;
33. menține corespondența electronică cu operatorii economici interesați și participanții la procedura de achiziții publice;
34. publică răspunsul la clarificările recepționate;
35. monitorizează executarea contractului de achiziții publice;
36. inițiază, semnează și transmite spre înregistrare acorduri adiționale la contractele de achiziții publice;
37. **Entitatea contractantă** - furnizor și destinatar al datelor sistemului MTender (registrului), care:
38. elaborează, opțional, planuri anuale și trimestriale de efectuare a procedurilor de achiziții;
39. creează grupuri de lucru responsabile de realizarea achizițiilor în cadrul acestor entități;
40. întocmește și publică invitațiile de participare în cadrul procedurilor de achiziții publice;
41. elaborează și publică în cadrul sistemului MTender documentația de atribuire și alte documente aplicabile în cadrul procedurilor de achiziții;
42. inițiază procedurile de achiziții publice;
43. examinează, evaluează și compară ofertele depuse în cadrul procedurilor de achiziție publică;
44. semnează contractele de achiziții publice, iar, ulterior, le transmite spre semnare participanților desemnați câștigători;
45. menține corespondența electronică cu operatorii economici interesați și participanții la procedura de achiziții publice;
46. publică răspunsul la clarificările recepționate;
47. monitorizează, opțional, executarea contractului de achiziții publice;
48. inițiază și semnează acorduri adiționale la contractele de achiziții încheiate anterior în cadrul sistemului MTender;
49. **Operatorul economic** - furnizor și destinatar al datelor sistemului MTender (registrului), care:
50. accesează documentația de atribuire pentru procedura de achiziții publice;
51. înaintează clarificări către autoritatea contractantă privind documentația de atribuire pentru procedura de achiziții publice și obține explicații;
52. se înregistrează la procedura de achiziții publice;
53. înaintează oferte la procedura de achiziții publice;
54. prezintă documente de calificare în cadrul procedurilor de achiziții publice;
55. prezintă informație suplimentară, la solicitarea autorității contractante;
56. participă la procedura de atribuire a contractului de achiziție publică;
57. semnează contractele de achiziții publice, în cazul desemnării în calitate de câștigător;
58. depune garanția de bună execuție a contractului de achiziții publice;
59. execută contractul de achiziții publice semnat;
60. **Platformele Electronice de Achiziții** - registratori ai sistemului MTender (registrului), care:
61. asigură fluxuri de lucru pentru organizarea procedurilor de achiziție publică de către autoritățile contractante, entitățile contractante;
62. asigură fluxuri de lucru pentru participarea operatorilor economici la procedura de achiziție publică;
63. colectează și transmit datele aferente procesului de organizare și desfășurare a procedurilor de achiziții către UCD;
64. asigură sincronizarea datelor între UCD și platformă;
65. oferă asistență de ordin tehnic autorităților contractante și operatorilor economici în procesul de utilizare a funcționalităților sistemului MTender la organizarea procedurilor de achiziție publică;
66. **Registrele și sistemele informaționale de stat** - furnizori de date în cadrul sistemului MTender (registrului), care:
67. oferă informația despre operatorii economici, autoritățile contractante, etc., în baza IDNO;
68. oferă informația despre persoanele fizice, în baza IDNP;
69. oferă informația cu privire la efectuarea regulată a plății impozitelor, contribuțiilor (conform datelor Serviciului Fiscal de Stat);
70. oferă informația despre existența licențelor și altor documente permisive în raport cu participantul la procedura de achiziție publică;
71. oferă informația despre existența resurselor financiare și plaților efectuate în cadrul contractului de achiziție publică;
72. furnizează informația privind facturile fiscale eliberate în procesul de executare a contractului de achiziție publică;
73. oferă informația despre existența/lipsa antecedentelor penale în raport cu participantul la procedura de achiziție publică.
74. **Serviciile electronice guvernamentale** - intermediari de furnizare a datelor în cadrul sistemului MTender (registrului), care:
75. asigură schimbul de date între sistemul MTender cu Registrele și sistemele informaționale de stat;
76. asigură realizarea proceselor interne în cadrul sistemului MTender cum ar fi: autentificarea utilizatorilor, semnarea electronică a documentelor, notificarea, înregistrarea evenimentelor, etc.;
77. **Portalul guvernamental pentru date deschise** - destinatar al datelor sistemului MTender (registrului), care asigură publicarea seturilor de date deschise în vederea facilitării accesului cetățenilor la datele privind procedurile de achiziții publice;
78. **Sistemele externe (TED)** - destinatar al datelor sistemului MTender (registrului), care asigură publicarea anunțului de participare și notificărilor în cadrul Jurnalului Oficial al Uniunii Europene;
79. **Administrația publică** - destinatar al datelor sistemului MTender (registrului), care:
80. monitorizează procedurile de achiziție publică;
81. vizualizează rapoartele statistice;
82. preia experiența de organizare a procedurilor de achiziție publică;
83. **Publicul larg** - destinatar al datelor sistemului MTender (registrului), care:
84. monitorizează procedurile de achiziție publică;
85. vizualizează rapoartele statistice;
86. obține seturile de date pentru analiza avansată a datelor privind procedurile de achiziții publice.
87. Posesorul Sistemului MTender este obligat să asigure condițiile de drept, organizaționale și financiare pentru crearea și funcționarea Sistemului MTender. Drepturile și obligațiile posesorului Sistemului MTender sunt determinate de art.11 din Legea nr.71-XVI din 22 martie 2007 cu privire la registre.
88. Deținătorul Sistemului MTender este obligat:
89. să asigure funcționarea Sistemului MTender în corespundere cu baza normativă actuală și acordului încheiat cu Posesorul;
90. să asigure posibilitatea de conectare a participanților autorizați la Registru;
91. să asigure crearea înscrierilor de evidență (conturilor) pentru utilizatorii Sistemului MTender cu atribuirea/modificarea rolurilor și drepturilor de acces la interfață și date;
92. să asigure veridicitatea, siguranța și integritatea datelor din Sistemul MTender;
93. să efectueze monitorizarea și controlul asupra accesării datelor din Sistemul MTender;
94. să asigure suportul metodologic prin elaborarea procedurilor, regulilor și instrucțiunilor de utilizare a funcționalităților sistemului MTender precum și accesarea și introducerea datelor;
95. să asigure securitatea Sistemului MTender și să aplice măsuri de monitorizare a respectării condițiilor de securitate și regulilor de exploatare a Sistemului MTender prin fixarea cazurilor și tentativelor de încălcare a măsurilor, precum și să ia măsurile corespunzătoare pentru prevenirea și eliminarea consecințelor lor;
96. să asigure securitatea accesului la informația din Sistemul MTender și să aplice măsuri de monitorizare privind respectarea securității accesului la datele sistemului prin fixarea cazurilor și tentativelor de încălcare a măsurilor prevăzute, precum și să ia măsurile corespunzătoare pentru prevenirea și eliminarea consecințelor lor;
97. să asigure, să organizeze și să amenajeze locurile de muncă corespunzătoare pentru persoanele responsabile pentru deservirea Sistemului MTender;
98. să asigure condițiile necesare pentru păstrarea securizată a purtătorilor de informație și copiilor de rezervă, precum și pentru excluderea accesului persoanelor, neautorizate la purtătorii corespunzători de informație;
99. să ofere suportul necesar persoanelor autorizate în utilizarea complexului de mijloace software a Sistemului MTender;
100. să informeze participanții Sistemului MTender despre schimbările condițiilor tehnice de funcționare a acestuia;
101. să asigure protecția împotriva virușilor și spam-ului;
102. să asigure implementarea măsurilor organizaționale și tehnice, necesare pentru asigurarea regimului de confidențialitate și securitate a datelor personale în corespundere cu legislația privind protecția datelor cu caracter personal;
103. să asigure accesul securizat la informația din Sistemul MTender, respectarea condițiilor de securitate și regulilor de exploatare;
104. să utilizeze informația obținută în cadrul Sistemului MTender numai în scopurile stabilite de legislația în vigoare și acordul cu Posesorul sistemului.
105. Registratorul Sistemului MTender este obligat:
106. să asigure înregistrarea informației în Sistemul MTender în corespundere cu formatele și regulile stabilite, indicate în instrucțiunile corespunzătoare;
107. să verifice respectarea condițiilor de înregistrare, evidentă și utilizare a datelor cu caracter personal;
108. să asigure corectitudinea, veridicitatea și autenticitatea datelor din Sistemul MTender;
109. să utilizeze informația obținută în cadrul Sistemului MTender numai în scopurile stabilite de legislația în vigoare și acordul Posesorului Sistemului MTender;
110. să ofere suportul necesar furnizorilor de informație în utilizarea complexului de mijloace software a Sistemului MTender.
111. Furnizorii și destinatarii datelor sânt obligați:
112. să furnizeze în cadrul Sistemului MTender doar informație corectă și veridică în corespundere cu formatele și regulile stabilite;
113. să utilizeze informația obținută din Sistemul MTender numai în scopurile stabilite de legislația în vigoare și in conformitate cu atribuțiile ce le revin;
114. să utilizeze funcționalitățile sistemului MTender în exclusivitate conform destinației acestora și conform atribuțiilor ce le revin, în strictă conformitate cu legislația în vigoare;
115. să asigure protejarea contra compromiterii și contra utilizării neautorizate a mijloacelor de autentificare și a credențialelor utilizate pentru autentificarea în cadrul Sistemului MTender;
116. să anunțe imediat prin orice mijloace de comunicare Deținătorul Sistemului MTender despre cazurile de încălcare a securității informaționale a Sistemului MTender;
117. să anunțe imediat Deținătorul Sistemului MTender despre apariția situațiilor de forță majoră, care pot compromite îndeplinirea atribuțiilor ce le revin.
118. Deținătorul Sistemului are dreptul:
119. să elaboreze și să înainteze propuneri de modificare și completare a cadrului legislativ și normativ privind Sistemul MTender;
120. să propună și să implementeze soluții pentru îmbunătățirea și sporirea eficacității procesului de funcționare a Sistemului MTender;
121. să monitorizeze respectarea cerințelor de securitate informațională de către participanții Sistemului MTender, să înregistreze cazurile și încercările de încălcare a acestora;
122. să inițieze procedura de suspendare a drepturilor de acces la Registru față de participanții care nu respectă regulile stabilite, standardele și normele din domeniul securității informaționale;
123. să verifice autenticitatea și veridicitatea datelor introduse de participanții Sistemului MTender;
124. să solicite de la participanți actualizarea și corectarea informației în baza de date a Sistemului MTender la detectarea erorilor și omisiunilor;
125. să solicite de la participanți informația necesară pentru completarea datelor în Sistemul MTender;
126. să refuze furnizarea informației din Sistemul MTender în cazurile prevăzute de legislația în vigoare;
127. să exercite alte drepturi delegate de către Posesorul Sistemului MTender.
128. Registratorul Sistemului MTender are dreptul:
129. să propună modificări și completări la cadrul legal de funcționare a Sistemului MTender;
130. să propună soluții pentru îmbunătățirea și sporirea eficacității procesului de funcționare a Sistemului MTender și a comodității de introducere a datelor;
131. să solicite de la furnizorii de informație informația, necesară pentru completarea datelor în Sistemul MTender;
132. să solicite de la furnizorii de informație, la detectarea erorilor și omisiunilor, actualizarea și corectarea datelor furnizate;
133. să exercite alte drepturi delegate de către Posesorul Sistemului MTender.
134. Furnizorii și destinatarii datelor au dreptul:
135. să primească informație veridică și actuală în cadrul sistemului MTender;
136. să solicite și să acceseze informația în cadrul Sistemului MTender în conformitate cu atribuțiile acestora;
137. să acceseze funcționalitățile Sistemului MTender în conformitate cu atribuțiile acestora.
138. Fiecare participant a Sistemului MTender are dreptul:
139. să participe la implementarea și dezvoltarea Sistemului MTender;
140. să înainteze Posesorului și Deținătorului propuneri privind modificarea și/sau completarea actelor normative și legislative, care reglementează funcționarea Sistemului MTender;
141. să solicite și să primească de la Deținător susținere metodologică și practică de funcționare a Sistemului MTender;
142. să înainteze Deținătorului propuneri privind perfectarea și sporirea eficacității funcționării Sistemului MTender.

#

**Capitolul IV**

# Gestionarea și asigurarea funcționării Sistemului

# Secțiunea 1

**Modul de ținere a sistemului (registrului)**

1. Registrul se ține în format electronic.
2. În procesul de exploatare a Sistemului MTender se formează resursa unică informațională de stat - Registrul, care reprezintă o totalitate de informație sistematizată, ce constituie obiectele informaționale de bază aferente procesului de achiziții, și anume:
3. autoritatea contractantă/entitatea contractantă;
4. operatorul economic;
5. linia de plan;
6. procedura de achiziție;
7. documentul;
8. criteriul;
9. cerința;
10. lotul;
11. poziția;
12. întrebarea;
13. explicația;
14. clarificarea;
15. actul organizatoric;
16. contestația;
17. oferta;
18. adjudecarea;
19. contractul;
20. amendamentul;
21. tranzacția;
22. livrabilul.
23. Deținătorul sistemului MTender efectuează administrarea acestuia cu ajutorul complexului de mijloace software și hardware, în corespundere cu prezentul Regulament.
24. Registrul se ține în limba de stat, iar produsul de program elaborat se traduce în limbile rusă și engleză.
25. Accesul la Registru și schimbul informațional se realizează prin intermediul rețelei globale Internet, comunicarea PEA cu UCD se realizează, utilizând canalele de schimb de date securizate.
26. Accesul la obiectele informaționale a Registrului și funcțiile acestuia se realizează prin nivelele de acces public și autorizat.
27. Sistemul MTender funcționează zilnic, 24/24, cu excepția timpului rezervat pentru lucrări de mentenanță, care vor fi programate, cu unele excepții, în afara orelor de lucru sau în zilele de odihnă sau sărbătoare.

# Secțiunea 2

**Utilizatorii sistemului**

1. Utilizatorii sistemului, în conformitate cu principalii participanți la procesul de achiziții, se împart în următoarele categorii:
2. Utilizatorii publici *–* categoria de utilizatori, care nu au trecut procedura de autentificare în Sistemul MTender. Această categorie de utilizatori are posibilitatea de a vizualiza obiectele informaționale fără a le putea modifica;
3. Utilizatorii autorității contractante/entității contractante *–* categoria de utilizatori, care au acces la funcționalitățile destinate planificării și organizării procedurii de achiziții, precum: specificarea planurilor de achiziții, anunțarea și desfășurarea procedurilor de achiziții, realizarea proceselor de evaluare a ofertelor, selectare și desemnare a câștigătorului, încheierea contractului, gestionarea și monitorizarea contractului, finalizarea procedurii de achiziții, generarea documentelor organizatorice, administrarea cataloagelor electronice, etc.;
4. Utilizatorii operatorilor economici *–* categoria de utilizatori, care au acces la funcționalitățile destinate participării la procedurile de achiziție, precum: înaintarea întrebărilor/clarificărilor, formarea și depunerea ofertelor, depunerea contestațiilor, participarea la licitația electronică, vizualizarea și semnarea contractului;
5. Utilizatorii AAP *–* categoria de utilizatori, care au acces la funcționalități specifice, precum administrarea anunțurilor de intenție, anunțurilor de participare, anunțurile de modificare a procedurilor de achiziții publice, administrarea Listelor agenților economici interziși, generarea rapoartelor statistice specifice, conlucrarea în procesul de soluționare a contestațiilor, etc.;
6. Utilizatorii Agenției Naționale pentru Soluționarea Contestațiilor *–* categoria de utilizatori, care au acces la funcționalități specifice destinate lucrului cu contestațiile depuse de participanții le procedurile de achiziții publice, precum: înregistrarea, examinarea, soluționarea contestațiilor și accesarea informației statistice privind contestațiile;
7. Utilizatorii instituțiilor de monitorizare și control *–* categoria de utilizatori, care au acces la funcționalitățile specifice destinate generării rapoartelor statistice avansate privind procedurile de achiziții publice, dar și alte instrumente de monitorizare și control, precum indicatori cheie, indicatori de risc, etc.;
8. Utilizatorii Organelor pentru Achiziții Centralizate *–* categoria de utilizatori, care au acces la funcționalități specifice destinate planificării, organizării și desfășurării achizițiilor centralizate;
9. Administratorul de sistem *–* categoria de utilizatori autentificați, care sunt angajați ai Deținătorului responsabili de administrarea Sistemului MTender. Această categorie de utilizatori deține acces avansat asupra funcționalităților sistemului, administrează clasificatoarele sistemului, dispune de instrumente de configurare și ajustare a sistemului și funcționalităților acestuia, administrează bazele de date și monitorizează activitatea utilizatorilor și a sistemului în general.
10. Fiecare categorie de utilizatori deține 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 organizații.
11. Un utilizator în cadrul sistemului poate reprezenta mai multe organizații. În acest scop la autentificare, utilizatorul va specifica organizația din numele căreia va lucra în sesiunea curentă.
12. Utilizatorul nu poate activa concomitent pentru mai multe organizații.

# Secțiunea 3

# Înregistrarea utilizatorilor în cadrul sistemului

1. Procesul de înregistrare a utilizatorilor se efectuează conform regulilor stabilite de Deținător, în conformitate cu condițiile pct.43 a Hotărârii 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.
2. Înregistrarea utilizatorului supervizor al organizației se efectuează de către administratorul de sistem, la cererea semnată de către conducătorul sau persoana autorizată a organizației solicitante.
3. Cererea de solicitare va conține cel puțin următoarea informație:
4. Data emiterii documentului;
5. Denumirea organizației;
6. Codul unic de identificare a organizației;
7. Numele prenumele conducătorului organizației;
8. Datele de contact ale organizației (adresa, telefon, email, persoane de contact);
9. Solicitarea privind alocarea rolului în cadrul sistemului;
10. Numele, Prenumele utilizatorului;
11. Funcția în cadrul organizației;
12. Codul unic de identificare a utilizatorului;
13. Acordul tuturor persoanelor menționate în cerere privind acceptul de prelucrare a datelor cu caracter personal;
14. Semnătura conducătorului organizației și ștampila umedă, dacă e cazul.
15. Înregistrarea/confirmarea utilizatorilor subordonați supervizorului se efectuează de către administratorul de sistem la cererea conducătorului organizației sau de către utilizatorul supervizor al organizației respective.
16. La înregistrarea în cadrul sistemului, fiecărui utilizator i se atribuie un identificator unic și rolul de care depinde dreptul de acces la obiectele informaționale, iar dacă este cazul, credențialele temporare, care urmează a fi modificate la prima accesare a sistemului de către utilizator.
17. Dreptul de acces a utilizatorilor la Sistem se revocă în următoarele cazuri:
18. în baza cererii/solicitării conducătorului organizației;
19. încetării raporturilor/relațiilor de muncă a utilizatorilor;
20. modificării raporturilor/relațiilor de muncă, când noile responsabilități nu presupun accesul la datele Sistemului;
21. încălcării obligațiilor contractuale de utilizare a Sistemului;
22. constatării de încălcare a securității informaționale de către utilizatorul Sistemului.

# Secțiunea 4

**Autentificarea și autorizarea utilizatorilor în cadrul sistemului**

1. Autorizarea utilizatorilor se va produce în conformitate cu nivelul de acces stabilit și utilizatorii vor avea posibilitate să acceseze funcționalitățile sau informațiile disponibile, în corespundere cu nivelul de acces (spre exemplu, utilizatorul care se autorizează în sistemul MTender în calitate de operator economic nu va avea posibilitate să acceseze funcționalitățile pentru organizarea procedurii de achiziție).
2. Procesul de autentificare și autorizare se va realiza pe doua căi, și anume:
3. autentificarea și autorizarea prin intermediul PEA: PEA vor asigura autentificarea electronică a utilizatorilor autorităților contractante, entităților contractante și operatorilor economici;
4. autentificarea și autorizarea prin intermediul web portalului mtender.gov.md. În vederea accesării cabinetelor amplasate pe UCD, web portalul mtener.gov.md va asigura autentificarea directă a utilizatorilor specifici ai AAP, Agenției Naționale pentru Soluționarea Contestațiilor, organelor de supraveghere și control, centrelor pentru achiziții centralizate.
5. La baza mecanismului de autentificare în cadrul UCD va sta serviciul guvernamental de autentificare și control al accesului MPass.
6. În cadrul PEA, pe lângă autentificarea prin serviciul guvernamental de autentificare și control al accesului MPass, se va asigura minimum un mecanism adițional de autentificare accesibil pentru utilizatorii nerezidenți.
7. Procedura de acordare a accesului (conectare) a PEA la UCD se va realiza în conformitate cu Regulamentul privind acreditarea PEA.

#

**Capitolul V**

# Interacțiunea cu alte sisteme informaționale

1. În vederea asigurării formării corecte a resursei informaționale, a calității datelor și sporirea eficienței proceselor de organizare și desfășurare a achizițiilor, se asigură interacțiunea și schimbul de date cu următoarele resurse informaționale:
2. Registrul de stat al populației– pentru verificarea informației privind persoana fizică la înregistrarea utilizatorului în cadrul sistemului;
3. Registrul de stat al unităților de drept – pentru verificarea informației privind persoana juridică la înregistrarea utilizatorului în cadrul sistemului, diferite etape de desfășurare a procedurii de achiziție, ținerea listelor operatorilor economici calificați/interziși, perfectarea contractului de achiziție, etc.;
4. Sistemele informaționale ale Serviciului Fiscal de Stat – pentru verificarea obligațiilor fiscale ofertantului în procesul desfășurării procedurii de achiziții publice;
5. Sistemul informațional trezorerial – pentru schimbul de informație privind disponibilitatea alocațiilor bugetare, informației privind datele contractului de achiziție și a datelor privind executarea contractului și a plăților efectuate;
6. Sistemul Informațional Automatizat pentru Gestionarea și Emiterea Actelor Permisive – pentru verificarea informației privind licențele și alte acte permisive, solicitate de către autoritatea contractantă/entitatea contractantă în cadrul procedurii de achiziție;
7. Registrul informației criminalistice și criminologice – pentru consultarea informației criminalistice a unei persoane fizice sau juridice;
8. Serviciile electronice guvernamentale, și anume:
9. eFactura – pentru recepționarea datelor privind facturile electronice emise în cadrul contractelor de achiziție;
10. MPass – pentru autentificarea și controlul accesului în cadrul Sistemului, utilizând diferite mecanisme de autentificare, precum: semnătura mobilă, semnătura electronică, buletinul de identitate electronic, numele de utilizator și parola;
11. MSign – pentru semnarea documentelor electronice. Utilizat în special la depunerea ofertelor și semnarea online a contractelor de achiziție;
12. MNotify – pentru transmiterea notificărilor în cadrul Sistemului, în special pentru expedierea notificărilor către operatorii economici și autoritățile/entitățile contractante, precum și altor utilizatori ai sistemului;
13. MConnect – Platforma guvernamentală de schimb de date și interoperabilitate utilizată pentru organizarea conexiunii cu registrele și sistemele informaționale de stat;
14. MCloud – Infrastructură informațională guvernamentală comună, care funcționează în baza tehnologiei de “cloud computing” utilizată pentru găzduirea sistemului;
15. MLog – ca instrument securizat și flexibil de jurnalizare și audit, care va asigura evidența operațiunilor (evenimentelor), produse în sistemul MTender;
16. MPay – pentru efectuarea plăților electronice.

#

**Capitolul VI**

# Cerințe privind informația plasată în Sistemul MTender

1. Toată informația prezentată în cadrul sistemului MTender are caracter oficial și reprezintă rezultatul deciziei instituției pe care o reprezintă utilizatorul, care a plasat informația respectivă.
2. Accesul la informația din cadrul sistemului MTender va fi asigurat în măsura prevăzută de Legea nr.131 din 03.07.2015 privind achizițiile publice și actele legislative secundare, care reglementează desfășurarea procedurilor de achiziție publică și prezentul Regulament.
3. Accesarea și utilizarea datelor registrului, precum și a funcționalităților este gratuită pentru utilizatorii Autorității contractante;
4. Autoritatea contractantă, participanții la procedura de achiziție, precum și alte instituții-utilizatori ai sistemului poartă răspundere de faptul că informația specificată în cadrul sistemului este actuală și corectă la momentul plasării acesteia, inclusiv cea prezentată în cadrul sistemului în formă de fișiere anexate.
5. Deținătorul MTender, precum și operatorii PEA, vor fi înregistrați în Registrul Operatorilor de Date cu Caracter Personal, gestionat de Centrul Național pentru Protecția Datelor cu Caracter Personal, iar prelucrarea datelor cu caracter personal se va realiza în conformitate cu prevederile Legii nr.133 din 08.07.2011 privind protecția datelor cu caracter personal și 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.
6. În cazul dacă sistemul MTender nu oferă un flux de lucru automatizat destinat procesului de pregătire și coordonare a informației și documentelor care urmează a fi plasate în cadrul sistemului MTender, acesta va avea loc în conformitate cu regulile interne ale organizației și în conformitate cu legislația în vigoare, ulterior informația va fi plasată în sistem.
7. Persoana responsabilă a autorității contractante organizează și controlează procesul de pregătire a informației în cadrul instituției, plasarea și actualizarea informației în cadrul sistemului MTender în conformitate cu prevederile legale.
8. Plasarea informației în sistemul MTender se realizează numai cu sancțiunea conducătorului instituției sau persoanei responsabile.
9. Temei pentru plasarea/actualizarea informației în cadrul sistemului MTender poate fi:
10. indicația directă a conducătorului instituției sau a persoanei responsabile;
11. necesitate dictată de normele legale;
12. apariția unor noi informații;
13. Informația se consideră plasată în cadrul sistemului MTender din momentul publicării acesteia pe portalul mtender.gov.md și/sau primirea recipisei de recepționare (de exemplu în cazul depunerii ofertelor);
14. Autoritatea contractantă/Entitatea contractantă nu trebuie să poată modifica versiunea inițială a dosarului procedurii de achiziție sau eventualele anexe după lansarea procedurii de achiziție. În cazul în care autoritatea trebuie să clarifice orice aspect al dosarului procedurii de achiziție, acest lucru va fi realizat printr-un amendament, care definește în mod clar ce s-a schimbat, dar nu înlocuirea documentelor existente. Totodată, versiunile precedente ar trebui păstrate și fiecare versiune nouă ar trebui să fie evidențiată pentru utilizatori. Operatorii economici înregistrați vor primi notificări privind modificările aplicate dosarului procedurii de achiziție. Astfel de modificări ar trebui să fie documentate/publicate pe PEA pentru a asigura transparența și accesul la date a operatorilor economici.

#

**Capitolul VII**

# Cerințe minime de securitate și operare

# Secțiunea 1

**Cerințe generale**

1. Atât operatorul UCD, cât și operatorii PEA, trebuie să aprobe un program de securitate cibernetică conceput pentru a proteja confidențialitatea, integritatea și disponibilitatea sistemului MTender. Programul se va baza pe evaluarea riscurilor organizației și va fi conceput pentru a îndeplini următoarele funcții principale de securitate cibernetică:
2. identificarea și evaluarea riscurilor de securitate cibernetică interne și externe, care ar putea amenința securitatea sau integritatea sistemului MTender;
3. reglementarea utilizării infrastructurii defensive;
4. implementarea politicilor și procedurilor pentru protejarea sistemului MTender și a informațiilor stocate în sistem împotriva accesului neautorizat, sau a altor acțiuni de rea intenție;
5. detectarea evenimentelor de securitate cibernetică;
6. să răspundă evenimentelor cibernetice identificate sau detectate pentru a atenua orice efecte negative;
7. recuperarea de pe urma evenimentelor cibernetice și restabilirea funcțiilor și serviciilor normale;
8. îndeplinirea obligațiilor de raportare aplicabile în domeniul securității cibernetice.
9. Operatorul UCD, cât și operatorii PEA, vor menține o politică de securitate cibernetică în formă scrisă, aprobată de conducerea organizației, care stabilește procedurile de protejare a sistemului MTender, precum și a datelor stocate. Politica privind securitatea informatică se bazează pe evaluarea riscurilor entității și va adresa următoarelor aspecte:
10. securitatea informațiilor;
11. administrarea și clasificarea datelor;
12. inventarierea activelor și gestionarea dispozitivelor;
13. controlul accesului și managementul identității;
14. asigurarea continuității de funcționare și planificarea recuperării în caz de dezastru;
15. exploatarea și disponibilitatea sistemelor;
16. securitatea sistemelor și a rețelelor;
17. monitorizarea sistemelor și a rețelelor;
18. dezvoltarea sistemelor și aplicațiilor prin prisma asigurării calității;
19. asigurarea securității fizice;
20. confidențialitatea datelor clienților;
21. utilizarea serviciilor subcontractate;
22. evaluarea riscurilor;
23. intervențiile în caz de incidente.
24. Operatorii UCD și PEA vor efectua evaluări periodice ale riscurilor legate de sistemul MTender. Evaluarea riscurilor va fi actualizată cu regularitate pentru a răspunde modificărilor survenite în cadrul sistemului MTender, datelor stocate sau business proceselor. Evaluarea riscurilor se va realiza în conformitate cu politicile și procedurile aprobate și va fi documentată, specificând:
25. criteriile de evaluare și clasificare a riscurilor sau amenințărilor de securitate cibernetică identificate;
26. criteriile de evaluare a gradului confidențialității, integrității, securității și disponibilității sistemului de achiziții electronice, inclusiv nivelul de corespundere a controalelor existente în contextul riscurilor identificate;
27. cerințele pentru descrierea modului în care riscurile identificate vor fi atenuate sau asumate în baza evaluării riscurilor și a modului în care programul de securitate cibernetică abordează riscurile.
28. Programul de securitate cibernetică include monitorizarea și testarea. Având la bază rezultatele evaluării riscurilor, monitorizarea și testarea au scopul să stabilească eficacitatea programului de securitate cibernetică. Monitorizarea și testarea includ monitorizarea continuă sau testarea periodică prin teste de penetrare și depistarea vulnerabilităților. Organizațiile urmează să prevadă și să desfășoare următoarele activități:
29. să comande testarea de penetrare a sistemului de achiziții electronice, înainte de lansarea versiunii noi și cel puțin o dată la doi ani, de către organizații terțe independente. Testarea urmează să fie bazată pe riscurile relevante identificate;
30. să evalueze anual gradul de vulnerabilitate, inclusiv scanări sistematice sau revizuiri ale sistemului MTender în vederea depistării și închiderii vulnerabilităților de securitate public cunoscute;
31. să implementeze politici, proceduri și controalelor bazate pe risc, menite să monitorizeze activitatea utilizatorilor înregistrați autorizați și să detecteze accesul neautorizat, utilizarea neconformă sau manipularea datelor de către acești utilizatori.
32. Anual, operatorii UCD și PEA vor prezenta către Posesorul sistemului un raport în scris pentru anul calendaristic precedent, care să confirme că sistemele lor au respectat cerințele stabilite. Fiecare organizație trebuie să mențină pentru o perioadă de minimum cinci ani, în scopuri de audit, toate înregistrările și datele întru susținerea acestui raport.
33. Operatorii UCD și PEA vor desemna o persoană calificată cu rolul de Responsabil de securitate informațională, care va răspunde de punerea în aplicare, supravegherea și aplicarea programului și politicii privind securitatea cibernetică.
34. Fiecare organizație trebuie să posede personal calificat în domeniul securității cibernetice și să utilizeze furnizorii de servicii sau terțele părți, care participă la procesele legate de exploatarea sistemului de achiziții electronice, ce corespund cerințelor de securitate cibernetică expuse în politica de securitate cibernetică a organizației.
35. În baza evaluării riscurilor, operatorii UCD și 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 informația din sistemul MTender.
36. Programul de securitate cibernetică a organizației va include proceduri scrise, instrucțiuni și standarde destinate să asigure utilizarea practicilor avansate de dezvoltare a aplicațiilor cu un nivel înalt de securitate, dar și procedurile de evaluare, apreciere sau testare a securității aplicațiilor dezvoltate de părți terțe utilizate în mediul tehnologic al organizației.
37. Organizațiile urmează să implementeze procese și proceduri riguroase pentru a asigura o pistă de audit suficient de detaliată a activităților desfășurate în cadrul sistemului MTender.
38. Atât operatorul UCD, cât și operatorii PEA, urmează să implementeze politici și proceduri riguroase de gestionare a riscurilor de securitate cibernetică de-a lungul întregului ciclu de viață al relațiilor cu părțile terțe. Aceste politici și proceduri se bazează pe evaluarea riscurilor și vor include în măsura aplicabilității următoarele aspecte:
39. identificarea și evaluarea riscurilor părților terțe față de organizație;
40. practicile minime de securitate cibernetică pe care trebuie să le întrunească furnizorii de servicii terțe, pentru ca organizația și accepte serviciile.
41. evaluarea periodică a furnizorilor de servicii terțe în baza riscului pe care îl prezintă și a respectării continue a practicilor de securitate cibernetică solicitate.
42. Operatorul UCD și operatorii PEA urmează să implementeze planuri și instrucțiuni eficiente de reacție la incidente, precum și mecanisme eficiente de notificare a Posesorului sau organului desemnat de acesta privind evenimentele legate de securitatea cibernetică. Programul de securitate cibernetică a organizației va include un plan scris și aprobat de răspuns la incidentele legate de securitate cibernetică, conceput să reacționeze prompt și să restabilească sistemul în urma oricărui incident de securitate cibernetică, care afectează confidențialitatea, integritatea sau disponibilitatea sistemului MTender. Un astfel de plan de răspuns la incidente va aborda următoarele aspecte:
43. procesele interne de reacție la un eveniment legat de securitatea cibernetică;
44. obiectivele planului de răspuns la incidente;
45. definirea unor roluri clare, responsabilități și nivelurile de luare a deciziilor;
46. comunicările interne și externe, precum și schimbul de informații;
47. identificarea cerințelor pentru remedierea oricăror deficiențe identificate;
48. documentarea și raportarea evenimentelor de securitate cibernetică, precum și a activităților legate de intervențiile în caz de incidente;
49. evaluarea și revizuirea planului de reacție la incidente în urma unui eveniment de securitate cibernetică;
50. organizația trebuie să notifice Posesorul sau organul desemnat de acesta, despre un eveniment de securitate cibernetică în cel mai scurt timp posibil, dar nu mai târziu de 72 de ore de la stabilirea faptului de producere a unui eveniment de securitate cibernetică.

# Secțiunea 2

**Cerințe specifice**

1. Operatorii UCD și PEA vor fi înregistrați în Registrul Operatorilor de Date cu Caracter Personal, gestionat de Centrul Național pentru Protecția Datelor cu Caracter Personal. Organizația va prelucra datele cu caracter personal în conformitate cu prevederile Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal și 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.
2. Operatorul UCD și operatorii PEA se angajează să respecte cerințele cadrului legal al Republicii Moldova privind protecția tehnică și criptografică a informațiilor, precum și procedura și cerințele stabilite în documentația Sistemului.
3. Operatorul UCD și operatorii PEA trebuie să adapteze serviciile de securitate utilizate (identificare și autentificare, control al accesului, jurnalizare, criptare, etc.) în conformitate cu cerințele stabilite în documentația Sistemului.
4. Operatorul UCD și operatorii PEA vor acordă asistență comprehensivă autorităților publice (inclusiv autorităților de monitorizare și control) și reprezentanților acestora în cazul investigării cazurilor în ceea ce privește securitatea informațiilor.
5. Mijloacele de protecție criptografică a informației, inclusiv mijloacele de semnătură electronică utilizate pentru funcționare, trebuie să respecte pe deplin cerințele naționale în domeniul protecției criptografice a informației și utilizare a semnăturii electronice.
6. Anual, sau în cazul unor incidente legate de securitatea informațiilor, Operatorul UCD și operatorii PEA vor prezenta rapoarte privind securitatea informațiilor către Posesorul sistemului sau organul abilitat de acesta.
7. Operatorul UCD și operatorii PEA se angajează să protejeze confidențialitatea utilizatorilor lor. Colectarea oricăror informații personale sau de afaceri nu va fi efectuată decât dacă utilizatorul furnizează informația către organizație în mod voluntar și conștient în timpul utilizării sistemului.
8. Atunci când utilizatorul alege să furnizeze informații personale sau de afaceri pentru a efectua o tranzacție online, informația va fi utilizată doar pentru a efectua tranzacția online specifică, solicitată de utilizator. Pentru fiecare tranzacție on-line, se va solicita doar cantitatea minimă de informații personale și de afaceri necesare procesării tranzacției respective.
9. Când utilizatorul vizitează sistemul pentru a naviga, citi pagini sau descărca informații, doar următoarele informații vor fi colectate automat și stocate, fără a fi solicitate direct de la utilizator:
10. numele de domeniu Internet și adresa IP de la care utilizatorul accesează sistemul;
11. data și ora în care utilizatorul accesează sistemul;
12. paginile vizitate;
13. în caz dacă utilizatorul accesează sistemul de pe un alt site Web, adresa site-ului respectiv.
14. Informațiile personale pot fi transmise, partajate, vândute sau transferate către o terță parte doar cu acceptul utilizatorului, cu excepția cazurilor interzise de Lege în mod explicit. Revizuirea, actualizarea și corectarea oricăror informații personale sau de afaceri poate fi efectuată direct în sistemul de achiziții publice electronice de către utilizatorul respectiv.
15. Operatorul UCD și operatorii PEA trebuie să implementeze măsuri extensive de securitate pentru protejarea împotriva pierderii, utilizării incorecte și/sau modificării neautorizate a informațiilor stocate.
16. Sistemele/subsistemele de achiziții electronice operate vor furniza resurse tehnologice de securitate adecvate pentru a asigura confidențialitatea și integritatea datelor prelucrate, astfel încât nici o persoană să nu aibă acces la datele și informațiile care nu sunt destinate lui, și în special la datele incluse în documentele de ofertă prezentate de candidați sau ofertanți, înainte de termenele limită stabilite.
17. Resursele de securitate menționate în paragraful anterior trebuie să permită detectarea și înregistrarea promptă a oricăror încălcări ale interdicției de acces.
18. Operatorul UCD și operatorii PEA trebuie să se asigure că documentele electronice, care includ oferta sau propunerea, pot fi criptate, precum și să asigure semnarea acestora pe cale electronică.
19. Operatorii UCD și PEA vor asigura verificarea că documentele electronice, care constituie oferta și contractele de achiziții publice, conțin semnături electronice valide, aplicate pe acestea.
20. Operatorul UCD și operatorii PEA trebuie să implementeze sisteme de securitate, care să permită identificarea codului malițios ce ar putea accesa și/sau deteriora datele stocate, sistemele de recepție, prelucrare și stocare a datelor sau componente ale acestora.
21. Resursele electronice utilizate de operatorul UCD și de operatorii PEA vor asigura că autoritatea contractantă și ceilalți utilizatori se pot familiariza cu conținutul ofertelor, sau părți ale acesteia, cererii de participare sau soluțiilor doar după expirarea termenelor limită pentru depunerea acestora.
22. Operatorul UCD și operatorii PEA trebuie să opereze un sistem care să permită determinarea sursei de transmitere a datelor, precum și identificarea entității sau a persoanei fizice care le-a transmis, astfel încât transmițătorul de date să nu poată respinge faptul că a remis informația respectivă sau data și/sau timpul de transmitere al acesteia.
23. Operatorul UCD și operatorii PEA trebuie să implementeze mecanisme, care să asigure că datele remise nu au fost modificate în timpul sau după transmiterea acestora.
24. Data și ora, la care a fost depusă oferta, se stabilește în funcție de momentul în care ofertantul finalizează transmiterea tuturor documentelor, care constituie oferta la etapa de depunere a ofertelor în cadrul procedurii de achiziție.
25. „Depunerea ofertei, a cererii sau a soluției” semnifică momentul, în care ofertantul sau candidatul accesează funcționalitățile pentru transmiterea setului de documente ce constituie oferta și, ulterior, confirmă finalizarea depunerii ofertei în sistem.
26. PEA urmează să asigure determinarea exactă a datei și orei de transmitere a informației menționate în aliniatul anterior. Informația privind data și ora transmiterii urmează să fie încorporată în ofertă la momentul acceptării acesteia de către sistem.
27. Informația privind recepționarea datelor menționate în aliniatul precedent vor fi comunicate părților interesate imediat după recepționare.
28. Eșecul recepționării de către sistem a datelor și documentelor atrage după sine faptul ca oferta, cererea sau soluția respectivă, va fi considerată ca nefiind prezentată. În acest caz, partea interesată trebuie să fie informată imediat despre acest fapt.
29. Operatorul UCD și operatorii PEA trebuie să implementeze mecanisme, care să asigure confidențialitatea ofertanților sau a candidaților până la expirarea termenului limită de depunere a ofertelor definit de autoritatea contractantă în cadrul procedurii de achiziție respective.
30. Operatorul UCD și operatorii PEA trebuie să documenteze (colecteze informație de serviciu) etapele de organizare a unei proceduri de achiziții publice pe cale electronică, care să permită furnizarea de informații fiabile și care reflectă corect situația prezentă sau trecută. Operatorul UCD și operatorii PEA trebuie să asigure din punct de vedere tehnic și funcțional respectarea acestei obligații, astfel încât documentele să poată fi păstrate în forma lor originală și stocate în mod corespunzător, precum și să asigure o înregistrare a tuturor evenimentelor legate de procedura de achiziție și accesarea documentelor, care ar putea ulterior servi ca dovadă în cazul unui litigiu.
31. Sistemul trebuie să permită identificarea cel puțin a următoarelor informații:
32. entitatea și/sau utilizatorul, care a inițiat operația;
33. timpul exact al inițierii operației;
34. documentele prezentate/accesate în cadrul operației, precum și entitatea și/sau persoana care le-a trimis/accesat;
35. rezultatul operației;
36. durata comunicării în cadrul acestor evenimente.
37. Informația menționată urmează să fie actualizată în permanență, inclusiv informația privind cronologia plasării și accesării documentației standard și cea privind atribuirea contractului.
38. Informația legată de procedura de achiziție, inclusiv documentele și informația de serviciu urmează a fi păstrată în conformitate cu Legea nr.131 din 03.07.2015 privind achizițiile publice, împreună cu aplicațiile și tehnologiile, care permit citirea acestei informații, până la expirarea termenului de păstrare. La expirarea termenului de păstrare, informația este arhivată, termenul de păstrare a arhivei fiind nelimitat.
39. Operatorii UCD și PEA asigură înregistrarea în sistem a tuturor ofertelor, inclusiv plasate incorect, chiar dacă acestea ulterior nu vor fi luate în considerare (vor fi descalificate) în cadrul următoarelor etape ale procedurii de achiziție.
40. Pentru fiecare procedură de achiziție, operatorii UCD și PEA asigură accesul tuturor părților interesate către: datele și documentele procedurii de achiziții electronice, inclusiv versiunile precedente; precizările și modificările operate de către organizatorul procedurii de achiziție; deciziile organizatorului de a modifica termenii de desfășurare a procedurii de achiziție; erorile și omisiunile identificate și raportate de părțile interesate, precum și faptul despre acceptarea sau respingerea acestora de către organizatorul procedurii de achiziții; comunicarea care a avut loc înainte de depunerea ofertelor, încheierea contractului sau solicitarea de informație suplimentară.
41. Ca urmare a deschiderii ofertelor de către grupul de lucru, operatorul UCD și operatorii PEA trebuie să asigure că toate părțile interesate au acces la toate ofertele depuse, clarificările privind ofertele depuse de ofertanții respectivi, documentele de calificare prezentate de ofertantul descalificat și câștigător, precum și toate celelalte acte sau formalități de procedură referitoare la etapa următoare depunerii ofertelor.
42. PEA trebuie să permită părților interesate să încarce toată oferta odată sau pe părți, până la data și ora limită de depunere a ofertelor, stabilită de autoritatea contractantă.
43. Încărcarea ofertelor, menționate în pct.95, se efectuează în zona rezervată exclusiv ofertantului respectiv în cadrul procedurii de achiziție în cauză.
44. PEA urmează să pună la dispoziția ofertantului funcționalitățile și/sau aplicațiile software, care îi permit să cripteze și semneze digital fișierele ofertei, local, pe propriul computer sau în sistem în momentul încărcării.
45. PEA poate permite părților interesate să încarce pe părți fișierele ofertei fără a fi nevoie de criptare și semnătura electronică, precum și să modifice documentele încărcate în orice moment, până la depunerea finală a ofertei.
46. Depunerea finală a ofertei este precedată în mod obligatoriu de semnarea electronică și criptarea acesteia.
47. Formularele ofertei, precum și orice alte formulare, care urmează a fi completate ca parte a procedurii de achiziție trebuie puse la dispoziția părții interesate atât prin oferirea unor formulare online, cât și prin oferirea spre descărcare pe calculatorul său a unui fișier cu conținut structurat (de exemplu XML), în scopul completării și încărcării ulterioare în sistem.
48. UCD și PEA vor asigura faptul că fișierele, menționate în pct.100, pot fi încărcate ulterior doar în cadrul procedurii din care au fost descărcate și de autoritatea pentru care au fost generate.
49. Ofertantul trebuie să aibă posibilitatea retragerii ofertei după depunerea finală a ofertei, dar până la data limită de depunere a ofertelor. Totodată, ofertantul poate modifica conținutul ofertei sau substitui oferta în întregime și după depunerea finală a ofertei, până la data și ora limită de depunere a ofertelor.
50. Prezentarea unei oferte este considerată finalizată atunci când ofertantul confirmă formal acest fapt, după finalizarea încărcării tuturor fișierelor și formularelor corespunzătoare, semnate și criptate în timp util.
51. După depunerea ofertelor, ofertantul primește o recipisă electronică, care atestă prezentarea ofertei, înregistrând identitatea autorității contractante, procedura de achiziții, lotul (dacă este cazul), ofertantul, data și ora depunerii ofertei.
52. Recipisa trebuie să fie disponibilă în zona rezervată exclusiv ofertantului, dublată printr-o copie trimisă la emailul ofertantului.
53. PEA asociază recipisa electronică cu oferta depusă, care devine parte integrantă a acesteia și, ca atare, este pusă la dispoziția grupului de lucru pentru organizarea procedurii de achiziție.
54. PEA va asigura că ofertanții pot consulta în orice moment ofertele depuse la procedura de achiziție, după data deschiderii ofertelor de către grupul de lucru.
55. La expirarea termenului limită de depunere a ofertelor, UCD și PEA se angajează să furnizeze grupului de lucru pentru organizarea procedurii de achiziție, toate ofertele depuse până la data și ora stabilită în documentația de atribuire și să ofere instrumente de deschidere a acestora, indiferent de apariția ulterioara a motivelor respingerii ofertelor.
56. Ofertele transmise în cadrul procedurii de achiziție prin intermediul PEA nu pot fi făcute publice înainte de expirarea termenului limită de depunere a ofertelor și înaintea deschiderii lor de către grupul de lucru pentru organizarea procedurii de achiziție în cauză.
57. Accesarea ofertelor de către membrii grupului de lucru în vederea deschiderii acestora se efectuează cu participarea și acceptul a minimum trei membri ai grupului de lucru.
58. Informația transmisă de către o PEA către UCD are destinația de a fi stocată și urmează să fie într-un format, capabil să suporte procesarea automată.
59. Pentru ca procesarea automată să se desfășoare fără erori, datele transmise urmează a fi codate corespunzător.
60. Codarea utilizată trebuie să fie sincronizată complet cu UCD, astfel încât să nu existe rupturi în identificarea corectă a obiectelor informaționale și a procedurilor la care se referă informațiile transmise.
61. Normele și cerințele privind interconectarea cu UCD vor fi descrise în documentația sistemului MTender.
62. Toate documentele ofertelor încărcate, precum și contractele rezultate în urma procedurii de achiziție, urmează a fi semnate digital, utilizând semnătura electronică avansat calificată.
63. În cazul, în care certificatul digital nu poate lega direct semnatarul de poziția și autoritatea pe care o reprezintă, partea interesată urmează să prezinte un document electronic oficial, care să indice legătura dintre persoana semnatară și autoritatea pe care o reprezintă.
64. Atât operatorul UCD, cât și operatorii PEA, urmează să asigure procesul de autorizare și controlul accesului utilizatorilor la serviciile pe care le prestează.
65. Orice accesare a serviciilor, aplicațiilor sau documente se va înregistra în jurnalele de evidență a accesului.
66. Operatorul UCD și operatorii PEA vor utiliza mecanisme de protecție și recuperare a informațiilor asociate cu procedurile de achiziție publică electronică.
67. Operatorul UCD și operatorii PEA urmează să asigure mecanisme, care să protejeze confidențialitatea informațiilor și să prevină accesul neautorizat la acestea.
68. Operatorul UCD și operatorii PEA trebuie să se asigure că informațiile sunt disponibile pentru utilizatori exclusiv în funcție de nivelul de acces al acestora.
69. Operatorul UCD și operatorii PEA vor pune la dispoziție tehnologii, care să permită efectuarea auditului tehnic și de conformitate.
70. Operatorul UCD și operatorii PEA vor garanta mecanisme de securitate fizică și logică pentru a proteja serviciile și informațiile stocate în sistem.
71. Toate serviciile trebuie să fie sincronizate cu NTP (Network Time Protocol), utilizând standardul de timp UTC (Coordinated Universal Time).
72. Toate informațiile și documentele publicate în sistemul MTender, în conformitate cu legislația în vigoare, sunt deschise și disponibile publicului. Documentele pot fi considerate confidențiale numai în cazuri excepționale, la cererea părții interesate, și în conformitate cu legislația relevantă, cum ar fi Legea nr. 171-XIII din 06.07.1994 privind secretul comercial sau alte acte normative relevante.
73. Prelucrarea și publicarea datelor cu caracter personal se va realiza în conformitate cu prevederile Legii nr.133 din 08.07.2011 privind protecția datelor cu caracter personal.

#

**Capitolul VIII**

# Controlul și responsabilitatea

1. Sistemul este supus unui control intern și extern. Controlul intern este efectuat de Posesor, iar controlul extern - de autoritatea administrației publice autorizată.
2. La efectuarea controlului intern sau extern, organul de control alcătuiește actul în două exemplare, din care unul este direcționat către Deținător, iar altul rămâne la organul de control. Deținătorul este obligat să ia măsuri pentru lichidarea încălcărilor identificate și să informeze despre aceasta organul de control.
3. Pentru organizarea controlului de funcționare a Sistemului este responsabil Deținătorul, care este obligat să asigure dreptul de acces la Registru și mijloacele de ținere a acestuia, precum și în încăperile în care se află mijloacele hardware, utilizate pentru aceasta.
4. Angajații responsabili pentru asigurarea funcționării Sistemului și înregistrării datelor poartă responsabilitatea personală în conformitate cu legislația în vigoare pentru autenticitatea, fiabilitatea, integritatea informației, precum și pentru păstrarea/stocarea și utilizarea acesteia.
5. Toți subiecții cu acces la Registru, precum și destinatarul informației, cu conținut de date personale, sînt responsabili pentru dezvăluirea, transferarea către o terță parte și utilizarea în scopuri personale a informației conform legislației în vigoare.
6. Păstrarea Registrului este asigurată de Deținător, până la luarea deciziei privind lichidarea sau transferul acestuia către un alt Deținător. În cazul lichidării Registrului, toate datele conținute în acesta, sunt stocate în arhivă în conformitate cu legislația în vigoare.

#

**Capitolul IX**

# Dispoziții finale

1. Sistemul MTender este dezvoltat pentru a satisface standardele avansate privind datele deschise și permite accesul nerestricționat la informațiile privind achizițiile publice pentru toți cetățenii Republicii Moldova și organizațiile societății civile. Datorită acestei abordări, fiecare cetățean este capabil să folosească informațiile furnizate de sistemul MTender pentru a monitoriza modul în care Guvernul își îndeplinește obligațiile publice și dacă principiile concurenței loiale, precum și raportul valoare/preț în achizițiile publice sunt respectate.
2. Sistemul MTender pune la dispoziția Societății Civile un portal de monitorizare dedicat pentru a oferi un feedback autorităților contractante, a discuta achizițiile specifice, a evalua calitatea livrării realizate în baza contractelor de achiziții publice și a iniția o cerere de verificare organelor de drept atunci cînd este necesar.