

GUVERNUL REPUBLICII MOLDOVA
HOTĂRÂRE nr. _____
din _____ 2026
Chișinău

**cu privire la aprobarea Regulamentului privind modul de ținere a resursei
informaționale formate de Subsistemul informațional „Management programe și
proiecte” aferentă Sistemului informațional național în domeniul eficienței energetice**

În temeiul art. 18 alin. (1) și art. 22 lit. c) și d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44) cu modificările ulterioare, art. 13¹ din Legea nr. 139/2018 cu privire la eficiența energetică, (Monitorul Oficial al Republicii Moldova, 2018, nr. 309-320 art. 476), cu modificările ulterioare, **Guvernul HOTĂRĂȘTE:**

1. Se instituie resursa informațională formată de Subsistemul informațional „Management programe și proiecte” aferentă Sistemului informațional național în domeniul eficienței energetice.

2. Se aprobă Regulamentul privind modul de ținere a resursei informaționale formate de Subsistemul informațional „Management programe și proiecte”, conform anexei.

3. Realizarea prevederilor prezentei hotărâri va fi asigurată din contul și în limitele mijloacelor alocate anual din bugetul de stat, precum și din alte surse, conform legislației.

4. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Energiei.

PRIM-MINISTRU

Alexandru MUNTEANU

Contrasemnează:

**Viceprim-ministru, ministrul Dezvoltării
Economice și Digitalizării**

Eugen OSMOCHEȘCU

Ministrul Energiei

Dorin JUNGHIETU

Ministrul Finanțelor

Andrian GAVRILIȚĂ

REGULAMENT
privind modul de ținere a resursei informaționale formate de Subsistemul
Informațional ”Management programe și proiecte”

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul privind modul de ținere a resursei informaționale formate de Subsistemul Informațional „Management programe și proiecte” (în continuare - *Regulament*) este elaborat în conformitate cu prevederile Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat și Conceptului Sistemului informațional național în domeniul eficienței energetice, aprobat prin Hotărârea Guvernului nr. 144/2025.

2. Regulamentul stabilește drepturile și obligațiile subiecților raporturilor juridice aferente creării și Ținerii resursei informaționale formată în vederea gestionării programelor și proiectelor de finanțare în domeniul eficienței energetice; modalitatea de ținere a resursei informaționale respective; procedura de înregistrare, modificare, completare și radiere a datelor; procedura de interacțiune cu furnizorii de date; măsurile privind asigurarea securității resursei informaționale în cadrul resursei informaționale.

3. Subsistemul Informațional „Management programe și proiecte” (în continuare – *Subsistem*) este o resursă informațională de stat, parte componentă a Sistemului informațional național în domeniul eficienței energetice, creată pentru gestionarea procesului de depunere a solicitărilor de finanțare a proiectelor în domeniul eficienței energetice, monitorizarea implementării și evaluarea post implementare, elaborarea documentelor și gestiunea datelor despre solicitanți, beneficiari de finanțare și proiecte în domeniul eficienței energetice.

4. Subsistemul are drept scop uniformizarea procesului de depunere a solicitărilor de finanțare a proiectelor în domeniul eficienței energetice și este destinat să ofere persoanelor fizice și juridice, precum și sectorului public, o platformă pentru depunerea și urmărirea solicitărilor de finanțare a proiectelor, prin intermediul mijloacelor electronice.

5. În sensul prezentului Regulament sunt utilizate noțiunile definite de articolul 3 Legea nr. 139/2018 cu privire la eficiența energetică, articolul 3 din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, HG nr. 144/2025 cu privire la aprobarea Conceptului Sistemului informațional național în domeniul eficienței energetice, precum și HG nr. 251/2024 cu privire la aprobarea Programului de finanțare „Fondul pentru eficiență energetică în sectorul rezidențial din Republica Moldova”.

Capitolul II
SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII,
EXPLOATĂRII ȘI UTILIZĂRII SUBSISTEMULUI INFORMAȚIONAL

6. Subiecții din domeniul creării, exploatării și al utilizării Subsistemului sunt:

- 6.1. proprietarul;
- 6.2. posesorul;
- 6.3. deținătorul;
- 6.4. utilizatorii.

7. Proprietarul Subsistemului este statul.

8. Posesorul Subsistemului este Ministerul Energiei.

9. Deținătorul Subsistemului este Instituția Publică Centrul Național pentru Energie Durabilă.

10. Utilizatorii Subsistemului sunt:

10.1. **Administrator** – persoană desemnată de deținător, responsabilă pentru administrarea Subsistemului.

10.2. **Specialist CNED** - în calitate de registrator și deținător al datelor, este persoana desemnată de deținător, responsabilă de verificarea solicitărilor și a documentației aferente, în raport cu criteriile și condițiile stabilite în cadrul programului sau proiectului.

10.3. **Decident CNED** - în calitate de registrator și deținător al datelor, este persoana desemnată de deținător, responsabilă de analizarea și evaluarea documentației depuse, precum și de luarea deciziilor privind acceptarea sau respingerea solicitărilor.

10.4. **Solicitant** – în calitate de furnizor al datelor, este persoana fizică sau juridică eligibilă să aplice pentru produsele de finanțare și să depună solicitări de finanțare în vederea implementării măsurilor de eficiență energetică. În cazul aprobării solicitării, solicitantul devine beneficiar al stimulentei financiare.

10.5. **Utilizator extern** – în calitate de furnizor al datelor, este persoana fizică sau juridică implicată în implementarea proiectelor, cu drepturi de gestionare a unor activități specializate aferente proiectelor în subsistem.

Capitolul III

DREPTURILE ȘI OBLIGAȚIILE SUBIECȚILOR ÎN DOMENIUL FORMĂRII ȘI EXPLOATĂRII SUBSISTEMULUI INFORMAȚIONAL

Secțiunea 1

Drepturile și obligațiile Posesorului

11. Posesorul este în drept:

11.1. să utilizeze informațiile disponibile în cadrul Subsistemului pentru îndeplinirea obligațiilor ce îi revin;

11.2. să exercite controlul intern asupra funcționării Subsistemului;

11.3. să verifice respectarea condițiilor juridice, organizatorice, de operare și exploatare a Subsistemului de către deținător și utilizatori, în limitele rolului atribuit;

11.4. să propună și să implementeze soluții de îmbunătățire și eficientizare a funcționării Subsistemului;

11.5. să autorizeze suspendarea activității Subsistemului în cazuri excepționale, incidente sau existența unor riscuri semnificative de securitate, în conformitate cu actele normative în vigoare, atunci când sunt afectate resurse informaționale de interes public.

12. Posesorul este obligat:

12.1. să elaboreze și/sau să aprobe, conform competențelor, cadrul normativ relevant Subsistemului;

12.2. să asigure cadrul juridic, organizatoric și financiar necesar pentru crearea, funcționarea, exploatarea, întreținerea și dezvoltarea Subsistemului;

12.3. să aprobe regulile și instrucțiunile referitoare la înscrierea, păstrarea, completarea, corectarea, eliminarea și utilizarea datelor, precum și la funcționarea generală a Subsistemului;

12.4. să stabilească planurile de dezvoltare ale Subsistemului;

12.5. să asigure dezvoltarea continuă a Subsistemului;

12.6. să monitorizeze și să evalueze performanțele Subsistemului;

12.7. să stabilească măsuri tehnice și organizatorice adecvate pentru protecția și securitatea Subsistemului.

Secțiunea 2

Drepturile și obligațiile Deținătorului

13. Deținătorul este în drept:

13.1. să utilizeze Subsistemul și să acceseze informațiile aferente în vederea îndeplinirii obligațiilor ce îi revin;

13.2. să suspende sau să revoce dreptul de acces la Subsistem pentru utilizatorii care nu respectă condițiile de securitate, regulile de exploatare, precum și standardele, normele și regulile general acceptate în domeniul securității informaționale;

13.3. să participe la procesul de creare, implementare și dezvoltare continuă a Subsistemului;

13.4. să înainteze posesorului propuneri pentru eficientizarea activității Subsistemului.

14. Deținătorul este obligat:

14.1. să asigure funcționarea Subsistemului în conformitate cu prevederile actelor normative aplicabile;

14.2. să monitorizeze utilizarea Subsistemului de către utilizatori;

14.3. să implementeze măsuri tehnice și organizatorice pentru protecția și securitatea Subsistemului;

14.4. să aplice măsuri organizatorice-tehnice pentru protejarea și asigurarea confidențialității informațiilor stocate în Subsistem, inclusiv împotriva distrugerii, modificării, blocării, copierii, răspândirii sau altor acțiuni ilicite, garantând un nivel adecvat de securitate în raport cu riscurile și natura datelor prelucrate;

14.5. să asigure atribuirea corectă a rolurilor și drepturilor de acces la interfețele Subsistemului;

14.6. să garanteze accesul securizat la informațiile conținute în Subsistem, precum și respectarea condițiilor de securitate și a regulilor de exploatare;

14.7. să organizeze activități de instruire și informare privind utilizarea Subsistemului;

14.8. să informeze utilizatorii cu privire la modificările condițiilor tehnice de funcționare ale Subsistemului;

14.9. să asigure funcționarea continuă a Subsistemului până la adoptarea unei decizii privind lichidarea acestuia, precum și arhivarea datelor, conform prevederilor legale

Secțiunea 3

Drepturile și obligațiile Administratorului

15. Administratorul este în drept:

15.1. să acceseze spațiul informațional personalizat al Subsistemului, în limitele rolului atribuit, cu utilizarea credențialelor proprii de autentificare, în vederea exercitării atribuțiilor de serviciu;

15.2. să vizualizeze integral informațiile din cadrul Subsistemului;

15.3. să genereze rapoarte și statistici privind proiectele de finanțare în domeniul eficienței energetice;

15.4. să formuleze și să înainteze propuneri de îmbunătățire și sporire a eficacității funcționării Subsistemului, în baza experienței practice și interacțiunii directe cu acesta.

16. Administratorul este obligat:

16.1. să administreze parametri tehnici și de business ai Subsistemului;

16.2. să configureze șabloanele solicitărilor de finanțare în cadrul Subsistemului;

16.3. să configureze apelurile de finanțare în cadrul Subsistemului;

16.4. să gestioneze rolurile și drepturile de acces ale utilizatorilor Subsistemului;

16.5. să administreze clasificatoarele și nomenclatoarele utilizate în Subsistem;

16.6. să gestioneze șabloanele de documente și rapoarte din cadrul Subsistemului;

16.7. să administreze conținutul paginilor Subsistemului;

16.8. să monitorizeze indicatorii tehnici de performanță ai Subsistemului;

16.9. să informeze în prealabil utilizatorii cu privire la intervențiile tehnice de mentenanță asupra Subsistemului;

16.10. să informeze utilizatorii cu privire la suspendarea activității Subsistemului în cazuri excepționale, incidente sau existența unor riscuri semnificative de securitate;

16.11. să acorde suport tehnic și să asigure instruirea utilizatorilor.

Secțiunea 4

Drepturile și obligațiile Specialistului CNED

17. Specialistul CNED este în drept:

17.1. să acceseze spațiul informațional personalizat al Subsistemului, în limitele rolului atribuit, cu utilizarea credențialelor proprii de autentificare, în vederea exercitării atribuțiilor de serviciu;

- 17.2. să utilizeze funcționalitățile Subsistemului, conform rolului și permisiunilor atribuite;
- 17.3. să acceseze datele din Subsistem, inclusiv ghiduri de utilizare, conform rolului atribuit;
- 17.4. să introducă, modifice și actualizeze datele în Subsistem, în vederea exercitării atribuțiilor de serviciu;
- 17.5. să genereze rapoarte și statistici privind solicitările analizate;
- 17.6. să solicite și să primească de la administrator ajutor metodologic și practic privind funcționarea Subsistemului;
- 17.7. să formuleze și să înainteze propuneri de îmbunătățire și sporire a eficacității funcționării Subsistemului, în baza experienței practice și interacțiunii directe cu acesta.
18. Specialistul CNED este obligat:
 - 18.1. să asigure veridicitatea, autenticitatea și integritatea datelor înregistrate în procesul de analiză a solicitărilor de finanțare;
 - 18.2. să analizeze solicitările depuse în cadrul Subsistemului, verificând conformitatea acestora cu criteriile de eligibilitate, documentele justificative și condițiile specifice aferente;
 - 18.3. să respecte condițiile de securitate și regulile de exploatare a Subsistemului;
 - 18.4. să utilizeze informațiile obținute din Subsistem exclusiv în scopurile prevăzute de cadrul legal și atribuțiile funcției;
 - 18.5. să informeze prompt deținătorul Subsistemului, despre orice încălcare a securității informaționale;
 - 18.6. să notifice deținătorul, în termen de o zi, cu privire la orice situație care împiedică îndeplinirea atribuțiilor și care poate afecta negativ exercitarea funcției.

Secțiunea 5

Drepturile și obligațiile Decidentului CNED

19. Decidentul CNED are dreptul:
 - 19.1. să acceseze spațiul informațional personalizat al Subsistemului, în limitele rolului atribuit, cu utilizarea credențialelor proprii de autentificare, în vederea exercitării atribuțiilor de serviciu;
 - 19.2. să utilizeze funcționalitățile Subsistemului, conform rolului și permisiunilor atribuite;
 - 19.3. să acceseze datele și documentația aferentă solicitărilor analizate;
 - 19.4. să introducă, modifice și actualizeze datele în Subsistem, în vederea exercitării atribuțiilor de serviciu;
 - 19.5. să ofere observații și recomandări în cadrul solicitărilor examinate, în limita competenței sale, în vederea facilitării circuitului decizional și de a asigura trasabilitatea procesului de analiză;
 - 19.6. să modifice statutul solicitărilor pentru finanțare în cadrul Subsistemului, în conformitate cu procedurile interne, în vederea facilitării circuitului decizional;
 - 19.7. să genereze rapoarte și statistici privind solicitările procesate;
 - 19.8. să vizualizeze alte informații din Subsistem, inclusiv ghiduri de utilizare, conform rolului atribuit;
 - 19.9. să solicite și să primească de la administrator ajutor metodologic și practic privind funcționarea Subsistemului;
 - 19.10. să formuleze și să înainteze propuneri de îmbunătățire și sporire a eficacității funcționării Subsistemului, în baza experienței practice și interacțiunii directe cu acesta.
20. Decidentul CNED este obligat:
 - 20.1. să asigure veridicitatea, autenticitatea și integritatea datelor înregistrate în procesul de analiză a solicitărilor de finanțare;
 - 20.2. să analizeze documentația și să adopte decizii în conformitate cu cadrul normativ aplicabil;
 - 20.3. să respecte condițiile de securitate și regulile de exploatare a Subsistemului;

20.4. să utilizeze informațiile obținute din Subsistem exclusiv în scopurile prevăzute de cadrul legal și atribuțiile funcției;

20.5. să informeze, în termen de o zi lucrătoare, atât verbal cât și în scris, deținătorul Subsistemului despre orice încălcare a securității informaționale;

20.6. să notifice deținătorul, în termen de o zi lucrătoare, cu privire la orice situație care împiedică îndeplinirea atribuțiilor și care poate afecta negativ exercitarea funcției;

20.7. să întreprindă toate măsurile necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal, în conformitate cu instrucțiunile deținătorului și cu prevederile legislației privind protecția datelor cu caracter personal;

20.8. să nu întreprindă anumite acțiuni în vederea obținerii accesului neautorizat la informații, indiferent de metodă.

Secțiunea 6

Drepturile și obligațiile Solicitantului

21. Solicitantul este în drept:

21.1. să acceseze spațiul informațional personalizat al Subsistemului, în limitele rolului atribuit, cu utilizarea credențialelor proprii de autentificare;

21.2. să vizualizeze informațiile publice disponibile în cadrul Subsistemului, inclusiv ghidurile solicitantului, apelurile active de finanțare, condițiile de eligibilitate și alte documente informative;

21.3. să aplice la proiecte de finanțare lansate de către deținătorul Subsistemului, prin completarea și transmiterea solicitărilor aferente, conform procedurilor stabilite;

21.4. să furnizeze și să actualizeze datele și documentele atașate solicitărilor de finanțare în perioada de depunere, înainte de transmiterea finală;

21.5. să salveze solicitările în format de schiță, cu posibilitatea de a reveni ulterior pentru completare și transmitere până la expirarea termenului de depunere;

21.6. să primească notificări privind statutul solicitărilor de finanțare depuse și să le vizualizeze în Subsistem, precum și în cadrul Portalului guvernamental integrat EVO;

21.7. să retragă solicitările de finanțare depuse, în perioada de depunere, în cazul în care dorește modificarea acestora sau renunțarea la participare;

21.8. să solicite și să beneficieze de suport metodologic și practic din partea deținătorului Subsistemului, în vederea utilizării corecte și eficiente a funcționalităților disponibile;

21.9. să formuleze și să înainteze propuneri de îmbunătățire și sporire a eficacității funcționării Subsistemului, în baza experienței practice și interacțiunii directe cu acesta.

22. Solicitantul este obligat:

22.1. să asigure veridicitatea, autenticitatea și integritatea datelor furnizate în procesul de depunere a solicitărilor de finanțare;

22.2. să furnizeze date sau documente suplimentare în termenii stabiliți;

22.3. să protejeze accesul la contul său personal din Subsistem, respectând măsurile de securitate și regulile de exploatare în vigoare;

22.4. să utilizeze Subsistemul doar în scopurile stabilite de cadrul normativ;

22.5. să informeze fără întârziere, atât verbal cât și în scris, deținătorul Subsistemului cu privire la orice incident de securitate informatică sau neregulă constatată în utilizarea acestuia.

Secțiunea 7

Drepturile și obligațiile Utilizatorului extern

23. Utilizatorul extern este în drept:

23.1. să acceseze spațiul informațional personalizat al Subsistemului, în limitele rolului atribuit, cu utilizarea credențialelor proprii de autentificare;

23.2. să acceseze funcționalitățile Subsistemului necesare desfășurării activităților sale, conform drepturilor de acces atribuite;

23.3. să vizualizeze și să gestioneze documentația aferentă proiectelor pentru care are drepturi de acces;

23.4. să înainteze propuneri de modificare a cadrului normativ care reglementează funcționarea Subsistemului, în scopul îmbunătățirii proceselor și procedurilor, către deținătorul și/sau posesorul sistemului;

23.5. să solicite și să beneficieze de suport metodologic și asistență tehnică din partea deținătorului, pentru utilizarea eficientă a funcționalităților aferente rolului său;

23.6. să formuleze și să înainteze propuneri de îmbunătățire și sporire a eficacității funcționării Subsistemului, în baza experienței practice și interacțiunii directe cu acesta.

24. Utilizatorul extern este obligat:

24.1. să asigure veridicitatea, autenticitatea și integritatea informațiilor și documentelor furnizate în Subsistem;

24.2. să furnizeze date sau documente suplimentare în termenii stabiliți;

24.3. să protejeze accesul la contul său personal din Subsistem, respectând măsurile de securitate și regulile de exploatare în vigoare;

24.4. să utilizeze Subsistemul exclusiv în scopurile prevăzute de cadrul normativ și în limita atribuțiilor asociate rolului său;

24.5. să informeze fără întârziere, atât verbal cât și în scris, deținătorul Subsistemului cu privire la orice incident de securitate informatică sau neregulă constatată în utilizarea acestuia.

Capitolul IV

ÎNREGISTRAREA, MODIFICAREA ȘI

COMPLETAREA DATELOR ÎN SUBSISTEMUL INFORMAȚIONAL

25. Înregistrarea și gestionarea datelor în Subsistem se realizează în format electronic, în limba română.

26. Introducerea datelor/informațiilor/documentelor în Subsistem se va efectua în conformitate cu Ghidurile de utilizare a Subsistemului, prezentul Regulament, precum și alte acte normative emise de posesor, cu suportul deținătorului.

27. Subsistemul oferă funcționalități dedicate pentru generarea, actualizarea și administrarea registrelor electronice, menite să asigure transparența, trasabilitatea și evidența centralizată a datelor aferente procesului de finanțare. În acest sens, Subsistemul permite formarea următoarelor registre:

27.1. Registrul solicitărilor și beneficiarilor de finanțare - ce conține evidența solicitărilor de finanțare depuse, inclusiv datele aferente solicitantului, stadiul procesării solicitării, deciziile luate, precum și informații despre beneficiarii finali ai stimulentele financiare;

27.2. Registrul proiectelor finanțate în domeniul eficienței energetice - reflectă detalii despre proiectele aprobate pentru finanțare, valoarea și sursa finanțării, etapele de implementare, indicatorii de performanță, precum și alte informații relevante privind monitorizarea și raportarea progresului.

28. Toate înregistrările și modificările operate în Subsistem se păstrează în ordine cronologică, cu păstrarea nemijlocită a istoricului acestora. Modificarea sau completarea datelor nu afectează accesarea și vizualizarea informației.

29. Obiectele informaționale și scenariile de bază ale Subsistemului sunt descrise în HG nr. 144/2025 cu privire la aprobarea Conceptului Sistemului informațional național în domeniul eficienței energetice.

30. Înregistrarea datelor cu privire la obiectele informaționale în Subsistem se efectuează de către utilizatorii Subsistemului.

31. Orice modificare și completare a obiectelor informaționale, precum și scoaterea din evidență a acestora se efectuează doar în baza faptelor sau documentelor justificative, cu indicarea motivului ce confirmă veridicitatea acțiunilor efectuate.

Capitolul V
REGIMUL JURIDIC DE UTILIZARE A DATELOR
SUBSISTEMULUI INFORMAȚIONAL

32. Accesul la datele din Subsistem este condiționat de rolul utilizatorului și permisiunile de utilizare.

33. Accesul utilizatorilor la informația din Subsistem se realizează prin intermediul interfețelor web, prin autentificare și autorizarea prin MPass.

34. Se interzice utilizarea datelor din Subsistem în scopuri care contravin legii.

35. Datele cu caracter personal se utilizează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

36. Pentru modificarea datelor se impun următoarele restricții:

36.1. utilizatorii Subsistemului pot modifica datele doar în conformitate cu atribuțiile pe care le au în cadrul Subsistemului;

36.2. destinatarii datelor din Subsistem nu sunt în drept să modifice datele obținute din acesta, iar la utilizarea acestora sunt obligați să indice sursa lor;

36.3. alte categorii de subiecți sunt restricționați în utilizarea datelor din Subsistemul în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

37. Consumatorii datelor din sistem nu sunt în drept să modifice datele obținute, iar la utilizarea acestora sunt obligați să indice sursa lor.

38. Termenul de păstrare a datelor cu caracter personal în cadrul Subsistemului constituie 10 ani de la data primei înregistrări. După expirarea termenului, datele cu caracter personal vor fi depersonalizate și stocate exclusiv în scopuri statistice, de cercetare istorică sau științifică.

39. Datele recepționate din sistem nu pot fi transmise persoanelor terțe, dacă legislația sau tratatele internaționale la care Republica Moldova este parte nu prevăd altfel.

Capitolul VI
INTERACȚIUNEA SUBSISTEMULUI CU ALTE SISTEME
INFORMAȚIONALE

40. În scopul efectuării operațiunilor de precompletare, verificare, actualizare și validare a datelor, Subsistemul asigură interoperabilitatea și schimbul de date prin intermediul următoarelor resurse informaționale automatizate:

40.1. sistemul informațional automatizat „Registrul de stat al populației”;

40.2. sistemul informațional automatizat „Registrul de stat al unităților de drept”;

40.3. sistemul informațional „Cadastrul bunurilor imobile”;

40.4. alte sisteme informaționale necesare pentru buna funcționare a subsistemului.

41. Subsistemul va interacționa cu următoarele sisteme informaționale guvernamentale partajate:

41.1. portalul guvernamental integrat EVO;

41.2. platforma de interoperabilitate (MConnect) – pentru schimbul de date și interoperabilitatea cu registrele și sistemele informaționale de stat;

41.3. serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea și autorizarea accesului utilizatorilor în cadrul subsistemului;

41.4. serviciul electronic guvernamental integrat de semnătură electronică (MSign) - pentru semnarea electronică a solicitărilor de aplicare la proiectele de finanțare;

41.5. serviciul guvernamental de plăți electronice (MPay) – pentru distribuirea plăților către beneficiarii proiectelor și programelor de finanțare în domeniul eficienței energetice;

41.6. serviciul guvernamental de notificare electronică (MNotify) – pentru transmiterea notificărilor electronice utilizatorilor în cadrul subsistemului;

41.7. registrul împuternicirilor de reprezentare în baza semnăturii electronice (MPower) – pentru împuternicirea persoanelor în vederea accesării și utilizării subsistemului;

41.8. serviciul electronic guvernamental de jurnalizare (MLog) – pentru jurnalizarea și evidența operațiunilor (evenimentelor) în cadrul subsistemului.

Capitolul VII

ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI

42. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul Subsistemului se efectuează de către subiecții acestuia, cu respectarea strictă a cerințelor față de asigurarea securității informației și a prevederilor legislației din domeniul protecției datelor cu caracter personal.

43. Subsistemul este găzduit pe platforma tehnologică guvernamentală comună (MCloud) și se conformează cerințelor de securitate prevăzute de legislație.

44. Asigurarea securității informației este realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 562/2025.

45. Protecția informației cu caracter personal la nivel de deținător al Subsistemului, se efectuează prin următoarele metode:

45.1. asigurarea măsurilor de protecție a datelor prin folosirea metodelor criptografice de transmitere a informației prin rețelele de transport de date guvernamentale;

45.2. excluderea accesului neautorizat la datele din Subsistemul;

45.3. elaborarea măsurilor speciale tehnice și de program, împotriva acțiunilor care cauzează pierderea, modificarea, denaturarea, distrugerea informațiilor conținute (difuzate) de Subsistem sau generează defecțiuni în funcționarea normală a complexului tehnic și de program;

45.4. efectuarea periodică planificată a copiilor de siguranță a datelor și fișierelor mijloacelor de program;

45.5. efectuarea tuturor măsurilor aferente asigurării restabilirii și continuității funcționării în cazul incidentelor.

46. Protecția informației cu caracter personal la nivel de utilizator, se efectuează prin următoarele metode:

46.1. prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor;

46.2. monitorizarea procesului de exploatare a Subsistemului prin intermediul mecanismului de jurnalizare efectuat de deținătorul acestuia.

47. Securitatea și confidențialitatea schimbului de date sunt asigurate de către toți furnizorii de date și deținătorul Subsistemului, în conformitate cu cerințele de securitate aplicabile categoriei respective de date.

48. Schimbul informațional se efectuează cu utilizarea mijloacelor software și hardware, doar prin canale securizate, asigurând integritatea și securitatea datelor.

49. Pentru asigurarea funcționalității eficiente și neîntrerupte a Subsistemului, schimbul informațional de date al Subsistemului este asigurat în regim nonstop.

50. Utilizatorii Subsistemului sunt autorizați să acceseze doar funcționalitățile și datele pentru care au permisiunile necesare, conform rolurilor atribuite.

51. Revocarea dreptului de acces a utilizatorilor la Subsistem, se efectuează în una dintre următoarele situații:

51.1. la încetarea raporturilor de muncă/de serviciu ale utilizatorului;

51.2. la intervenirea modificărilor raporturilor de muncă/de serviciu, în cazul în care noile atribuții nu impun accesul la datele Subsistemului;

51.3. la constatarea de către deținător sau posesor a încălcării sistemului securității informaționale a Subsistemului, cum ar fi:

51.3.1. acces neautorizat sau tentativa de acces neautorizat la datele Subsistemului;

51.3.2. divulgarea neautorizată a datelor Subsistemului;

51.3.3. modificarea, ștergerea sau distrugerea neautorizată a datelor datele Subsistemului;

51.3.4. utilizarea necorespunzătoare a drepturilor de acces acordate;

51.3.5. orice alte acțiuni sau inacțiuni care compromit confidențialitatea, integritatea sau disponibilitatea datelor din Subsistem.

Capitolul VIII

CONTROLUL ȘI RESPONSABILITATEA

52. Subsistemul este supus unui control intern și extern. Controlul intern este efectuat anual de către Posesor, iar controlul extern este efectuat de către instituțiile abilitate și certificate în domeniul auditului.

53. Subiecții în ale căror atribuții intră administrarea Subsistemului, introducerea datelor, furnizarea informațiilor și asigurarea funcționării Subsistemului, poartă răspundere personală, în conformitate cu legislația, pentru completitudinea, autenticitatea, veridicitatea, integritatea informației, precum și pentru păstrarea și utilizarea acesteia.

54. Toți subiecții Subsistemului, poartă răspundere contravențională, penală sau civilă, pentru prelucrarea, divulgarea sau transmiterea informației cu caracter personal, contrar prevederilor legislației.

55. În cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware ale Subsistemului din vina terțelor persoane, este posibilă suspendarea funcționării acestuia, cu informarea subiecților prin mijloacele tehnice disponibile.