



GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din _____ 2022

Chișinău

**Cu privire la aprobarea Conceptului
Sistemului informațional „Vulnerabilitatea Energetică”**

În temeiul art. 6 alin. (1) din Legea nr. 241/2022 privind Fondul de reducere a vulnerabilității energetice (Monitorul Oficial al Republicii Moldova, 2022, nr. 246-250, art. 498), și al 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, Guvernul HOTĂRĂȘTE:

1. Se aprobă Conceptul Sistemului informațional „Vulnerabilitatea Energetică”, conform anexei.

2. Asigurarea condițiilor juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea Sistemului informațional „Vulnerabilitatea energetică” se realizează de către Ministerul Muncii și Protecției Sociale, în calitate de posesor al acestuia.

3. Ministerul Muncii și Protecției Sociale:

1) va asigura crearea Sistemului informațional „Vulnerabilitatea Energetică”;

2) înainte de punerea în exploatare a sistemului informațional, va elabora și va prezenta Guvernului spre aprobare Regulamentul de organizare și funcționare a Sistemului informațional „Vulnerabilitatea energetică”.

4. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Muncii și Protecției Sociale.

5. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

Prim-ministru

NATALIA GAVRILIȚA

Contrasemnează:

Ministrul muncii
și protecției sociale

Marcel Spatari

Aprobat
prin Hotărârea Guvernului nr.

CONCEPTUL Sistemului informațional „Vulnerabilitatea Energetică”

CAPITOLUL I INTRODUCERE

Pe fundalul crizei gazului la nivel global, care a generat o creștere a prețurilor gazelor naturale la peste 1000 USD/metru cub (de 5-10 ori nivelurile din 2020) și urmare a negocierii unui nou contract de furnizare a gazelor naturale Republicii Moldova cu SAP „Gazprom” („Gazprom”) din Federația Rusă, unde prețul de achiziție depășește 450 USD pentru 1000 de metri cubi, tarifele la gaze naturale pentru majoritatea utilizatorilor au crescut, devenind inaccesibile pentru unii consumatori casnici. Noul contract cu Gazprom (care a intrat în vigoare la 1 noiembrie 2021), bazat pe o formulă corelată atât la prețul petrolului, cât și al gazului, a influențat dublarea facturilor la energie pentru consumatori în comparație cu perioada similară a anului trecut. De asemenea, prețurile energiei electrice au crescut în medie cu 40%.

Toate aceste aspecte, dar și nivelul ridicat al inflației (27,3% pentru anul 2022 conform estimărilor BNM), eficiența energetică redusă, veniturile mici în rândul populației vor afecta în mod semnificativ sărăcia în Republica Moldova, două forme importante de sărăcie devenind în mod special proeminente: sărăcia energetică și sărăcia alimentară. Astfel, creșterea numărului persoanelor vulnerabile din punct de vedere energetic ar putea crește semnificativ. Prin sărăcie energetică poate fi înțeleasă situația în care gospodăriile nu pot avea acces la servicii energetice esențiale, cum sunt încălzirea, iluminatul și resurse de energie adecvate pentru alimentarea aparatelor electrocasnice - servicii esențiale care susțin un standard de viață și sănătate decent.

În acest context, pentru prevenirea creșterii nivelului de sărăcie energetică în rândurile consumatorilor vulnerabili este important să se asigure forme de ajutor și protecție socială, pentru care în prezent există un deficit de finanțare. Drept răspuns la această criză, pentru a aborda sistematic vulnerabilitatea energetică și pentru a promova eficiența energetică, Guvernul intenționează să creeze un Fond de reducere a vulnerabilității energetice pentru a oferi compensații pentru prețurile la gaze naturale, energie termică și energie electrică.

Totodată, o serie de acte normative în vigoare stabilesc drept obiectiv reducerea consumului de energie prin creșterea eficienței energetice și utilizarea surselor de energie regenerabilă, în special Legea nr. 139/2018 cu privire la eficiență energetică, Legea nr. 10/2016 privind promovarea utilizării energiei din surse regenerabile, etc. În special, Legea cu privire la eficiență energetică nr. 142/2010 prevede că politica de stat în domeniul eficienței energetice este parte

integrantă a politicii energetice a statului și urmărește, printre altele, promovarea utilizării, la consumatorii finali, a utilajelor și echipamentelor eficiente din punct de vedere energetic, precum și a surselor regenerabile de energie.

Astfel, de către Parlamentul Republicii Moldova a fost adoptată Legea nr. 241/ 2022 cu privire la Fondul de vulnerabilitate energetică, care prevede modul de organizare și funcționare a Fondului de reducere a vulnerabilității energetice, măsurile și programele finanțate din mijloacele acestui fond, îndreptate spre prevenirea și combaterea vulnerabilității energetice a populației și creșterea accesibilității energiei în rândul consumatorilor vulnerabili, precum și spre promovarea creșterii eficienței energetice.

Pentru a asigura activitatea eficientă a Fondului de Vulnerabilitate Energetică, este oportună implementarea unei soluții informatice care să poată asigura aplicabilitatea sistemului de compensații energetice pentru cetățenii (vulnerabili) săraci energetic din Republica Moldova, precum și să ofere posibilități de înființare și ajustare metodologică și modificări legislative pentru a sprijini Ministerul Muncii și Protecției Sociale în acest efort.

Prezentul document oferă o viziune conceptuală pentru înființarea și operarea unui sistem informațional destinat implementării Fondului de Vulnerabilitate Energetică, incluzând aspecte legate de scop și obiective, principii, caracteristici principale, funcționalitate și arhitectură conceptuală, cerințe funcționale și nefuncționale ale sistemului informațional.

CAPITOLUL II

DISPOZIȚII GENERALE

1. Sistemul Informațional „Vulnerabilitatea Energetică” (în continuare – SIVE) reprezintă totalitatea mijloacelor software, informaționale, organizaționale, a sistemelor de transmitere a datelor, a tehnologiilor de utilizare a acestora, a normelor de drept, precum și a infrastructurii destinată gestionării și monitorizării compensației oferite consumatorilor casnici.

2. Resursa informațională a SIVE reprezintă un spațiu informațional unic pentru stocarea și evidența solicitărilor înregistrate a consumatorilor casnici pentru încadrarea în categoria de vulnerabilitate energetică, a furnizorilor de energie .

3. SIVE este parte integrantă a Resurselor informaționale de stat.

4. Noțiunile utilizate în prezentul Concept semnifică următoarele:

1) *proces informațional* – proces de colectare, prelucrare, păstrare, actualizare și furnizare a informației documentate;

2) *compensație* – sumă monetară, plătită furnizorilor din mijloacele Fondului de reducere a vulnerabilității energetice în contul consumatorilor casnici, reflectată în factură, având drept scop acoperirea unei părți din cheltuielile pentru consumul de energie (gaze naturale, energie termică și/sau energie

electrică), în funcție de categoria de vulnerabilitate energetică atribuită acestora și conform normelor stabilite;

3) *numărul locului de consum* - codul de identificare a consumatorului casnic în factură al consumatorului casnic de energie, format dintr-un cod numeric sau alfanumeric, utilizat de furnizori pentru identificarea consumatorului în sistemul informațional al furnizorului de energie;

4) *solicitant* – unul dintre membrii familiei sau persoana singură care depune solicitarea de încadrare în categoriile de vulnerabilitate energetică prin intermediul interfeței Sistemului informațional „Vulnerabilitatea energetică”;

5) *furnizor de gaze naturale* – întreprindere de gaze naturale titular de licență pentru furnizarea gazelor naturale care furnizează gaze naturale în condițiile legii nr. 108/2016 cu privire la gazele naturale;

6) *furnizor de energie termică* - agent economic care furnizează energie termică consumatorilor în condițiile Legii nr. 92/2014 cu privire la energia termică și promovarea cogenerării. Furnizorul poate fi concomitent producător și/sau distribuitor de energie termică;

7) *furnizor de energie electrică* – întreprindere electroenergetică titular de licență pentru furnizarea energiei electrice care furnizează energie electrică consumatorilor casnici în condițiile legii nr. 107/2016;

8) *prețul reglementat pentru furnizarea gazelor naturale în contextul obligației de serviciu public* - prețul aprobat de către Agenția Națională pentru Reglementare în Energetică, în conformitate cu legislația de profil, și care este în vigoare la momentul livrării gazelor naturale consumatorilor casnici;

9) *servicii intermediare* – servicii, inclusiv de utilități publice, cum ar fi alimentarea cu energie termică, alimentarea cu gaze naturale, alimentarea cu energie electrică, alimentarea cu apă caldă menajeră, asigurarea cu apă potabilă, canalizarea și epurarea apelor uzate și pluviale, salubritatea, de care se folosesc ori se pot folosi proprietarii unităților și posesorii acestora, dar care, în funcție de situația concretă, din motive tehnice sau legale, trebuie intermediare de către asociație în temeiul contractului cu furnizorul și nu pot fi contractate individual de către proprietarii ori posesorii unităților ori facturate individual acestora;

10) *tariful reglementat la energia termică* - tariful aprobat de către Agenția Națională pentru Reglementare în Energetică, în conformitate cu legislația de profil, și care este în vigoare la momentul livrării energiei termice consumatorilor casnici;

11) *tarif reglementat la energia electrică* – tariful aprobat de către Agenția Națională pentru Reglementare în Energetică, în conformitate cu legislația de profil, și care este în vigoare la momentul livrării energiei electrice consumatorilor casnici;

12) *perioadă rece a anului* – perioadă cuprinsă între 1 noiembrie – 31 decembrie și 1 ianuarie – 31 martie.

Alte noțiuni utilizate în Concept corespund noțiunilor respective definite în Legea nr.241/2022 privind Fondul de reducere a vulnerabilității energetice și

Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat.

5. Scopul de bază al SIVE constă în gestionarea mecanismului de acordare a compensațiilor consumatorilor vulnerabili de energie, ca urmare a creșterii prețurilor reglementate la gazele naturale, energie electrică și/sau a tarifelor reglementate la energia termică, atribuirea consumatorilor în categoriile de vulnerabilitate energetică în baza criteriilor stabilite.

1) La crearea SIVE se urmărește atingerea următoarelor scopuri specifice:

a) evidența centralizată automatizată a solicitanților și beneficiarilor de compensații;

b) evidența centralizată a furnizorilor de energie, pe categoriile de energie furnizată;

c) sporirea nivelului de calitate al asigurării informaționale, a autorităților publice și locale, prin utilizarea unei informații complexe și veridice despre solicitanții și beneficiarii de compensații la energie, inclusiv sprijinirea persoanelor fizice și juridice, partenerilor, donatorilor, organizațiilor non-guvernamentale în coordonarea acțiunilor și eforturile privind abordarea problematicei de vulnerabilitate energetică;

d) sporirea posibilității de soluționare a problemelor abordate de către solicitanții și beneficiarii de compensații, persoanele fizice și juridice, autoritățile administrației publice centrale și locale, parteneri, donatori, organizații non-guvernamentale prin reducerea timpului necesar soluționării cazului;

6. Principalele obiective ale SIVE sunt:

1) automatizarea procesului de gestionare a compensațiilor privind compensarea cheltuielilor la energie, excluderea factorului uman în procesul de acordare a compensațiilor;

2) asigurarea integrării și interoperabilității cu alte resurse și sisteme informaționale pentru a prelua informații în scopul automatizării procesului de acordare a compensațiilor la energie;

3) oferirea consultanței și ajutorului informațional la cererea solicitanților;

4) oferirea unui instrument de lucru celor implicați în oferirea măsurilor de asistență;

5) acordarea necesarului de informație relevantă domeniului tuturor autorităților implicate, precum și specialiștilor din domeniile complementare, acordarea de suport în monitorizarea, prognozarea situației și luarea deciziilor;

6) integrarea surselor de informații indispensabile ce țin de managementul, analiza și planificarea măsurilor de asistență, furnizarea către utilizatori a informațiilor sub formă de rapoarte;

7) asigurarea vizualizării informației stocate (cu diferite nivele de acces) și generarea de rapoarte predefinite și specifice.

7. Principiile de bază ale creării SIVE sunt următoarele:

1) *principiul legalității* – presupune înființarea și operarea sistemului informațional în conformitate cu legislația națională și cu normele și standardele internaționale recunoscute în domeniu;

2) *principiul concentrării asupra nevoilor părților interesate*, ceea ce implică faptul că soluția informațională va furniza capabilități funcționale complete pentru a răspunde nevoilor tuturor părților interesate de procesele de evaluare a resurselor umane;

3) *principiul împărțirii arhitecturii pe nivele* – presupune proiectarea și implementarea componentelor funcționale ale sistemului în conformitate cu standardele de interfață între niveluri;

4) *principiul autenticității datelor, plenitudinii datelor și a integrității datelor* – toate datele din sistemele informaționale ale participanților la schimbul de date, furnizate prin intermediul platformei de interoperabilitate, se prezumă a fi autentice, se consideră integre și veridice și stau la baza actelor juridice, iar furnizorii de date sânt obligați să asigure integritatea și veridicitatea acestora;

5) *principiul arhitecturii orientate pe servicii (SOA)* – care presupune distribuirea componentelor funcționale ale sistemului informațional în componente mai mici, distincte – numite servicii – care pot fi distribuite într-o rețea și pot fi utilizate împreună pentru a crea aplicații menite să implementeze funcțiile de afaceri ale sistemul informatic.

6) *principiul modelului de date deschis și interoperabil* – care presupune că modelul de date susținut de sistem este documentat și comunicat tuturor părților interesate. Sistemul ar trebui dezvoltat pe baza standardelor bune din zonă și aliniat la modelul de date guvernamental și departamental (adoptarea taxonomiei și semanticii deja existente la nivel național și departamental și îmbogățirea lor pentru a răspunde nevoilor specifice din zonă), inclusiv capacitate tehnică a sistemului informațional și organizatorică a participanților de a reutiliza date printr-un proces eficient de schimb de date;

7) *principiul confidențialității informației* – presupune restricționarea accesului persoanelor neautorizate la informația cu accesibilitate limitată în conformitate cu legislația la datele cu caracter personal sau cauzării prejudiciilor persoanelor fizice și juridice. Este asigurat prin definirea dreptului de acces și delimitarea nivelului de acces;

8) *principiul securității prin proiectare* – care presupune proiectarea sistemului cu cunoștințe privind riscurile de securitate a informațiilor care pot afecta buna funcționare a sistemului informațional. Cerințele legale aplicabile pentru protecția datelor cu caracter personal vor fi luate în considerare la proiectarea sistemului și implementate în etapa de dezvoltare. Sistemul va asigura accesul controlat, transparent și responsabil la informații;

9) *principiul modularii și scalabilității* – posibilitatea extinderii și completării sistemului informațional cu noi funcții sau a îmbunătățirii celor existente;

10) *principiul neexcesivității și pertinentei datelor*, care relevă necesitatea

limitării volumului de informații cu accesibilitate limitată prelucrate, în așa fel încât să fie prelucrate doar informațiile relevante și necesare în contextul realizării sarcinilor Sistemului;

CAPITOLUL II

SPAȚIUL JURIDICO-NORMATIV AL FUNCȚIONĂRII SIVE

8. Cadrul normativ aferent creării și implementării SIVE include următoarele acte normative:

- 1) Legea nr. 1069/2000 cu privire la informatică;
- 2) Legea nr. 982/2000 privind accesul la informație;
- 3) Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;
- 4) Legea nr. 71/2007 cu privire la registre;
- 5) Legea nr. 133/2011 privind protecția datelor cu caracter personal;
- 6) Legea nr. 91/2014 privind semnătura electronică și documentul electronic;
- 7) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;
- 8) Legea nr. 241/2022 privind Fondul de reducere a vulnerabilității energetice;
- 9) Hotărârea Guvernului nr. 1123/2010 privind aprobarea cerințelor față de asigurarea datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal ;
- 10) Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- 11) Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
- 12) Hotărârea Guvernului nr. 405/2014 privind serviciul guvernamental integrat de semnătură electronică (MSign);
- 13) Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);
- 14) Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică ;
- 15) Hotărârea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;
- 16) Hotărârea Guvernului nr. 433/2021 cu privire la măsurile de atenuare a crizei;
- 17) Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);
- 18) Hotărârea Guvernului nr. 375/2020 privind Conceptul Sistemului informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) și a Regulamentului privind modul de ținere a Registrului împuternicirilor de reprezentare în baza semnăturii electronice;

19) Hotărârea Guvernului nr. 376/2020 privind serviciul guvernamental de notificare electronică (MNotify);

20) Hotărârea Guvernului nr. 712/2020 cu privire la serviciul guvernamental de plăți electronice (MPay);

21) Hotărârea Guvernului nr. 149/2021 cu privire la organizarea și funcționarea Ministerului Muncii și Protecției Sociale;

22) Hotărârea Guvernului cu privire la aprobarea Regulamentului privind încadrarea în categoriile de vulnerabilitate energetică și modul de stabilire și plată a compensațiilor pentru achitarea facturilor la energie;

23) Reglementarea tehnică RT 38370656 – 002:2006 „Procese ciclului de viață al software-ului”, aprobată prin Ordinul Ministrului Tehnologiei Informației și Comunicațiilor nr.78/2006;

9. La elaborarea și implementarea Sistemului se vor respecta următoarele standarde:

1) Standardul Republicii Moldova SM EN ISO 9001:2015 „Sisteme de management al calității. Cerințe”, adoptat prin Hotărârea Institutului de Standardizare din Moldova nr. 198/2015;

2) Standardul Republicii Moldova SM EN ISO/CEI/IEEE 15288:2015 „Ingineria sistemelor și software-ului. Procesele ciclului de viață ale sistemului”, adoptat prin Hotărârea Institutului Național de Standardizare din Moldova nr. 202/2015;

3) Standardul Republicii Moldova SM EN ISO/IEC 27002:2017 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul”, adoptat prin Hotărârea Institutului Național de Standardizare din Moldova nr. 255/2015.

CAPITOLUL IV SPAȚIUL FUNCȚIONAL AL SIVE

10. Sistemul va oferi o interfață ergonomică, intuitivă și accesibilă tuturor tipurilor de utilizatori prin intermediul unui explorator WEB. Interfața utilizator al sistemului va reprezenta un design grafic, echilibrat, distinct și adaptabil pentru majoritatea dispozitivelor utilizate (calculator desktop, notebook, tabletă, smartphone).

11. Sistemul va furniza o interfață bilingvă în limbile română (implicită) și rusă.

12. În dependență de categoriile utilizatorilor (drepturile și rolurile acestora) sistemul va furniza o interfață personalizată fiecărei categorii de utilizator și aplicații.

13. Una din funcțiile de bază ale SIVE este gestionarea informațională a atribuirii categoriilor de vulnerabilitate atribuite consumatorilor casnici de energie. Spațiul funcțional al SIVE reprezintă mai multe funcții realizate de componentele sistemului, care interacționează reciproc.

14. SIVE va avea următoarele contururi de bază, care asigură următoarele funcții specifice:

1) Conturul „Înregistrare solicitant” în SIVE:

a) înregistrarea și autentificarea prin intermediul interfeței SIVE a solicitantului/solicitanților;

b) îndeplinirea formularului online de către solicitant pentru atribuirea categoriei de vulnerabilitate.

2) Conturul „Profilul Furnizorului” :

a) autentificarea prin intermediul interfeței SIVE, adăugarea de utilizatori a profilului furnizorului;

b) expedierea de către furnizorii de energie prin intermediul interfeței SIVE a listei locurilor de consum a consumatorilor casnici referitor la energia consumată;

c) extragerea listei locurilor de consum cu categoria de vulnerabilitate energetică atribuită fiecărui loc de consum, conform tipului de energie și a furnizorului;

d) expedierea raportului generalizat privind valoarea mijloacelor financiare necesare pentru compensații, numărul de consumatori casnici, datele detaliate per consumator casnic și volumul consumat de gaze naturale, energie termică, energie electrică în funcție de categoria de vulnerabilitate energetică atribuită acestora și normelor stabilite.

3) Conturul „Notificări” :

a) notificarea privind atribuirea după criteriile de vulnerabilitate energetică pentru solicitanții de compensație la energie în cabinetul solicitantului;

b) notificarea furnizorilor de energie referitor la atribuirea categoriilor de vulnerabilitate solicitanților de compensații la energie și a cuantumului compensației.

4) Conturul „Procesarea datelor” în SIVE:

a) clasificarea cererilor depuse de solicitanți după furnizor tipul de energie;

b) procesarea cererile solicitanților și compararea cu datele încărcate în SIVE de către furnizorii de energie;

c) atribuirea categoriei de vulnerabilitate solicitanților - SIVE automat procesează cererile solicitanților și le atribuie una din cele cinci categorii de vulnerabilitate energetică;

d) consumatorii (Gospodăria) casnici de energie sunt încadrați în următoarele categorii:

consumatori cu vulnerabilitate energetică foarte ridicată;

consumatori cu vulnerabilitate energetică ridicată;

consumatori cu vulnerabilitate energetică medie;

consumatori cu vulnerabilitate energetică scăzută;

consumatori fără vulnerabilitate energetică.

e) locurilor de consum care nu au fost înregistrate de solicitanți în SIVE li se atribuie categoria de vulnerabilitate energetică medie.

La atribuirea categoriilor de vulnerabilitate a consumatorilor (locului de consum) de energie se vor aplica criteriile de eligibilitate stabilite prin Regulamentul cu privire la încadrarea în categoriile de vulnerabilitate energetică și modul de stabilire și plată a compensațiilor pentru achitarea facturilor la energie aprobat de Guvern, în baza datelor introduse în cererea de acordare a compensației depuse și a celor consumate din alte sisteme și resurse informaționale de stat.

5) Conturul „Liste locurilor de consum cu categoria de vulnerabilitate atribuite” în SIVE:

a) va genera/elabora automat listele beneficiarilor cu categoriile de vulnerabilitate atribuite;

b) va transmite furnizorilor de energie listele beneficiarilor cu categoriile de vulnerabilitate atribuite.

6) Conturul „Rapoarte” - a cărei funcție specifică constă în generarea de rapoarte prestabilite și ad-hoc privind conținutul informațional al sistemului informațional.

7) Conturul Administrare - nivel caracteristic utilizatorului cu privilegii de administrare a accesului, configurare, audit și depanări în cadrul SIVE. Acest nivel de acces, dat fiind rolul său de a administra buna funcționare a soluției informatice, va asigura funcția specificată de acces la toate funcționalitățile interfeței utilizator și conținutul bazei de date livrate de interfața utilizator, care include acțiuni de:

a) delimitarea drepturilor de acces pentru utilizatori, gestionarea utilizatorilor;

b) administrarea nomenclatoarelor ;

c) stabilește fluxurile și modelele de documente;

d) setează parametrii funcționali ai sistemului;

e) jurnalizarea tuturor evenimentelor aferente utilizării sistemului prin documentarea acțiunilor tuturor utilizatorilor sistemului;

f) administrarea (menținerea și actualizarea) algoritmilor specifici calculării valorilor criteriilor de eligibilitate;

g) alte activități de administrare și acces la funcționalitățile sistemului.

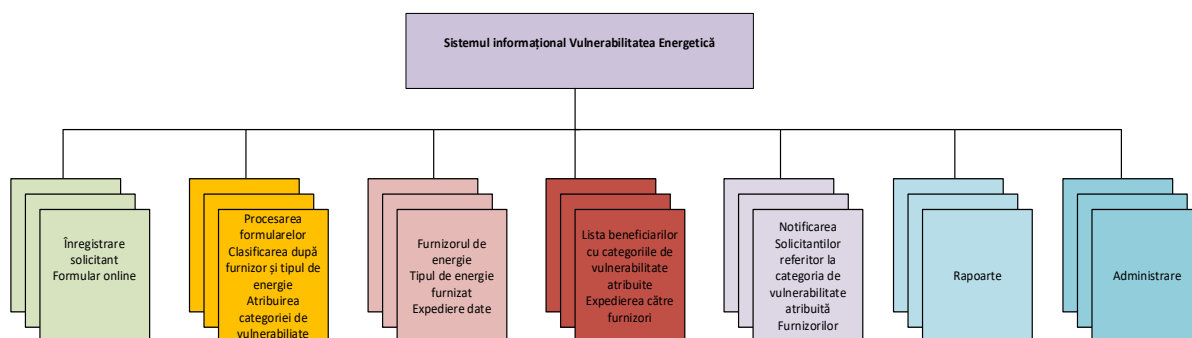


Figura 1. Contururile funcționale

CAPITOLUL IV

SPAȚIUL ORGANIZAȚIONAL AL SISTEMULUI

15. Funcțiile de bază privind formarea și exploatarea sistemului sunt divizate între proprietarul, posesorul, deținătorul, administratorul tehnic și utilizatorii sistemului.

16. Proprietarul sistemului este statul care își realizează dreptul de proprietate, gestionare și utilizare a datelor din acesta. Resursele financiare pentru dezvoltarea și mentenanța sistemului sunt asigurate din bugetul de stat, proiecte de asistență internațională și alte mijloace financiare, conform cadrului normativ.

17. Posesorul și Deținătorul sistemului este MMPS (în continuare - posesor). Rolul de posesor al sistemului reflectă aspectul administrativ ce ține de competențele deținute și necesare administrării și dezvoltării continue a sistemului informațional.

18. Registratorii de date sunt următoarele categorii de utilizatori ai sistemului informațional:

1) Persoanele responsabile din cadrul autorităților publice locale, inclusiv specialiștii centrelor unificate de prestare a serviciilor (CUPS), ce vor fi autorizate să opereze în SIVE, și anume la introducerea, modificarea datelor solicitanților de atribuire a categoriei de vulnerabilitate;

2) Persoanele împuternicite de către posesorul SIVE la înregistrarea, solicitanților de atribuire a categoriei de vulnerabilitate;

3) Persoanele fizice care dispun de telefon mobil conectat la rețeaua națională de telefonie mobilă, se pot înregistra prin intermediul interfeței SIVE.

19. Destinatarii datelor din SIVE sunt autoritățile publice centrale și locale, persoanele fizice sau juridice, organizațiile non guvernamentale mandatate cu dreptul de a primi informațiile conform prevederilor legale.

20. Furnizorii de date sunt următoarele categorii de utilizatori ai sistemului informațional:

1) persoanele fizice, care utilizează interfața SIVE pentru înregistrare și depunerea cererii privind atribuirea criteriilor de vulnerabilitate inclusiv persoanele fizice, care se înregistrează și depun cereri privind atribuirea criteriilor de vulnerabilitate, prin intermediul registratorilor indicați la pct.18 sbp.1) și 2) ;

2) persoanele juridice ce prestează servicii de furnizare a energiei, care prin intermediul interfeței SIVE vor introduce datele consumatorilor casnici de energie și vor extrage listele locurilor de consum cu categoriile de vulnerabilitate energetică atribuite.

21. Administratorul tehnic al sistemului este Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, care își exercită atribuțiile în conformitate cu cadrul normativ aferent domeniului administrării tehnice a sistemelor informaționale de stat.

CAPITOLUL V

DOCUMENTELE SISTEMULUI

22. În cadrul SIVE se utilizează documente de intrare, ieșire și tehnologice.

1) documentele de intrare includ:

- a) formular de înregistrare a solicitantului de compensație la energie;
- b) formular de înregistrare a furnizorului de energie.

1) documentele de ieșire includ:

a) tabele de date statistice agregate pe domenii și subdomenii, rapoarte statistice și analitice;

b) listele de beneficiari cu categoriile de vulnerabilitate atribuite.

2) documentele tehnologice includ:

- a) glosare de termeni și definiții;
- b) notificarea solicitanților privind atribuirea categoriei de vulnerabilitate;
- c) notificarea furnizorilor de energie;
- d) șabloane ale formularelor de înregistrare ale solicitantului de atribuire a categoriei de vulnerabilitate;
- e) documente privind descrierea procesului de repartizare a solicitanților pe categoriile de vulnerabilitate;
- f) documente tehnologice privind parametrii de sistem;
- g) ghiduri de utilizare și administrare a sistemului;
- h) registru cu înregistrări privind acțiunile și interacțiunea utilizatorilor interni;
- i) rapoarte și statisticile agregate privind utilizarea sistemului;
- j) alte documente necesare funcționării și dezvoltării sistemului.

23. SIVE va utiliza datele până la atingerea scopului, ulterior sistemul permite arhivarea datelor și documentelor în format electronic, în vederea eficientizării procesului de prelucrare și furnizare către utilizator a informației documentate;

24. Procedura de înregistrare, modificare, completare și radiere, precum și termenul de păstrare a datelor în cadrul Sistemului informațional „Vulnerabilitatea energetică” se reglementează în Regulamentul de organizare și funcționare a sistemului informațional, aprobat de către Guvern;

CAPITOLUL VI SPAȚIUL INFORMAȚIONAL

Secțiunea 1. Obiectele informaționale ale sistemului

25. Spațiul informațional al SIVE cuprinde totalitatea obiectelor informaționale, cu atributele și identificadorii săi.

26. Obiectul informațional al SIVE este caracterizat prin următoarele particularități de bază:

1) unicitate (unicitatea obiectului semnifică existența identificatorului unic, care deosebește obiectul respectiv de alte obiecte similare);

2) stare (starea obiectului este descrisă printr-un set de atribute, adică proprietățile variabile ale obiectului luate în considerare în sistem);

3) comportament (comportamentul obiectului este descris printr-o listă de evenimente/scenarii prin care trece acesta și care sunt luate în considerare în sistem).

4) obiectele informaționale care reprezintă resursele informaționale ale sunt determinate conform destinației și, după caz, vor fi preluate de la autoritățile și instituțiile care le dețin nemijlocit. Obiectele informaționale se identifică după un număr de identificare unic, specific fiecărui obiect separat.

27. Obiectele informaționale ale SIVE sunt următoarele:

- 1) Solicitant;
- 2) Furnizorul de energie;
- 3) Lista punctelor de consum;
- 4) Cererea de atribuire a categoriei de vulnerabilitate;
- 5) Listele beneficiarilor finali cu categoria de vulnerabilitate energetică atribuită;

28. SIVE urmează să asigure unicitatea, integritatea și consistența datelor stocate și procesate.

29. Fiecărui obiect informațional i se va atribui un identificator unic. Obiectele informaționale împrumutate, vor fi identificate în conformitate cu regulile sistemului în care au fost introduse/create.

30. Identificator al obiectului informațional „Solicitant” cuprinde numărul de identificare de stat (IDNP), din Registrul de Stat al Populației, numele prenumele, membrii familiei, adresa, numărul de telefon, adresa de email (dacă există).

31. Identificator al obiectului informațional „Furnizor de energie” cuprinde numărul de identificare de stat (IDNO) datele sunt preluate din Registrul de Stat al Unităților de Drept, denumirea juridică, adresa juridică, datele de contact.

32. Identificator al obiectului informațional „Lista punctelor de consum” reprezintă numărul de identificare unic care este automat atribuit de către SIVE.

33. Identificator al obiectului informațional „Cererea de atribuire a categoriei de vulnerabilitate” este numărul de identificare unic, atribuit de SIVE la crearea înregistrării.

34. Identificator al obiectului informațional „Listele beneficiarilor finali” este numărul de identificare unic, atribuit de SIVE la crearea înregistrării;

Secțiunea 2 - a

Scenariile de bază asociate obiectelor informaționale

35. Scenariul de bază reprezintă o listă de evenimente aferente obiectului informațional și care sunt puse în evidență de sistem. În sistem se vor ține în evidență următoarele evenimente (Figura 2).

36. Pentru obiectul informațional „Solicitant” :

1) solicitant accesează portalul www.compensatii.gov.md pentru înregistrare în SIVE, cu introducerea următoarelor date:

- a) numărul de telefon mobil;
- b) SIVE expediază un mesaj cu codul unic de acces;
- c) introducerea de către solicitant a codului unic pentru înregistrarea în interfața SIVE pentru înregistrare și actualizarea contului personal în SIVE;
- d) notificarea automatizată a solicitantului de către SIVE în cabinetul personal referitor la categoria de vulnerabilitate atribuită;

2) solicitantul sau registratorul după autentificare în SIVE efectuează actualizarea datelor prin introducerea sistematică a modificărilor în SIVE, în conformitate cu procedurile de lucru specifice fiecărui eveniment survenit;

3) scoaterea obiectului informațional din evidență și transferarea datelor despre el în arhivă se efectuează de către registrator.

37. Pentru obiectul informațional „Furnizor de energie”:

a) furnizorul se înregistrează în SIVE prin autentificare accesând portalul www.compensatii.gov.md;

b) scoaterea din evidență a furnizorilor de energie se efectuează la momentul obținerii stării „lichidat/radiat”, odată cu recepționarea informației în SIVE de la ASP despre lichidarea persoanei juridice . Scoaterea din evidență presupune doar modificarea statutului obiectului informațional, nu și eliminarea fizică din baza de date, astfel fiind păstrat istoricul acestuia.

c) notificare automatizată privind aprobarea listelor beneficiarilor finali și expedierea spre plată.

38. Pentru obiectul informațional „Lista punctelor de consum” - clasificarea automatizată a listelor punctelor de consum a consumatorilor casnici comunicată în SIVE de către furnizorii de energie conform:

- 1) tipului de energie furnizat;
- 2) numărului locului de consum indicat în factura consumatorului casnic;
- 3) adresei locului de consum;
- 4) datele consumatorului.

39. Pentru obiectul informațional „Cererea de atribuire a categoriei de vulnerabilitate” - solicitantul înregistrat în SIVE sau registratorul introduce în cerere următoarele date prin intermediul interfeței SIVE pentru atribuirea categoriei de vulnerabilitate energetică, cu următorul set de date:

1) informații despre solicitant - solicitantul sau registratorul care introduce datele solicitantului;

2) date despre locuință – solicitantul sau registratorul care va introduce datele solicitantului, introduce în cerere următoarele date:

- a) bifează dacă solicitantul este proprietar al imobilului;
 - b) în caz că solicitantul închiriază locuința bifează în cerere;
 - c) se bifează în cererea online sursa principală de încălzire a anului gaze naturale, încălzire centralizată, electricitate, sobă sau cazan bazat pe combustibil solid;
 - d) se introduc datele dacă locuința este conectată la următoarele tipuri de energie – gaze natural, încălzire centralizată, electricitate cu introducerea pentru fiecare tip de energie a numărului locului de consum și selectarea furnizorului de energie;
 - e) se bifează dacă factura pentru energie este eliberată de către Asociația de Locatari cu selectarea asociației;
 - f) opțional se bifează dacă locuința dispune de surse alternative de energie;
- 3) după îndeplinirea datelor menționate solicitantul sau registratorul care a introdus datele există opțiunea de a selecta:
- a) atribuirea unei categorii de vulnerabilitate familiei/locuinței;
 - b) atribuirea categoriei de non-vulnerabilitate familiei/locuinței.
- 4) membrii locuinței – în cerere se adăugă membrii locuinței care locuiesc în aceeași locuință, introdusă în cerere pentru atribuirea categoriei de vulnerabilitate energetică;
- 5) transmiterea cererii completate de către solicitant sau registrator spre procesare;
- 6) dacă cererea solicitantului prin intermediul interfeței SIVE a fost îndeplinită de către registrator, atunci cererea se va imprima din SIVE cu datele de acces la contul personal al solicitantului;
- 7) scoaterea de la evidență și arhivarea obiectului se efectuează de utilizatorul care a introdus datele, și a expedit spre procesare datele;
- 8) solicitanților înregistrați în SIVE li se atribuie o singură categorie de vulnerabilitate energetică în funcție de informația indicată în cerere și cea obținută prin intermediul platformei guvernamentale MConnect din alte sisteme informaționale guvernamentale, după cum urmează:
- a) clasificarea cererilor solicitanților de atribuire a categoriei de vulnerabilitate conform tipului de energie și furnizor;
 - b) atribuirea categoriei de vulnerabilitate de către SIVE se efectuează automat conform criteriile de eligibilitate stabilite în Regulamentul cu privire la atribuirea categoriilor de vulnerabilitate energetică și modul de stabilire și plată a compensațiilor pentru achitarea facturilor la energie.
 - c) categoriile de vulnerabilitate atribuite de către SIVE solicitanților sunt următoarele:
 - consumatori cu vulnerabilitate energetică foarte ridicată;
 - consumatori cu vulnerabilitate energetică ridicată;
 - consumatori cu vulnerabilitate energetică medie;
 - consumatori cu vulnerabilitate energetică scăzută;
 - categoria de consumatori fără vulnerabilitate energetică.

9) atribuirea categoriilor de vulnerabilitate energetică prin metoda indirectă pentru locurile de consum neînregistrate de solicitanți în SIVE :

a) furnizorii comunică în SIVE datele de identificare a tuturor punctelor de consum;

b) locurilor de consum care nu au fost înregistrate de solicitanți în SIVE li se atribuie categoria de vulnerabilitate energetică medie.

10) notificarea solicitanților despre atribuirea categoriei de vulnerabilitate energetică.

11) scoaterea din evidență și arhivarea obiectului se efectuează de către sistem, după atribuirea categoriei de vulnerabilitate energetică.

40. Pentru obiectul informațional „Listele beneficiarilor finali ” se efectuează următoarele scenarii :

1) generarea automatizată a listelor locurilor de consum și datele referitoare la datele consumatorilor (locuințelor) casnici cu categoriile de vulnerabilitate atribuite;

2) expedierea automatizată către furnizorii de energie a listelor locurilor de consum cu datele consumatorilor casnici și categoriile de vulnerabilitate atribuite;

3) notificarea automatizată a furnizorului referitor la expedierea listelor locurilor de consum;

4) scoaterea de la evidență și arhivarea obiectului are loc după ce furnizorul va extrage lista locurilor de consum, în mod automatizat.

5) scoaterea de la evidență și arhivarea obiectului, care se efectuează de către registratorul la primirea informației de către furnizorii de energie (date) despre încetarea activității obiectului (confirmarea privind transferarea mijloacelor financiare) .

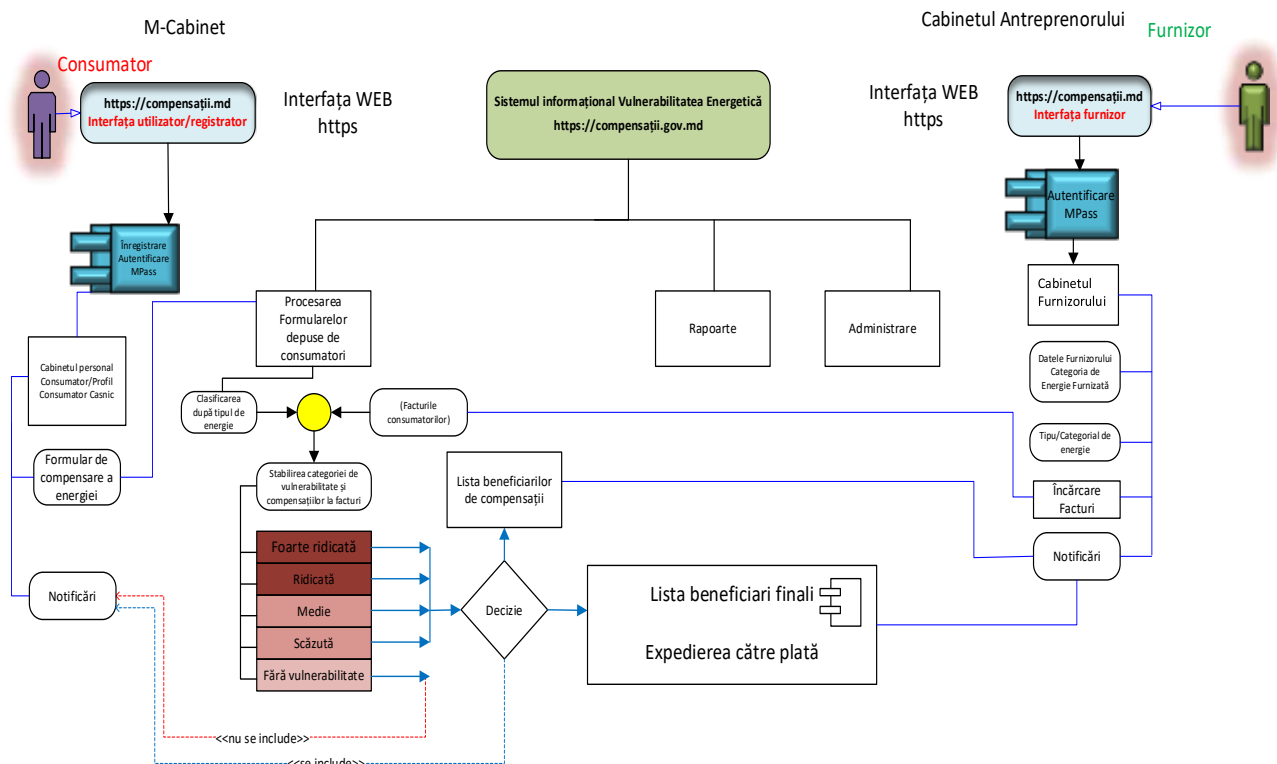


Figura 2: Scenariul asociat obiectelor informaționale.

Secțiunea 4 - a Datele obiectelor informaționale

41. Obiectele informaționale reprezintă totalitatea de date care le caracterizează, după cum urmează:

- 1) datele despre solicitantul (persoană fizică):
 - a) numele;
 - b) prenumele;
 - c) IDNP;
 - d) seria și numărul actului de identitate;
 - e) data nașterii;
 - f) numărul de telefon mobil;
 - g) adresa de email;
 - h) adresa:
 - raionul/municipiul;
 - localitatea;
 - strada;
 - casa;
 - blocul;
 - apartamentul.
- 2) datele despre furnizorul de energie:
 - a) denumirea juridică;

- b) IDNO;
- c) adresa juridică;
- d) datele de contact;
- e) contul bancar;
- f) tipul de furnizare a energiei:
 - gaze naturale;
 - energie termică;
 - energie electrică
- 3) datele pentru obiectul informațional „Lista punctelor de consum”:
 - a) furnizorul și tipul de energie;
 - b) numele, prenumele;
 - c) numărului locului de consum indicat în factura consumatorului;
 - d) adresa locului de consum.
- 4) datele pentru obiectul informațional „Cererea de atribuire a categoriei de vulnerabilitate”:
 - a) informații despre solicitant și membrii locuinței:
 - numele prenumele;
 - IDNP;
 - adresa;
 - numărul de telefon mobil;
 - email;
 - rata creditului ipotecar achitat ultima lună;
 - numărul cadastral al locuinței.
 - b) date despre locuință:
 - solicitantul bifează dacă este proprietarul locuinței;
 - solicitantul bifează dacă este chiriaș;
 - indicarea sursei principale de energie :
 - gaze naturale;
 - încălzire centralizată;
 - electricitate;
 - sobă/cazan bazat pe combustibil solid.
 - c) locuința este conectată la următoarele tipuri de energie:
 - gaze naturale – introducerea numărului locului de consum;
 - încălzire centralizată - introducerea numărului locului de consum ;
 - electricitate – introducerea numărului locului de consum
 - d) numărul Asociației de Locatari;
- 5) datele pentru obiectul informațional „Procesarea cererilor de atribuire a categoriei de vulnerabilitate”:
 - a) plafonul eligibil pentru calculul cheltuielilor gospodăriei casnice;
 - b) datele prezentate de furnizorii de energie;
 - c) venitul global mediu al familiei;
 - d) venitul disponibil pentru achitarea energiei;

- e) calculul costului energiei în perioada rece a anului pentru gospodăria casnică;
- f) mulțimea locurilor de consum de referință;
- g) categoria de vulnerabilitate energetică de referință;
- h) atribuirea categoriei de vulnerabilitate.
- i) notificarea automată a solicitantului privind atribuirea categoriei de vulnerabilitate energetică.
- 6) datele pentru obiectul informațional „Listele beneficiarilor finali”:
 - a) numele, prenumele consumatorului de energie;
 - b) datele de contact;
 - c) furnizorul de energie;
 - d) tipul de energie;
 - e) numărul locului de consum;
 - f) categoria de vulnerabilitate atribuită.

Secțiunea 5 - a

Integrarea cu alte sisteme informaționale

42. Pentru asigurarea funcționalității al sistemului este necesară realizarea interacțiunii cu următoarele sisteme informaționale (Figura 3):

1) **Registrul de stat al populației** - necesar schimbului de date care va permite identificarea solicitantului și a membrilor familiei. Modificările în componența familiei (nașterea/decesul unui membru), modificarea statutului unui membru din copil în adult, starea familială (existența membrilor văduvi) influențează la determinarea dreptului pentru atribuirea categoriei de vulnerabilitate energetică.

2) **Registrul Bunurilor Imobile** - înscrisurile referitoare la bunul imobil, drepturile și restricțiile înregistrate și titularii acestora, necesar schimbului automatizat de date referitor la bunurile imobile deținute de solicitanții ce va influența la atribuirea categoriei de vulnerabilitate energetică.

3) **RSUD (Registrul de Stat al Unităților de Drept)** – este un sistem informațional destinat evidenței unităților de drept prin înregistrarea de stat a acestora, în condițiile și în conformitate cu prevederile Legii nr. 220/2007 privind înregistrarea de stat a persoanelor juridice și întreprinzătorilor individuali – pentru preluarea datelor în sistem a persoanelor juridice.

4) **Sistemul informațional al Serviciului Fiscal de Stat** – extragerea datelor aferente datele privind salariul lunar net /veniturile nete din salarizare, ale deținătorilor de gospodării țărănești, deținătorilor de patentă, obținerea informației, dacă solicitantul nu obține venituri din activități antreprenoriale, inclusiv a familiei acestora, fapt care va influența la atribuirea categoriei de vulnerabilitate energetică și a cuantumului de compensare a sumei la factura pentru energie.

5) **Sistemul informațional „Protecția Socială” al Casei Naționale de Asigurări Sociale (CNAS)** – schimbul de informații referitor la prestațiile sociale achitate solicitanților de compensații și membrilor familiei. Modificarea mărimii acestor prestații sociale influențează la determinarea și atribuirea categoriei de vulnerabilitate a solicitantului.

6) **Sisteme informaționale partajate:**

a) **platforma de interoperabilitate (MConnect)** – în scopul asigurării la schimbului de date cu alte sisteme și resurse informaționale de stat;

b) **serviciul electronic guvernamental de autentificare și control al accesului (MPass)** – necesar pentru autentificarea prin intermediul interfeței SIVE a utilizatorilor;

c) **serviciul electronic guvernamental integrat de semnătură electronică (MSign)** – necesar pentru semnarea electronică a documentelor;

d) **serviciul guvernamental de notificare electronică (MNotify)** – necesar pentru notificarea utilizatorilor referitor la atribuirea categoriei de vulnerabilitate energetică a solicitanților;

e) **serviciul electronic guvernamental de jurnalizare (MLog)** – necesar pentru jurnalizarea evenimentelor în SIVE;

registruul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) - registru de împuterniciri de reprezentare, care furnizează date privind mandatul deținut al utilizatorilor autorizați de a efectua acțiuni specifice în sistem.

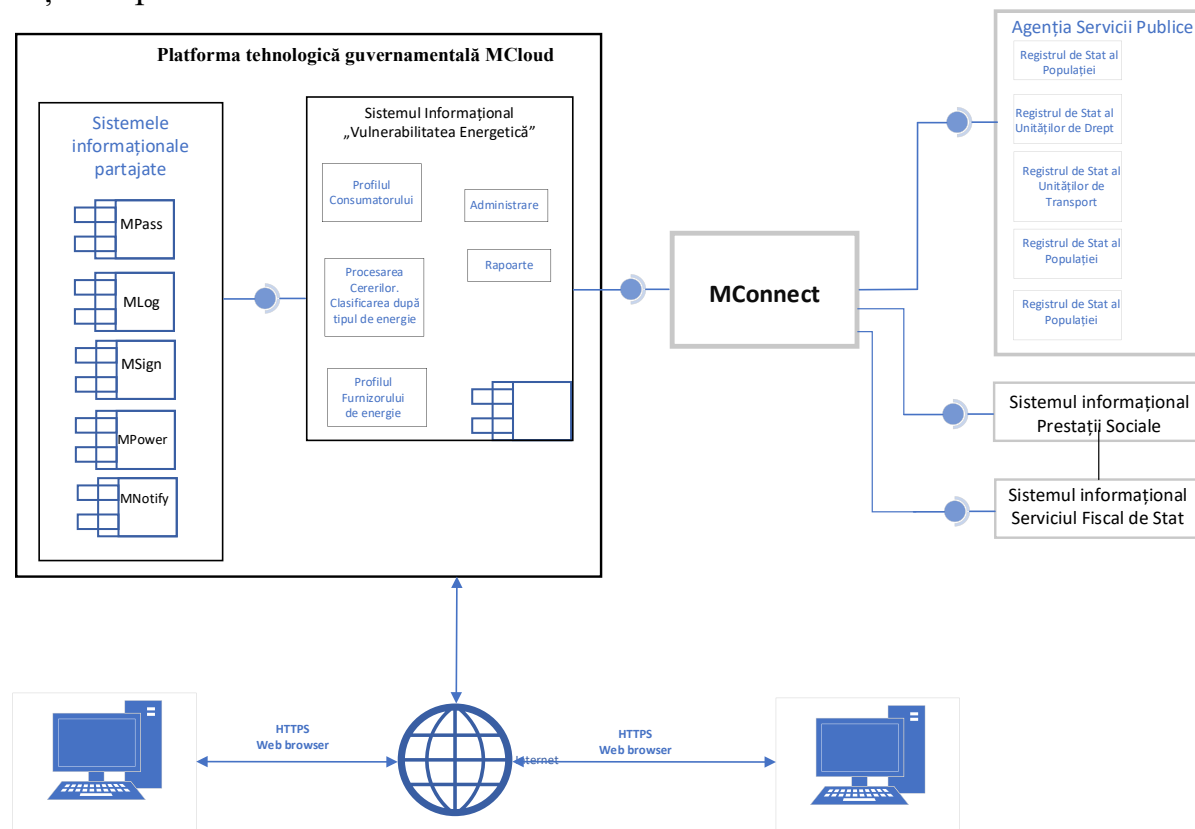


Figura 3. Interacțiunea cu alte sisteme informaționale

Secțiunea 6

Fluxurile informaționale ale sistemului

43. SIVE urmează a fi implementat în baza principiului tranzacțional, când orice adăugare, actualizare a datelor se procesează în baza unor fluxuri de lucru specializate.

44. Pentru asigurarea funcționalității în bune condiții a SIVE este necesară implementarea următoarelor categorii de fluxuri:

1) Fluxul destinat configurării criteriilor de eligibilitate reprezintă un flux de lucru prin intermediul căruia urmează a fi create și configurate noile criterii de eligibilitate, modificate criteriile de eligibilitate, lansate în producție/scoase din producție la crearea și modificarea criteriilor de eligibilitate se realizează în conformitate cu Regulamentului cu privire la atribuirea categoriilor de vulnerabilitate energetică și modul de stabilire și plată a compensațiilor pentru achitarea facturilor la energie;

2) Fluxul destinat calculării valorilor criteriilor și clasificării după criteriile de eligibilitate prin intermediul căruia sistemul automat va calcula și clasifica în categoriile de vulnerabilitate și va clasifica valorile cu statut în producție;

3) Fluxul destinat schimbului de date cu alte sisteme informaționale cuprinde procesele de interpelare a datelor din surse externe, combinarea acestora și formarea obiectelor informaționale specifice sistemului prin intermediul interfeței utilizator, sau furnizarea lor către sisteme informaționale externe prin intermediul platformei de interoperabilitate (MConnect);

Secțiunea 7

Clasificatoarele și nomenclatoarele sistemului

45. În scopul asigurării veridicității și interoperabilității sistemului cu alte sisteme informaționale se vor utiliza clasificatoare și nomenclatoare, după cum urmează:

- 1) clasificatoare internaționale;
- 2) clasificatoare oficiale naționale;
- 3) clasificatoare/nomenclatoare de interoperabilitate;
- 4) clasificatoare/nomenclatoare interne.

CAPITOLUL VII

SPAȚIUL TEHNOLOGIC

46. Sistemul este proiectat ca un sistem modular și bazat pe componente integrate, compatibil cu tehnologia de cloud computing, care asigură posibilitatea dezvoltării sale fără a afecta continuitatea funcționării și va permite operarea modificărilor și posibilitate în implementare.

47. Platforma urmează să fie dezvoltată componentă cu componentă, precum și cu luarea în considerare a priorităților posesorului/deținătorului.

48. Arhitectura sistemului este compusă din trei nivele, caracterizată prin următoarele componente de bază sunt interdependente, realizează schimb reciproc de date și sunt grupate după cum urmează:

1) **Nivelul de prezentare a datelor** – reprezintă interfețele destinate utilizatorilor;

2) **Nivelul aplicațiilor** – este destinat pentru executarea proceselor de business-logică a sistemului pentru accesarea, prelucrarea, transformarea datelor și asigurării coerenței și preciziei acestora;

3) **Nivelul de date** - destinat pentru stocarea și actualizarea datelor în sistemul de gestionare a bazelor de date relaționale (SGBDR).

49. Platforma tehnică a sistemului va utiliza tehnologii bine – cunoscute și general acceptate și va fi compatibilă cu sisteme care, la fel, utilizează standarde non proprietare, precum și standardele deja existente.

50. Arhitectura platformei software, lista de produse software și mijloacele tehnice utilizate pentru crearea infrastructurii informaționale sunt determinate de Posesor/Deținător, în etapele ulterioare de dezvoltare a sistemului, luând în considerare următoarele:

1) implementarea unei soluții bazată pe arhitectură software orientată spre servicii (Service Oriented Architecture), care oferă posibilitatea reutilizării unor funcții ale sistemului în cadrul altor procese sau permite extinderea sistemului cu noi funcționalități, fără a perturba funcționarea sistemului;

2) implementarea funcționalităților de arhivare a informațiilor, crearea de copii de rezervă și restaurarea datelor în caz de incidente;

3) aplicațiile și infrastructura software să se bazeze pe licențe perpetue pentru toate produsele software incluse în sistem și să asigure suportul de la producători;

4) asigurarea ca sistemele IT să fie operaționale în cazul unor perturbări (defecțiuni hardware, coruperi de date) sau să permită extensii ulterioare pentru un centru alternativ folosit în cazul unor dezastre naturale;

5) protecția corespunzătoare a datelor confidențiale, limitarea accesului la informațiile din sistemul de producție conform unei matrici de drepturi, în funcție de roluri, și monitorizarea astfel încât să prevină divulgarea sau utilizarea neautorizată a datelor din sistem;

6) sistemul informațional va asigura următoarele funcționalități generale:

a) partajarea eficientă a informației între utilizatorii sistemului;

b) crearea de fluxuri de proces automatizate suportate de aplicații;

c) accesul „online”, pe baza de servicii web, la informațiile utile utilizatorilor;

d) suport tehnologic sigur (mentenanța pentru corectarea bug-urilor și asigurarea completărilor necesare) și scalabil astfel încât să susțină numărul necesar de utilizatori;

e) administrarea identității utilizatorilor și controlul accesului la toate resursele sistemului;

f) administrarea și operarea la costuri reduse a infrastructurii și componentelor soluției.

7) sistemul informațional va implementa următoarele caracteristici generice:

- a) principiile standard ale industriei de profil pentru utilizarea prietenoasă;
- b) facilități de securitate și administrare de sistem;
- c) facilități de management al datelor (informațiilor), cu atribute de protecție corespunzătoare.

51. Tipurile principale de standarde tehnologice utilizate vor fi:

- 1) standardele datelor;
- 2) standardul meta datelor (ISO 11179);
- 3) standardele schimburilor de informații;
- 4) standardele căutării informațiilor;
- 5) standardele de calitate;
- 6) standardele de securitate;
- 7) standardele de multilingvism.

52. Conformitatea cu standardele tehnologice va consta în:

- 1) susținerea interfeței browser-ului public pentru accesare;
- 2) utilizarea standardelor Internet și WWW – HTML, TCP/IP, SMTP;
- 3) utilizarea standardelor naționale și internaționale privind calitatea și securitatea.

CAPITOLUL VIII

ASIGURAREA SECURITĂȚII INFORMAȚIONALE

53. Prin securitatea informațională se subînțelege starea de protecție a sistemului la etapele procesului de preluare, prelucrare, stocare și transmitere a datelor de la acțiuni accidentale sau intenționate, cu caracter natural sau artificial, care au drept scop crearea prejudiciului participanților în procesul de schimb de date.

54. Sistemul complex al securității informaționale reprezintă totalitatea mijloacelor legislative, organizatorice și economice, precum și a mijloacelor tehnologice și metodelor de protecție software-hardware și criptografică a informației, orientate spre asigurarea unui nivel necesar de integritate, confidențialitate și accesibilitate a resurselor informaționale.

55. Principalele sarcini ale asigurării securității informaționale sunt:

- 1) **asigurarea integrității informației** - menținerea și asigurarea integrității datelor pe parcursul întregului ciclu de viață;
- 2) **asigurarea confidențialității** - protecția împotriva accesului neautorizat la date, dar și a diseminării datelor de către Posesor/Deținător ținând cont de

regulile de confidențialitate - cele generale stabilite prin lege și celor specifice, ce țin de reguli de asigurare a confidențialității - prin regulamentele ale MMPS;

3) **asigurarea disponibilității accesibilității** - protecția împotriva blocării accesului utilizatorilor autorizați la resursele informaționale.

56. În scopul asigurării securității informaționale sistemul, va sprijini următoarele mecanisme:

1) *Autentificare*: garantează faptul că zonele restricționate ale serviciului sunt accesibile numai utilizatorilor cu identitatea verificată prin serviciul electronic guvernamental de autentificare și control al accesului (MPass).

2) *Autorizare*: garantează că utilizatorii autentificați pot accesa numai serviciile și datele care corespund rolurilor și drepturilor de acces ale acestora.

3) *Confidențialitate*: garantează că datele schimbate între persoana care o solicită și furnizorul nu pot fi interceptate sau accesate de o terță parte neautorizată și că datele nu pot fi accesate într-un moment necorespunzător.

4) *Integritate*: garantează că fluxul de date realizat între solicitant și furnizor nu a fost modificat sau manipulat de o terță parte neautorizată sau datele nu au fost accesate înainte de un termen anumit sau un timp anumit.

5) *Non-repudiare*: măsura prin care se asigură faptul că, după emiterea/recepționarea unei informații, expeditorul/destinatarul nu poate nega, în mod fals, că a expediat/primit informații.

6) *Înregistrarea și monitorizarea acțiunilor utilizatorilor sistemului*: pentru a detecta într-o etapă incipientă încercarea de a accesa date confidențiale sau de a afecta intenționat sau accidental integritatea informației prin serviciul electronic guvernamental de jurnalizare (MLog).

7) *Mentenanța*: sistemul trebuie asigurat în permanență cu suportul și mentenanța necesară conform nivelului agreeat de servicii (SLA).

8) *Auditul IT*.

9) *Criptarea informațiilor*.

10) *Continuarea activității și recuperarea în caz de dezastru*.

57. Pentru a atinge aceste obiective de asigurare a securității informaționale, se va utiliza următoarele mecanisme de securitate:

1) *Firewall-uri*: acestea fac parte din arhitectura tehnică a sistemului pentru a oferi o linie de apărare atunci când utilizatorii externi încearcă să se conecteze la sistem de pe Internet sau dintr-o altă rețea. Firewall-urile trebuie să fie configurate astfel, încât să permită numai serviciile de rețea absolut necesare și protocoalele pentru operarea sistemului. Nu pot fi activate servicii și/sau protocoale adiționale (principiul privilegiilor minime). De asemenea, acestea trebuie să sprijine reluarea, în caz de nereușită (*failover*), pentru asigurarea unui nivel de disponibilitate ridicată. Acest mecanism se va asigura prin utilizarea resurselor informaționale ale MMPS și platformei tehnologice guvernamentale comune (MCloud), în conformitate cu prevederile legislației în vigoare și ținând cont de bunele practici internaționale în domeniu.

2) *Antivirus / Anti-spam*: soluțiile hardware și / sau software trebuie să

asigure protecție antivirus și anti-spam pentru toate serverele. Fișierele vor fi scanate în timp ce se încarcă în sistem. În cazul în care un fișier infectat este depistat, procedura de încărcare va fi stopată iar fișierul va fi respins. Sistemul trebuie să fie configurat să actualizeze zilnic automat definițiile în timpul orelor nelucrătoare. Acest mecanism se va asigura prin utilizarea resurselor informaționale ale MMPS și utilizarea platformei tehnologice guvernamentale comune (MCloud).

3) *Sistem de detectare a intruziunilor*: acest sistem va include toți agenții necesari pentru toate serverele. Acest mecanism se va asigura prin utilizarea resurselor informaționale ale MMPS și utilizarea platformei tehnologice guvernamentale comune (MCloud).

4) *Comunicații securizate (transfer de date) între serverele web și utilizatori*: schimbul de date sensibile urmează a fi securizat în mod corespunzător. În acest context, urmează a fi utilizat un protocol securizat, cum ar fi HTTPS, pentru a evita accesul neautorizat la datele transmise. Acest protocol securizat trebuie să fie utilizat în mod consistent pe toate site-urile sistemului, excluzând posibilitatea transmiterii necriptate a informației. În caz contrar, utilizatorii ar putea fi expuși la mai multe tipuri de atacuri. În mod ideal, site-ul Web ar trebui să posede proprietatea de "securitate perfectă" („forward secrecy”).

5) *Copierea de rezerva sistematică a datelor stocate*: permite recuperarea rapidă și fiabilă a datelor, în cazul unor incidente, care au ca rezultat pierderea sau deteriorarea datelor. Acest mecanism se va asigura prin utilizarea resurselor informaționale ale MMPS și utilizarea platformei tehnologice guvernamentale comune (MCloud);

6) *Criptarea datelor*: toate datele stocate în diferitele componente ale sistemului (i.e. servere, stocare de date, LDAP) vor fi criptate.

7) *Certificate digitale*: sistemul va utiliza certificatele digitale pentru a asigura principiile integrității și non-repudiare. Acest mecanism este asigurat prin integrarea cu serviciul electronic guvernamental de autentificare și control al accesului (MPass).

8) *Abilitatea de auditare a acțiunilor realizate*: toate activitățile efectuate de utilizatori, fie cu succes sau nu (cum ar fi încercările de logare nereușite), vor fi monitorizate și înregistrate în jurnalele cu acces limitat a sistemului. Acest mecanism este asigurat prin integrarea cu serviciul electronic guvernamental de jurnalizare (MLog).

58. Adicional, sistemul va include și alte instrumente conceptuale de securitate, în special:

1) *Arhitectura tehnică securizată*: sistemul va implementa cel puțin o arhitectură pe trei niveluri (baza de date, aplicații și nivelul de prezentare), fiind împărțită în diferite zone de securitate, și va conține cel puțin un DMZ și o zonă internă;

2) *Controalele de securitate incorporate în sistem*: de exemplu, rolurile utilizatorilor cu drepturi de acces predefinite, principiul "patru ochi", pentru luarea

deciziilor cheie, validarea datelor la introducere, etc.;

3) *Mecanismul de marcare temporală*: asigura înregistrarea timpului tuturor tranzacțiilor din cadrul sistemului;

4) Totodată, sistemul va respecta cerințele obligatorii minime privind securitatea cibernetică, aprobate prin Hotărârea Guvernului nr.201/2017;

59. Organizarea sistemului de protecție a datelor cu caracter personal constituie o parte componentă a mecanismului de asigurare a securității informaționale a sistemului. Sistemul de protecție a datelor cu caracter personal se constituie în baza:

- 1) raportului privind rezultatele efectuării auditului intern;
- 2) listei datelor cu caracter personal, care trebuie să fie protejate;
- 3) actului de clasificare a sistemului informațional, care prelucrează date cu caracter personal;
- 4) modelelor de pericole pentru securitatea datelor cu caracter personal;
- 5) prevederilor privind delimitarea drepturilor de acces la datele cu caracter personal prelucrate;
- 6) documentelor de reglementare și politicilor de securitate elaborate.

60. Colectarea, prelucrarea, stocarea și furnizarea datelor cu caracter personal se realizează în conformitate cu prevederile Legii nr. 133/2011 privind protecția datelor cu caracter personal și Hotărârii Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, astfel:

1) în condițiile prezentului Concept, Posesorul și registratorii vor prelucra doar datele cu caracter personal strict necesare, neexcesive scopului prestabilit, conform competențelor atribuite, respectând principiile stabilite de legislația privind protecția datelor cu caracter personal;

2) la prelucrarea datelor cu caracter personal, Posesorul/Deținătorul va asigura măsuri organizatorice și tehnice necesare pentru protecția datelor cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrarea și caracterul datelor prelucrate;

3) în cazul incidentelor de securitate, Posesorul/Deținătorul va întreprinde măsuri necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea Centrului National pentru Protecția Datelor cu Caracter Personal al Republicii Moldova;

4) în cadrul operațiunilor de prelucrare a datelor cu caracter personal efectuate conform Regulamentului resursei informaționale formată de sistem, Posesorul/Deținătorul va asigura respectarea drepturilor subiecților de date cu caracter personal.

Capitolul IX ÎNCHEIEREA

61. Impactul generat de sistem

Sistemul oferă beneficii importante părților implicate, fiind caracterizat de o serie de avantaje de ordin strategic, printre care se numără:

1) este conceput și dezvoltat pentru asigurarea aplicabilității sistemului de compensații energetice pentru cetățenii vulnerabili;

2) urmărește digitalizarea proceselor de stabilire a gradului de vulnerabilitate a solicitantului și calcularea cuantumului de compensare la energie;

3) urmărește implementarea unor mecanisme de monitorizare și control a proceselor de stabilire a gradului de vulnerabilitate și calcularea cuantumului de compensare la energie, inclusiv a proceselor de achitare a compensațiilor către furnizorii de energie;

4) asigură în permanență protecția datelor cu și are posibilitatea interoperabilității sale cu alte sisteme informatice;

5) asigură trasabilitatea prin sisteme de interconectare (web-servicii cu grad înalt de securitate și platforma de interoperabilitate MConnect) a activităților oferind utilizatorilor informații utile și exacte cu privire la istoricul beneficiarilor de compensații în timp real.

62. Implementarea sistemului va conduce la asigurarea și aplicabilitatea sistemului de compensații energetice pentru cetățenii (vulnerabili) săraci energetic din Republica Moldova, precum și să ofere posibilități de înființare și ajustare metodologică și modificări legislative pentru a sprijini Ministerul Muncii și Protecției Sociale în acest efort.

63. Având în vedere complexitatea sistemului, implementarea acestuia va fi efectuată pe etape, în funcție de mijloacele financiare disponibile din bugetul de stat, din proiecte de asistentă tehnică și alte mijloace financiare, conform legislației în vigoare.

NOTĂ INFORMATIVĂ

la proiectul hotărârii Guvernului pentru aprobarea Conceptului Sistemului Informațional „Vulnerabilitatea Energetică”

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului

Proiectul hotărârii Guvernului cu privire la aprobarea Conceptului Sistemului Informațional „Vulnerabilitatea Energetică”, elaborat de către Ministerul Muncii și Protecției Sociale împreună cu suportul Programului Națiunilor Unite pentru Dezvoltare (UNDP Moldova).

2. Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile urmărite

Pe fundalul crizei la nivel global, care a generat o creștere a prețurilor gazelor naturale a influențat la majorarea semnificativă a facturilor la energie pentru consumatori, comparativ cu perioada similară a anului trecut. Toate aceste aspecte, dar și nivelul ridicat al inflației, eficiența energetică redusă, veniturile mici în rândul populației vor afecta în mod semnificativ sărăcia în Republica Moldova, două forme importante de sărăcie devenind în mod special proeminente: sărăcia energetică și sărăcia alimentară. Astfel, creșterea numărului persoanelor vulnerabile din punct de vedere energetic ar putea crește semnificativ. Prin sărăcie energetică poate fi înțeleasă situația în care gospodăriile nu pot avea acces la servicii energetice esențiale, cum sunt încălzirea, iluminatul și resurse de energie adecvate pentru alimentarea aparatelor electrocasnice sunt servicii esențiale care susțin un standard de viață și sănătate decent. În acest context, pentru prevenirea creșterii nivelului de sărăcie energetică în rândurile consumatorilor vulnerabili, este important să se asigure forme de ajutor și protecție socială, pentru care în prezent există un deficit de finanțare. Drept răspuns la această criză, pentru a aborda sistematic vulnerabilitatea energetică și pentru a promova eficiența energetică, prin Legea nr. nr. 241/2022 a fost creat Fond de reducere a vulnerabilității energetice pentru a oferi compensații în factură pentru consumatorii de gaze naturale, energie termică și energie electrică, în dependență de categoria de vulnerabilitate la care vor fi atribuiți.

Astfel, Legea nr. 241/2022 cu privire la Fondul de reducere a vulnerabilității energetice, prevede modul de organizare și funcționare a Fondului de reducere a vulnerabilității energetice, măsurile și programele finanțate din mijloacele acestui fond, îndreptate spre prevenirea și combaterea vulnerabilității energetice a populației și creșterea accesibilității energiei în rândul consumatorilor vulnerabili, precum și spre promovarea creșterii eficienței energetice. Pentru a asigura activitatea eficientă a Fondului de reducere a vulnerabilității energetice, Legea menționată prevede la art. 6, implementarea unei soluții informatice/crearea Sistemului informațional „Vulnerabilitatea Energetică” care să poată asigura aplicabilitatea sistemului de compensații pentru cetățeni în dependență de categoria de vulnerabilitate. Respectiv,

pentru dezvoltarea Sistemului informațional „Vulnerabilitatea Energetică” a fost elaborat și se propune pentru aprobare Conceptul acestuia.

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

Proiectul de hotărâre nu are drept scop armonizarea legislației naționale cu legislația Uniunii Europene

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

Proiectul hotărârii Guvernului prevede aprobarea Conceptului Sistemului informațional „Vulnerabilitatea Energetică” - resursa informațională a sistemului reprezintă un spațiu informațional unic, destinat:

- dezvoltarea unui sistem informațional de compensare a energiei sigur și fiabil pentru Republica Moldova;
- crearea, funcționarea și întreținerea unui sistem de înregistrare și prelucrarea solicitărilor privind compensarea cheltuielilor la consumul de energie a consumatorilor casnici;
- evidența centralizată automatizată a solicitanților și beneficiarilor de compensații, evidența centralizată a furnizorilor de energie;
- asigurarea operativității în activitatea de gestionare a compensațiilor la energie pentru consumatorii casnici;
- automatizarea procesului de gestionare a compensațiilor privind compensarea cheltuielilor la energie, excluderea factorului uman în procesul de acordare a compensațiilor;

Principiile de bază ale proiectului sunt:

- Compensația oferită va avea un caracter cuprinzător și va acoperi consumul de gaze naturale, energie termică și energie electrică;
- Compensația pentru energie se reflectă direct pe factură, prin reducerea sumei facturii (i.e. consumatorii eligibili nu vor primi compensații în bani, dar vor beneficia de o reducere a costului facturii la consumul casnic de energie).
- Măsura de sprijin este destinată pentru consumatorii cei mai vulnerabili. Prin urmare, profilul de vulnerabilitate al fiecărui beneficiar va fi dedus printr-o categorizare, luând în considerare mai multe criterii obiective.
- Valoarea compensației se va stabili în funcție de prețurile la energie, cu posibilitatea de a fi revizuită și stabilită periodic de Guvern.

Pentru a putea beneficia de compensații în baza legii, consumatorul vulnerabil se va înregistra prin intermediul interfeței Sistemului informațional „Vulnerabilitatea Energetică”, Sistem informațional administrat de Ministerul Muncii și Protecției Sociale, în care se date privind parametrii de vulnerabilitate energetică a consumatorilor casnici, în modul stabilit de Guvern. În baza informațiilor furnizate, consumatorului îi va fi atribuită o categorie de vulnerabile. Clasificarea categoriilor de consumatori

vulnerabili se bazează pe o serie de parametri, inclusiv venitul, costurile cu energia ca pondere din venit, mărimea gospodăriei, tipul sistemului de încălzire utilizate, aprobate de Guvern.

5. Fundamentarea economico-financiară

Implementarea prezentului proiect nu implică surse financiare suplimentare din bugetul de stat. Proiectul în cauză va avea impact asupra bugetului începând cu anul 2024 în cuantum de 50 000,00 MDL/an pentru mentenanța Sistemului Informațional. Sursele financiare nu se regăsesc în Cadrul Bugetar pe Termen Mediu 2023-2025. Prin urmare, costurile respective urmează a fi încadrate în volumul resurselor estimate sectorului și incluse în procesul cadrului bugetar pe termen mediu. Dezvoltarea Sistemului Informațional va fi finanțată de către Programul Națiunilor Unite pentru Dezvoltare (UNDP Moldova), care va aloca în acest scop mijloace financiare în cuantum de 40 000,00 USD.

6. Modul de încorporare a actului în cadrul normativ în vigoare

Proiectul nu presupune modificarea altor acte legislative în mod complementar. Guvernul urmează să aprobe regulamentele prevăzute de proiectul de Legea nr. 241/2022 cu privire la Fondul de reducere a vulnerabilității energetice.

7. Avizarea și consultarea publică a proiectului

În scopul respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional, anunțul privind inițierea elaborării proiectului este plasat pe pagina web a Ministerului Muncii și Protecției), în compartimentul „Transparența Decizională”, precum și a fi supus avizării și consultării publice în conformitate cu procedura stabilită prin Legea nr. 100/2017 cu privire la actele normative și Legea nr. 239/2008 privind transparența în procesul decizional.

8. Constatările expertizei anticorupție

Informația privind rezultatele expertizei anticorupție va fi inclusă după recepționarea raportului de expertiză anticorupție în sinteza obiecțiilor și propunerilor la proiectul de hotărâre.

9. Constatările expertizei de compatibilitate

Proiectul de hotărâre nu are drept scop armonizarea legislației naționale cu legislația Uniunii Europene.

10. Constatările expertizei juridice

Informația referitoare la concluziile expertizei privind compatibilitatea proiectului de hotărâre cu alte acte normative în vigoare, precum și respectarea normelor de tehnică legislativă va fi inclusă după recepționarea expertizei juridice în sinteza obiecțiilor și propunerilor/recomandărilor la proiectul de hotărâre.

11. Constatările altor expertize

Alte expertize nu au fost elaborate.