proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. _____
din _____

cu privire la Sistemul Informațional „Monitorizarea și coordonarea antifraudă”

În temeiul 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 și completările ulterioare, Guvernul HOTĂRĂȘTE:

1. Se instituie Sistemul informațional „Monitorizarea și coordonarea antifraudă” și resursa informațională formată de acesta.

2. Se aprobă:

2.1. Conceptul Sistemului informațional „Monitorizarea și coordonarea antifraudă”, conform anexei nr. 1;

2.2. Regulamentul resursei informaționale formate de Sistemul informațional „Monitorizarea și coordonarea antifraudă”, conform anexei nr. 2.

3. Inspectoratul Control Financiar de Stat, în calitate de posesor și deținător al Sistemul Informațional „Monitorizarea și coordonarea antifraudă”, va asigura condiţiile juridice, financiare şi organizatorice pentru crearea, administrarea, funcţionarea şi dezvoltarea continuă a acestuia în conformitate cu legislaţia şi acordurile internaţionale la care Republica Moldova este parte.

4. Instituția Publică „Centrul de Tehnologii Informaționale în Finanțe”, în calitate de administrator tehnic al Sistemului informațional „Monitorizarea și coordonarea antifraudă”, va asigura administrarea tehnică, mentenanţa și dezvoltarea acestuia, precum și implementarea cerinţelor de securitate stabilite de actele normative în domeniu.

5. Crearea, administrarea, mentenanţa şi dezvoltarea Sistemului informațional „Monitorizarea și coordonarea antifraudă”, se va realiza din contul şi în limitele alocaţiilor aprobate în acest scop în bugetul Inspectoratului Control Financiar de Stat, precum şi din alte surse, conform legislaţiei.

6. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Finanțelor.

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

PRIM-MINISTRU **Alexandru MUNTEANU**

Contrasemnează:
Viceprim-ministru,
Ministru al dezvoltării
economice şi digitalizării **Eugeniu OSMOCHESCU**

Ministru al finanțelor **Andrian GAVRILIȚĂ**

Anexa nr.1 la Hotărârea Guvernului
nr.____din_____

Conceptul Sistemului informațional „Monitorizarea și coordonarea antifraudă”

Capitolul I. Introducere

În contextul modernizării mecanismelor de gestionare a fondurilor publice și externe, autoritățile Republicii Moldova au identificat necesitatea consolidării capacităților instituționale pentru prevenirea și detectarea timpurie a neregulilor. Experiența acumulată în implementarea programelor finanțate din surse naționale și internaționale a evidențiat oportunitatea introducerii unui cadru tehnologic și operațional care să permită monitorizarea integrată a proceselor, precum și coordonarea eficientă a acțiunilor instituțiilor cu atribuții în domeniu.

Crearea Sistemului Informațional „Monitorizarea și coordonarea antifraudă” (*în continuare SI „MCAF”)* reprezintă o etapă necesară în consolidarea mecanismelor de guvernanță și integritate financiară ale Republicii Moldova, având ca obiectiv principal dezvoltarea unui cadru modern de prevenire și gestionare a riscurilor asociate utilizării fondurilor publice și externe. Necesitatea acestui sistem rezultă din procesul firesc de modernizare a administrației publice și din angajamentele asumate de stat în raport cu partenerii internaționali, în special în contextul cooperării cu Uniunea Europeană pentru protejarea intereselor sale financiare.

Fundamentul deciziei de a institui SI „MCAF” este legat de necesitatea unei coordonări eficiente între instituțiile care exercită funcții de control, audit, supraveghere și investigație, precum și de crearea unui mecanism unitar de colectare și gestionare a informațiilor privind potențiale nereguli. În lipsa unei astfel de structuri centralizate, procesele de reacție instituțională pot fi fragmentate, ceea ce limitează capacitatea administrației publice de a interveni în timp util pentru prevenirea incidentelor ce pot afecta buna gestiune financiară.

SI „MCAF” va funcționa ca o platformă integrată care va permite înregistrarea și administrarea centralizată a informațiilor privind suspiciuni sau indicii preliminare de fraudă, facilitând coordonarea dosarelor cu instituțiile abilitate pentru examinare și acțiuni ulterioare. Totodată, sistemul va contribui la îmbunătățirea schimbului de date între autoritățile naționale, la creșterea capacității de analiză și la coordonarea intervențiilor instituționale în situațiile ce necesită o reacție promptă și bine fundamentată.

Prin instituirea acestui sistem, Republica Moldova va dispune de un cadru consolidat pentru monitorizarea, prevenirea și tratarea neregulilor într-o manieră coerentă, predictibilă și transparentă, ceea ce va contribui la întărirea încrederii în modul de utilizare a resurselor publice și a celor provenite din fonduri externe, precum și la modernizarea continuă a practicilor de guvernanță financiară.

Prezentul concept stabilește cadrul general pentru implementarea SI „MCAF”, definind aspectele tehnice și operaționale necesare pentru asigurarea unui sistem eficient, rezilient și pe deplin integrat în infrastructura națională de monitorizare și coordonare antifraudă.

Capitolul II. Dispoziții generale

1. Conceptul SI „MCAF” stabilește scopul, obiectivele, funcțiile, structura organizațională și cadrul normativ necesar pentru crearea şi exploatarea acestuia, obiectele informaționale, lista seturilor de date care se păstrează în acesta și se furnizează, infrastructura tehnologică și măsurile pentru asigurarea securității și protecției informației, precum şi măsurile privind crearea, implementarea, exploatarea şi mentenanța SI „MCAF”.

2. SI „MCAF” reprezintă o platformă informațională integrată, destinată colectării, analizării și gestionării centralizate a datelor privind neregulile și riscurile de fraudă, precum și coordonării interinstituționale a acțiunilor de prevenire și monitorizare a utilizării fondurilor publice și externe.

3. În sensul prezentului concept, sunt prezentate următoarele noțiuni principale ce semnifică:

3.1. *Date* - informația despre persoane, subiecte, fapte, evenimente, fenomene, procese, obiecte, situații etc. prezentate într-o formă care permite comunicarea și prelucrarea lor;

3.2. *Proces* - succesiune de acțiuni sau de operații prin care se realizează o lucrare;

3.3. *Semnătură electronică* - conform semnificației din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;

3.4 *Actori* - oameni, organizații, sisteme sau dispozitive care folosesc sau interacționează cu sistemul;

3.5. *Business-proces* - consecutivitatea fixată a evenimentelor, realizată printr-un grup de activități legate logic, care utilizează resursele organizației pentru obținerea rezultatului la realizarea scopurilor organizației;

3.6. *MPass* - are înțelesul noțiunii definite în Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);

3.7. *MSign* - are înțelesul noțiunii definite în Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);

3.8. *MLog* – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);

3.9. *MCloud* – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);

3.10. *MConnect* – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);

3.11. *MNotify* – are înțelesul noțiunii definite în Hotărârea Guvernului nr. 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);

3.12. *coordonare antifraudă* - ansamblu de acțiuni care asigură coordonarea eforturilor, schimbul de informații și desfășurarea activităților legale în comun, care vizează întregul spectru de acțiuni potrivit domeniului de competență al fiecărei componente a sistemului, în scopul acordării sprijinului necesar și asigurării mecanismului de protecție a intereselor financiare ale statului și ale partenerilor externi de dezvoltare pentru a nu admite fraudarea fondurilor de asistență externă;

3.13. *raportorii de nereguli și/sau suspiciuni de fraudă* - persoane care informează despre nereguli și/sau suspiciuni de fraudă.

4. Obiectivele de bază stabilite pentru SI „MCAF”:

4.1. *Centralizarea și gestionarea informațiilor* - sistemul permite colectarea și stocarea centralizată a datelor referitoare la incidente, rapoarte și evaluări de risc. Această centralizare facilitează accesul rapid la informații corecte și actualizate, permițând luarea deciziilor pe baze obiective și informate;

4.2. *Cooperarea și coordonarea interinstituțională* - sistemul asigură un cadru pentru schimbul de informații între instituțiile statului implicate în activități antifraudă. Prin coordonare eficientă, se evită suprapunerile, se optimizează resursele și se garantează un răspuns unit la incidentele semnalate;

4.3. *Sprijinirea procesului decizional* - prin analiza datelor și generarea de rapoarte și evaluări de risc, Sistemul contribuie la fundamentarea deciziilor strategice și operaționale ale autorităților. Astfel, măsurile luate sunt mai eficiente, iar prioritizarea resurselor se face în funcție de riscurile reale identificate;

4.4. *Creșterea încrederii partenerilor externi de dezvoltare* - implementarea unui mecanism coerent și sigur de monitorizare antifraudă întărește încrederea donatorilor și partenerilor internaționali în capacitatea administrativă a statului de a gestiona resursele publice și fondurile externe în mod transparent și responsabil;

4.5. *Crearea unei baze de date istorice și statistice* - colectarea centralizată a informațiilor despre incidentele și dosarele antifraudă permite realizarea de analize statistice, identificarea tendințelor și modelarea riscurilor viitoare;

5. La dezvoltarea și implementarea sistemului informatic se va ține cont de următoarele principii generale:

5.1. *Principiul legalității* care presupune crearea și exploatarea sistemului informatic în conformitate cu legislația națională în vigoare, a normelor și standardelor internaționale recunoscute în domeniu;

5.2. *Principiul respectării standardelor deschise* care presupune adopția exclusivă a standardelor deschise destinate conceptualizării și funcționării sistemului conform recomandărilor și practicilor internaționale în domeniu destinate publicării, comunicării, interoperabilității și definirii sistemului de meta-date al soluției informatice;

5.3. *Principiul divizării arhitecturii pe nivele* care constă în proiectarea independentă a subsistemelor în conformitate cu standardele de interfață dintre nivele;

5.4. *Principiul independenței de platformă* conform căruia interfața utilizator a sistemului informatic nu va impune o anumită platformă software și hardware pentru calculatorul client al utilizatorului;

5.5. *Principiul datelor sigure* care presupune asigurarea procedurilor de introducere în sistem doar a datelor veridice utilizându-se canale autorizate și autentificate;

5.6. *Principiul securității informaționale* care presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și de acces nesancționat;

5.7. *Principiul protecției datelor cu caracter personal* care presupune crearea și exploatarea sistemului de evidență a accesului la serviciile electronice în conformitate cu acordurile și convențiile internaționale, precum și cu legislația națională în vigoare în domeniul protecției datelor cu caracter personal;

5.8. *Principiul accesibilității informației cu caracter public* care presupune implementarea procedurilor de asigurare a accesului solicitanților la informația cu caracter public furnizată de soluția informatică;

5.9. *Principiul transparenței* care presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicații, întru accesarea liberă a tuturor sistemelor, a informațiilor generate prin intermediul sistemelor, precum și monitorizarea datelor înregistrate aferent entității;

5.10. *Principiul expansibilității* care stipulează posibilitatea extinderii și completării sistemului informatic cu noi funcții sau îmbunătățirea celor existente;

5.11. *Principiul scalabilității* care presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului informatic;

5.12. *Principiul simplității și comodității utilizării* care presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor sistemului informatic, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție;

5.13. *Principiul centralizării* care presupune unificarea mai multor business-procese într-un singur sistem uniform și unificat, precum și centralizarea acestora în cadrul aparatului central pentru monitorizarea funcționării eficiente;

5.14. *Principiul adaptabilității și flexibilității* care constă în asigurarea posibilității de a ajusta configurația sistemelor la necesitate, ce au tangență cu procesul de oferire a accesului la serviciile electronice, pentru rezolvarea dificultăților noi și pentru funcționarea în condiții și regimuri în schimbare;

5.15. *Principiul controlului* care presupune monitorizarea măsurilor ce asigură calitatea, fiabilitatea resurselor și sistemelor informaționale ale Inspectoratului, precum și păstrarea și utilizarea rațională a acestora.

6. Sarcinile de bază ale SI „MCAF” derivă din necesitatea asigurării unui cadru unitar de monitorizare și coordonare a acțiunilor antifraudă la nivel național. Sistemul este conceput pentru a sprijini activitatea instituțiilor în identificarea timpurie a riscurilor, gestionarea eficientă a informațiilor și coordonarea intervențiilor necesare. În acest sens, sarcinile de bază ale sistemului includ:

6.1. Colectarea și consolidarea informațiilor relevante, provenite de la instituțiile publice responsabile de monitorizarea, controlul și prevenirea neregulilor și fraudelor;

6.2. Evidența și monitorizarea sesizărilor, controalelor, investigațiilor și altor acțiuni antifraudă, pentru a asigura trasabilitatea completă a fiecărei etape din procesul operațional;

6.3. Gestionarea integrată a fluxurilor informaționale, inclusiv recepționarea, procesarea, transmiterea și arhivarea datelor în format digital, conform cerințelor legale și procedurale;

6.4. Asigurarea unui mecanism unitar de coordonare interinstituțională, prin facilitarea schimbului de informații și comunicării operative între autoritățile implicate;

6.5. Generarea rapoartelor, analizelor și indicatorilor, necesare pentru evaluarea eficienței măsurilor și fundamentarea deciziilor la nivel managerial și strategic;

6.6. Integrarea cu serviciile și platformele guvernamentale, precum MPass, MLog, MConnect, MSign și MNotify, pentru a asigura autentificarea sigură, jurnalizarea completă, interoperabilitatea și comunicarea automatizată;

6.7. Asigurarea protecției și securității datelor, prin respectarea standardelor naționale și internaționale privind confidențialitatea, integritatea și disponibilitatea informațiilor gestionate.

Capitolul III. Spațiul juridico-normativ al funcționării SI ”MCAF”

7. Cadrul normativ al SI „MCAF” cuprinde ansamblul actelor normative care reglementează procesele de elaborare, implementare și monitorizare a politicilor publice, precum și domeniul tehnologiilor informaționale și al transformării digitale. La baza creării sistemului stă Hotărârea Guvernului nr. 271/2025 cu privire la organizarea și funcționarea Sistemului Național Antifraudă, care stabilește principiile, regulile și responsabilitățile de funcționare, asigurând conformitatea sistemului

cu standardele naționale și cu cerințele instituțiilor abilitate. În plus, funcționarea sistemului este reglementată și de alte acte normative, precum:

7.1 Legea nr. 1069/2000 cu privire la informatică;
7.2 Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;
7.3 Legea nr. 158/2008 cu privire la funcția publică și statutul funcționarului public;
7.4 Legea nr. 199/2010 cu privire la statutul persoanelor cu funcții de demnitate publică;
7.5 Legea nr. 133/2011 privind protecția datelor cu caracter personal;
7.6 Legea nr. 155/2011 pentru aprobarea Clasificatorului unic al funcțiilor publice;
7.7 Legea nr. 98/2012 privind administrația publică centrală de specialitate;
7.8 Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;
7.9 Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;
7.10 Legea nr. 148/2023 privind accesul la informațiile de interes public;
7.11 Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;
7.12 Hotărârea Guvernului nr. 710/2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare);
7.13 Hotărârea Guvernului nr. 656/2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate;
7.14 Hotărârea Guvernului nr. 857/2013 cu privire la aprobarea Strategiei naționale de dezvoltare a societății informaționale „Moldova Digitală 2020”;
7.15 Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
7.16 Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
7.17 Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
7.18 Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);
7.19 Hotărârea Guvernului nr. 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a acestuia;
7.20 Hotărârea Guvernului nr. 712/2020 cu privire la serviciul guvernamental de plăți electronice (MPay);
7.21 Hotărârea Guvernului nr. 323/2021 pentru aprobarea Conceptului Sistemului informațional „Catalogul semantic” și a Regulamentului privind modul de ținere a Registrului format de Sistemul informațional „Catalogul semantic”;
7.22 Hotărârea Guvernului nr. 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023–2030;
7.23 Hotărârea Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice;
7.24 Ordin nr. 78/2006 cu privire la aprobarea reglementării tehnice Procesele ciclului de viaţă al software-ului” RT 38370656 - 002:2006.

Capitolul IV. Spațiul funcțional al SI ”MCAF”

8. Funcțiile de bază ale SI „MCAF” sunt următoarele:

8.1. *Colectare și gestionare centralizată a datelor antifraudă* - asigurarea înregistrării, actualizării și administrării într-o bază unică a informațiilor privind sesizările, neregulile și măsurile întreprinse;

8.2. *Generarea rapoartelor și a indicatorilor de performanță* – asigurarea instrumentelor pentru generarea rapoartelor operative, analitice și statistice, necesare managementului pentru evaluarea performanței activităților antifraudă;

8.3. *Interoperabilitatea* – asigurarea schimbului de date cu alte sisteme informaționale prin intermediul platformei de interoperabilitate (MConnect);

8.4. *Jurnalizarea evenimentelor* – asigurarea jurnalizării automatizate a tuturor evenimentelor de business prin mecanisme speciale de verificare și audit (MLog etc.);

8.5. *Asigurarea calității informației* – asigurarea calității informației din contul creării și menținerii componentelor sistemului calității, bazat pe abordare procesuală;

8.6. *Securitatea și confidențialitatea* – corespunderea cerințelor în materie de securitate și confidențialitate, și anume:

8.6.1. protejarea datelor subiectului de date cu caracter personal, prin mecanisme adecvate de securitate;

8.6.2. integritatea informațiilor și autenticitatea utilizatorilor prin mecanisme de autentificare care prevăd utilizarea certificatelor calificate ale cheilor publice, eliberate în condițiile actelor normative în domeniul semnăturii electronice și documentului electronic;

8.6.3. aplicarea politicii corespunzătoare de securitate la nivelul serviciilor web.

8.7. *Administrarea și monitorizarea* – asigurarea următoarelor funcții:

8.7.1. administrarea utilizatorilor, rolurilor și accesului la sistem;

8.7.2. asigurarea integrității logice a sistemului;

8.7.3. administrarea bazelor de date ale sistemului;

8.7.4. gestionarea copiilor de rezervă;

8.7.5. monitorizarea performanței sistemului;

8.7.5. suport tehnic și mentenanță.

9. Contururile funcționale de bază ale SI „MCAF" sunt:

9.1. *Conturul destinat raportorilor de nereguli și/sau suspiciuni de fraudă* - acest contur este dedicat persoanelor fizice, juridice, angajaților instituțiilor publice sau altor entități autorizate care raportează nereguli, suspiciuni de fraudă, utilizare necorespunzătoare a fondurilor sau alte acțiuni ce pot afecta integritatea proceselor administrative:

9.1.1 depunerea online a sesizărilor privind posibile fapte de fraudă, delapidare de fonduri sau nereguli procedurale;

9.1.2. înregistrarea automată a sesizării și generarea unui număr unic de identificare;

9.1.3. posibilitatea atașării materialelor probante (documente, imagini, fișiere audio/video);

9.1.4. verificarea statutului de examinare a sesizării, în funcție de nivelul de confidențialitate;

9.1.5. primirea notificărilor automatizate privind etapele procesării sesizării.

9.2. *Conturul destinat instituțiilor implicate în procesul de coordonare antifraudă* - acest contur este destinat funcționarilor și specialiștilor instituțiilor responsabili de gestionarea sesizărilor și dosarelor:

9.2.1. înregistrarea și gestionarea dosarelor de nereguli;

9.2.2. analizarea sesizărilor și efectuarea investigațiilor interne;

9.2.3. gestionarea acțiunilor de urmările și monitorizarea implementării acestora;

9.2.4. acces la informații relevante prin integrarea interoperabilă cu alte sisteme;

9.2.5. evidența și trasabilitatea tuturor operațiunilor asociate unui dosar antifraudă;

9.2.6. cabinet personal al funcționarului, cu vizualizarea sarcinilor și notificărilor;

9.2.7. interacțiunea digitală cu alte instituții pentru coordonarea măsurilor antifraudă.

9.3. *Conturul destinat entităților partenere și donatorilor externi* - include structurile de audit extern, organizațiile internaționale, partenerii de dezvoltare și alte instituții autorizate:

9.3.1. consultarea rapoartelor privind măsurile antifraudă;

9.4. *Conturul destinat instituției coordonatoare* - acest contur este destinat instituției care coordonează implementarea și monitorizarea politicilor antifraudă:

9.4.1. vizualizarea și extragerea analizelor consolidate;

9.4.2. acces la rapoarte și indicatori;

9.4.3. acces la tablourile de bord cu situația riscurilor și neregulilor;

9.5. *Conturul de administrare a sistemului* - acest contur permite gestionarea centralizată a parametrilor sistemului, configurărilor și controlului operațional:

9.5.1. administrarea utilizatorilor și gestionarea drepturilor de acces;

9.5.2. administrarea parametrilor și configurațiilor sistemului;

9.5.3. jurnalizarea evenimentelor, monitorizarea activităților și auditarea acestora;

9.5.4. gestionarea copiilor de rezervă și restaurarea datelor;

9.5.5. gestionarea clasificatoarelor, nomenclatoarelor și șabloanelor documentare;

9.5.6. monitorizarea performanței sistemului;

9.5.7. asigurarea securității și integrității datelor.

10. Interacțiunea SI „MCAF" cu alte platforme și resurse digitale guvernamentale reprezintă un element esențial pentru asigurarea unei funcționări eficiente, coerente și integrate la nivel interinstituțional. Sistemul va utiliza infrastructura națională de interoperabilitate pentru a obține, verifica și corela date relevante necesare proceselor antifraudă, reducând duplicarea informațiilor și sporind acuratețea analizelor. SI „MCAF" se va integra cu următoarele platforme și sisteme informaționale partajate instituite de Guvern:

10.1. *Platforma de interoperabilitate MConnect* – pentru schimbul securizat de date între instituții, necesar preluării informațiilor privind entitățile, persoanele, tranzacțiile și alte date relevante investigațiilor și proceselor de prevenire a fraudei;

10.2. *Serviciul de autentificare MPass* – pentru identificarea și autentificarea utilizatorilor, asigurând acces diferențiat în funcție de roluri și niveluri de autorizare;

10.3. *Serviciul guvernamental de semnătură electronică MSign* – pentru semnarea electronică a documentelor;

10.4. *Serviciul guvernamental de notificare MNotify* – pentru transmiterea automată a notificărilor către utilizatori privind stadiul dosarelor, sesizărilor, termenelor procedurale și altor acțiuni relevante din sistem;

10.5. *Serviciul de jurnalizare MLog* – pentru păstrarea evidenței tuturor operațiunilor efectuate în sistem, în scopul asigurării trasabilității și auditării activităților;

10.6. *Sisteme informaționale instituționale relevante (precum cele ale MF, MAI, ANI, CNA, Curtea de Conturi, Cancelaria de Stat, autorități de management ale proiectelor finanțate extern)* - în vederea schimbului de date operative privind beneficiarii, contractele, riscurile identificate, istoricul neregulilor și statusul acțiunilor corective;

10.7. *Sisteme de gestiune financiară și contabilă* utilizate în cadrul programelor de finanțare naționale sau externe, pentru verificarea și corelarea datelor privind utilizarea fondurilor și detectarea eventualelor anomalii.

11. Interacțiunea cu aceste sisteme va fi realizată în conformitate cu standardele naționale de interoperabilitate, cerințele de securitate cibernetică, principiul minimizării datelor și regulile de protecție a datelor cu caracter personal. Comunicarea între platforme se va efectua prin canale securizate, iar toate schimburile de date vor fi documentate și supuse mecanismelor de audit.

Capitolul V. Structura organizațională a SI ”MCAF”

12. Proprietarul SI „MCAF” este statul, care îşi realizează dreptul de proprietate, de gestionare și utilizare a datelor din sistemul informațional.

13. Posesorul și deținătorul SI „MCAF” este Inspectoratul Control Financiar de Stat, instituție care este responsabilă de asigurarea dezvoltării, implementării, operării și întreținerii sistemului pe întreaga durată a ciclului său de viață.

14. Administratorul tehnic al SI „MCAF” este Instituția Publică „Centrul de Tehnologii Informaționale în Finanțe”, care își exercită atribuțiile în conformitate cu actele normative în domeniul administrării tehnice și menținerii sistemelor informaționale de stat.

15. Utilizatorii SI „MCAF” sunt persoanele desemnate din cadrul instituțiilor competente, cărora le sunt atribuite drepturi de acces în funcție de responsabilitățile funcționale, precum și persoanele fizice și juridice care pot depune sesizări privind nereguli sau suspiciuni de fraudă.

16. În figura 1 sunt ilustrate, într-o formă grafică, principalele părți implicate/instituțiile statului care vor avea roluri active în furnizarea datelor pentru gestionarea și soluționarea dosarelor aflate în lucru:

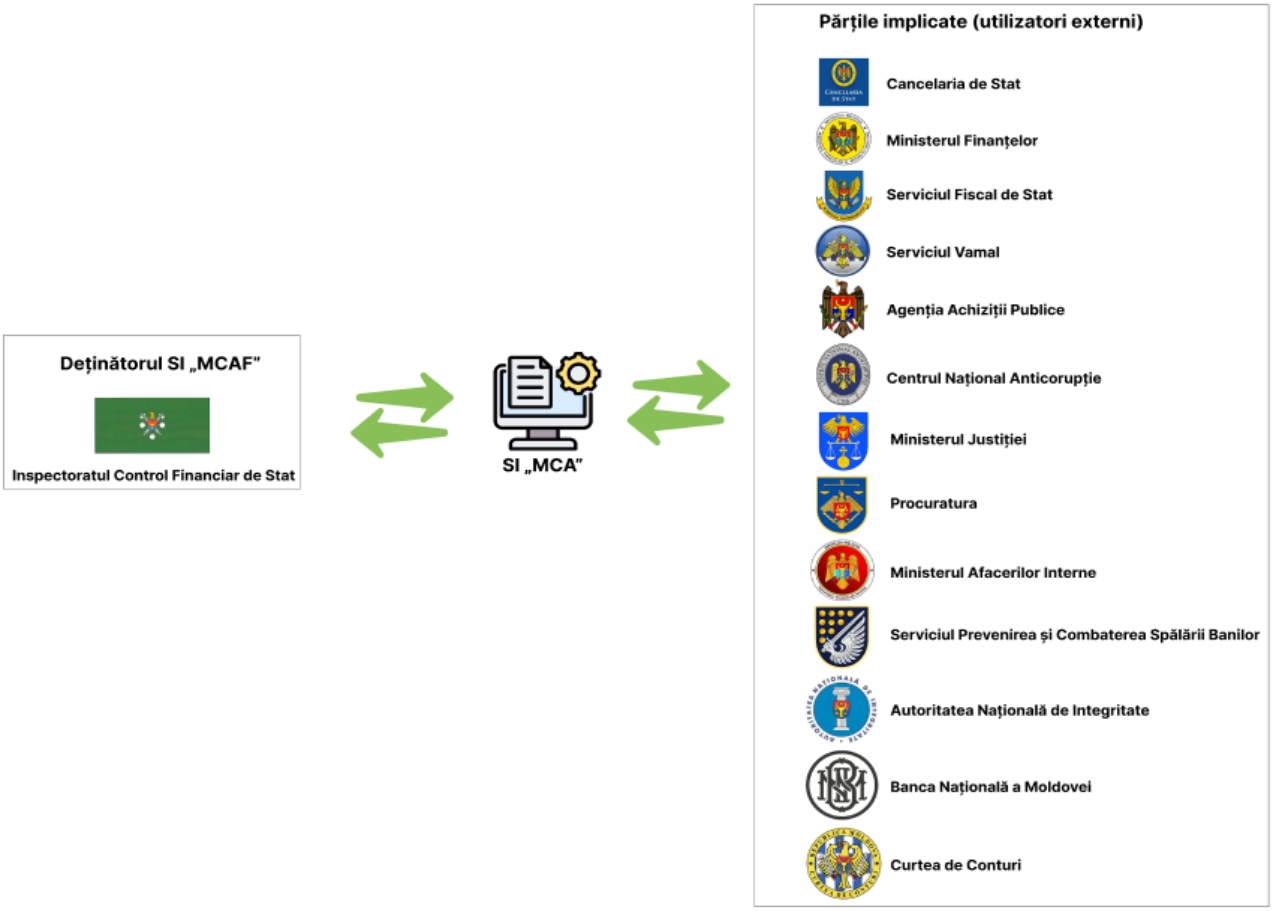

Figura 1. Furnizorii de date

16.1. *Cancelaria de Stat* are rolul de coordonare a activităților interinstituționale legate de implementarea proiectelor și programelor de asistență externă. În cadrul SI „MCAF", aceasta furnizează informații privind derularea proiectelor, eventualele nereguli sau riscuri identificate și contribuie la consolidarea cooperării dintre instituțiile publice și partenerii de dezvoltare;

16.2. *Ministerul Finanțelor* este responsabil de gestionarea datelor financiare privind fondurile externe și fluxurile de finanțare. Prin intermediul SI „MCAF", ministerul transmite informații despre beneficiari, monitorizează utilizarea fondurilor și oferă suport analitic pentru identificarea abaterilor și neregulilor financiare;

16.3. *Serviciul Fiscal de Stat* interacționează cu SI „MCAF" prin furnizarea datelor fiscale necesare verificărilor și analizelor de risc. Instituția contribuie la detectarea potențialelor fraude prin corelarea informațiilor despre contribuabili, tranzacții și obligații fiscale;

16.4. *Serviciul Vamal* oferă sistemului SI „MCAF" acces la datele privind operațiunile de import și export, facilitând documentarea cazurilor suspecte de fraudă vamală sau deturnare a fondurilor. De asemenea, colaborează în cadrul acțiunilor comune de control;

16.5. *Agenția Achiziții Publice* colaborează cu SI „MCAF" prin transmiterea informațiilor despre contractele de achiziție finanțate din fonduri externe. Rolul său este de a asigura transparența și verificarea corectitudinii proceselor de achiziție publică;

16.6. *Inspectoratul Control Financiar de Stat* oferă sistemului date privind rezultatele controalelor efectuate la nivelul instituțiilor beneficiare de fonduri. Prin integrarea în SI „MCAF", Inspectoratul contribuie la centralizarea și analiza neregulilor constatate;

15.7. *Centrul Național Anticorupție* interacționează cu SI „MCAF" prin furnizarea informațiilor referitoare la investigațiile desfășurate în cazurile ce implică fonduri externe. Instituția sprijină sistemul în activitățile de prevenire, detectare și investigare a fraudelor și actelor de corupție;

16.8. *Ministerul Justiției* are rolul de a oferi expertiză juridică și de a asigura conformitatea cadrului normativ utilizat în SI „MCAF". Acesta contribuie la formularea politicilor și procedurilor juridice care reglementează prevenirea și combaterea neregulilor;

16.9. *Procuratura* utilizează SI „MCAF" pentru documentarea cazurilor și accesarea informațiilor relevante în procesul de urmărire penală. Instituția contribuie la consolidarea cooperării interinstituționale în gestionarea cazurilor de fraudă și corupție;

16.10. *Ministerul Afacerilor Interne* colaborează cu SI „MCAF" prin furnizarea informațiilor operative și de investigație, necesare în documentarea cazurilor ce afectează interesele financiare ale statului. De asemenea, sprijină activitățile de control și investigare comună;

16.11. *Serviciul Prevenirea și Combaterea Spălării Banilor* contribuie la sistemul SI „MCAF” prin transmiterea datelor despre tranzacțiile și activitățile financiare suspecte. Instituția asigură cooperarea și schimbul de informații privind riscurile de fraudă și spălare a banilor;

16.12. *Autoritatea Națională de Integritate* colaborează cu SI „MCAF” prin furnizarea informațiilor despre controalele efectuate privind averile și interesele personale ale funcționarilor. Aceasta contribuie la identificarea situațiilor care pot genera riscuri de integritate sau conflicte de interese;

16.13. *Banca Națională a Moldovei* interacționează cu SI „MCAF” prin schimbul de informații referitoare la activitățile și tranzacțiile financiare relevante, contribuind la detectarea anomaliilor și riscurilor sistemice care pot indica posibile fraude;

16.14. *Curtea de Conturi* colaborează cu SI „MCAF” prin furnizarea rapoartelor de audit și a constatărilor privind gestionarea fondurilor. Prin integrarea acestor informații, sistemul sprijină procesele de monitorizare, analiză și raportare la nivel național.

17. SI „MCAF” va furniza un mecanism dinamic și flexibil de configurare a rolurilor și drepturilor deținute de utilizatori. La implementarea SI „MCAF” următoarele roluri, conform figurii 2, urmează a fi implementate:

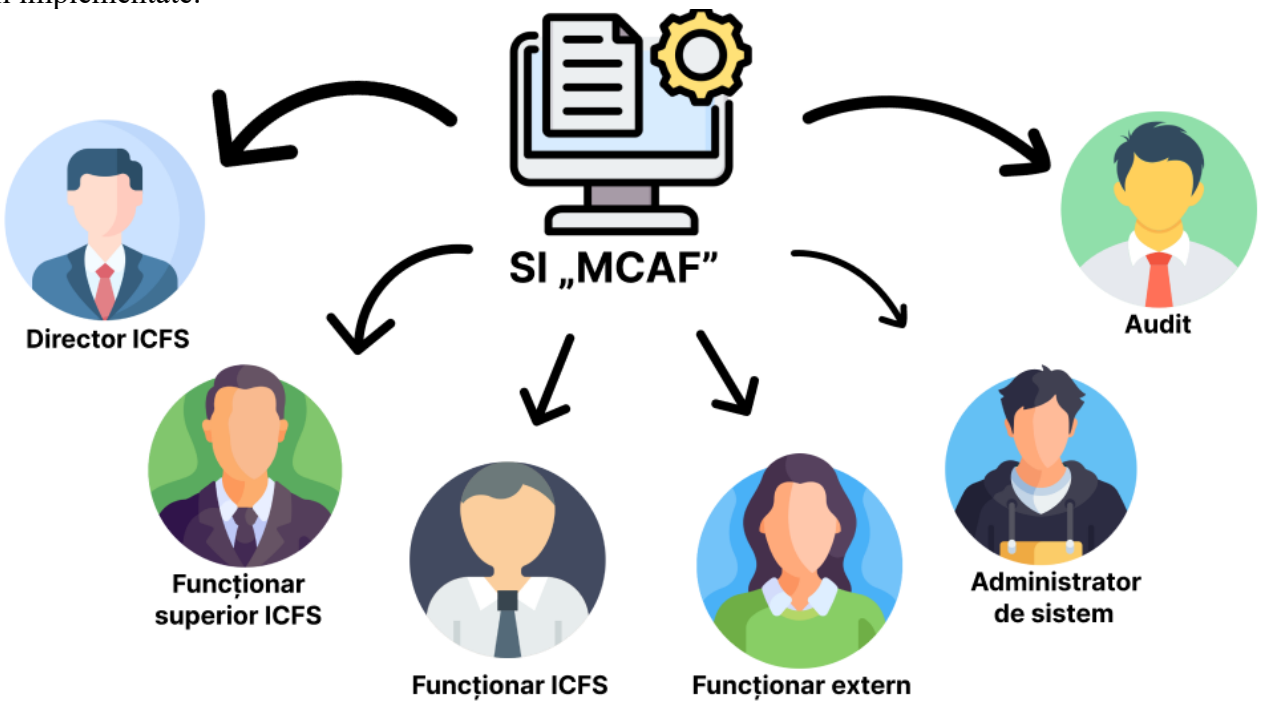

Figura 2. Rolurile în cadrul Sistemului Informațional

17.1. *Director ICFS* - utilizator în cadrul sistemului, responsabil de aprobarea finală a documentelor, sesizărilor, deciziilor și rapoartelor transmise de funcționarii și funcționarii superiori ICFS. Funcționalități disponibile rolului:

17.1.1. Autentificare în sistem prin serviciul guvernamental de autentificare și control (MPass);

17.1.2. Vizualizarea tuturor sesizărilor, dosarelor și documentelor care necesită aprobare la nivel de conducere;

17.1.3. Semnarea electronică a documentelor și deciziilor transmise de funcționarii și funcționarii superiori ICFS;

17.1.4. Validarea finală a închiderii investigațiilor;

17.1.5. Monitorizarea indicatorilor generali de activitate și performanță ai ICFS;

17.1.6. Acces la vizualizarea consolidată a tuturor dosarelor active și istorice, fără posibilitatea modificării datelor operative;

17.1.7. Primirea notificărilor privind documentele și acțiunile ce necesită semnătură.

17.2. *Funcționar superior ICFS* - utilizator cu drepturi avansate, responsabil de validarea, aprobarea și coordonarea activităților funcționarilor subordonați. Funcționalități disponibile rolului:

17.2.1. Autentificare în sistem prin serviciul guvernamental de autentificare și control (MPass);

17.2.2. Vizualizarea și validarea sesizărilor și dosarelor create de funcționarii ICFS;

17.2.3. Aprobarea inițierii investigațiilor și desemnarea echipelor responsabile;

17.2.4. Gestionarea fluxului de lucru pentru cazurile active (alocare, redirecționare, suspendare, închidere);

17.2.5. Vizualizarea rapoartelor consolidate și a indicatorilor statistici;

17.2.6. Gestionarea accesului limitat al funcționarilor la dosarele sub coordonare;

17.2.7. Validarea transmiterii informațiilor către instituții externe.

17.3. *Funcționar ICFS* - utilizator operațional al sistemului, responsabil de introducerea, actualizarea și consultarea datelor referitoare la sesizări și investigații. Funcționalități disponibile rolului:

17.3.1. Autentificare în sistem prin serviciul guvernamental de autentificare și control (MPass);

17.3.2. Vizualizarea tabloului de bord personal (taskuri, notificări, dosare active);

17.3.3. Completarea și transmiterea sesizărilor către funcționarii superiori;

17.3.4 Crearea și gestionarea dosarelor de investigație (în limitele competenței atribuite);

17.3.5. Atașarea documentelor și probelor electronice la dosare;

17.3.6. Actualizarea stadiului investigației;

17.3.7. Consultarea registrelor și bazelor de date integrate (în funcție de permisiuni);

17.3.8. Generarea de rapoarte operaționale;

17.3.9. Primirea notificărilor automate privind modificările din dosarele atribuite;

17.3.10. Participarea la schimbul de informații cu funcționarii externi (prin interfață securizată).

17.4. *Funcționar extern* - reprezentant al unei instituții partenere sau colaboratoare (de ex. SFS, SV, MF, alte autorități), care interacționează cu sistemul pentru transmiterea sau recepționarea informațiilor relevante. Funcționalități disponibile rolului:

17.4.1. Autentificare în sistem prin MPass (nivel corespunzător identității instituționale);

17.4.2. Vizualizarea și descărcarea datelor/informațiilor partajate de ICFS;

17.4.3. Transmiterea către ICFS a documentelor, sesizărilor sau informațiilor complementare;

17.4.4. Răspuns la solicitări de date din partea funcționarilor ICFS;

17.4.5. Consultarea statutului solicitărilor trimise;

17.4.6. Acces limitat la modulele sistemului, conform protocolului de colaborare;

17.4.7. Notificare automată privind actualizările relevante.

17.5. *Administrator de sistem* - responsabil de administrarea tehnică a sistemului, gestionarea conturilor de utilizator, a drepturilor de acces și asigurarea funcționării optime a infrastructurii informatice. Funcționalități disponibile rolului:

17.5.1. Administrarea conturilor utilizatorilor (creare, suspendare, reactivare);

17.5.2. Atribuirea și modificarea rolurilor și permisiunilor în sistem;

17.5.3. Monitorizarea utilizării resurselor și performanței sistemului;

17.5.4. Administrarea jurnalelor de sistem și efectuarea backupurilor;

17.5.5. Gestionarea versiunilor aplicației și actualizărilor software;

17.5.6. Suport tehnic și rezolvarea incidentelor raportate;

17.5.7. Generarea rapoartelor de audit tehnic și securitate.

17.6. *Audit* - utilizator independent, cu acces doar în regim de citire, destinat verificării conformității, trasabilității și integrității datelor din sistem. Funcționalități disponibile rolului:

17.6.1. Acces securizat la jurnalele electronice de activitate;

17.6.2. Vizualizarea istoricului acțiunilor utilizatorilor;

17.6.3. Consultarea rapoartelor de audit privind accesările, modificările și operațiunile efectuate;

17.6.4. Generarea de rapoarte privind conformitatea cu politicile interne și reglementările legale;

17.6.5. Verificarea respectării regulilor de acces și a nivelurilor de autorizare;

17.6.6. Acces la date în mod read-only, fără posibilitatea de modificare.

Capitolul VI. Documentele SI ”MCAF”

18. În cadrul SI „MCAF” se gestionează următoarele categorii de documente:

18.1. *documente de intrare* - care constituie temeiul legal și operațional pentru înregistrarea, actualizarea și procesarea datelor în sistem;

18.2. *documente de ieșire* - generate în rezultatul funcționării sistemului și utilizate în activitățile de monitorizare, coordonare, analiză și raportare;

18.3. *documente tehnologice* - elaborate în scopul asigurării operabilității, interoperabilității și securității sistemului.

19. Documentele de intrare includ setul de acte și informații utilizate pentru inițierea, raportarea și documentarea situațiilor ce implică riscuri, nereguli sau suspiciuni de fraudă. Acestea includ, fără a se limita la:

19.1. Sesizări privind nereguli sau suspiciuni de fraudă, depuse de:

19.1.1. persoane fizice sau juridice;

19.1.2. raportori interni din cadrul instituțiilor publice;

19.1.3. instituții ale statului cu atribuții de control sau investigare;

19.1.4. parteneri externi de dezvoltare.
19.2. Rapoarte interne ale instituțiilor implicate, inclusiv:
19.2.1. rapoarte de control financiar;
19.2.2. note de constatare;
19.2.3. procese-verbale privind verificări tematice;
19.2.4. notificări privind risc sporit sau incidente repetate.
19.3. Date și informații recepționate prin interoperabilitate, provenite de la alte sisteme informaționale de stat, cum ar fi:
19.3.1. informații fiscale și vamale;
19.3.2. date despre proiecte finanțate din surse externe;
19.3.3. date privind beneficiarilor programelor publice;
19.3.4. informații contabile și financiare relevante.
19.4. Documente justificative transmise în format electronic, precum:
19.4.1. documente contabile sau financiare;
19.4.2. contracte, anexe, facturi și rapoarte de cheltuieli;
19.4.3. documente de corespondență oficială;
19.4.4. dovezi, fișiere media sau documente informative atașate sesizărilor.
20. Documentele de ieșire reprezintă setul de informații generate automat sau manual de sistem, utilizate pentru luarea deciziilor, monitorizare și raportare. Acestea includ:
20.1. Rapoarte privind gestionarea sesizărilor, inclusiv:
20.1.2. confirmări de înregistrare;
20.1.3. extrase privind stadiul examinării;
20.1.4. informări privind rezultatele evaluării preliminare;
20.1.5. răspunsuri oficiale către raportori sau instituțiile implicate.
20.2. Documente analitice, precum:
20.2.1. rapoarte statistice privind tipurile și frecvența neregulilor;
20.2.2. analize de risc și tendințe;
20.2.3. sinteze privind evoluția indicatorilor antifraudă;
20.2.4. rapoarte tematice destinate conducerii ICFS și altor autorități interesate.
20.3 Documente de coordonare interinstituțională, cum ar fi:
20.3.1. notificări transmise altor autorități;
20.3.2. solicitări de completare a datelor;
20.3.3. extrase generate pentru partenerii externi de dezvoltare.
20.4. Acte generate în cadrul dosarelor electronice, inclusiv:
20.4.1. fișe de dosar;
20.4.2. note conceptuale privind acțiunile întreprinse.
21. Documentele tehnologice sunt utilizate pentru funcționarea tehnică, operarea, securitatea și administrarea sistemului. Acestea includ:
21.1. Proceduri tehnice și ghiduri de utilizare, precum:
21.1.1. instrucțiuni pentru operatori și administratori;
21.1.2. proceduri operaționale standard;
21.1.3. manuale privind fluxurile de procesare.
21.2. Documentație pentru instalare, configurare și interoperabilitate, care include:
21.2.1. cerințe privind infrastructura hardware și software;
21.2.2. specificații ale interfețelor programatice;
21.2.3. protocoale de schimb de date cu serviciile MPass, MLog, MConnect, MNotify, MSign.
21.3. Documente privind securitatea informațională, inclusiv:
21.3.1. politici de acces și autentificare;
21.3.2. proceduri de protecție și criptare a datelor;
21.3.3. protocoale de prevenire și reacție la incidente cibernetice.
21.4. Documente de administrare și mentenanță, precum:
21.4.1. proceduri de backup și restaurare;
21.4.2. manuale pentru monitorizarea performanței și integrității datelor.

Capitolul VII. Spațiul informațional al SI ”MCAF”

22. În cadrul SI „MCAF” se gestionează un ansamblu de obiecte informaționale esențiale pentru funcționarea proceselor de monitorizare, investigare și raportare a neregulilor și riscurilor asociate gestionării resurselor publice. Obiectele informaționale constituie unitățile principale de date ale

sistemului, fiind structurate și administrate conform cadrului normativ aplicabil și necesităților operaționale ale autorităților implicate.

23. Obiectele informaționale de bază a sistemului sunt următoarele (reprezentate grafic în figura 3):

23.1. Obiectul „Sesizare;
23.2. Obiectul „Dosar antifraudă”;
23.3. Obiectul „Entitate monitorizată”;
23.4. Obiectul „Utilizator al sistemului”;
23.5. Obiectul „Raport”;
23.6. Obiectul „Eveniment de sistem (Log)”;
23.7. Obiectul „Clasificator / Nomenclator”.

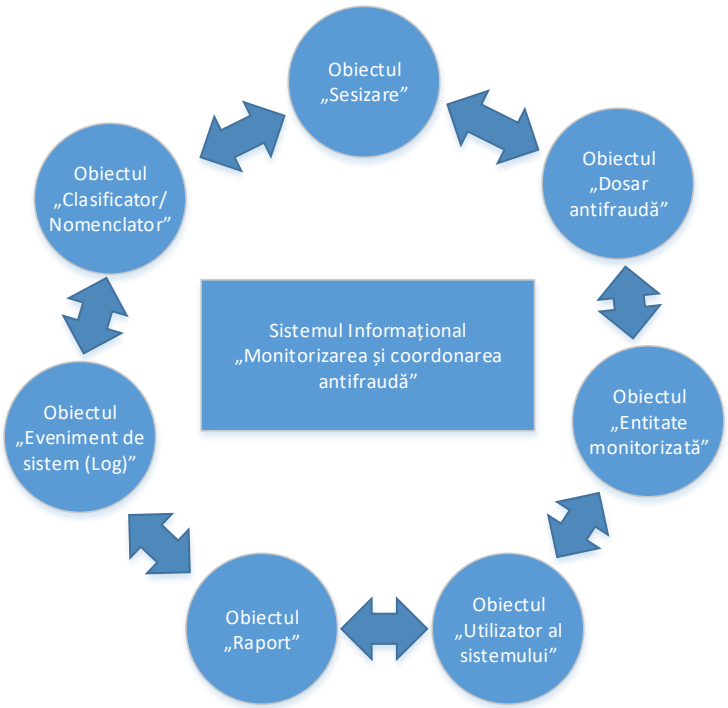

Figura 3. Obiectele informaționale de bază

24. *Obiectul „Sesizare”*- Include informații privind notificările depuse de raportori, persoane fizice, juridice sau instituții, referitoare la posibile nereguli, abateri, fraude, conflicte de interese sau alte incidente aferente utilizării fondurilor publice. Elemente tipice:

24.1. identificator sesizare;
24.1. date despre raportor (în funcție de tipul raportării: nominală sau anonimă);
24.2. circumstanțele sesizării;
24.3. descrierea neregulii sau suspiciunii;
24.4. documente justificative anexate;
24.5. data și modalitatea depunerii;
24.6. statutul sesizării (înregistrată, în examinare, soluționată etc.).

25. *Obiectul „Dosar antifraudă” – r*eprezintă unitatea centrală de gestiune a activităților de analiză, verificare și coordonare a acțiunilor întreprinse în legătură cu o sesizare sau situație de risc. Elemente tipice:

25.1. identificator dosar;
25.1. date generale despre dosar;
25.2. participanți și instituții implicate;
25.3. documente interne generate pe parcursul procesării dosarului;
25.4. decizii, măsuri, concluzii și recomandări;
25.5. istoricul tuturor acțiunilor reprezentând trasabilitatea completă.

26. *Obiectul „Entitate monitorizată”* - reprezintă datele privind instituțiile publice, operatorii economici sau alți beneficiari ai fondurilor publice supuși proceselor de monitorizare sau investigație. Elemente tipice:

26.1. identificare (denumire, IDNO, statut);
26.2. programe/ granturi/ proiecte în derulare;
26.3. istoricul controalelor și verificărilor;
26.4. persoanele responsabile și date de contact.

27. *Obiectul „Utilizator al sistemului”* - include informații despre utilizatorii autorizați ai SI „MCAF”, Elemente tipice:

27.1. Identificator al obiectului informațional - numărul de identificare de stat al persoanei fizice (IDNP) preluat din Registrul de stat al populației sau, după caz, numărul de identificare de stat al persoanei juridice (IDNO) preluat din Registrul de stat al unităților de drept.;

27.2. roluri și drepturi de acces;

27.3. instituția de apartenență;

27.4. istoricul acțiunilor efectuate în sistem.

28. *Obiectul „Raport”* - include rezultatele consolidate ale proceselor de monitorizare și evaluare. Elemente tipice:

28.1. identificator raport;

28.1. statistici privind sesizările;

28.2. rapoarte pentru Guvern, donatori, instituții de control.

29. Obiectul „Eveniment de sistem (Log)” - gestionează toate evenimentele de audit, inclusiv autentificări, modificări de date, accesări, erori, încercări neautorizate de acces, conform cerințelor MLog.

29.1. identificator eveniment de sistem;

30. Obiectul „Clasificator / Nomenclator” - Include liste standardizate utilizate în întregul sistem, cum ar fi:

30.1. identificator clasificator/nomenclator;

30.1. categorii de sesizări;

30.2. tipuri de documente;

30.3. statutul sesizărilor și dosarelor;

30.4. instituții și autorități publice;

30.5. clasificatoare de interoperabilitate.

31. Scenariile operaționale asociate fiecărui obiect informațional gestionat în cadrul SI „MCAF”. Scenariile descriu ciclul de viață al datelor, interacțiunile principale ale utilizatorilor cu sistemul și regulile specifice de procesare.

31.1. *Obiectul „Sesizare”* - scenarii principale:

31.1.1. Depunerea unei sesizări:

31.1.1.1. Raportorul completează formularul electronic;

31.1.1.2. Sistemul validează datele obligatorii și atribuie număr unic de înregistrare.

31.1.2. Evaluarea preliminară a sesizării:

31.1.2.1. Funcționarul ICFS verifică conformitatea formală;

31.1.2.2. Sistemul generează statut „în examinare” și notifică raportorul (dacă nu este anonim).

31.1.3. Transmiterea spre analiză detaliată:

31.1.3.1. Sesizarea este asociată unui dosar antifraudă existent sau generează un dosar nou.

31.1.4. Soluționarea și arhivarea:

31.1.4.1. Se întocmește decizia finală;

31.1.4.2. Statutul sesizării devine „soluționată”, iar documentele rămân arhivate în dosarul aferent.

31.2. *Obiectul „Dosar antifraudă”* - scenarii principale:

31.2.1. Crearea unui dosar:

31.2.1.1. Sistemul creează dosar nou la primirea unei sesizări relevante sau a unui risc confirmat.

31.2.2. Actualizarea dosarului:

31.2.2.1. Documentele, măsurile și rezultatele intermediare sunt încărcate continuu;

31.2.2.2. Sistemul păstrează istoricul modificărilor.

31.2.3. Închiderea dosarului:

31.2.3.1. Se emit concluziile finale și recomandările;

31.2.3.2. Dosarul se arhivează cu statutul final (Soluționat/Anulat,etc).

31.3. *Obiectul „Entitate monitorizată”* - scenarii principale:

31.3.1. Înregistrarea unei entități:

31.3.1.1. Sistemul importă date din surse externe (ex.: ASP, MF, alte registre);

31.3.1.2. Asocierea cu dosare și sesizări.

31.4. *Obiectul „Utilizator al sistemului”* - scenarii principale:

31.4.1. Autentificarea în sistem:

31.4.1.1. Utilizatorul accesează SI „MCAF” prin MPass.

31.4.2. Atribuirea rolurilor:

31.4.2.1. Administratorul de sistem acordă sau revocă drepturi.

31.4.3. Monitorizarea activităților utilizatorului:
31.4.3.1. Sistemul înregistrează toate acțiunile în logurile de audit.
31.5. *Obiectul „Raport”* - scenarii principale:
31.5.1. Generarea rapoartelor periodice:
31.5.1.1. Sistemul compilează date privind sesizările și dosarele.
31.5.2. Exportul și distribuirea:
31.5.2.1. Rapoartele pot fi exportate în formatele aprobate (PDF, XLSX).
31.5.3. Vizualizări interactive:
31.5.3.1. Utilizatorii interni pot accesa tablouri de bord (dashboards).
31.6. *Obiectul „Eveniment de sistem (Log)”* - scenarii principale:
31.6.1. Înregistrarea evenimentelor de audit:
31.6.1.1. Autentificări, accesări și modificări sunt logate automat.
31.6.2. Monitorizarea tentativelor neautorizate:
31.6.2.1. Sistemul generează alerte către administrator.
31.6.3. Exportul logurilor în MLog:
31.6.3.1. Conform standardelor de securitate.
31.7. *Obiectul „Clasificator / Nomenclator”* - scenarii principale:
31.7.1. Actualizarea clasificatoarelor/nomenclatoarelor:
31.7.1.1. Administratorul poate actualiza clasificatoarele/nomenclatoarele.
31.7.2. Propagarea modificărilor:
31.7.2.1. Sistemul actualizează automat obiectele dependente.
31.7.3. Integrarea cu nomenclatoare externe:
31.7.3.1. Sincronizare periodică cu sistemele naționale interoperabile.

32. Dacă pentru înregistrarea datelor referitoare la monitorizarea și coordonarea antifraudă este necesară preluarea informațiilor disponibile în resursele informaționale ale altor autorități publice, acestea sunt consumate și furnizate prin intermediul platformei de interoperabilitate MConnect, cu respectarea legislației privind protecția datelor cu caracter personal și securitatea informațională, inclusiv cu utilizarea MConnect Events, în vederea automatizării Public fluxurilor de date și realizării funcționalităților/serviciilor proactive, în conformitate cu ghidul tehnic relevant publicat de Agenția de Guvernare Electronică.

Capitolul VIII. Spațiul tehnologic al SI ”MCAF”

33. Fluxul operațional constă din pașii următori, reprezentat grafic în figura 4:

33.1. Raportare sesizare – înregistrarea unei sesizări privind existența unei situații, acțiuni sau inacțiuni susceptibile de a necesita examinare. În această etapă se consemnează circumstanțele faptice inițiale, sursa sesizării, data raportării, precum și orice informații ori materiale justificative puse la dispoziție. Raportarea constituie temeiul juridic pentru inițierea procedurii de analiză;

33.2. Deschidere dosar – ca urmare a constatării caracterului întemeiat al sesizării, urmează deschiderea unui dosar, care se atribuie unui identificator unic și în cadrul căruia sunt administrate toate actele și informațiile aferente. În această etapă se stabilesc responsabilul desemnat, categoria juridică a cazului, precum și statutul procesual inițial, în conformitate cu prevederile normative incidente;

33.3. Agregarea informațiilor aferente dosarului – în vederea realizării unei examinări complete și obiective, se efectuează colectarea, solicitarea și centralizarea tuturor informațiilor relevante. Acestea pot proveni din registre oficiale, sisteme informaționale, instituții publice, după caz. Activitățile întreprinse includ verificarea veridicității datelor, corelarea acestora și completarea informațiilor necesare pentru fundamentarea soluției ce urmează a fi emisă;

33.4. Documentarea materialelor – materialele și informațiile administrate sunt sistematizate și consemnate în actele dosarului. Documentarea se realizează cu respectarea cerințelor de formă și conținut stabilite de cadrul normativ aplicabil, asigurându-se integritatea, acuratețea și trasabilitatea elementelor probatorii;

33.5. Decizie – pe baza materialelor acumulate în dosar, autoritatea competentă deliberează și adoptă decizia corespunzătoare cadrului legal. Decizia este motivată în fapt și în drept, indicând circumstanțele constatate, temeiurile juridice aplicate, precum și măsurile dispuse, după caz. Actul decizional se consemnează formal și devine parte integrantă a dosarului;

33.6. Arhivare dosar – după emiterea deciziei și finalizarea procedurii, dosarul se închide și se transmite spre arhivare, în conformitate cu normele privind evidența și păstrarea documentelor.

Arhivarea asigură conservarea, accesibilitatea și integritatea actelor dosarului pentru eventuale verificări ulterioare, audit, controale sau alte necesități legale.

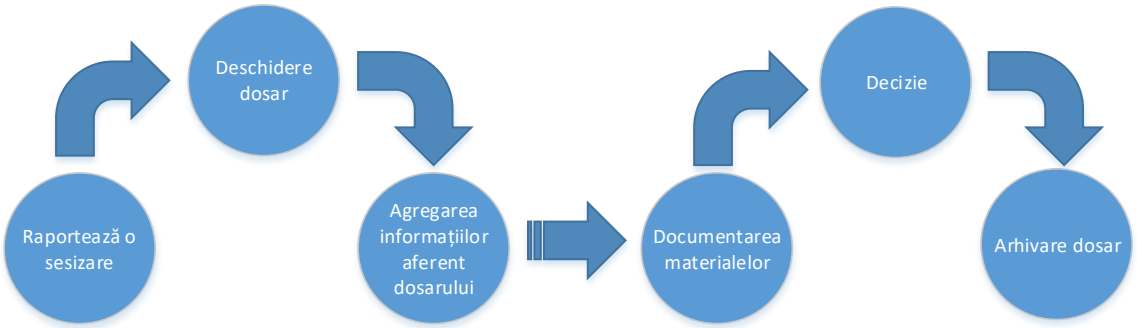

Figura 4. Fluxul operațional

34. SI „MCAF” utilizează standarde deschise și este compatibil cu sistemele informaționale care aplică atât standarde non-proprietare, cât și standarde tehnologice existente la nivel guvernamental.

35. Arhitectura complexului software-hardware, precum și lista produselor software și a echipamentelor tehnice necesare pentru crearea infrastructurii informaționale se stabilesc de către posesorul SI „MCAF” la etapele ulterioare de dezvoltare și implementare a sistemului, cu respectarea următoarelor principii:

35.1. implementarea unei soluții bazate pe arhitectura orientată pe servicii (Service-Oriented Architecture – SOA), care să permită reutilizarea funcționalităților SI „MCAF” în dezvoltările ulterioare, fără afectarea funcționării existente;

35.2. implementarea mecanismelor de arhivare (backup) periodică și de restabilire rapidă a datelor în caz de incidente operaționale sau de securitate.

36. SI „MCAF” va asigura posibilitatea de scalare verticală și orizontală a resurselor hardware, pentru a garanta suportul necesar în exploatare, atât în regim normal de lucru, cât și în perioadele de vârf generate de creșterea numărului de utilizatori și a volumelor de date procesate.

37. Sistemul de comunicații utilizat de SI „MCAF” se va baza pe infrastructura rețelelor guvernamentale, asigurând conectivitate permanentă și posibilitatea de acces la internet. Configurarea infrastructurii va fi realizată astfel încât să ofere nivele corespunzătoare de performanță, disponibilitate și capacitate.

38. Interfața utilizator a SI „MCAF” se va adapta automat la diferite rezoluții și tipuri de dispozitive, pentru a permite utilizarea sistemului atât pe stații fixe, cât și pe dispozitive mobile, cu păstrarea funcționalităților și accesibilității.

39. SI „MCAF” va fi găzduit pe platforma tehnologică guvernamentală comună (MCloud) și va fi compatibil cu platformele de găzduire bazate pe tehnologii de tip container, în vederea asigurării portabilității, elasticității și eficienței resurselor utilizate. Diagrama de arhitectură este prezentată în figura 5.

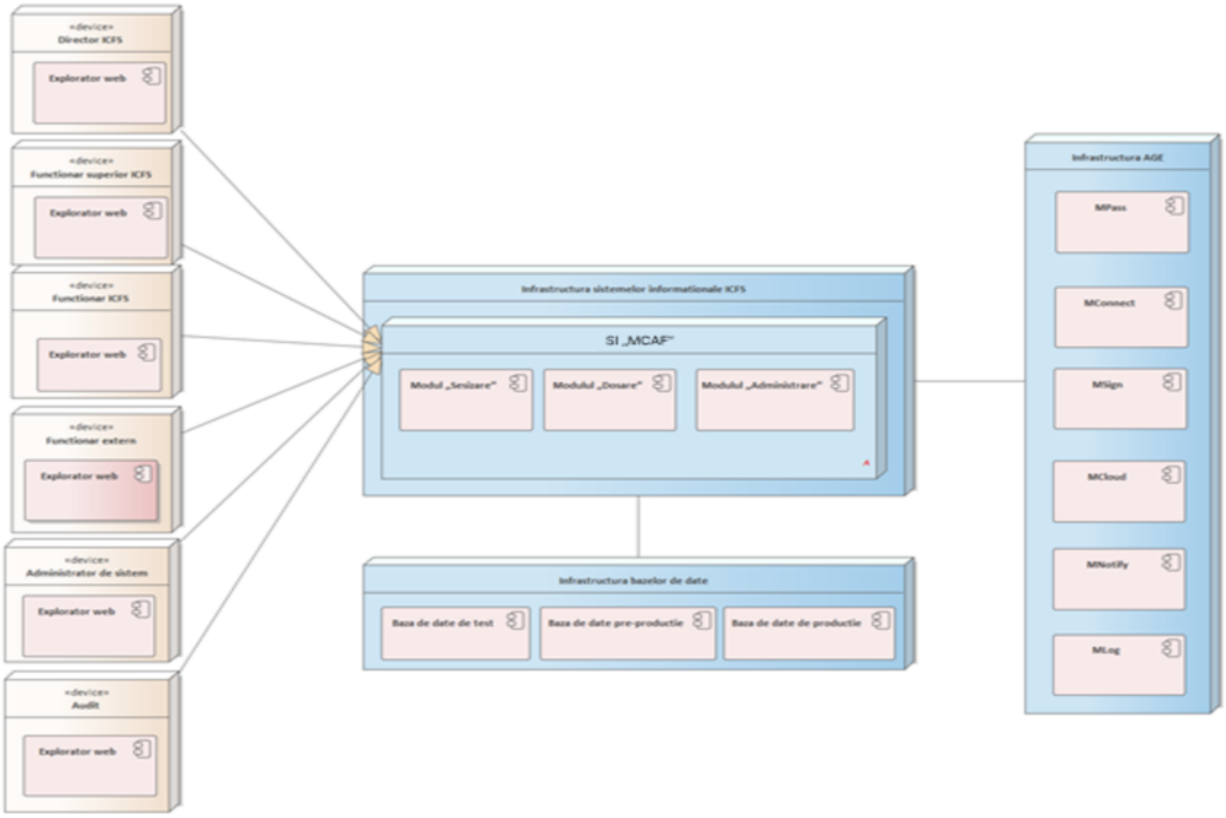

Figura 5. Diagrama de arhitectură

Capitolul IX. Asigurarea securității informaționale a SI ”MCAF”

40. Securitatea informațională a SI „MCAF” reprezintă totalitatea măsurilor tehnice, organizatorice și procedurale destinate protecției datelor și proceselor de prelucrare împotriva acțiunilor accidentale sau intenționate, naturale sau artificiale, care pot cauza prejudicii posesorului, deținătorului sau utilizatorilor sistemului.

41. Asigurarea securității informaționale va fi realizată în strictă conformitate cu Cerințele minime obligatorii de securitate cibernetică aprobate prin Hotărârea Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, precum și cu actele normative din domeniul protecției datelor cu caracter personal.

42. Pentru gestionarea riscurilor, posesorul și deținătorul SI „MCAF” vor implementa o Politică generală de securitate, care va include obligații privind instruirea personalului, audituri periodice de securitate, monitorizarea implementării regulilor și identificarea domeniilor care necesită îmbunătățiri.

43. Pentru a garanta protecția datelor și funcționarea fiabilă a SI „MCAF”, posesorul, deținătorul și registratorii vor aplica următoarele măsuri esențiale:

43.1. Măsuri organizatorice:

43.1.1. implementarea unei politici interne de securitate;

43.1.2. instruirea continuă a personalului privind riscurile informatice;

43.1.3. controlul accesului fizic în încăperile unde se află infrastructura sistemului;

43.1.4. utilizarea exclusivă a tehnologiilor certificate și conforme cadrului normativ.

43.2. Măsuri tehnice:

43.2.1. utilizarea mecanismelor de autentificare și autorizare prin MPass;

43.2.2. implementarea semnăturii electronice pentru garantarea integrității;

43.2.3. aplicarea firewall-urilor, soluțiilor antivirus și anti-spam la nivel de platformă;

43.2.4. utilizarea unui sistem de detectare și prevenire a intruziunilor;

43.2.5. asigurarea comunicării sigure între componente prin protocoale criptate;

43.2.6. realizarea copiilor de rezervă (backup) și proceduri de recuperare (restore);

43.2.7. monitorizarea și înregistrarea evenimentelor prin MLog.

43.3. Măsuri privind protecția datelor cu caracter personal:

43.3.1. prelucrarea exclusivă a datelor necesare scopului legal;

43.3.2. aplicarea măsurilor tehnice pentru prevenirea distrugerii, modificării, copierii sau răspândirii neautorizate a datelor;

43.3.3. respectarea drepturilor subiecților de date.

44. Principalele pericole la adresa securității informaționale a SI „MCAF” includ, dar nu se limitează la:

44.1. Pericole legate de date;
44.1.1. colectarea, stocarea și utilizarea ilegală a datelor;
44.1.2. încălcarea tehnologiei de prelucrare;
44.1.3. interceptarea, copierea sau falsificarea informației;
44.1.4. scurgerea informațiilor prin canale tehnice.
44.2. Pericole legate de infrastructură:
44.2.1. deteriorarea, nimicirea sau distrugerea echipamentelor;
44.2.2. instalarea de dispozitive neautorizate de interceptare;
44.2.3. utilizarea tehnologiilor necertificate sau vulnerabile.
44.3. Pericole cibernetice:
44.3.1. atacuri informatice, malware, programe care afectează funcționarea normală;
44.3.2. acces neautorizat la baze de date și aplicație;
44.3.3. compromiterea cheilor criptografice și a altor mecanisme de protecție.
44.4. Pericole legale sau procedurale:
44.4.1. nerespectarea restricțiilor privind răspândirea informației;
44.4.2. încălcarea Legii privind protecția datelor cu caracter personal.
45. Pentru atingerea obiectivelor de securitate, SI „MCAF" dispune de următoarele mecanisme de securitate:
45.1. *Semnătura electronică* – mecanism care asigură integritatea și non-repudierea datelor înregistrate în SI MCAF;
45.2. *Firewall* – filtrul firewall face parte din arhitectura tehnică a platformei tehnologice (MCloud), oferind protecție împotriva accesului neautorizat din exterior;
45.3. *Antivirus/anti-spam* – soluțiile hardware și/sau software asigură protecția antivirus și antispam pentru toate serverele. Fișierele încărcate în SI „MCAF" sunt scanate, iar în cazul detectării unui fișier infectat, procedura de încărcare este oprită, iar fișierul este respins;
45.4. *Sistem de detectare a intruziunilor* – detectează accesul neautorizat la nivelul componentelor de sistem ale SI „MCAF";
45.5. *Comunicare sigură* – schimbul de informații confidențiale între serverele web și utilizatori este securizat;
45.6. *Backup sistematic al datelor* – permite recuperarea rapidă și fiabilă a datelor în cazul unui incident care a dus la pierderea sau deteriorarea acestora;
45.7. *Instrument de înregistrare a evenimentelor de audit* – toate activitățile desfășurate de utilizatori, inclusiv încercările de conectare nereușite, sunt monitorizate și înregistrate în jurnalele SI „MCAF", cu acces strict limitat utilizatorilor neautorizați.

Capitolul X. Încheiere.

46. Implementarea SI „MCAF" va consta în crearea unei soluții moderne de colaborare, gestiune și automatizare a fluxurilor de lucru aferente sesizărilor și investigațiilor antifraudă, precum și în dezvoltarea unei arhive electronice centralizate a tuturor dosarelor și documentelor aferente sesizărilor și măsurilor dispuse. Se preconizează:
46.1. Îmbunătățirea calității și relevanței informațiilor, asigurând integritatea, exactitatea, accesibilitatea, comparabilitatea și coerența datelor colectate și procesate în cadrul sistemului;
46.2. Creșterea transparenței și a eficienței procesului decizional prin furnizarea rapidă de informații corecte și consistente către toate autoritățile implicate în monitorizarea și investigarea neregulilor;
46.3. Reducerea consumului de resurse materiale (hârtie, rechizite) și optimizarea fluxurilor de lucru prin digitalizarea proceselor;
46.4. Asigurarea continuității și securității datelor prin proceduri automate de backup, arhivare și restaurare a documentelor electronice;
46.5. Facilitarea comunicării și colaborării între instituțiile implicate în prevenirea și investigarea fraudelor, prin acces la informații centralizate și actualizate.
47. Implementarea SI „MCAF" va aduce următoarele beneficii concrete:
47.1. Creșterea transparenței activităților desfășurate de autoritățile implicate în gestionarea și investigarea sesizărilor de nereguli și fraude;
47.2. Securizarea accesului la date și aplicații, prin aplicarea politicilor de securitate, profilurilor de identitate și soluțiilor de gestiune a accesului;
47.3. Acces la informații autentice și consistente pentru toate autoritățile și persoanele implicate în investigarea și monitorizarea dosarelor;

47.4. Reducerea timpului de răspuns și sprijin decizional, prin acces rapid la date și rapoarte consolidate;

47.5. Acces rapid și garantat la date și informații, indiferent de locația utilizatorului;

47.6. Informarea continuă și promptă a actorilor implicați în derularea sesizărilor și investigațiilor antifraudă, inclusiv prin acces online la dosarele electronice;

47.7. Îmbunătățirea calității informațiilor prin asigurarea relevanței, integrității, exactității și coerenței acestora;

47.8. Consolidarea unei arhive digitale a dosarelor și documentelor procesate, cu proceduri automate de salvare și restaurare pentru protecția pe termen lung a datelor.

48. Implementarea sistemului se va face în conformitate cu Reglementarea tehnică „Procesele ciclului de viață al software-lui” RT 38370656-002:2006 și va avea următoarele activități obligatorii:

48.1. Analiza, proiectarea, dezvoltarea, implementarea şi testarea tuturor componentelor informatice;

48.2. Livrarea şi instalarea bunurilor constitutive ale sistemului, precum şi efectuarea tuturor lucrărilor aferente punerii în funcțiune a acestuia;

48.3. Acceptanţa, punerea în funcțiune, garanție şi suportul operaţional pentru componentele sistemului şi pentru sistemul integrat;

48.4. Managementul implementării proiectului, inclusiv pregătirea şi livrarea documentației aferente proiectului, în conformitate cu specificaţiile tehnice;

48.5. Trainingul şi transferul de know-how corespunzător, atât pentru operarea sistemului, cât şi pentru înregistrarea în sistem a procedurilor administrative;

48.6. Mentenanţa activă a sistemului este perioada în care dezvoltatorul sistemului îşi asumă obligaţiunea faţă de Inspectoratul Control Financiar de Stat de a-l asista în menţinerea capacităţii SIA „MCAF” de a presta servicii, precum şi de a modifica produsul software, păstrând integritatea lui.

Anexa nr.2 la Hotărârea Guvernului
nr. ___din___

Regulamentul resursei informaționale formate de Sistemul informațional „Monitorizarea și coordonarea antifraudă”

Capitolul I. Dispoziții generale

1. Regulamentul resursei informaționale formate de Sistemul informațional „Monitorizarea și coordonarea antifraudă” (în continuare – *Regulament*) stabilește drepturile și obligațiile subiecților raporturilor juridice aferente creării, exploatării și ținerii resursei informaționale, modalitatea de ținere a resursei informaționale, procedura de înregistrare, de modificare, de completare și de radiere a datelor, procedura de interacțiune cu furnizorii de date și măsurile privind asigurarea securității resursei informaționale.

2. Resursa informațională formată de Sistemul informațional „Monitorizarea și coordonarea antifraudă” (în continuare – *RI MCAF*) este un registru departamental de stat și constituie unica platformă informațională de automatizare a procesului de colectare, analiză și gestionare centralizată a datelor privind neregulile și riscurile de fraudă, precum și coordonarea interinstituțională a acțiunilor de prevenire și monitorizare a utilizării fondurilor publice și externe. RI MCAF va contribui la facilitarea schimbului de date între autoritățile naționale în domeniul prevenirii, depistării și combaterii fraudei, la creșterea capacității de analiză și la coordonarea intervențiilor instituționale în situațiile ce necesită o reacție promptă și bine fundamentată.

3. În prezentul Regulament sunt utilizate noțiunile și termenii definiți în Legea nr. 467/2003 cu privire la informatizare și resursele informaționale de stat și Legea nr. 71/2007 cu privire la registre, precum și Conceptul din Anexa nr. 1 a prezentei hotărâri.

4. RI MCAF este menținută în format electronic în limba română.

Capitolul II. Subiecții raporturilor juridice în domeniul creării și ținerii RI MCAF

5. Subiecții din domeniul creării, exploatării și al utilizării RI MCAF sunt:

5.1. proprietarul;

5.2. posesorul;

5.3. deținătorul;

5.4. furnizorul de date;

5.5. registratorul;

5.6. destinatarul datelor.

6. Proprietarul RI MCAF este statul, care realizează dreptul său de posesie, folosință și dispoziție asupra RI MCAF.

7. Posesorul și deținătorul RI MCAF este Inspectoratul Control Financiar de Stat care are următoarele atribuții:

7.1. asigură condițiile juridice, organizatorice și financiare pentru funcționarea și dezvoltarea RI MCAF;

7.2. stabilește scopurile și sarcinile funcționale ale RI MCAF;

7.3. asigură funcționarea, administrarea și dezvoltarea continuă a RI MCAF, inclusiv prin identificarea și integrarea noilor tipuri de funcționalități, în conformitate cu nivelul agreat de servicii și în limitele bugetului alocat;

7.4. autorizează, suspendă și revocă dreptul de acces la RI MCAF;

7.5. exercită alte atribuții necesare asigurării bunei funcționări a RI MCAF;

8. Registratorul de date este angajat al posesorului, care are posibilitatea și responsabilitatea de a înregistra, a actualiza și a radia date din cadrul RI MCAF.

9. Furnizorul de date este persoana juridică de drept public, care utilizează RI MCAF în vederea prezentării informației aferente detectării potențialelor fraude în cazurile ce implică fonduri externe.

10. Destinatarul datelor din RI MCAF este persoana juridică de drept public, care asigură procesul de investigare a potențialelor fraude în cazurile ce implică fonduri externe.

Capitolul III. Drepturile și obligațiile subiecților RI MCAF

Secțiunea 1

Drepturile și obligațiile posesorului și deținătorului

11. Posesorul și deținătorul RI MCAF are dreptul:

11.1. să utilizeze informația disponibilă în cadrul RI MCAF, în scopul executării atribuțiilor sale;

11.2. să solicite, în bază de contract, administratorului tehnic îmbunătățirea funcționalităților RI MCAF;

11.3. să inițieze procedura de suspendare a drepturilor de acces la RI MCAF pentru utilizatorii care nu respectă regulile de utilizare a RI MCAF;

11.4. să verifice autenticitatea și veridicitatea datelor transmise de către utilizatorii RI MCAF, după caz;

11.5. să asigure implementarea modificărilor, rectificărilor și dezvoltărilor solicitate;

11.6. să stabilească condițiile tehnice de funcționare a RI MCAF;

11.7. să înainteze propuneri de îmbunătățire a funcționalităților RI MCAF, precum și să le pună în aplicare;

11.8. să acorde suport consultativ pentru furnizorii și destinatarii de date din RI MCAF;

11.9. să autorizeze suspendarea activității RI MCAF în caz de situații excepționale, incidente sau riscuri semnificative de securitate pentru resursele informaționale de importanță publică, stabilite conform legislației.

12. Posesorul și deținătorul RI MCAF este obligat:

12.1. să asigure funcționarea, administrarea, dezvoltarea și promovarea continuă a RI MCAF, în conformitate cu nivelul agreat de servicii și în limitele bugetului alocat;

12.2. să asigure planificarea mijloacelor financiare pentru mentenanța și securitatea informațională a RI MCAF;

12.3. să asigure administrarea, mentenanța și securitatea informațională a RI MCAF;

12.4. să asigure atribuirea rolurilor și a drepturilor de acces la RI MCAF;

12.5. să monitorizeze procesul de înregistrare și de prelucrare a datelor în cadrul RI MCAF;

12.6. să supravegheze respectarea cerințelor de securitate a datelor de către subiecții RI MCAF și să identifice cazurile și tentativele de încălcare ale acestora;

12.7. să efectueze măsuri organizatorice și tehnice necesare pentru asigurarea protecției și a confidențialității informației disponibile în cadrul RI MCAF, inclusiv pentru prevenirea distrugerii, modificării, blocării, copierii neautorizate, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în raport cu riscurile prezentate de prelucrare și caracterul datelor prelucrate;

12.8. să asigure implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu cadrul normativ;

12.9. să asigure accesul securizat la informația conținută în RI MCAF și să respecte condițiile de securitate și regulile de exploatare a acestuia;

12.10. să dețină auditul accesărilor, care conține evidența operațiunilor ce au fost efectuate de către utilizatorii portalului și, la solicitare, în conformitate cu actele normative, să ofere informații despre auditul cu privire la accesări;

12.11. să intervină pentru investigarea, soluționarea și îndepărtarea erorilor identificate sau comunicate de către utilizatorii RI MCAF;

12.12. să informeze participanții RI MCAF despre modificările condițiilor tehnice de funcționare a acestuia;

12.13. să asigure suport metodologic și practic prin elaborarea procedurilor, a regulilor și a instrucțiunilor privind înregistrarea, acumularea, păstrarea, completarea, corectarea, sistematizarea și utilizarea datelor.

Secțiunea a 2-a

Drepturile și obligațiile furnizorului de date

13. Furnizorul de date al RI MCAF are dreptul:

13.1. să utilizeze funcționalitățile RI MCAF, conform rolului atribuit și competenței legale;

13.2. să solicite și să primească de la posesor suport consultativ metodologic și tehnic privind utilizarea RI MCAF;

13.3. să înainteze posesorului propuneri privind modificarea actelor normative care reglementează ținerea RI MCAF;

13.4. să înainteze posesorului propuneri cu privire la îmbunătățirea și sporirea eficacității funcționării RI MCAF.

14. Furnizorul de date al RI MCAF este obligat:

14.1. să respecte regulile de utilizare a RI MCAF;

14.2. să asigure corectitudinea, autenticitatea, veridicitatea și integritatea datelor furnizate, precum și respectarea termenelor de prezentare a acestora;

14.3. să colaboreze cu posesorul RI MCAF pentru asigurarea securității accesului la servicii și să informeze despre orice acțiune suspicioasă de care are cunoștință și care ar putea să reprezinte un atentat la serviciile respective;

14.4. să verifice procesul de plasare a informației în RI MCAF;

14.5. să nu plaseze în RI MCAF informații care pot fi obscene, defăimătoare sau ilegale;

14.6. să nu utilizeze RI MCAF într-un mod care poate duce la încălcarea drepturilor de proprietate/utilizare sau a cerințelor de securitate ale altor sisteme informaționale;

14.7. să nu folosească nicio aplicație software și niciun dispozitiv care să bruieze RI MCAF și să nu încarce sau să pună la dispoziție fișiere conținând date eronate sau viruși, prin niciun fel de metodă;

14.8. să nu obțină sau să nu încerce să obțină acces neautorizat la informații, indiferent de metodă;

14.9. să nu utilizeze RI MCAF în scop publicitar sau pentru orice fel de cerere/ofertă cu caracter comercial;

14.10. să efectueze acțiuni pentru asigurarea securității informației, să documenteze cazurile și tentativele de încălcare a acesteia, precum și să întreprindă măsurile necesare pentru prevenirea și lichidarea consecințelor.

Secțiunea a 3-a
Drepturile și obligațiile registratorului și destinatarului

15. Registratorul și destinatarul RI MCAF au dreptul:

15.1. să solicite și să primească de la deținător asistență în utilizarea RI MCAF;

15.2. să solicite, în baza unei cereri aprobate în scris, și să recepționeze de le posesorul RI MCAF accesul la date/informații în conformitate cu scopul prelucrării și atribuțiile deținute;

15.3. să vizualizeze datele, informațiile și documentele din RI MCAF în conformitate cu drepturile de acces stabilite, fără dreptul de a modifica aceste date, informații și documente.

16. Registratorul și destinatarul RI MCAF sunt obligați:

16.1. să asigure respectarea cerințelor privind protecția datelor cu caracter personal utilizate în cadrul RI MCAF, în conformitate cu prevederile actelor normative;

16.2. să întreprindă măsuri pentru evitarea accesului neautorizat al persoanelor terțe;

16.3. să utilizeze funcționalitățile RI MCAF exclusiv conform destinației acestora și în strictă conformitate cu legislația;

16.4. să asigure protecția, securitatea și confidențialitatea datelor, a informațiilor și a documentelor vizualizate sau prelucrate în RI MCAF;

16.5. să raporteze eventuale neconcordanțe, erori sau riscuri identificate.

Capitolul IV. Ținerea și funcționarea RI MCAF

17. Funcția principală a RI MCAF constituie asigurarea unui cadru centralizat, complet și actualizat de date care permite monitorizarea, analizarea și coordonarea unitară a tuturor informațiilor privind neregulile și riscurile de fraudă asociate gestionării fondurilor publice și externe.

18. RI MCAF se accesează prin intermediul paginii-web https://mcaf.gov.md/login (cu acces prin rețeaua internet). Pentru a accesa sistemul utilizatorii (persoane juridice) vor folosi exclusiv serviciul electronic guvernamental de autentificare și control al accesului (MPass). Accesul la datele și funcționalitățile RI MCAF este condiționat de rolurile alocate utilizatorilor acestuia.

19. RI MCAF oferă următoarele funcționalități de bază:

19.1.înregistrarea și autentificarea utilizatorilor sistemului;

19.2. completarea dosarului/actualizarea profilului;

19.3. crearea sesizării și înregistrarea neregulilor, cu încărcarea actelor confirmative;

19.4. crearea dosarului antifraudă, cu încărcarea actelor confirmative;

19.5. monitorizarea entităților implicate (gestionarea datelor despre beneficiari, proiecte, controale și istoricul riscurilor);

19.6. schimbul automatizat de date cu alte registre și sisteme naționale**;**

19.7. generarea datelor statistice și a rapoartelor specifice;

19.8. expedierea și recepționarea notificărilor privind recepția, acceptarea, respingerea și corectarea înregistrărilor, în baza cererilor depuse de către utilizatori;

19.9. funcționarea RI MCAF este asigurată de către posesor până la luarea unei decizii de scoatere din exploatare. În cazul scoaterii din exploatare, datele și documentele generate în cadrul RI MCAF se arhivează în condițiile cadrului normativ aplicabil.

Capitolul V. Înregistrarea, modificarea, completarea și radierea datelor în RI MCAF

20. Înregistrarea, modificarea și/sau completarea, precum și radierea datelor din cadrul RI MCAF se efectuează de către posesorul acestuia, prin intermediul registratorului de date desemnat, conform procedurilor aprobate.

21. RI MCAF asigură posibilitatea de a accesa și de a vizualiza informația la orice etapă de înregistrare, de modificare și/sau de completare, de radiere a datelor, precum și evidența tuturor modificărilor și completărilor. Toate modificările operate în RI MCAF se păstrează în ordine cronologică.

22. În cazul în care furnizorul de date sau destinatarul consideră că datele înregistrate, modificate, completate sau radiate în cadrul RI MCAF sunt incorecte, incomplete sau nejustificate, acesta are dreptul de a solicita motivat verificarea și corectarea acestora. Posesorul RI MCAF va examina solicitarea în termen de 10 zile lucrătoare de la data recepționării, informând solicitantul despre rezultatul verificării și măsurile întreprinse. În caz de respingere a solicitării, răspunsul va fi motivat.

23. Verificarea și corectarea datelor se efectuează prin intermediul registratorului desemnat, cu documentarea acțiunilor realizate, iar posesorul validează decizia finală.

24. Utilizatorii RI MCAF au obligația de a consulta și a respecta condițiile de utilizare ale datelor şi serviciilor publicate în cadrul RI MCAF și în Ghidul utilizatorului.

Capitolul VI. Interacțiunea cu furnizorii de date

25. RI MCAF interacționează și realizează schimbul de date, prin intermediul platformei de interoperabilitate (MConnect), cu sistemele și resursele informaționale de stat indicate în Conceptul Sistemului informațional „Monitorizarea și coordonarea antifraudă”, necesare pentru realizarea funcționalităților sistemului.

26. Datele din cadrul RI MCAF se actualizează și se sincronizează cu datele din cadrul resurselor informaționale formate în alte sisteme informaționale de stat cu care acesta interacționează.

Capitolul VII. Asigurarea protecției și securității informației

27. Datele din RI MCAF fac parte din categoria datelor care necesită a fi protejate. Asigurarea securității, confidențialității și a integrității datelor prelucrate în cadrul RI MCAF se efectuează de către subiecții cu drepturi de acces la sistem, cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

28. Măsurile de protecție și securitate a datelor din RI MCAF reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a RI MCAF și se respectă de către toți subiecții RI MCAF.

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

30. Prelucrarea datelor cu caracter personal în cadrul RI MCAF se efectuează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

31. În condițiile prezentului Regulament, datele cu caracter personal se prelucrează exclusiv în măsura în care sunt necesare scopului și obiectivelor stabilite, conform competențelor atribuite subiecților raporturilor juridice legate de crearea și ținerea RI MCAF, asigurându-se un nivel de securitate și confidențialitate corespunzător în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate, conform principiilor stabilite de legislația privind protecția datelor cu caracter personal.

32. Obiecte ale asigurării protecției și securității informației din cadrul RI MCAF se consideră tot complexul de mijloace software și hardware care asigură realizarea proceselor informaționale:

32.1.bazele de date și suporturile materiale care conțin informații privind date cu caracter personal;

32.2. sistemele informaționale, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații care asigură activitatea RI MCAF;

32.3. sistemele de comunicații electronice, rețelele, serverele, calculatoarele și alte echipamente și mijloace tehnice de captare și prelucrare a informației.

33. Protecția datelor se efectuează prin următoarele metode:

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

33.2. excluderea accesului neautorizat la datele din RI MCAF, prin utilizarea funcționalităților de autentificare ale serviciului guvernamental de autentificare și control al accesului (MPass);

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

33.4. utilizarea obligatorie a produselor de program licențiate aprobate;

33.5. coordonarea solicitării de instalare a unui produs de program cu posesorul RI MCAF;

33.6. monitorizarea procesului de exploatare al RI MCAF prin intermediul mecanismului de jurnalizare;

33.7. păstrarea și actualizarea registrelor importante de securitate necesare pentru menținerea înregistrărilor de audit și analiza integrității sistemului, precum și pentru monitorizarea activității utilizatorilor.

34. Posesorul RI MCAF elaborează și implementează politica de securitate informațională pentru asigurarea respectării regulilor, a standardelor și a normelor acceptate în domeniul securității informaționale, conform Hotărârii Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice.

35. Politica de securitate se aduce la cunoștința fiecărui utilizator care trebuie să cunoască obligațiile de serviciu privind respectarea securității informaționale și totalitatea procedurilor formale pe care trebuie să le respecte în strictă conformitate cu politica de securitate.

36. În cadrul RI MCAF se prelucrează datele cu caracter personal strict necesare, neexcesive scopului prestabilit de acesta, asigurându-se un nivel de securitate și confidențialitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor.

Capitolul VIII. Controlul și răspunderea

37. Crearea, organizarea și funcționarea RI MCAF este supusă controlului intern. Controlul intern privind organizarea și funcționarea RI MCAF se efectuează de către posesor.

38. Utilizatorii în ale căror atribuții intră administrarea RI MCAF, introducerea datelor, furnizarea/recepționarea informațiilor și asigurarea funcționării RI MCAF poartă răspundere personală, în conformitate cu legislația, pentru completitudinea, autenticitatea, veridicitatea, integritatea informației, precum și pentru păstrarea și utilizarea ei.

39. Toți subiecții RI MCAF poartă răspundere conform legislației pentru prelucrarea, divulgarea și transmiterea informației din sistem ce conține date cu caracter personal terțelor persoane, contrar prevederilor legislative.

40. Pentru asigurarea funcționalității și eficienței RI MCAF, posesorul poate întrerupe funcționalitatea RI MCAF în scopul efectuării operațiunilor de întreținere. Prin urmare, nu se garantează disponibilitatea permanentă sau faptul că va putea fi accesat întotdeauna cu o anumită viteză sau cu o anumită funcționalitate.

41. Posesorul nu își asumă nicio răspundere în cazul în care anumite informații sunt furnizate cu întârziere, sunt pierdute, șterse sau nu pot fi stocate pe serverele RI MCAF din orice motive care au survenit fără vina lor și nu sunt responsabili pentru folosirea incorectă de către utilizator a funcționalităților acestuia. Posesorul nu poartă răspundere pentru datele transmise în RI MCAF, pentru erorile, lacunele, ștergerea datelor, schimbarea funcțiilor, reținerile și defectele ce au loc în timpul transmiterii datelor, care au survenit fără vina lor. Posesorul, furnizorul și destinatarul nu poartă răspundere pentru daunele indirecte cauzate posesorului, inclusiv venitul ratat, economii ratate, oportunități ratate, netransmiterea sau transmiterea cu întârziere a informației, alterarea sau pierderea informației.

42. Funcționarea RI MCAF se suspendă de către posesor în caz de apariție a uneia dintre următoarele situații:

42.1. în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al RI MCAF;

42.2. la apariția impedimentelor justificatoare;

42.3. la încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea RI MCAF;

42.4. în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și

hardware al RI MCAF;

43. În cazul apariției impedimentelor justificatoare și a dificultăților tehnice în funcționarea complexului de mijloace software și hardware al RI MCAF din vina terțelor persoane, este posibilă suspendarea funcționării RI MCAF, cu informarea subiecților prin mijloace tehnice disponibile.