Caiet de sarcini
pentru achiziția serviciilor de crearea a Sistemului informațional „Registrul de Stat VioData”

1. Context

Violența împotriva femeilor și violența în familie constituie în continuare o problemă gravă în Republica Moldova, afectând profund femeile și copiii din toate categoriile sociale. În conformitate cu cadrul normativ național, în special cu prevederile Legea nr. 45/2007 cu privire la prevenirea și combaterea violenței împotriva femeilor și a violenței în familie, violența se manifestă prin acțiuni sau inacțiuni intenționate care pot cauza prejudicii fizice, psihologice, sexuale, economice sau morale victimei. Formele principale includ violența fizică, psihologică (emoțională), sexuală și economică, precum și alte forme de constrângere sau control abuziv. Deși fenomenul poate afecta orice persoană, datele și practica instituțională relevă un impact disproporționat asupra femeilor și fetelor, în contextul inegalităților de gen persistente.

Republica Moldova a realizat progrese importante în prevenirea și combaterea violenței prin consolidarea cadrului legislativ, dezvoltarea politicilor publice sectoriale, instituirea mecanismelor de protecție și extinderea serviciilor specializate pentru victime. Cu toate acestea, rămân provocări semnificative în ceea ce privește identificarea timpurie și gestionarea eficientă a cazurilor, asigurarea unei intervenții integrate și centrate pe victimă, precum și consolidarea coordonării interinstituționale între autoritățile publice, organele de drept și furnizorii de servicii specializate.

În prezent, datele referitoare la cazurile de violență în familie și violență bazată pe gen sunt gestionate de diferite autorități și instituții, în limitele competențelor legale, prin sisteme și registre distincte. Această fragmentare a evidenței îngreunează monitorizarea integrată a cazurilor, evaluarea intervențiilor realizate și analiza datelor statistice necesare pentru fundamentarea politicilor publice. Profesioniștii implicați în prevenirea și combaterea violenței — inclusiv asistenții sociali, personalul medical, organele de drept și alți furnizori de servicii specializate — necesită un mecanism informațional interoperabil, care să permită gestionarea eficientă a cazurilor, evidența măsurilor de protecție și a referirilor interinstituționale, cu respectarea strictă a cadrului normativ privind protecția datelor cu caracter personal și confidențialitatea informațiilor referitoare la victime.

În acest context, dezvoltarea și implementarea Sistemului informațional „Registrul de stat VioData" (SI RS VioData) reprezintă o măsură necesară pentru consolidarea mecanismului național de evidență și monitorizare a cazurilor. Sistemul va constitui o platformă informațională centralizată, destinată colectării, stocării, prelucrării și raportării datelor în domeniul prevenirii și combaterii violenței, în conformitate cu legislația în vigoare.

Implementarea SI RS VioData va contribui la asigurarea securității și confidențialității datelor, la îmbunătățirea coordonării interinstituționale și la sporirea eficienței intervențiilor, precum și la consolidarea procesului de elaborare, monitorizare și evaluare a politicilor publice în domeniu.

Principalii actori implicați în proiect includ:

- Agenția Națională de Prevenire și Combatere a Violenței împotriva Femeilor și a Violenței în Familie (ANPCV). ANPCV implementează și coordonează politicile publice împotriva violenței asupra femeilor și violenței domestice și promovează dialogul între sectorul public, non-profit și societatea civilă pentru protejarea drepturilor femeilor.
- Ministerul Afacerilor Interne (MAI) și Inspectoratul General al Poliției (IGP). Aceste instituții au un rol fundamental în lupta împotriva violenței de gen prin asigurarea aplicării legii, protecția victimelor, investigarea cazurilor și tragerea la răspundere a agresorilor. MAI este deținătorul mai multor sisteme de informații și registre esențiale referitoare la supraviețuitoarele și agresorii violenței de gen.
- Ministerul Muncii și Protecției Sociale (MMPS) și Agențiile teritoriale de asistență socială (ATAS). MMPS asigură un cadru de politici naționale și finanțare pentru serviciile destinate combaterii violenței de gen, în timp ce Agențiile teritoriale de asistență socială/structurile teritoriale de asistență socială (STAS) oferă asistență directă supraviețuitoarelor prin gestionarea cazurilor, servicii de adăpost și programe de reintegrare socială. MMPS este deținătorul Sistemului de Informații e-Social, care centralizează toate programele de protecție socială și activitățile de gestionare a cazurilor referitoare la victimele violenței de gen.
- Ministerul Sănătății (MS) și furnizorii de servicii medicale. MS are un rol important în identificarea cazurilor de violență de gen, îngrijirea medicală, documentarea și referirea victimelor. De asemenea, Ministerul Sănătății administrează sistemele de informații legate de asistența medicală și îngrijirea primară.

- Ministerul Justiției (MJ). MJ joacă un rol esențial în elaborarea cadrului juridic, a procedurilor judiciare și în facilitarea accesului la justiție pentru cazurile de violență de gen.
- Consiliul Național pentru Asistență Juridică Garantată de Stat (CNAJGS). CNAJGS asigură accesul supraviețuitoarelor violenței de gen la asistență juridică gratuită în Republica Moldova. Funcțiile sale sunt prevăzute în Legea privind Asistența Juridică Garantată de Stat (Legea nr. 198/2007) și Legea cu privire la prevenirea și combaterea violenței împotriva femeilor și a violenței în familie (Legea nr. 45/2007). Consiliul își desfășoară activitatea prin intermediul oficiilor teritoriale, care oferă asistență juridică grupurilor vulnerabile, inclusiv supraviețuitoarelor violenței de gen.

Roluri și responsabilități

Instituție	Rol și responsabilități
ANPVC	Deținător al sistemului. Supraveghează execuția proiectului, asigură implicarea părților interesate și monitorizează progresul.
Contractor tehnic	Companie locală sau internațională care va fi contractat și responsabil pentru proiectarea, dezvoltarea și implementarea sistemului.
MAI, MMPS, MS, MS, CNAJGS	Rolul de consultanta în cadrul proiectului si asigurarea conformității cu cadrele legale. Furnizori cheie de date și informații pentru sistemul informațional.

2. Obiective

Obiectivele principale ale Sistemului informațional „Registrul de stat VioData” (în continuare – SI RS VioData) sunt stabilite în concordanță cu cadrul normativ național aplicabil, astfel încât să asigure colectarea, protecția și gestionarea eficientă a datelor privind violența bazată pe gen și violența în familie.

Primul obiectiv îl constituie **îmbunătățirea colectării datelor**, prin standardizarea proceselor de introducere și raportare a informațiilor, pentru a garanta consistența și fiabilitatea datelor privind violența bazată pe gen în toate regiunile Republicii Moldova, în conformitate cu Programul Național privind prevenirea și combaterea violenței împotriva femeilor și a violenței în familie pentru anii 2023–2027. Această standardizare va permite colectarea de date dezagregate, inclusiv pe criterii de sex, vârstă, tip de violență și mediu de reședință, facilitând identificarea tendințelor și a modelelor de manifestare a violenței, cât în Offline, atât și Online. Totodată, sistemul va sprijini realizarea de audituri periodice pentru a verifica acuratețea datelor și a elimina eventualele duplicate.

Al doilea obiectiv este **asigurarea confidențialității datelor**, prin implementarea unor mecanisme avansate de criptare și autentificare securizată, în conformitate cu legislația națională privind protecția datelor cu caracter personal și normele privind securitatea cibernetică. Vor fi dezvoltate și aplicate protocoale stricte de acces, astfel încât datele să fie disponibile exclusiv utilizatorilor autorizați, cărora li se vor atribui roluri clar definite. Sistemul va integra funcții de consimțământ al utilizatorilor, asigurând informarea adecvată a supraviețuitoarelor cu privire la modul de utilizare a datelor lor.

Al treilea obiectiv vizează **îmbunătățirea coordonării interinstituționale**, prin integrarea SI RS VioData cu furnizorii de servicii existenți, inclusiv servicii medicale, asistență juridică și adăposturi. Această integrare va permite referirea eficientă a cazurilor și colaborarea între instituții, precum și notificarea automată a părților implicate în situațiile în care sunt necesare actualizări sau intervenții.

Al patrulea obiectiv este **sprijinirea procesului decizional**, prin furnizarea de tablouri de bord interactive și rapoarte personalizate, care vor permite factorilor de decizie și practicienilor să identifice punctele critice și să analizeze tendințele incidentelor de violență bazată pe gen. Sistemul va facilita elaborarea de rapoarte la nivel național, regional și local și va sprijini alocarea eficientă a resurselor, pe baza distribuției cazurilor și a cererii de servicii.

Prin realizarea acestor obiective, Sistemul informațional „Registrul de stat VioData” va contribui la consolidarea mecanismului național de monitorizare și răspuns la violența bazată pe gen și violența în familie, respectând legislația în vigoare, principiile protecției datelor și standardele de securitate și confidențialitate aplicabile.

3. Domeniul de aplicare

Proiectul cuprinde procesul complet de proiectare, implementare și întreținere a unui Sistemului informațional „Registrul de Stat VioData” (***aprobat prin Hotărârea Guvernului nr. 530/2025 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat VioData” și a Regulamentului privind modalitatea de ținere a Registrului de stat VioData***).

Activitățile specifice includ:

Implicarea părților interesate și evaluarea nevoilor. Organizarea de consultări cu părțile interesate-cheie, inclusiv agenții guvernamentale, furnizori de servicii medicale, forțe de ordine și ONG-uri, pentru a colecta informații despre provocările întâmpinate în procesul actual de gestionare a cazurilor și pentru a prioritiza caracteristicile sistemului pe baza acestor informații. Evaluarea și validarea tuturor cerințelor tehnice necesare înainte de dezvoltarea sistemului.

Proiectarea și dezvoltarea sistemului. Crearea arhitecturii sistemului informațional bazată pe specificațiile tehnice și conformă ***Hotărârii Guvernului nr. 530/2025 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat VioData” și a Regulamentului privind modalitatea de ținere a Registrului de stat VioData***, precum și cu legislația națională privind prevenirea și combaterea violenței împotriva femeilor, reglementările de protecție a datelor și standardele de securitate IT.

Proiectarea și dezvoltarea Sistemului informațional „Registrul de stat VioData”, incluzând funcționalități de bază precum:

1. Administrare pentru configurarea sistemului și gestionarea utilizatorilor,
2. Gestionarea și evidența cazurilor de violență printr-un dosar electronic,
3. Gestionarea și evidența registrului victimelor și a agresorilor în cazurile de violență.
4. Integrarea cu serviciile de suport destinate asistenței și protecției victimelor (adăposturi, consiliere psihologică și juridică),
5. Implementarea planurilor de acțiune/intervenție personalizate, care să includă măsuri de protecție, sprijin psihologic și asistență legală,
6. Monitorizarea cazurilor de violenţă, în mediul offline și online și urmărirea referirilor către serviciile de suport,
7. Generarea și transmiterea alertelor sau notificărilor către autoritățile competente ori organizațiile de suport, în cazul apariției unor evenimente noi sau al modificării situației unui caz,
8. Instrumente de analiză a datelor și raportare pentru susținerea deciziilor bazate pe dovezi.
9. Integrare cu serviciile de e-Guvernare,
10. Interoperabilitate cu sistemele de informații guvernamentale,
11. Stocare și recuperare securizată a datelor pentru asigurarea protecției datelor personale ale victimelor și agresorilor.

Interoperabilitate și integrări. Se asigură că Sistemul informațional „Registrul de stat VioData” (SI RS VioData), este interoperabil cu alte sisteme de informații guvernamentale și permite schimbul de date și informații relevante. Aceasta include dezvoltarea de API-uri pentru integrarea registrelor medicale, bazelor de date ale forțelor de ordine și platformelor de protecție socială prin intermediul platformei guvernamentale de interoperabilitate – MConnect.

Testarea și pilotarea sistemului. Pilotarea SI RS VioData trebuie realizată înainte de implementarea completă a sistemului pentru a evalua funcționalitatea acestuia conform specificațiilor, a identifica provocările și a îmbunătăți sistemul pe baza utilizării reale. Faza de pilotare trebuie să garanteze că sistemul este sigur, ușor de utilizat și eficient pentru utilizatori și pentru luarea deciziilor bazate pe date.

Instruire și dezvoltarea capacităților. Un element esențial al dezvoltării sistemului este formarea și consolidarea capacităților. Acest proces include dezvoltarea și implementarea unor programe de instruire adaptate diferitelor grupuri de utilizatori, cum ar fi administratorii de sistem,

managerii de caz, asistenții sociali, profesioniștii din domeniul sănătății și ofițerii de aplicare a legii. Dezvoltarea capacităților trebuie să includă și documentație detaliată și actualizată a sistemului, precum și manuale de utilizare cu instrucțiuni pas cu pas, disponibile în format digital.

Lansarea sistemului și mentenanța. Domeniul de activitate include suportul complet pentru lansarea națională a Sistemului informațional „Registrul de stat VioData", asigurând asistență tehnică adecvată și instruirea utilizatorilor. După implementarea sistemului, se prevede o garanție de un an, care include suport tehnic și actualizări ale sistemului.

4. Livrabile

La finalizarea Contractului Prestatorul va asigura predarea următoarelor livrabile:

Livrabil	**Descrierea livrabil**
1. Raport de inițiere a lucrărilor	• Un raport detaliat care descrie metodologia proiectului, cronologia și planul de implicare a părților interesate. • Identificarea părților interesate primare și secundare, împreună cu rolurile lor în proiect. Evaluarea riscurilor și strategii de atenuare
2. Raport de evaluare a nevoilor	• Constatări și recomandări bazate pe consultările cu părțile interesate și analiza lacunelor. • Documentarea provocărilor, priorităților și nevoilor tehnice pentru sistem.
3. Raport de Cost Total de Proprietate (TCO)	• Raport TCO trebuie să fie elaborat pe o perioadă de minimum 3 ani. • Raportul TCO trebuie să permită identificarea tuturor costurilor reale asociate ciclului de viață al SI RS VioData, și planificarea costurilor de exploatare, mentenanță și modernizare a sistemului.
4. Document de proiectare a sistemului	• Documentație cuprinzătoare despre arhitectura sistemului, fluxurile de lucru, structurile de date și măsurile de securitate. • Proiecte detaliate ale interfeței utilizator (UI) și experienței utilizator (UX) pentru fiecare modul al sistemului. • Diagrame ale fluxurilor de date și planuri de integrare a sistemului.
5. Sistem Funcțional (SI RS VioData)	• Un sistem de gestionare a cazurilor complet operațional, implementat pe serviciul guvernamental de cloud – MCloud, cu funcționalități esențiale, inclusiv: **1. Contur de administrare cu următoarele funcții:** a) asigurarea vizualizării, explorării și administrării bazelor de date ale sistemului informațional; b) definirea și gestionarea drepturilor de acces ale utilizatorilor; c) administrarea registrelor și înregistrărilor; d) configurarea setărilor de acces pentru utilizatori conform drepturilor acordate; e) asigurarea securității, protecției și păstrării informațiilor; f) realizarea auditului de date și a jurnalizării accesului; g) asigurarea interfeței multilingve; h) configurarea conținutului și a aspectului interfeței publice. **2. Conturul managementul raportării cazurilor de violență, cu următoarele funcții:** a) introducerea, structurarea și clasificarea automată a datelor privind tipurile de violență (fizică, sexuală, psihologică, spirituală, economică sau alte forme asociate infracțiunilor conexe) și asocierea acestora cu profilurile victimei și ale agresorului, cu identificatori unici și legături între entități; b) selectarea și înregistrarea instituției raportoare printr-un meniu prestabilit (forțe de ordine, sănătate, asistență socială, educație etc.), inclusiv atribuirea automată a unui cod de sursă a raportării și a datei de înregistrare.

	3. Conturul urmărirea cazurilor, cu următoarele funcții: a) urmărirea statutului cazului (deschis, în desfășurare, închis, respins, referit sau inactiv); b) introducerea și actualizarea datelor demografice ale persoanelor implicate în caz, cu câmpuri predefinite; c) evaluarea riscurilor și a nevoilor victimei, în funcție de tipuri și profiluri de risc; d) gestionarea intervențiilor de urgență în caz de necesitate. **4. Conturul urmărirea referirilor, cu următoarele funcții:** a) furnizarea informațiilor privind istoricul cazurilor și serviciile accesate; b) servicii medicale – înregistrarea referirilor către sectorul sănătăți; c) suport juridic – înregistrarea asistenței juridice oferite; d) servicii de adăpost (plasament) – monitorizarea plasamentului victimelor în centrele de adăpost, evidența duratei ședерii și a eventualelor modificări privind statutul acestora; e) servicii sociale – urmărirea referirilor către serviciile sociale, inclusiv prestațiile sociale; **5. Conturul caz de violență, cu următoarele funcții:** a) evidența plângerilor, a denunțurilor, a autodenunțurilor, a sesizărilor și a altor informații despre actele de violență împotriva femeilor și de violență în familie parvenite de la cetățeni, organul de constatare, autorități, organizații și de la instituții cu privire la situațiile de conflict în familie, actele de violență împotriva femeilor, aplicarea măsurilor de protecție, emiterea hotărârilor judecătorești; b) evidența cazurilor înregistrate de violență împotriva femeilor și violență în familie. 6. Conturul evidența măsurilor de protecție include instrumente de evaluare a riscurilor și letalității, de emitere a ordinelor de restricție de urgență și a ordonanțelor de protecție emise de instanțele de judecată, aplicate agresorului. 7. Conturul de raportare și analiză, care generează rapoarte personalizate și vizualizări de date precum și rapoarte statistice, inclusiv cazurile de violență online. 8. Conturul acces autorizat pentru autentificare a utilizatorilor și control al accesului bazat pe roluri (RBAC). 9. Conturul gestionarea nomenclatoarelor SI RS VioData care conține instrumentele necesare pentru crearea și modificarea listelor interne de valori, care vor fi introduse în actele de evidență în procesul utilizării SI RS VioData. • Integrare cu serviciile de e-Guvernare (MPass, MSign, MLog, MNotify). • Interoperabilitate cu sistemele de informații guvernamentale prin MConnect. Conformitate cu GDPR și legislația națională privind protecția datelor, garantând un management securizat și etic al informațiilor.
6. Raport de Pilotare / Raport de Testare a Sistemului informațional „Registrul de stat VioData”	• Include o evaluare detaliată a fazei pilot, analizând performanța sistemului, feedback-ul utilizatorilor și aspectele care necesită îmbunătățiri. Raportul trebuie să acopere următoarele activități: - Evaluarea utilizabilității sistemului pentru colectarea datelor și monitorizarea cazurilor. - Identificarea nevoilor de interoperabilitate cu serviciile medicale, forțele de ordine și serviciile sociale.

	- Testarea protocoalelor de securitate și confidențialitate. - Verificarea integrării cu serviciile de e-Guvernare. - Evaluarea funcționalităților de raportare și analiză a datelor. - Colectarea feedback-ului de la utilizatorii finali pentru îmbunătățirea designului sistemului înainte de implementarea la scară largă.
7. Raport de integrare a Sistemului informațional „Registrul de stat VioData”	• Acest raport este un document tehnic care detaliază procesul, rezultatele și provocările integrării sistemului cu alte platforme, precum baze de date ale forțelor de ordine, sisteme de sănătate, servicii sociale și instrumente de gestionare a cazurilor. Raportul trebuie să includă: - Diagramă care prezintă componentele sistemului, API-urile și fluxurile de date. - Metodele de integrare utilizate – API-uri RESTful, servicii web SOAP, transferuri securizate de fișiere (SFTP). - Standardele și protocoalele de date respectate. - Rezultatele testării și validării integrării.
8. Instruirea utilizatorilor și materialele de instruire	• Manuale detaliate pentru utilizatori, adaptate diferitelor roluri conform nivelului de acces. • Ghiduri de instruire cu instrucțiuni pas cu pas, video ghid și scenarii pentru învățare practică.
9. Raport de lansare a Sistemului informațional „Registrul de stat VioData”	• Implementarea completă a sistemului la nivel național, încorporând perfecționări din faza pilot. • Asistență pentru integrare, inclusiv servicii de asistență pentru utilizatorii finali.
10. Plan de inițiere	• O strategie detaliată pentru întreținerea continuă, inclusiv actualizări programate ale sistemului și îmbunătățiri ale funcțiilor, protocoale de răspuns la incidente pentru probleme tehnice și încălcări de date. • Include un an de întreținere adaptivă și corectivă. • Codul sursă final. • Raport care documentează vulnerabilitățile descoperite urmare a testelor de penetrare, metodele de atac utilizate și recomandările pentru îmbunătățirea securității.

5. Cerințele tehnice funcționale

Prezentul capitol stabilește cerințele funcționale operaționale obligatorii ale Sistemului informațional „Registrul de stat VioData” (în continuare – SI RS VioData), elaborate în conformitate cu Conceptul Sistemului informațional „VioData” aprobat prin Hotărârea Guvernului nr. 530/2025.

Cerințele funcționale operaționale transpuse în prezentul capitol:

- reflectă integral contururile funcționale prevăzute în Concept;
- sunt obligatorii pentru implementare;
- constituie bază pentru estimarea efortului, evaluarea ofertelor și recepția livrabilelor.

Prestatorul este obligat să implementeze toate cerințele funcționale operaționale descrise mai jos, inclusiv:

- fluxurile operaționale complete;
- regulile de business;
- mecanismele de control și validare;
- criteriile de acceptanță și testare.

Sistemul informațional „Registrul de stat VioData” (*Hotărârea Guvernului nr. 530/2025 cu privire la aprobarea Conceptului Sistemului informațional „Registrul de stat VioData” și a Regulamentului privind modalitatea de ținere a Registrului de stat VioData*), trebui să fie dezvoltat utilizând tehnologii open-source și urmând o metodologie agilă (Agile Methodology) de dezvoltare software, care să permit o mai bună adaptare și îmbunătățiri iterative ale sistemului.

Pentru gestionarea bazelor de date, se recomandă utilizarea platformelor open-source precum PostgreSQL sau MySQL, asigurând eficiență din punct de vedere al costurilor și suport din partea comunității.

Pentru dezvoltarea backend, se recomandă utilizarea Django, Flask sau Node.js, iar pentru dezvoltarea frontend, utilizarea framework-urilor React, Vue.js sau Angular, pentru o interfață receptivă și ușor de utilizat.

Docker este recomandat pentru containerizare, facilitând implementarea eficientă și menținerea consistenței între medii.

Pipeline-urile Continuous Integration și Continuous Delivery (CI/CD) trebui să includă instrumente precum GitLab CI, Jenkins sau GitHub, pentru automatizarea testării, integrării și implementării, asigurând actualizări rapide cu întreruperi minime.

Arhitectura la nivel înalt a Sistemul informațional „Registrul de stat VioData” ar trebui să includă următoarele componente:

- Interfață web pentru utilizatori (UI)
- Strat de aplicație (Application Layer)
- Strat de date (Data Layer)
- Strat de integrare (Integration Layer)
- Strat de securitate (Security Layer)
- Strat de implementare (Deployment Layer)

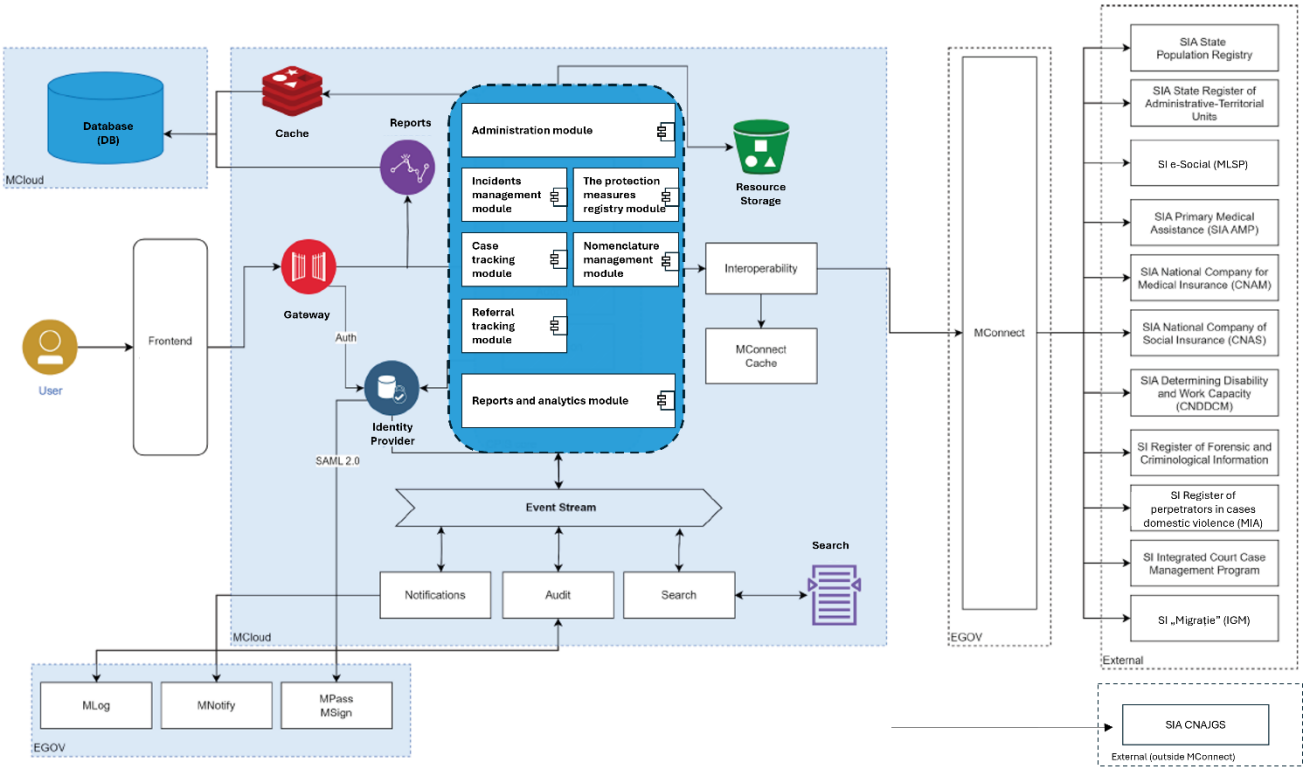

Figura nr. 1: Sistemul informațional „Registrul de stat VioData” High-Level Architecture

5.1. Cerințe de utilizare și design

Cerințe	Descrierea cerințelor
5.1.1 Interfață utilizator multilingvă	• Sistemul informațional „Registrul de stat VioData” trebuie să fie disponibil în limbile română, rusă și engleză. Limba implicită va fi româna cu acuratețea de 100%.
5.1.2. Accesibilitate	• Conformare cu standardele Web Content Accessibility Guidelines (WCAG), cel puțin nivelul de bază (nivel A).

5.1.3. Suport pentru dispozitive multiple	• Sistemul informațional „Registrul de stat VioData” va funcționa pe diverse dispozitive (PC, laptopuri, smartphone-uri, tablete) utilizând design web adaptiv pentru diferite dimensiuni de ecran (320px până la 1600px).

5.2 Contur funcțional: Administrare

Cerințe	Descrierea cerințelor	Criteriu de acceptanță
5.2.1. Administrarea utilizatorilor și rolurilor	5.2.1.1. SI RS VioData trebuie să permită administrarea completă a utilizatorilor, incluzând: • crearea, modificarea, activarea, dezactivarea și ștergerea utilizatorilor; • asocierea fiecărui utilizator cu unul sau mai multe roluri; • definirea drepturilor de acces în funcție de rol, modul și obiect informațional.	Cerința se consideră acceptată dacă sunt îndeplinite cumulativ următoarele condiții: a) Sistemul permite crearea, modificarea, dezactivarea și ștergerea utilizatorilor prin interfață grafică, fără intervenție tehnică; b) Pentru minimum trei roluri distincte (ex.: administrator, manager de caz, utilizator raportor) se demonstrează: • drepturi de acces diferite; • restricționarea funcționalităților neautorizate; c) Autentificarea utilizatorilor se realizează prin MPass, iar rolurile sunt preluate și aplicate corect; d) Orice modificare a rolurilor sau drepturilor este reflectată imediat în comportamentul sistemului; e) Sistemul împiedică accesul utilizatorilor fără rol valid.
	5.2.1.2. Sistemul trebuie să fie integrat cu Serviciul guvernamental de autentificare și control al accesului (MPass) pentru: • autentificarea utilizatorilor; • preluarea și gestionarea rolurilor.	
	5.2.1.3. Fiecare utilizator trebuie să aibă atribuit cel puțin un rol activ.	
5.2.2. Securitate, jurnalizare și audit	5.2.2.1. Sistemul trebuie să asigure jurnalizarea tuturor acțiunilor utilizatorilor și evenimentelor de sistem, inclusiv: • autentificări; • accesări și modificări de date; • schimbări de stare ale cazurilor; • operațiuni administrative.	Cerința se consideră acceptată dacă: a) Toate acțiunile utilizatorilor (autentificare, creare, modificare, vizualizare, ștergere) sunt înregistrate automat în jurnal; b) Jurnalele conțin cel puțin: • identificator utilizator; • dată și oră; • tip acțiune; • obiect afectat; c) Sistemul este integrat funcțional cu serviciul MLog; d) Jurnalele pot fi filtrate și exportate; e) Se demonstrează posibilitatea realizării unui audit ex-post pentru un caz selectat.
	5.2.2.2. SI RS VioData trebuie să fie integrat cu Serviciul guvernamental de jurnalizare (MLog)	
	5.2.2.3. Jurnalele de audit trebuie să fie: • consultabile de utilizatorii autorizați; • filtrabile; • exportabile.	

5.3. Contur funcțional: Managementul raportării cazurilor de violență

Cerințe	Descrierea cerințelor	Criteriu de acceptanță
5.3.1. Înregistrarea cazurilor de violență	5.3.1.1. Sistemul trebuie să permită înregistrarea cazurilor de violență prin: • generarea automată a unui identificator unic de caz;	Cerința se consideră acceptată dacă: a) Sistemul generează automat un identificator unic pentru fiecare caz;

	• completarea unui formular standardizat; • validarea câmpurilor obligatorii.	b) Formularul de raportare conține toate câmpurile prevăzute în Concept; c) Sistemul blochează salvarea cazului dacă lipsesc câmpuri obligatorii; d) După salvare, cazul este vizibil în lista de cazuri și poate fi accesat conform rolului; e) Datele introduse sunt persistente și corect afișate la reîncărcare. f) În cazul violenței Online, fișa cazului trebuie să conțină link postare sau canal pentru monitorizare.
	5.3.1.2. Formularul de raportare trebuie să includă, cel puțin: • date despre victimă; • date despre agresor; • tipul și circumstanțele violenței; • instituția raportoare.	
	5.3.1.3. Sistemul nu trebuie să permită salvarea unui caz fără completarea tuturor câmpurilor obligatorii.	
5.3.2. Consimțământ și confidențialitate	5.3.2.1. Sistemul trebuie să includă mecanisme de colectare și evidență a consimțământului pentru prelucrarea datelor cu caracter personal.	Cerința se consideră acceptată dacă: a) Sistemul permite înregistrarea explicită a consimțământului; b) Accesul la datele cu caracter personal este controlat pe roluri; c) Toate accesările datelor sensibile sunt jurnalizate; d) Se demonstrează diferență de vizibilitate între minimum două roluri.
	5.3.2.2. Accesul la datele sensibile trebuie să fie restricționat în funcție de rolul utilizatorului.	
	5.3.2.3. Toate accesările datelor cu caracter personal trebuie să fie jurnalizate.	

5.4. Contur funcțional: Urmărirea cazurilor

Cerințe	**Descrierea cerințelor**	**Criteriu de acceptanță**
5.4.1. Monitorizarea ciclului de viață al cazului	5.4.1.1. Sistemul trebuie să permită gestionarea ciclului de viață al cazului, incluzând cel puțin următoarele stări: • deschis; • în desfășurare; • referit; • închis; • respins sau inactiv.	Cerința se consideră acceptată dacă: a) Sistemul permite schimbarea stării cazului doar conform fluxului definit; b) Tranzițiile nepermise sunt blocate automat; c) Fiecare schimbare de stare este jurnalizată; d) Starea curentă este vizibilă clar în interfața utilizatorului.
	5.4.1.2. Tranzițiile între stările cazului trebuie să fie guvernate de reguli de business configurabile.	
5.4.2. Evaluarea riscului și planul de intervenție	5.4.2.1. Sistemul trebuie să permită evaluarea riscului pe baza criteriilor definite.	Cerința se consideră acceptată dacă: a) Sistemul permite completarea unei evaluări de risc; b) Evaluarea este asociată unui caz concret; c) Se poate crea un plan de intervenție cu acțiuni, termene și responsabili; d) Modificările sunt salvate și jurnalizate; e) Planul de intervenție poate fi actualizat pe durata ciclului de viață al cazului.
	5.4.2.2. Pentru fiecare caz trebuie să poată fi creat și actualizat un plan de intervenție.	
	5.4.2.3. Acțiunile din planul de intervenție trebuie să fie asociate cu termene și responsabili.	

5.5. Contur funcțional: Urmărirea referirilor

Cerințe	**Descrierea cerințelor**	**Criteriu de acceptanță**

5.5.1. Gestionarea referirilor	5.5.1.1. Sistemul trebuie să permită înregistrarea și urmărirea referirilor către: • servicii medicale; • servicii juridice; • servicii sociale; • servicii de adăpost.	Cerința se consideră acceptată dacă: a) Sistemul permite înregistrarea unei referiri pentru un caz; b) Tipul serviciului (medical, juridic, social etc.) este selectabil; c) Statutul referirii poate fi actualizat; d) Istoricul complet al referirilor este vizibil per caz; e) Referirile sunt corect corelate cu cazul.
	5.5.1.2. Istoricul referirilor trebuie să fie păstrat și consultabil pentru fiecare caz.	
5.5.2. Interoperabilitatea referirilor	5.5.2.1. Sistemul trebuie să permită schimbul de date privind referirile prin Platforma de interoperabilitate (MConnect).	Cerința se consideră acceptată dacă: a) Sistemul transmite și recepționează date prin MConnect; b) Structura datelor este documentată; c) Se demonstrează un schimb de date real sau simulat cu un sistem extern; d) Erorile de integrare sunt gestionate și jurnalizate; e) Sunt respectate principiile once-only.
	5.5.2.2. Arhitectura trebuie să permită utilizarea mecanismelor sincrone și asincrone (inclusiv MConnect Events), unde este cazul.	

5.6. Contur funcțional: Evidența măsurilor de protecție

Cerințe	**Descrierea cerințelor**	**Criteriu de acceptanță**
5.6.1. Evidența a măsurilor de protecție aplicate în cazurile de violență	5.6.1.1. Sistemul trebuie să permită evidența ordinelor de restricție de urgență aplicate agresorului și include: • autoritatea emitentă; • numărul și data ordinului; • perioada de aplicare; • tipurile de restricții impuse; • statutul ordinului.	Cerința se consideră acceptată dacă: a) Sistemul permite evidența a ordinelor de restricție și a ordonanțelor de protecție; b) Ordinele și ordonanțele sunt corelate asociate cu cazul și agresorul; c) Statutul ordinelor și ordonanțelor este actualizat și gestionat corect; d) Sistemul generează alerte privind expirarea; e) Operațiunile sunt auditabile și jurnalizate.
	5.6.1.2. Sistemul trebuie să permită evidența ordonanțelor de protecție emise de instanțele de judecată • instanța emitentă; • numărul și data ordonanței; • perioada de aplicare; • măsurile dispuse; • statutul ordonanței.	
	5.6.2.1. Corelarea măsurilor de protecție cu fluxul cazului și vizualizarea în fișa cazului: • ordinelor de restricție de urgență; • ordonanțelor de protecție.	**Cerința se consideră acceptată dacă:** a) Măsurile de protecție sunt vizibile centralizat în fișa cazului; b) Sistemul blochează închiderea cazului cu măsuri active; c) Excepțiile sunt controlate prin roluri; d) Corelările sunt realizate tehnic, nu doar procedural.

5.7. Contur funcțional: Raportare și analiză

Cerințe	**Descrierea cerințelor**	**Criteriu de acceptanță**

5.7.1. Raportare operațională și statistică	5.7.1.1. Sistemul trebuie să permită generarea rapoartelor standard și personalizate.	Cerința se consideră acceptată dacă: a) Sistemul generează rapoarte standard; b) Rapoartele includ indicatorii prevăzuți de Concept; c) Rapoartele pot fi filtrate; d) Exportul în PDF, CSV și Excel este funcțional; e) Datele din raport corespund datelor din sistem.
	5.7.1.2. Sistemul trebuie să calculeze indicatorii naționali prevăzuți în Conceptul SI „VioData”.	
	5.7.1.3. Sistemul trebuie să recepționeze rezultatele de analiză a tendințelor pe rețelele de socializare și să genereze rapoarte personalizat în baza acestor date.	
	5.7.1.4. Rapoartele trebuie să poată fi exportate cel puțin în formatele PDF, CSV și Excel.	
5.7.2. Tablouri de bord și analiză	5.7.2.1. Sistemul trebuie să includă tablouri de bord interactive și configurabile.	Cerința se consideră acceptată dacă: a) Sistemul include tablouri de bord vizuale; b) Datele se actualizează dinamic; c) Filtrele modifică rezultatele afișate; d) Vizualizările sunt lizibile și coerente; e) Tablourile sunt accesibile conform rolului.
	5.7.2.2. Vizualizările trebuie să permită filtrarea datelor după criterii relevante (perioadă, regiune, tip de violență etc.).	

5.8. Contur funcțional: Crearea și administrarea nomenclatoarelor

Cerințe	**Descrierea cerințelor**	**Criteriu de acceptanță**
5.8.1. Crearea, modificarea și administrarea nomenclatoarelor interne	5.8.1.1. Sistemul trebuie să permită crearea, modificarea și administrarea nomenclatoarelor interne. Pentru fiecare nomenclator, sistemul trebuie să permită definirea cel puțin a următoarelor elemente: • denumirea nomenclatorului; • descrierea și scopul utilizării; • lista valorilor permise; • statutul nomenclatorului (activ/inactiv); • data intrării în vigoare.	Cerința se consideră acceptată dacă: a) Sistemul permite crearea și modificarea nomenclatoarelor prin interfață grafică; b) Valorile pot fi adăugate, modificate și dezactivate fără ștergere; c) Nomenclatoarele pot fi activate/dezactivate; d) Nu este necesară intervenție tehnică; e) Operațiunile sunt jurnalizate.
	5.8.1.2. Sistemul trebuie să permită: • adăugarea de valori noi; • modificarea valorilor existente; • dezactivarea valorilor, fără ștergerea istorică a acestora.	
5.8.2. Utilizarea nomenclatoarelor în actele de evidență	5.8.2.1. Nomenclatoarele trebuie să fie utilizate obligatoriu în formularele și actele de evidență relevante.	
	5.8.2.2. Sistemul trebuie să prevină introducerea de valori libere acolo unde este definit un nomenclator.	
	5.8.2.3. Valorile din nomenclatoare trebuie afișate în interfață sub formă de liste derulante sau selecții controlate	

5.9. Contur funcțional: Acces autorizat și interfață publică

Cerințe	Descrierea cerințelor	Criteriu de acceptanță
5.9.1. Acces autorizat	5.9.1.1. Sistemul trebuie să asigure acces securizat pentru utilizatorii autorizați prin MPass.	Cerința se consideră acceptată dacă: a) Accesul se realizează exclusiv prin MPass; b) Interfața diferă în funcție de rol; c) Funcționalitățile neautorizate sunt inaccesibile; d) Notificările sunt afișate corect utilizatorilor vizați.
	5.9.1.2. Interfața trebuie să fie personalizată în funcție de rolul utilizatorului.	
5.9.2. Acces public	5.9.2.1. Dacă sunt expuse date publice, sistemul trebuie să asigure separarea strictă între datele publice și cele confidențiale.	Cerința se consideră acceptată dacă: a) Datele publice sunt strict separate de cele confidențiale; b) Nu există acces public la date cu caracter personal;
	5.9.2.2. Accesul public trebuie să respecte cadrul guvernamental privind portalurile unice de acces la servicii publice electronice.	

5.10. Documentele de bază ale registrului de stat VioData

Sistemul informațional „Registrul de stat VioData” trebuie să asigure gestionarea completă, trasabilă și auditată a documentelor de bază ale registrului, în conformitate cu Conceptul SI „VioData” aprobat prin Hotărârea Guvernului nr. 530/2025.
Documentele de bază ale registrului constituie element structural esențial al funcționării SI RS VioData și trebuie transpuse în cerințe funcționale operaționale, implementate și testate.
Sistemul trebuie să asigure ciclul complet de viață al documentelor:

- creare;
- validare;
- aprobare;
- utilizare;
- arhivare;
- audit și trasabilitate.

5.10.1. Clasificarea documentelor de bază	SI RS VioData trebuie să gestioneze următoarele categorii de documente de bază: a) Documente de intrare, inclusiv: • formulare de raportare a indicatorilor; • cereri, sesizări și notificări; • fișe de referire către alte autorități și instituții; • date raportate de instituții partenere. b) Documente de ieșire, inclusiv: • notificări privind statutul cazului și al raportării; • decizii asupra cazurilor și referirilor; • rapoarte statistice și analitice; • rapoarte de activitate. c) Documente tehnologice, inclusiv: • șabloane de formulare; • nomenclatoare și clasificatori; • ghiduri de utilizare și administrare; • jurnale de audit; • politici și reguli de utilizare a sistemului.

5.10.2. Cerințe funcționale pentru documentele de intrare	5.10.2.1. Sistemul trebuie să permită crearea și completarea documentelor de intrare prin formulare electronice standardizate. 5.10.2.2. Fiecare document de intrare trebuie să: • fie asociat unui caz, unei raportări sau unui proces specific; • conțină un identificator unic; • fie validat automat conform regulilor de business definite. 5.10.2.3. Sistemul trebuie să asigure: • controlul completitudinii datelor; • validarea câmpurilor obligatorii; • versionarea documentelor modificate.
5.10.3. Cerințe funcționale pentru documentele de ieșire	5.10.3.1. Sistemul trebuie să permită generarea automată a documentelor de ieșire, în baza datelor existente în sistem. 5.10.3.2. Documentele de ieșire trebuie să poată fi: • vizualizate în sistem; • descărcate în formate standard (PDF, CSV, Excel, după caz); • transmise prin mecanismele de notificare guvernamentale (MNotify). 5.10.3.3. Fiecare document de ieșire trebuie să fie: • asociat unui eveniment, caz sau raportare; • marcat cu dată, oră și autor; • păstrat în arhiva electronică a sistemului.
5.10.4. Cerințe funcționale pentru documentele tehnologice	5.10.4.1. Sistemul trebuie să permită administrarea documentelor tehnologice, inclusiv: • șabloane de formulare; • nomenclatoare și clasificatori; • documentație de utilizare și administrare. 5.10.4.2. Modificarea documentelor tehnologice trebuie să fie permisă doar utilizatorilor autorizați, conform rolurilor definite. 5.10.4.3. Toate modificările documentelor tehnologice trebuie să fie: • jurnalizate; • versionate; • recuperabile (rollback).
5.10.5. Trasabilitate, audit și conformitate	5.10.5.1. Sistemul trebuie să asigure trasabilitatea completă a documentelor de bază, incluzând: • cine a creat documentul; • cine l-a modificat; • când a fost utilizat; • în ce context operațional. 5.10.5.2. Sistemul trebuie să permită consultarea istoricului complet al fiecărui document. 5.10.5.3. Documentele de bază trebuie să fie incluse în mecanismele de audit intern și extern.
5.10.6. Arhivare și păstrare	5.10.6.1. Sistemul trebuie să asigure arhivarea documentelor de bază în conformitate cu: • legislația națională aplicabilă; • regulamentele interne ale registrului. 5.10.6.2. Accesul la documentele arhivate trebuie să fie controlat pe bază de rol. 5.10.6.3. Sistemul trebuie să permită exportul documentelor arhivate pentru scopuri de control și audit.

5.11. Obiecte informaționale și identificatori ai registrului de stat VioData

Sistemul informațional „Registrul de stat VioData” trebuie să gestioneze un set clar definit de obiecte informaționale, care constituie resursa informațională a registrului, în conformitate cu Conceptul SI „VioData” aprobat prin Hotărârea Guvernului nr. 530/2025.

Fiecare obiect informațional trebuie:

- să fie descris formal;
- să aibă un identificator unic;
- să fie gestionat pe întreg ciclul său de viață;
- să fie supus regulilor de securitate, confidențialitate și audit.

Obiectele informaționale și identificatorii acestora constituie elemente obligatorii ale arhitecturii funcționale și informaționale a SI RS VioData.

5.11.1. Lista obiectelor informaționale de bază	a) Caz de violență Obiect informațional principal care reprezintă un incident sau un set de incidente corelate de violență. b) Victimă Obiect informațional care conține datele persoanei afectate de violență. c) Agresor Obiect informațional care conține datele persoanei presupuse sau confirmate ca agresor. d) Incident de violență Obiect informațional asociat unui caz, care descrie un eveniment concret de violență. e) Evaluare de risc Obiect informațional care reflectă analiza riscurilor asociate cazului. f) Plan de intervenție Obiect informațional care conține măsurile stabilite pentru gestionarea cazului. g) Referire Obiect informațional care reflectă transmiterea cazului sau a victimei către un serviciu sau instituție. h) Serviciu furnizat Obiect informațional care descrie serviciul efectiv acordat (medical, juridic, social etc.). i) Raport și indicator Obiect informațional care conține date agregate, indicatori și rezultate de raportare. j) Document Obiect informațional care include documente de intrare, ieșire și tehnologice. k) Utilizator Obiect informațional care descrie persoana autorizată să utilizeze sistemul. l) Rol și permisiune Obiect informațional care definește drepturile de acces. m) Nomenclator / clasificator Obiect informațional care conține liste controlate de valori. n) Înregistrare de audit (log) Obiect informațional utilizat pentru evidența și controlul activităților din sistem.
5.11.2. Cerințe privind identificatorii unici	5.11.2.1. Fiecare obiect informațional trebuie să fie identificat printr-un identificator unic, generat automat de sistem. 5.11.2.2. Identificatorii trebuie să respecte următoarele principii: • unicitate la nivel de sistem;

	• stabilitate în timp (nu se modifică); • imposibilitatea reutilizării; • utilizare în toate relațiile dintre obiecte. 5.11.2.3. Pentru obiectele care reprezintă persoane (victimă, agresor, utilizator), sistemul trebuie să permită: • asocierea cu identificatori naționali (ex.: IDNP), unde este permis legal; • utilizarea identificatorilor interni ai sistemului în toate procesele operaționale.
5.11.3. Relaționarea obiectelor informaționale	5.11.3.1. Sistemul trebuie să permită relaționarea explicită între obiectele informaționale, inclusiv: • un caz poate include mai multe incidente; • un caz poate avea una sau mai multe victime; • un caz poate include unul sau mai mulți agresori; • un caz poate avea mai multe evaluări de risc; • un caz poate avea mai multe referiri și servicii furnizate. 5.11.3.2. Relațiile dintre obiecte trebuie să fie: • documentate; • trasabile; • reflectate în interfața utilizator.
5.11.4. Reguli de versionare și istoric	5.11.4.1. Sistemul trebuie să păstreze istoricul modificărilor pentru obiectele informaționale critice, inclusiv: • datele despre victimă; • evaluările de risc; • planurile de intervenție; • stările cazului. 5.11.4.2. Istoricul trebuie să includă: • versiunea anterioară; • utilizatorul care a efectuat modificarea; • data și ora modificării. 5.11.4.3. Versiunile anterioare nu pot fi șterse.
5.11.5. Validare, deduplicare și integritate	5.115.1. Sistemul trebuie să implementeze mecanisme de validare a datelor la nivel de obiect informațional. 5.115.2. Sistemul trebuie să prevină duplicarea obiectelor informaționale, inclusiv prin: • detectarea înregistrărilor similare; • avertizarea utilizatorului; • reguli de deduplicare configurabile. 5.115.3. Integritatea relațiilor dintre obiecte trebuie să fie garantată tehnic.
5.11.6. Audit și securitate pentru obiectele informaționale	5.11.6.1. Orice creare, modificare, vizualizare sau ștergere logică a unui obiect informațional trebuie să fie jurnalizată. 5.11.6.2. Accesul la obiectele informaționale trebuie să fie controlat pe bază de rol și permisiuni. 5.11.6.3. Obiectele informaționale care conțin date cu caracter personal trebuie să fie protejate conform legislației în vigoare.

5.12. Scenarii operaționale (use cases)

Prezentul capitol definește scenariile operaționale de bază ale Sistemului informațional „Registrul de stat VioData”, prevăzute de Conceptul aprobat prin Hotărârea Guvernului nr. 530/2025 și obligatorii pentru implementare.

Fiecare scenariu operațional trebuie să fie implementat sub formă de:

- flux funcțional end-to-end;
- reguli de business clare;

- stări și tranziții controlate;
- jurnalizare completă.

Scenariile operaționale constituie baza pentru:

- proiectarea funcțională;
- estimarea efortului;
- testarea și recepția sistemului.

Scenarii operaționale (use cases)

Denumire scenariu (use case)	**Descriere generală**	**Flux operațional**	**Reguli obligatorii**
SO-01 – Înregistrarea unui caz de violență	Prezentul capitol definește scenariile operaționale de bază ale Sistemului informațional „Registrul de stat VioData	a) Utilizatorul autorizat se autentifică în sistem; b) Inițiază crearea unui caz nou; c) Sistemul generează automat identificatorul unic de caz; d) Utilizatorul completează formularul de raportare a incidentului; e) Sistemul validează datele introduse; f) Sistemul salvează cazul și îl setează în starea „Deschis”.	• Cazul nu poate fi salvat fără câmpurile obligatorii; • Identificatorul de caz este unic și nemodificabil; • Toate acțiunile sunt jurnalizate.
SO-02 – Evaluarea riscului	Scenariul descrie procesul de evaluare a riscului asociat cazului, conform metodologiilor aplicabile.	a) Utilizatorul selectează un caz existent; b) Inițiază evaluarea riscului; c) Completează criteriile de evaluare; d) Sistemul calculează și/sau înregistrează nivelul de risc; e) Evaluarea este salvată și asociată cazului. f) În cazul Online, Sistemul primește rezultatul de analiză de la sistemul terț și clasificarea de violență de analiză a rețelelor sociale.	• Fiecare evaluare este versionată; • Evaluările anterioare rămân accesibile; • Evaluarea este obligatorie înainte de planul de intervenție.
SO-03 – Elaborarea planului de intervenție	Scenariul descrie procesul de stabilire a măsurilor de intervenție pentru un caz.	a) Utilizatorul selectează un caz evaluat; b) Creează un plan de intervenție; c) Definește acțiuni, responsabili și termene; d) Salvează planul; e) Sistemul asociază planul cu cazul.	• Planul este obligatoriu pentru cazurile active; • Modificările sunt jurnalizate; • Istoricul planurilor este păstrat.
SO-04 – Monitorizarea și actualizarea cazului	Scenariul descrie procesul de urmărire	a) Utilizatorul accesează cazul; b) Actualizează informații	• Stările cazului sunt controlate;

	longitudinală a cazului.	relevante, inclusiv în regim automat din sistem de analiză a rețelelor sociale; c) Adaugă note și documente; d) Modifică starea cazului, dacă este cazul; e) Sistemul salvează și jurnalizează modificările.	• Tranzițiile nepermise sunt blocate; • Istoricul modificărilor este complet.
SO-05 – Referirea către servicii și instituții	Scenariul descrie procesul de referire a cazului sau a victimei către servicii externe.	a) Utilizatorul inițiază o referire; b) Selectează tipul de serviciu; c) Completează datele necesare; d) Sistemul transmite referirea; e) Statusul referirii este actualizat.	• Fiecare referire are identificator unic; • Referirea este asociată cazului; • Istoricul referirilor este păstrat.
SO-06 – Monitorizare ordine de restricție și ordonanțe de protecție	Scenariul descrie procesul de monitorizare a ordinelor de restricție și ordonanțelor de protecție corelate cu cazul de violență	a) Sistemul verifică existența măsurilor active; b) Blochează închiderea cazului, dacă există măsuri active c) Sistemul verifică periodic termenele ordinelor de restricție și ordonanțele de protecție din sistemele informaționale; d) Generează alertă înainte de expirare; e) Marchează ordinul ca „Expirat” la termen; f) Actualizează starea în fișa cazului.	• Ordinul de restricție este asociat cazului și agresorului; • Ordonanța de protecție este asociat cazului și victimei; • Termenul de valabilitate este monitorizat automat; • Ordinul de restricție este afișat în fișa cazului • Ordonanța de protecție este afișată în fișa cazului • Accesul este controlat pe roluri.
SO-07 – Gestionarea nomenclatoarelor	Scenariul descrie gestionarea nomenclatoarelor – crearea, modificarea, dezactivarea și audit istoric al nomenclatoarelor.	Creare nomenclator a) Utilizatorul accesează „Administrare nomenclatoare”; b) Selectează „Nomenclator nou”; c) Completează denumirea și descrierea; d) Adaugă valori inițiale; e) Salvează nomenclatorul. Modificare și dezactivare nomenclator f) Utilizatorul selectează un nomenclator existent;	• Doar utilizator cu rol autorizat poate crea, modifica sau dezactiva nomenclatoare; • La modificarea nomenclatorului datele istorice rămân intacte;

		g) modifică/dezactivează o valoare; g) Modificarea este salvată cu versionare.	
SO-08 – Închiderea cazului	Scenariul descrie procesul de închidere formală a cazului.	a) Utilizatorul solicită închiderea cazului; b) Completează justificarea; c) Sistemul validează condițiile; d) Starea cazului se schimbă în „Închis”; e) Cazul este arhivat logic.	• Cazurile închise nu pot fi șterse; • Redeschiderea este permisă doar cu rol autorizat; • Toate acțiunile sunt jurnalizate.
SO-09 – Raportare și utilizare date agregate	Scenariul descrie procesul de generare și utilizare a rapoartelor și indicatorilor.	a) Utilizatorul selectează perioada și criteriile; b) Sistemul agregă datele; c) Indicatorii sunt calculați; d) Raportul este generat; e) Raportul poate fi exportat.	

5.13. Interoperabilitate și schimb de date

Sistemul informațional „Registrul de stat VioData” (SI RS VioData) trebuie să asigure interoperabilitatea funcțională, semantică și tehnică cu sistemele informaționale guvernamentale și sectoriale.

Prestatorul trebuie să proiecteze și implementeze interoperabilitatea respectând următoarele principii:

1. Principiul once-only – datele sunt colectate o singură dată de la sursa primară și reutilizate prin schimb de date;
2. Separarea rolurilor – fiecare sistem participant are rol clar (furnizor, consumator sau bidirecțional);
3. Trasabilitate – fiecare schimb de date este jurnalizat și auditat;
4. Securitate și confidențialitate – datele sunt protejate pe întreg fluxul de schimb;
5. Interoperabilitate standardizată – schimbul se realizează exclusiv prin platformele guvernamentale.

Schimbul de date trebuie realizat obligatoriu prin Platforma guvernamentală de interoperabilitate MConnect.

Arhitectura SI RS VioData trebuie să permită:

- schimb de date sincron prin MConnect;
- schimb de date asincron cu sistem de analiză a rețelelor sociale, pentru analiza cazurilor de violență Online;
- schimb de date asincron / evenimente prin componenta MConnect Events, pentru scenarii de notificare și sincronizare aproape în timp real.

Implementarea schimbului de date direct (point-to-point) este interzisă.

5.13.1. SI RS VioData trebuie să fie interoperabil, cel puțin, cu următoarele categorii de sisteme, conform Conceptului:

a) *Sisteme din domeniul sănătății, pentru:*

- transmiterea informațiilor relevante despre asistența medicală acordată;
- recepționarea datelor medicale necesare gestionării cazului;

b) *Sisteme din domeniul ordinii publice și justiției, pentru:*

- schimb de informații privind măsurile de protecție;
- stadiul procedurilor legale, acolo unde este permis legal;

c) *Sisteme din domeniul protecției sociale, pentru:*
- schimb de date privind serviciile sociale;
- evitarea dublei raportări;

d) *Sisteme guvernamentale comune, inclusiv:*
- MPass (autentificare);
- MSign (semnătură electronică);
- MNotify (notificări);
- MLog (jurnalizare).

Pentru fiecare integrare, Prestatorul trebuie să specifice explicit:
- obiectele informaționale schimbate;
- structura datelor;
- sensul schimbului (furnizare/consum);
- frecvența schimbului;
- condițiile de declanșare.

Schimbul de date poate include, fără a se limita la:
- identificatori de caz;
- date despre victimă și agresor (în limitele legii);
- statutul cazului;
- informații despre referiri și servicii furnizate;
- indicatori agregați.

5.13.2. Scenarii operaționale de interoperabilitate

SI RS VioData trebuie să implementeze cel puțin următoarele scenarii operaționale de interoperabilitate:

a) Preluare date din sisteme externe pentru completarea automată a cazului;
b) Transmitere date către alte sisteme în urma unei referiri;
c) Notificare prin evenimente la schimbarea stării cazului;
d) Sincronizare periodică a datelor relevante;
e) Recepționare feedback privind serviciile furnizate.

5.13.3. Gestionarea erorilor și continuitatea schimbului de date

Sistemul trebuie să detecteze și să gestioneze:
- indisponibilitatea temporară a sistemelor externe;
- erori de validare a datelor;
- erori de comunicare.

Pentru fiecare eroare, sistemul trebuie să:
- înregistreze evenimentul în jurnal;
- notifice utilizatorii autorizați, unde este cazul;
- permită reluarea schimbului de date.

5.13.4. Documentare și testare

Prestatorul trebuie să livreze documentație completă privind interoperabilitatea, incluzând:
- descrierea arhitecturii de integrare;
- specificații API / mesaje;
- diagrame de flux de date;
- scenarii de testare.

Toate integrările trebuie să fie supuse **testelor de interoperabilitate** și demonstrate în cadrul recepției.

6. Cerințele non-funcționale

Cerințe	Descrierea cerințelor
6.1. Tehnologii open-source și arhitectură	• Dezvoltarea sistemului informațional „Registrul de stat VioData” ar trebui să utilizeze tehnologii și standarde open-source pentru a asigura sustenabilitatea. • Sistemul ar trebui să fie proiectat modular, cu interfețe interschimbabile, pentru a permite înlocuirea sau actualizarea

	individuală a modulelor fără a necesita o reproiectare a altor module care interacționează. • Sistemul informațional „Registrul de stat VioData” trebuie să corespundă cu Modelul Unitar de Design – care este standardul național de design pentru toate soluțiile web și mobile utilizate de autoritățile publice din Republica Moldova. Principiile Modelului Unitar de Design și ghid-ul de implementare este disponibil pe https://egov-moldova.github.io/egov4dev/mud/ • *Tehnologii recomandate (Technology stack):* o **Frontend:** Aplicațiile web sunt construite cu MudBlazor ▪ MudBlazor – NuGet: MudBlazor – componente reutilizabile ale interfeței utilizator ▪ Blazor Server / WebAssembly – pentru aplicații interactive în NET o **Backend:** Logica de business este implementată în cadrul ecosistemului.NET ▪ ASP.NET Core – NuGet: Microsoft.AspNetCore.* – pentru servicii REST și aplicații web scalabile ▪ Entity Framework Core – NuGet: Microsoft.EntityFrameworkCore – pentru acces la baze de date relaționale ▪ FluentValidation – NuGet: FluentValidation – pentru validări declarative ▪ Swashbuckle.AspNetCore – NuGet: Swashbuckle.AspNetCore – pentru generarea documentației Swagger o **Baza de date** (Databases) ▪ SQL Server, PostgreSQL – pentru stocarea datelor relaționale ▪ Redis – NuGet: StackExchange.Redis – pentru caching și optimizarea performanței ▪ Structuri JSON – utilizate pentru configurarea dinamică a regulilor și categoriilor
6.2. Mediul de sistem	• Sistemul informațional „Registrul de stat VioData” trebui să fie găzduit pe Platforma Cloud Guvernamentală – MCloud. • Implementarea proiectului ar trebui să includă un mediu de dezvoltare pentru scrierea, testarea și depanarea codului sistemului și un mediu de producție în care sistemul să fie implementat și accesibil utilizatorilor finali. • Orchestrare și containere o Kubernetes – pentru orchestrarea serviciilor containerizate o Docker – pentru împachetarea aplicațiilor în containere portabile o Helm – pentru gestionarea implementărilor în Kubernetes, oferind versiuni controlate, revenire rapidă la versiune și configurare declarativă prin intermediul diagramelor • CI/CD și DevOps o Azure DevOps – pentru gestionarea livrărilor, a sarcinilor și a erorilor o Conducte automatizate pentru compilare, testare și implementare o GitLab – pentru controlul versiunilor și integrare continuă • Monitorizare și SRE o Centralizare prin Azure DevOps o Sisteme de alertare, înregistrare în jurnal, auditare și urmărire

	○ Elasticsearch – pentru indexarea și căutarea rapidă a jurnalelor și a datelor operaționale ○ Kibana – pentru vizualizarea datelor din Elasticsearch ○ Prometheus + Grafana – pentru monitorizarea și vizualizarea indicatorilor de performanță
NFR 03: Integrarea sistemului	• Sistemul informațional „Registrul de stat VioData" ar trebui să fie integrat cu următoarele servicii ale platformelor guvernamentale: 1. MPass – servicii guvernamentale de autentificare și autorizare. 2. MSign – serviciul guvernamental integrat de semnătură electronică și semnare de fișiere. 3. MNotify – serviciul guvernamental de notificare electronică pentru informarea utilizatorilor despre evenimentele generate. 4. MLog – pentru înregistrarea acțiunilor/evenimentelor de afaceri și extragerea statisticilor privind utilizarea serviciilor. 5. MConnect – platforma guvernamentală de interoperabilitate pentru schimbul de date cu sistemele informatice externe relevante.
6.3. Interoperabilitate sistemului	• Sistemul informațional „Registrul de stat VioData" trebuie să se integreze fără probleme cu sistemele externe și să facă schimb de date prin intermediul platformei guvernamentale de interoperabilitate – MConnect. Integrarea principală include: ○ Integrarea cu forțele de ordine și sistemul juridic pentru a permite urmărirea ordinelor de restricție și a statusului cazurilor în cadrul sistemului judiciar, precum și partajarea securizată a probelor criminalistice pentru procedurile judiciare. ○ Integrarea cu sistemul de sănătate, care include referirea către spitale și clinici pentru asistență medicală și examinare medico-legală. ○ Integrarea cu serviciile sociale și adăposturile, pentru a urmări ajutorul financiar și programele de reintegrare. ○ Integrarea cu sistemul de analiză automatizată al rețelelor sociale pentru identificarea și monitorizarea cazurilor de violență Online. • Sistemul trebuie să furnizeze API-uri bine documentate pentru integrarea cu sisteme externe. • Pentru integrarea sistemului trebuie utilizate standarde din industrie (ex.: REST, GraphQL). • Trebuie să asigure suport pentru formate de date interoperabile precum JSON, XML sau CSV.
6.4. GPS Geo-etichetare	• Frontend pentru geo-etichetare GPS ○ Utilizează HTML5 Geolocation API pentru urmărirea bazată pe browser. ○ Integrare cu hărți utilizând Google Maps API, OpenStreetMap (OSM) sau Mapbox. • Backend pentru geo-etichetare GPS ○ Stochează latitudinea/longitudinea utilizând PostGIS (PostgreSQL) sau MongoDB cu indexare geospațială. ○ Puncte de acces API securizate pentru actualizarea locațiilor (REST/GraphQL)
6.5. Securitatea sistemului	• Sistemul informațional „Registrul de stat VioData" trebuie să respecte standardele din industrie precum OWASP (Open Web Application Security Project) pentru a asigura respectarea celor mai bune practici de securitate acceptate. • Sistemul informațional „Registrul de stat VioData" ar trebui să cripteze toate datele în tranzit utilizând TLS (ex.: HTTPS).

	• Trebuie să respecte standardele ISO/IEC 27001 pentru gestionarea securității informațiilor. • Sistemul informațional „Registrul de stat VioData” trebuie să fie în conformitate cu Hotărârea Guvernului privind aprobarea cerințelor minime obligatorii de securitate cibernetică – Hotărârea nr. 201 din 9 martie 2017.
6.6. Protecția datelor	• Sistemul trebuie să respecte reglementările naționale privind protecția datelor, în special cerințele pentru asigurarea securității datelor personale în timpul procesării acestora în cadrul sistemelor informatice de date personale (HG nr.1123/2010). • Sistemul trebuie să respecte Regulamentul General privind Protecția Datelor (GDPR) (UE) 2016/679.
6.7. Scalabilitate și fiabilitate	• Sistemul trebuie să suporte un număr tot mai mare de utilizatori și cazuri fără degradarea performanței. • Trebuie să fie proiectat pentru a gestiona accesul simultan din mai multe agenții și regiuni pentru cel puțin 500 de utilizatori simultan. Să permită scalarea până la 1.000 de utilizatori simultan în situații de urgență sau perioade de trafic intens. • Asigurarea unei disponibilități a sistemului de cel puțin 99,9% cu întreruperi minime. • Includerea mecanismelor de failover și protocoale de recuperare în caz de dezastru.
6.8. Performanța sistemului	• Timpul de recuperare a datelor (ex.: încărcarea unui dosar de caz): ≤ 2 secunde. • Generarea de rapoarte: ≤ 5 secunde pentru rapoartele standard. • Notificări în timp real: livrate în ≤ 1 secundă. • Latența pentru apelurile API intra-sistem: ≤ 50 de milisecunde. • Latența pentru integrările API externe: ≤ 200 de milisecunde. • Procesarea analizei la nivel de caz (ex.: tendințele incidentelor): ≤ 10 secunde. • Gestionarea seturilor de date de până la 1 milion de înregistrări fără întârzieri semnificative. • Sincronizarea datelor cu platformele externe (ex.: sisteme de sănătate, forțe de ordine): ≤ 1 secundă pe înregistrare. • Timp de răspuns al API-urilor pentru cererile externe: ≤ 200 de milisecunde.
6.9. Garanția și întreținerea sistemului	• Sistemul trebuie actualizat periodic cu funcționalități noi, bazate pe feedback-ul utilizatorilor și nevoile în evoluție după faza pilot. • Perioada de garanție: dezvoltatorul este responsabil pentru remedierea tuturor defectelor și soluționarea tuturor incidentelor raportate de client în perioada de garanție de 12 luni, gratuit. • Dezvoltatorii trebuie să ofere întreținere corectivă și adaptivă pentru sistem timp de până la un an după implementarea sistemului. • Menținerea documentației actualizate pentru arhitectura sistemului, fluxurile de lucru și API-uri. Păstrarea unui jurnal detaliat al tuturor activităților de întreținere, inclusiv actualizări, patch-uri și rezolvarea problemelor.

În vederea asigurării conformității SI RS VioData cu arhitectura digitală guvernamentală a Republicii Moldova, Prestatorul are obligația de a se familiariza, analiza și aplica prevederile tehnice, metodologice și arhitecturale prezentate în platforma *eGov4Dev* **(https://egov-moldova.github.io/egov4dev/),** elaborată și administrată de Agenția de Guvernare Electronică.

Platforma *eGov4Dev* constituie sursa oficială de documentație tehnică pentru dezvoltarea, integrarea și operarea sistemelor informaționale guvernamentale și include, fără a se limita la:

- principii de arhitectură a sistemelor informatice guvernamentale;
- cerințe și recomandări privind interoperabilitatea și schimbul de date prin platformele naționale;
- descrierea serviciilor comune guvernamentale, mecanismele de integrare și interfețele API aferente;
- bune practici de securitate, management al identității, autentificare și autorizare;
- exemple de implementare, ghiduri pentru dezvoltatori și instrumente suport pentru testare și validare.

Prestatorul va lua în considerare aceste ghiduri în toate etapele ciclului de viață al sistemului (analiză, proiectare, dezvoltare, integrare, testare și punere în producție), astfel încât soluția SI RS VioData să fie compatibilă cu ecosistemul digital guvernamental, să permită integrarea coerentă cu alte sisteme informaționale ale statului și să respecte cerințele naționale de interoperabilitate, securitate și sustenabilitate tehnică. Nerespectarea acestor ghiduri va fi considerată neconformitate tehnică în procesul de evaluare și acceptanță a livrabilelor.

7. Alte cerințe şi reguli privind prestarea serviciilor

Mod de lucru. Modalități de intervenție

Pe tot parcursul prestării serviciilor este important de păstrat o comunicare corectă între echipa Prestatorului și cea a Beneficiarului. Toate operațiunile se vor desfășura în condițiile maxime de securitate cibernetică, cu respectarea strictă a legislației în vigoare.

Pe perioada contractului vor fi disponibile din partea Prestatorului următoarele modalități de intervenție în cazul incidentelor dar și pentru operațiuni normale de întreținere:

a) intervenții tehnice și recomandări telefonice, prin mail sau prin alte mijloace de comunicație electronică, inclusiv videoconferință;
b) intervenții on-site la sediul Beneficiarului sau/și a Prestatorului, în situațiile în care specialiștii apreciază că este necesară o astfel de abordare a situației.

Soluționarea divergențelor

Orice divergențe apărute între Părți vor fi soluționate cu efort comun şi prin strânsă conlucrare între Părți. În acest scop, vor fi aplicate următoarele reguli:

Părțile vor forma un grup comun de lucru în scopul soluționării divergențelor. De comun acord, în grupul de lucru pot fi acceptați reprezentanți ai părților terțe, inclusiv experți independenți. La necesitate, părțile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergență.

Grupul de lucru se va convoca şi va examina subiectul divergențelor şi probele existente la subiect. Părțile vor aplica prevederile Contractului şi prezentele Reguli în scopul clarificării tuturor aspectelor disputate şi identificării unei soluții echitabile pentru divergențele ivite.

Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru.

Securitatea informației

În cazul unui incident de securitate a informației, Partea ce a constatat incidentul va notifica imediat şi cealaltă Parte, dacă aceasta poate fi de asemenea afectată de incident. Părțile vor coordona măsurile necesar a fi întreprinse în scopul diminuării impactului incidentului şi soluționării acestuia.

La solicitarea Beneficiarului, Presatorul va întreprinde acțiunile de rigoare în scopul colectării şi conservării probelor ce pot fi necesare la investigarea incidentului şi la probarea juridică a responsabilității pentru incident. În acest scop, Prestatorul, la solicitarea Beneficiarului, poate efectua:

a) colectarea şi conservarea fişierelor log ce conţin informaţia privind accesul la nivelul componentelor de reţea;
b) efectuarea copiilor de rezervă depline pentru softul aplicativ, stocarea acestora în condiţii ce asigură integritatea copiilor de rezervă efectuate;
c) menţinerea formalizată a Registrului privind deţinerea probelor conservate.

După soluționarea unui incident de securitate, Părțile vor întocmi rapoarte individuale privind gestiunea incidentului. De comun acord vor întocmi un plan de acțiuni pentru prevenirea repetării incidentelor similare.

Cerințe privind compania dezvoltatoare și experiența personalului implicat

Ofertantul trebuie să demonstreze capacitatea tehnică, profesională și organizațională necesară pentru dezvoltarea și implementarea unui sistem informațional guvernamental. În acest sens, ofertantul va îndeplini cumulativ următoarele cerințe minime:

1. să fie persoană juridică înregistrată legal, cu drept de desfășurare a activităților de dezvoltare software și servicii IT.
2. să aibă minimum 5 ani de experiență în dezvoltarea și implementarea sistemelor informaționale sau aplicațiilor software.
3. să fi implementat, în ultimii 3 ani, cel puțin 3 proiecte relevante, care să includă una sau mai multe dintre următoarele componente:
   - sisteme informaționale guvernamentale sau publice;
   - registre sau platforme de management al cazurilor / datelor;
   - sisteme cu integrare API și interoperabilitate;
4. Să dispună de capacitatea de a asigura suport post-implementare, mentenanță și evoluție a sistemului pe durata contractuală.

Echipa de proiect trebuie să includă specialiști de înaltă calificare cu experiență în domeniile respective. În cazul concediilor (ex: de odihnă, concedii medicale, deplasări, etc) sau alte situații ce duc la încetarea temporară a atribuțiilor de muncă a specialiștilor din cadrul echipei, sau situații în care specialistul nu poate fi disponibil pentru îndeplinirea activităților aferente caietului de sarcini, Ofertantul va asigura înlocuirea imediată a membrilor existenți cu alți membri noi ținând cont de cerințele prezentului caiet de sarcini. În cazul înlocuirii unui expert pe parcursul implementării, acesta va avea calificări și experiență **cel puțin echivalente** cu cele ale expertului evaluat inițial.

Componența minimă obligatorie a echipei:

Rolul	Cerințele de experiență
Manager de proiect (project manager)	• Studii superioare finalizate în domeniul IT, management, economie sau domeniu conex. • Experiență profesională totală ≥ 5 ani în proiecte IT • Minimum 3 proiecte IT complexe coordonate în calitate de manager de proiect. • Cunoștințe și experiență în metodologii de management de proiect.
Analist de business (business analyst)	• Studii superioare finalizate. • Experiență profesională ≥ 5 ani în analiza de business pentru sisteme informatice. • Experiență în colectarea și documentarea cerințelor funcționale și nefuncționale. • Experiență în elaborarea use-case-urilor, diagramelor de proces sau modelelor de date.
Arhitect IT	• Studii superioare în domeniul IT • Minimum 5 ani experiență profesională în domeniul

	• Minimum 3 ani experiență în rol de arhitect de sistem Experiență în proiectarea arhitecturii sistemelor distribuite și a mecanismelor de integrare (API, servicii web, microservicii)
Dezvoltator backend	• Studii superioare sau experiență profesională echivalentă • Minimum 4 ani experiență în dezvoltare backend • Experiență în dezvoltarea de aplicații web și serviciilor API • Experiență în lucrul cu baze de date relaționale și/sau NoSQL • Experiență în implementarea mecanismelor de securitate (autentificare și autorizare)
Dezvoltator frontend	• Studii superioare sau experiență profesională echivalentă • Minimum 3 ani experiență în dezvoltare frontend. • Experiență în dezvoltarea interfețelor web moderne • Experiență în integrarea interfețelor cu servicii API Cunoștințe privind bune practici de accesibilitate și experiență a utilizatorului
Specialist UX/UI	• Studii superioare sau formare relevantă în design UX/UI • Minimum 3 ani experiență în design UX/UI pentru aplicații software • Experiență în elaborarea wireframes, prototipuri și design-uri funcționale
Specialist QA / testare	• Studii superioare sau experiență relevantă în domeniul IT • Minimum 3 ani experiență în testarea aplicațiilor software • Experiență în testare funcțională, de regresie și de acceptanță

8. Implementarea proiectului

Prestatorul trebuie să implementeze SI RS VioData utilizând o metodologie etapizată cu livrări incrementale, aliniată Conceptului Sistemului informațional „VioData” aprobat prin Hotărârea Guvernului nr. 530/2025. Metodologia de implementare trebuie să combine:

- structura secvențială pe etape (conform Conceptului);
- livrări iterative/incrementale (elemente Agile), rezultând într-o abordare hibridă.

Etapele de implementare

Etapa	**Descriere**	**Livrabile minime obligatorii**	**Perioada de realizare**	**Costurile**
Etapa I – Inițiere și analiză detaliată	• analiza cerințelor funcționale și operaționale; • validarea cerințelor cu Beneficiarul; • analiza interoperabilității; • analiza riscurilor.	• Raport de inițiere; • Specificație funcțională detaliată; • Matrice de trasabilitate Concept–Cerință–Use-case.		
Etapa II – Proiectare	• arhitectura sistemului; • modelul informațional; • fluxurile operaționale; • design UI/UX.	• Document de proiectare a sistemului; • Modele de date și diagrame; • Specificații de interoperabilitate.		

Etapa III – Dezvoltare și integrare	• funcționalitățile sistemului; • integrările prin MConnect și MConnect Events; • mecanismele de securitate și audit.	• Versiuni incrementale funcționale; • Cod sursă; • Documentație tehnică.		
Etapa IV – Testare și pilotare	• testare funcțională; • testare de interoperabilitate; • testare de securitate; • pilotare cu utilizatori.	• Raport de testare; • Raport de pilotare; • Remedierea neconformităților.		
Etapa V – Lansare și recepție	• lansarea sistemului; • recepția finală.	• Raport de instruire a utilizatorilor; • Raport de lansare.		
Etapa VI – Garanție și mentenanță	• suport corectiv; • remedierea defectelor.	• Raport de remedieri corective post-lansare.		

Fiecare livrare va fi testată de deținătorul Sistemului Informațional în 5 zile lucrătoare. Acceptanța finală este condiționată de testarea completă, instruirea utilizatorilor și funcționarea stabilă.

Instruire:

- Administratori: 16 ore instruire tehnică
- Utilizatori: 24 ore instruire funcțională
- Materiale: Ghiduri de instruire cu instrucțiuni pas cu pas, video ghid și scenarii pentru învățare practică.

Asumarea serviciilor implică acordarea garanției asupra SI RS VioData pentru o perioadă de minim 12 luni după încetarea contractului. De asemenea, Prestatorul serviciilor va documenta toate operațiunile de elaborare și modificare a sistemului și le va prezenta Beneficiarului împreună cu codul sursă SI RS VioData, descrierea privind parametrii funcționali și configurările aplicate, credențiale de acces, astfel încât acestea să fie aplicabile, ulterior, în perioada de exploatare a sistemului și alte etape a ciclului de viață a sistemului.

Modalitatea de întocmire a ofertelor

Toate cerințele incluse în Caietul de sarcini reprezintă condiții obligatorii. Nerespectarea, chiar și parțială, a oricăreia dintre aceste cerințe va conduce automat la declararea ofertei ca neconformă și, în mod implicit, la descalificarea acesteia. Asumarea condițiilor în care se desfășoară proiectul și îndeplinirea cerințelor tehnice, de personal sau asupra modului de lucru pentru toate punctele precizate în capitolele documentației sunt condiții obligatorii și eliminatorii pentru conformitatea ofertelor și sunt totodată termeni considerați contractuali.

Prestatorul trebuie să elaboreze un Raport de Cost Total de Proprietate (TCO) pentru o perioadă de minimum 3 ani. Raportul TCO trebuie să includă, cel puțin:

- costuri de dezvoltare;
- costuri de infrastructură;
- costuri de licențiere (dacă există);
- costuri de mentenanță;
- costuri de suport;
- costuri de instruire;
- costuri de securitate;

- costuri de extindere și scalare.

Estimarea de efort. Prestatorul trebuie să prezinte estimarea efortului în: om-zile sau om-ore; acesta trebuie să fie defalcat pe rol, pe etapă și pe activități (analiză, proiectare, dezvoltare, integrare, testare, instruire, mentenanță). Estimarea trebuie să fie corelată cu cerințele funcționale, scenariile operaționale și use-case-urile indicate.

Scoaterea din exploatare

SI RS VioData trebuie să fie proiectat și implementat astfel încât să permită scoaterea din exploatare controlată, sigură și auditată a sistemului, total sau parțial, la finalul ciclului său de viață sau în cazul înlocuirii cu un alt sistem. Astfel, sistemul trebuie să permită exportul bazei de date, obiectelor informaționale, documentelor de bază și jurnalelor de audit. Sistemul trebuie să permită migrarea către un alt sistem prin fișiere de export sau API-uri de extragere. Sistemul trebuie să permită arhivarea datelor și documentelor în conformitate cu legislația privind arhivarea documentelor electronice, registrele de stat și protecția datelor cu caracter personal.

Dezactivarea controlată a sistemului și ștergerea sigură a datelor. Sistemul trebuie să permită blocarea introducerii de date noi, oprirea controlată a serviciilor și posibilitatea de ștergere sigură și ireversibilă a datelor.

Președintele grupului de lucru

Digitally signed by Lelenco Neli
Date: 2026.03.11 14:26:12 EET
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

Neli LELENCO