Anexa nr. 22
la Documentația standard aprobată prin
Ordinul Ministrului Finanțelor nr. 115/15.09.2021

OFERTA TEHNICĂ DETALIATĂ

Sistemul informațional „Registrul de stat Viodata”

(SI RS Viodata)

Beneficiar:
Agenția Națională de Prevenire și Combatere a Violenței Împotriva Femeilor și a Violenței în Familie (ANPCV)

Pregătit de:

UPCODE GROUP SRL (LIDER ASOCIERE) și SMART ITWORKS SRL (ASOCIAT)

Administrator: Vadim Jeleascov (LIDER ASOCIERE — UPCODE GROUP S.R.L.)

Data depunerii ofertei: 04 / 05 / 2026

Procedura de achiziție: SIA RSAP — achiziții.md

Cod CPV: 72212610-8

Cuprins

Secțiunea 1: Înțelegerea Obiectivelor Proiectului

1.1 Obiectivele Proiectului

Înțelegem pe deplin obiectivul fundamental al acestui proiect: dezvoltarea și implementarea unui sistem informațional integrat (SI RS Viodata) care să modernizeze și să optimizeze toate procesele legate de evidență cazurilor de violență împotriva femeilor și violență în familie, asigurand colectarea precisa a datelor, coordonarea interinstituțională eficiența și protecția strictă a datelor sensibile ale victimelor și beneficiarilor.

Prin analiză aprofundata a Caietului de sarcini, a Conceptului aprobat prin HG nr. 530/2025 și a celor 21 de clarificări primite (răspunsuri din 24.03.2026 și 02.04.2026), am identificat următoarele obiective cheie care vor ghida implementarea soluției noastre:

- Centralizare și Standardizare: Crearea unei baze de date unice pentru toate cazurile de violență în familie și bazată pe gen, stabilind un „punct unic de adevar” care elimina fragmentarea actuală între ANPCV, MAI/IGP, MMPS, MS și CNAJGS, asigurand consistența informațiilor.
- Confidențialitate și Securitate: Implementarea unor mecanisme avansate de criptare (TLS 1.3 în tranzit, AES-256 în repaus), autentificare prin MPass, autorizare prin RBAC granular și jurnalizare integrală în MLog, asigurand conformitate cu GDPR (UE) 2016/679, HG nr. 1123/2010 (securitate date personale) și HG nr. 201/2017 (securitate cibernetica).
- Coordonare Interinstituțională: Integrarea sistemului cu cele 13 sisteme guvernamentale identificate (Registrul Populatiei ASP, eSocial, SIA AMP, IGP, Procuratura E-Dosar, instanțe PIGD, etc.) prin platforma MConnect, plus integrări directe cu CNAJGS, UNFPA și Centrul Justiție Familiala, pentru referirea eficiența a cazurilor și schimbul securizat de date.
- Sprijin Decizional: Implementarea funcționalității de generare a rapoartelor predefinite (Setul de indicatori naționali aprobat prin Hotărârea de Guvern) și tablourilor de bord interactive pentru factorii de decizie, permițând identificarea tendintelor de violență și alocarea optima a resurselor pe baza datelor reale, în toate regiunile Republicii Moldova.
- Conformitate cu Modelul Unitar de Design (MUD): Sistemul va respectă standardul național de design pentru toate soluțiile web utilizate de autoritățile publice din Republica Moldova (https://egov-moldova.github.io/egov4dev/mud/), asigurand o experiență de utilizare consistența cu celelalte servicii guvernamentale.

Recunoaștem că cerințele funcționale prezentate în documentație reprezintă baza fundamentală a proiectului. Analiză detaliată a proceselor de business, modelarea fluxurilor de lucru „As-Is” și „To-Be” și definirea specificațiilor detaliate vor constitui o prima etapă esențială a colaborarii noastre pentru a asigură succesul implementării.

1.2 Riscuri posibile și măsuri de atenuare

Identificarea proactiva și gestionarea riscurilor sunt esențiale pentru succesul unui proiect de o asemenea anvergură. Prezentam în continuare o lista de riscuri specifice, demne de a fi luate în considerare la implementarea proiectului SI RS Viodata, împreună cu acțiunile de prevenție și răspuns pe care le vom intreprinde.

Descriere risc	Nivel impact	Probabilitate	Măsură de atenuare
Complexitatea integrărilor cu cele 13 sisteme guvernamentale, cu potentiale întârzieri în adaptarea API-urilor MConnect și în încheierea acordurilor bilaterale (CNAJGS, UNFPA, ME)	Ridicata	Medie	- Inițierea discuțiilor tehnice cu detinatorii sistemelor inca din prima săptămână. - Crearea unor interfețe simulate (mock APIs) pentru a permite dezvoltarea în paralel. - Prioritizare integrări critice (ASP, eSocial, IGP) în primele sprinturi. - Adapter generic pentru sisteme în dezvoltare (ANP, UNFPA).
Disponibilitatea redusa a experților din partea ANPCV și a institutiilor partenere pentru atelierele de analiză și validare, din cauza sarcinilor operaționale curente	Medie	Medie	- Stabilirea de la început a unui calendar fix și agreat de comun acord pentru toate sesiunile de lucru. - Utilizarea unor instrumente colaborative online pentru a colecta feedback asincron. - Desemnarea unui Product Owner dedicat din partea ANPCV, cu autoritate decizionala.
Volumul și sensibilitatea datelor procesate (date despre victime, agresori, minori), cu cerințe stricte GDPR și HG 1123/2010	Critic	Medie	- Elaborare DPIA (Data Protection Impact Assessment) în Etapă I. - Consultare DPO al ANPCV pentru fiecare flux de date personale. - Data minimization: colectare doar a datelor strict necesare. - Pseudonymization unde tehnic posibil.

			- Audit trimestrial GDPR.
Cresterea necontrolata a cerințelor (Scope Creep) pe parcursul dezvoltarii agile, care ar putea afecta termenul de livrare 25.12.2028	Ridicat	Medie spre Ridicata	Mitigare mulți-strat: (a) scope baseline congelat la finalul Etapei I și confirmat în PV semnat de ANPCV; (b) procedura formală de Change Request — orice modificare necesita Impact Analysis (efort, calendar, cost) și aprobare comună; (c) buffer planificare 10% efort dezvoltare pentru schimbări minore (în cadrul scope); (d) modificări substantiale tratate prin acte aditionale conform Legii 131/2015 (cu pragul de 15% — confirmat de ANPCV în răspunsul la Întrebarea 18); (e) ședința saptamanala de project board cu decideri ANPCV pentru a alinia așteptările.
Asigurarea performanței sistemului la volumul de date și numărul de utilizatori concurenti specificat (min 500 utilizatori, scalare la 1000 în situații de urgența, gestionare 1 milion+ înregistrări)	Ridicata	Joasa	- Proiectarea unei arhitecturi scalabile (microservicii) de la bun început. - Efectuarea testelor de performanță și stres dedicate înainte de lansarea în producție (k6, JMeter). - Monitorizarea continuă a performanței după lansare cu

			Prometheus + Grafana.
Dependenta de schimbările legislative pe parcursul proiectului 2026-2028 (cadrul VG, formate raportare indicatori naționali, GDPR adaptari)	Medie	Medie	- Arhitectură modulară cu nomenclatoare configurabile. - Mentenanță adaptiva planificata (~15% din efort dezvoltare per clarif. 18). - Monitor regular schimbări MO și MB. - Comunicare constanta cu DJ ANPCV pentru ajustari premergatoare.
Disponibilitatea redusa a serviciilor STISC pentru certificate TLS, configurare DNS, acces MCloud	Mica	Medie	- Cerere clara la începutul proiectului (Etapă I). - Documentare clara a nevoilor. - Buffer de 2-3 săptămâni pentru obtinerea certificatelor. - Plan de fallback cu certificat self-signed pentru dev/test.
Acceptanță utilizatori finali scazuta (asistenti sociali, ofiteri poliție, cadre medicale, juristi)	Medie	Medie	- User research intensiv în Etapă I. - Pilotare cu utilizatori reali din toate sectoarele. - Training comprehensiv: 16h admin + 24h utilizatori. - Train-the-trainer pentru formatori interni ANPCV.
Inlocuirea personalului-cheie pe parcursul implementării 2026-2028	Medie	Medie	- Backup pe roluri-cheie (PM, Arhitect, Dev seniori). - Documentare zilnică (sprint logs, wiki) — nici o cunoștință critica nu sta într-un singur loc. - Onboarding rapid (max 5 zile) pentru inlocuitori. - Calificări echivalente

			obligatoriu (cf. Caiet Sarcini).
Plata lunară fără avans 0% — cash flow negativ pentru ofertant și subcontractanți în primele luni	Medie	Mare	- Aliniere grafic prestare cu efort real — sume lunare reflectă muncă. - Clauza „pay-when-paid” în contractele de subcontractare. - Rezerva financiară minim 2 luni de salarii. - Comunicare proactiva cu ANPCV privind alocari bugetare anuale.

Secțiunea 2: Planul și metodologia de implementare

2.1 Planul de implementare

Pentru implementarea sistemului SI RS Viodata, vom aplica o metodologie hibridă care combină structură secvențială pe etape (cerința a Conceptului HG 530/2025) cu cadrul de lucru SCRUM pentru etapă de dezvoltare. Aceasta este o implementare specifică a principiilor Agile, mentionata în Caietul de sarcini, și este concepută pentru a livra valoare în mod iterativ și incremental, asigurand în acelasi timp flexibilitate și transparența maximă. SCRUM organizează muncă în cicluri regulate numite sprinturi de două săptămâni.

Rolurile principale

Procesul Scrum se bazează pe o colaborare strânsă între trei roluri cheie:

- Product Owner (reprezentant ANPCV): Este vocea clientului și a părților interesate. Principală să responsabilitate este de a gestiona și prioritiza lista de cerințe (Product Backlog) pentru a maximiza valoarea produsului dezvoltat de echipă. Va consulta părțile interesate primare (MAI, MMPS, MS, MJ, CNAJGS) pentru deciziile cu impact intersectorial.
- Scrum Master (din partea noastră): Acționează ca un lider-servitor pentru echipă. Rolul său nu este de a conduce echipa, ci de a facilita procesul Scrum, de a înlătura impedimentele, de a proteja echipa de întreruperi externe și de a se asigură că metodologia este înțeleasă și aplicata corect.
- Echipa de Dezvoltare (echipa noastră + subcontractanți): Este un grup auto-organizat de profesioniști (dezvoltatori, ingineri QA, designeri UX/UI, analiști business, arhitect IT) care au competențele necesare pentru a transforma cerințele din backlog într-un increment funcțional al sistemului la finalul fiecărui sprint.

Artefacte Scrum

Transparența în Scrum este asigurată prin intermediul a două artefacte principale:

- Product Backlog: O lista dinamică și ordonată a tuturor funcționalităților, cerințelor și îmbunătățirilor necesare pentru produs. Aceasta este sursa unică de muncă pentru echipa de dezvoltare și este gestionată exclusiv de Product Owner-ul ANPCV.
- Sprint Backlog: Un set de elemente selectate din Product Backlog pentru a fi implementate într-un sprint, împreună cu planul de a livra incrementul de produs. Sprint Backlog-ul este creat și gestionat de Echipa de Dezvoltare.

Evenimente Scrum (Ceremonii)

Fiecare sprint, pe care îl propunem a avea o durata de două săptămâni, este un eveniment în sine și conține următoarele ceremonii:

- Planificarea sprintului (Sprint Planning): La începutul fiecărui sprint, întreaga echipă colaborează pentru a selecta un set de elemente din Product Backlog care vor fi implementate. Echipa de Dezvoltare prognozează ce poate fi realizat și definește un obiectiv clar pentru sprint (Sprint Goal).

- Ședința zilnică (Daily Scrum): O întâlnire scurtă, de maximum 15 minute, care are loc în fiecare zi a sprintului. Membrii Echipei de Dezvoltare se sincronizează, discută progresul către obiectivul sprintului și identifică eventualele blocaje.
- Revizuirea sprintului (Sprint Review): La finalul sprintului, Echipa de Dezvoltare prezintă incrementul de produs funcțional tuturor părților interesate (inclusiv conducerii ANPCV și reprezentanților părților interesate primare). Scopul este de a demonstra muncă realizată, de a colecta feedback și de a adapta Product Backlog-ul daca este necesar.
- Retrospectiva sprintului (Sprint Retrospective): Este ultima ceremonie a sprintului. Echipa Scrum reflectă asupra procesului de lucru din sprintul încheiat și identifică acțiuni concrete de îmbunătățire pentru următorul sprint.

Fazele principale ale metodologiei noastre, conform Caietului de sarcini și Conceptului HG 530/2025:

1. Inițiere și analiză detaliată (Etapă I — durata 2 luni): Stabilirea fundatiei proiectului, alinierea echipelor, analiză interoperabilității cu cele 13 sisteme guvernamentale, DPIA și definirea arhitecturii. Livrabile minime obligatorii: Raport de inițiere; Specificație funcțională detaliată; Matrice de trasabilitate Concept-Cerința-Use-case.
2. Proiectare (Etapă II — durata 3 luni): Arhitectură sistemului; modelul informațional; fluxurile operaționale; design UI/UX conform Modelului Unitar de Design. Livrabile minime: Document de proiectare a sistemului; Modele de date și diagrame; Specificații de interoperabilitate.
3. Dezvoltare și integrare (Etapă III — durata 9 luni): Construirea și livrarea sistemului funcțional în cicluri scurte și iterative (18 sprinturi de două săptămâni). Implementarea celor 9 contururi funcționale + integrările prin MConnect și MConnect Events + mecanismele de securitate și audit. Livrabile minime: Versiuni incrementale funcționale; Cod sursa; Documentație tehnică.
4. Testare și pilotare (Etapă IV — durata 3 luni): Testare funcțională, interoperabilitate, securitate, pilotare cu utilizatori reali. Livrabile minime: Raport de testare; Raport de pilotare; Remedierea neconformitatilor.
5. Lansare și recepție (Etapă V — durata 3 luni): Lansarea sistemului la nivel național, instruire utilizatori (administratori 16h, utilizatori 24h), recepția finală. Livrabile minime: Raport de instruire a utilizatorilor; Raport de lansare.
6. Garanție și mentenanță (Etapă VI — durata 12 luni): Suport corectiv și mentenanță adaptiva (~15% efort dezvoltare per clarif. 18) timp de 12 luni de la recepția finală. Livrabile minime: Raport de remedieri corective post-lansare.

2.2 Etapă de inițiere și analiză (durata: 2 luni)

Această prima etapă este fundamentală pentru succesul întregului proiect, deoarece stabileste bazele tehnice, strategice și organizatorice. Vom desfășura activități intensive pentru alinierea completa cu echipă ANPCV și părțile interesate primare (MAI, MMPS, MS, MJ, CNAJGS, UNFPA), pentru a asigură o înțelegere comună și detaliată a viziunii și cerințelor.

Activitățile principale ale acestei etape includ:

- Ședința de kick-off: Organizarea unei întâlniri formale pentru a prezenta membrii echipei, a stabili rolurile și responsabilitatile, a defini fluxurile de comunicare și a valida obiectivele proiectului. Vor participa reprezentanți ai tuturor părților interesate primare.
- Analiză aprofundata a proceselor: Vom organiza ateliere de lucru cu personalul operațional, managementul și departamentele tehnice ale ANPCV, ATAS/STAS, IGP, Centrul Justiție Familiala, spitale și centre medicina legala, oficii CNAJGS, pentru a analiză în detaliu procesele de afaceri existente și a identifică cerințele funcționale și tehnice specifice.
- Definirea arhitecturii detaliate: Pe baza analizei, vom finaliza și vom prezenta documentația cuprinzatoare despre arhitectură sistemului pe microservicii, fluxurile de lucru, structurile de date și măsurile de securitate ce urmează a fi implementate.
- Analiză interoperabilității: Cartografierea exhaustiva a celor 13 sisteme guvernamentale țintă + 5 servicii e-Guv (MPass, MSign, MNotify, MLog, MConnect) + UNFPA. Pentru fiecare integrare: scope tehnic, capabilități MConnect, fluxuri de date, acorduri bilaterale necesare (CNAJGS, ME, UNFPA).
- DPIA — Data Protection Impact Assessment: Evaluare obligatorie GDPR pentru sistemul ce procesează date sensibile (categorii speciale art. 9 GDPR) — victime, agresori, minori. Consultare CNPDCP daca necesar.
- Crearea și prioritizarea backlog-ului: Vom colabora cu ANPCV pentru a crea lista inițială de cerințe (product backlog), care va fi apoi administrata și prioritizata de către dumneavoastra pe parcursul proiectului.
- Analiză riscurilor — actualizare matrice riscuri pe baza informațiilor primite în timpul atelierelor de analiză.

Livrabilele la finalul acestei etape vor fi:

- Raportul de inițiere: Document detaliat care descrie metodologia proiectului, cronologia și planul de implicare a părților interesate. Identificarea părților interesate primare și secundare, evaluarea riscurilor.
- Raportul de evaluare a nevoilor: Constatari și recomandari bazate pe consultarile cu părțile interesate și analiză lacunelor. Documentarea provocarilor, prioritatilor și nevoilor tehnice pentru sistem.
- Specificație funcțională detaliată și Matrice de trasabilitate Concept HG 530/2025 — Cerința — Use-case.
- Raportul TCO (Total Cost of Ownership) pentru minimum 3 ani — DISTINCT de ofertă financiară (per clarificarea 1).
- DPIA preliminara conform GDPR.

2.3 Etapă de proiectare (durata: 3 luni)

În această etapă, transformam înțelegerea funcțională obtinuta în Etapă I într-o arhitectură tehnică detaliată, ready for development. Activitățile includ:

- Arhitectură sistemului: finalizarea modelului de microservicii Viodata (vezi secțiunea 3.2), comunicarea inter-servicii, design data model, strategia de scalare în MCloud.
- Modelul informațional: definirea celor 11 obiecte informaționale principale (Caz violență, Victimă, Agresor, Incident, Evaluare risc, Plan intervenție, Referire, Serviciu furnizat, Raport, Document, Utilizator) cu identificatori unici și schema relationala.
- Fluxurile operaționale: BPMN diagrame pentru toate procesele cheie (înregistrare caz, evaluare risc, planificare intervenție, referire, urmarire, închidere caz).
- Design UI/UX: Wireframes, prototipuri interactive, design system aliniat la Modelul Unitar de Design (MUD); testare utilizabilitate cu 5-7 utilizatori finali; conformitate WCAG 2.1 AA.
- Specificații de interoperabilitate: Documente tehnice pentru fiecare integrare (specificații API, formate JSON/XML, scenarii de schimb date, gestionare erori).

Livrabile la finalul Etapei II:

- Document de proiectare a sistemului — documentație cuprinzatoare arhitectură, fluxuri lucru, structuri de date, măsuri de securitate, UI/UX pentru fiecare modul, diagrame fluxuri date.
- Modele de date și diagrame ER complete.
- Specificații de interoperabilitate cu cele 13 sisteme guvernamentale + 5 servicii e-Guv.
- Prototipuri UI/UX validate cu utilizatori-pilot.

2.4 Etapă de dezvoltare incrementală (durata: 9 luni)

Aceasta este etapă centrala a proiectului, în care sistemul informațional va fi construit. Vom utiliza o abordare bazată pe metodologia Agile/SCRUM, care ne permite să livram valoare rapid și să ne adaptam eficient la feedback-ul primit. Implementarea va urma un model de dezvoltare incrementală, prin etape scurte și repetabile (sprinturi).

Procesul de lucru:

- Structură în sprinturi: Perioadă de 9 luni va fi impartita în 18 sprinturi, fiecare cu o durata de două săptămâni. La începutul fiecarei etape, se vor selecta elementele din backlog ce urmează a fi dezvoltate.
- Dezvoltare și testare continuă: Pe parcursul fiecărui sprint, echipa noastră va proiecta, dezvolta și integra funcționalitățile planificate. Totodată, vom realiza teste unitare și teste de integrare pentru a asigură calitatea și stabilitatea codului. Coverage țintă: >= 80% line coverage.
- Livrarea unui increment funcțional: La încheierea fiecărui ciclu (sprint), vom preda un pachet complet de funcționalități, care va fi integral operațional, documentat corespunzător și cu cod clar. Acesta va fi prezentat echipei ANPCV în cadrul unei ședințe de Sprint Review pentru a colecta feedback și a valida progresul.

Focusul dezvoltarii pe sprinturi (rezumat):

Sprint-uri	Module dezvoltate

Sprint 1-2	Modul UserHub (gestionare utilizatori, MPass, RBAC, 5 roluri); modul DataHub (nomenclatoare)
Sprint 3-4	Modul CaseHub — înregistrare cazuri, ciclu de viață, evaluare risc, plan intervenție
Sprint 5-6	Modul SubjectHub — victime, agresori, integrare ASP/MConnect (preluare date IDNP)
Sprint 7-8	Modul ReferralHub — referiri către servicii (medicale, juridice, sociale, adapost)
Sprint 9-10	Modul ProtectionHub — ordine restricție urgența, ordonante protecție judecatoresti
Sprint 11-12	Modul Notification (integrare MNotify); modul Audit (integrare MLog)
Sprint 13-14	Modul ObjectStorage (MinIO pentru documente); integrare MSign pentru semnare
Sprint 15-16	Modul MConnect — integrări cu IGP, Procuratura, instanțe PIGD, eSocial, SIA AMP
Sprint 17-18	Modul Reporting (Metabase) — Set indicatori naționali; tablouri de bord; finalizari

Livrabilele la finalul acestei etape:

- Sistem funcțional SI RS Viodata — toate cele 9 contururi funcționale operaționale, în MCloud, cu integrări e-Guv și MConnect.
- Codul sursa necompilat — acces continuu prin Azure DevOps, predare integrală la finalul proiectului.
- Documentație tehnică actualizata — arhitectură, API specs (OpenAPI 3.0), runbooks operaționale.
- Raport de integrare a sistemului — documentare integrări, diagrame componente/API, metode (REST/SOAP/SFTP), rezultate testare.

2.5 Etapă de testare și pilotare (durata: 3 luni)

Scopul acestei etape este de a valida în mod exhaustiv sistemul dezvoltat, pentru a garanta că acesta corespunde integral cerințelor funcționale, de performanță și de securitate înainte de lansarea în producție. Aceasta este o fază critica de asigurare a calității, realizată în strânsă colaborare cu echipă ANPCV și cu utilizatorii pilot din toate sectoarele relevante.

Activitățile principale ale acestei etape includ:

- Testare internă finală: Înainte de predarea pentru acceptanță, echipa noastră va executa un ciclu complet de teste de integrare, performanță și securitate în medii controlate. Acestea vor asigură că sistemul este stabil și funcționează conform specificațiilor. Instrumente: xUnit, Playwright, k6, OWASP ZAP.
- Testarea de acceptanță (UAT): Sistemul va fi livrat către ANPCV pentru a derula teste funcționale și de acceptare. Această testare se va realiza cu date reale (anonimizate) și scenarii operaționale complete pentru a simula utilizarea reala a platformei.

- Pilotarea sistemului: Vom implementa sistemul pentru un grup limitat de utilizatori desemnati de ANPCV: 1-2 ATAS/STAS pilot, 1-2 inspectorate de poliție, 1 spital pilot, 1 oficiu CNAJGS. Această fază de pilotare are că scop validarea finală a funcționalităților în mediul de lucru real și optimizarea performantelor pe baza feedback-ului direct de la utilizatori.
- Pen-test extern în fază pilot: Audit de securitate cu firma specializată (subcontractant). Verificare OWASP Top 10 + ASVS Level 2.
- Remedierea defectelor: Orice neconformitate sau defect identificat pe parcursul testarii de acceptanță sau a pilotarii va fi analizat și remediat de către echipa noastră fără costuri suplimentare.

Livrabile:

- Raport de pilotare / Raport de testare a sistemului — evaluare detaliată fază pilot: utilizabilitate, interoperabilitate, securitate, integrare e-Guv, raportare, feedback utilizatori finali.
- Sistemul validat — versiune stabila, pregătită pentru implementare în producție.
- Raport pen-test cu vulnerabilitati identificate și remedieri.

2.6 Etapă de lansare și recepție (durata: 3 luni)

Această etapă marcheaza tranziția de la mediul de testare la cel de producție și are ca obiectiv principal asigurarea unei adoptari facile și corecte a noului sistem de către toți utilizatorii la nivel național.

Activitățile principale:

- Implementarea în producție: Vom realiza instalarea versiunii finale și validate a sistemului SI RS Viodata pe infrastructură de producție MCloud. Acest proces va include configurarile finale și verificarile de stabilitate și performanță. Certificatele TLS/SSL vor fi furnizate de STISC (per clarif. 16).
- Monitorizare post-lansare: După lansare, echipa noastră tehnică va monitoriza activ sistemul (Prometheus + Grafana + ELK) pentru a asigură funcționarea stabila a acestuia în condiții de utilizare reala și pentru a interveni prompt în cazul oricarei probleme.
- Transferul de cunoștințe și instruirea utilizatorilor: Vom organiza sesiunile de formare, adaptate specific fiecărui rol, conform cerințelor caietului de sarcini:
- Administratori (16 ore): Instruire tehnică aprofundata — configurarea sistemului, managementul utilizatorilor, procedurile de backup și mentenanță de baza, gestionare incidente, monitoring.
- Utilizatori (24 ore): Instruire funcțională completa — fluxuri de lucru zilnice, înregistrare cazuri, evaluare risc, planificare intervenție, referiri, generare rapoarte. Sesiuni dedicate pe sector (poliție, sănătate, asistență sociala, juridic).
- Train-the-trainer: Formare a 5-7 trainers ANPCV pentru continuarea instruirii post-contract.

- Predarea documentației finale: Vom livra toate materialele de suport, inclusiv manualele de utilizare RO/RU/EN, ghiduri pas cu pas, video tutorial, scenarii practice, knowledge base online, quick reference cards.

Livrabile:

- Sistem funcțional în mediul de producție, accesibil tuturor utilizatorilor autorizati la nivel național.
- Raport de instruire a utilizatorilor — sesiuni efectuate, evaluări, materiale predate.
- Raport de lansare a sistemului — implementare națională, suport integrare.
- Materiale de instruire complete — manuale, video, scenarii, knowledge base.
- Transferul complet al codului sursa către ANPCV cu drepturi nelimitate de utilizare.

2.7 Etapă de garanție și suport (durata: 12 luni)

Această etapă finală asigură tranziția lina către operarea autonoma a sistemului de către ANPCV și garantează stabilitatea și performanță soluției pe termen lung. Perioadă de garanție va începe imediat după semnarea Procesului-verbal de recepție finală (per clarif. 19).

Activitățile principale:

- Suport tehnic și mentenanță: Vom oferi suport tehnic și mentenanță corectiva și adaptiva pentru o perioadă de 12 luni. Acest serviciu va include soluționarea oricaror incidente tehnice, precum și implementarea actualizarilor de securitate și a îmbunătățirilor necesare ale sistemului. Volumul de mentenanță este de aproximativ 15% din efortul total de dezvoltare (per clarif. 18).
- Categorii de mentenanță adaptiva (per clarif. 18):
- Actualizari API ale serviciilor guvernamentale (MPass, MSign, MNotify, MLog, MConnect)
- Schimbări în infrastructură MCloud
- Patch-uri de securitate pentru tehnologii open-source (.NET, PostgreSQL, Docker, Kubernetes)
- Ajustari legislative minore — formate raportare, nomenclatoare, fără modificare arhitectură
- Respectarea acordului privind nivelul de servicii (SLA): Vom asigură intervenția prompta pentru orice problema aparuta, respectand cu strictete timpii de răspuns și de rezolvare definiti în caietul de sarcini, în funcție de severitatea incidentului (Critic, Mare, Mediu, Mic).
- Monitorizare continuă: Vom continuă să monitorizăm performanță și stabilitatea sistemului în producție pentru a identifică și a adresa proactiv orice potentiala problema.
- Consolidarea transferului de cunoștințe: Pe parcursul acestei perioade, vom oferi asistență echipei tehnice a ANPCV pentru a asigură un transfer complet de cunoștințe și pentru a consolida abilitatile de administrare a noii platforme.

Livrabile la finalul acestei etape:

- Plan de mentenanță: Strategie detaliată pentru întreținerea continuă, actualizari, îmbunătățiri, protocoale răspuns incidente.
- Cod sursa final, în repository ANPCV, drepturi de proprietate exclusive ANPCV.
- Raport care documenteaza vulnerabilitatile descoperite urmare a testelor de penetrare, metodele de atac utilizate și recomandarile pentru îmbunătățirea securității.
- Rapoarte periodice de suport — incidente, timpi de răspuns, soluții implementate.
- Versiuni actualizate ale sistemului — toate patch-urile și îmbunătățirile.

2.8 Graficul de implementare

Activitate	Durata	Start estimat	Sfârșit estimat
Etapă I — Inițiere și analiză detaliată	2 luni	01.05.2026	30.06.2026
Ședința kick-off și alinierea echipelor	1 săptămână	01.05.2026	08.05.2026
Ateliere analiză procese (ANPCV + părți interesate)	3 săptămâni	11.05.2026	29.05.2026
DPIA și analiză interoperabilitate	2 săptămâni	01.06.2026	12.06.2026
Definire arhitectură + product backlog inițial	2 săptămâni	15.06.2026	30.06.2026
Etapă II — Proiectare	3 luni	01.07.2026	30.09.2026
Arhitectură detaliată + model informațional	1 lună	01.07.2026	31.07.2026
Design UI/UX + prototipuri (MUD-aligned)	1 lună	03.08.2026	31.08.2026
Specificații interoperabilitate complete	1 lună	01.09.2026	30.09.2026
Etapă III — Dezvoltare incrementală (18 sprinturi)	9 luni	01.10.2026	30.06.2027
Sprint 1-6 (Core: UserHub, CaseHub, SubjectHub, DataHub)	3 luni	01.10.2026	31.12.2026
Sprint 7-12 (Funcțional: ReferralHub, ProtectionHub, Notif, Audit)	3 luni	04.01.2027	31.03.2027
Sprint 13-18 (Integrări: MConnect, ObjectStorage, Reporting, finalizari)	3 luni	01.04.2027	30.06.2027
Etapă IV — Testare și pilotare	3 luni	01.07.2027	30.09.2027
Testare internă finală (integrare,	3 săptămâni	01.07.2027	23.07.2027

performanță, securitate)			
Pen-test extern	2 săptămâni	26.07.2027	06.08.2027
Pilotare cu utilizatori reali (5-7 instituții)	5 săptămâni	09.08.2027	10.09.2027
Remediere neconformitati	3 săptămâni	13.09.2027	30.09.2027
Etapă V — Lansare și recepție	3 luni	01.10.2027	30.12.2027
Implementare producție + monitorizare inițială	1 lună	01.10.2027	31.10.2027
Instruire administratori (16h) + utilizatori (24h)	1 lună	03.11.2027	30.11.2027
Recepție finală + transfer cunoștințe	1 lună	01.12.2027	30.12.2027
Total dezvoltare și livrare	20 luni	01.05.2026	30.12.2027
Etapă VI — Garanție și suport (12 luni post-recepție)	12 luni	02.01.2028	31.12.2028

(Datele exacte vor fi confirmate la semnarea contractului. Termenul final 25.12.2028 (Luni — zi de Crăciun, nelucrătoare conform Codului muncii art. 111). Livrarea finală a Etapei VI este planificată pentru 22.12.2028 (Vineri) — ultima zi lucrătoare anterioară termenului — pentru a respecta termenul cu marjă).

Capitolul 3: Abordarea tehnică

Abordarea noastră tehnică este centrata pe construirea unui sistem informațional modern, robust și scalabil, capabil să raspunda nu doar cerințelor actuale ale ANPCV, ci și să ofere flexibilitate pentru dezvoltari viitoare. Am proiectat o arhitectură care prioritizeaza securitatea, performanță și mentenabilitatea pe termen lung, în conformitate cu Modelul Unitar de Design (MUD) și cu prevederile platformei eGov4Dev.

3.1 Descrierea arhitecturii la nivel inalt

Soluția propusa se va baza pe o arhitectură moderna de microservicii, containerizata și orchestrata, proiectata pentru scalabilitate, reziliență și o mentenanță simplificata. Această abordare modulară permite dezvoltarea și actualizarea independentă a componentelor sistemului. Arhitectură va include următoarele straturi și componente esențiale:

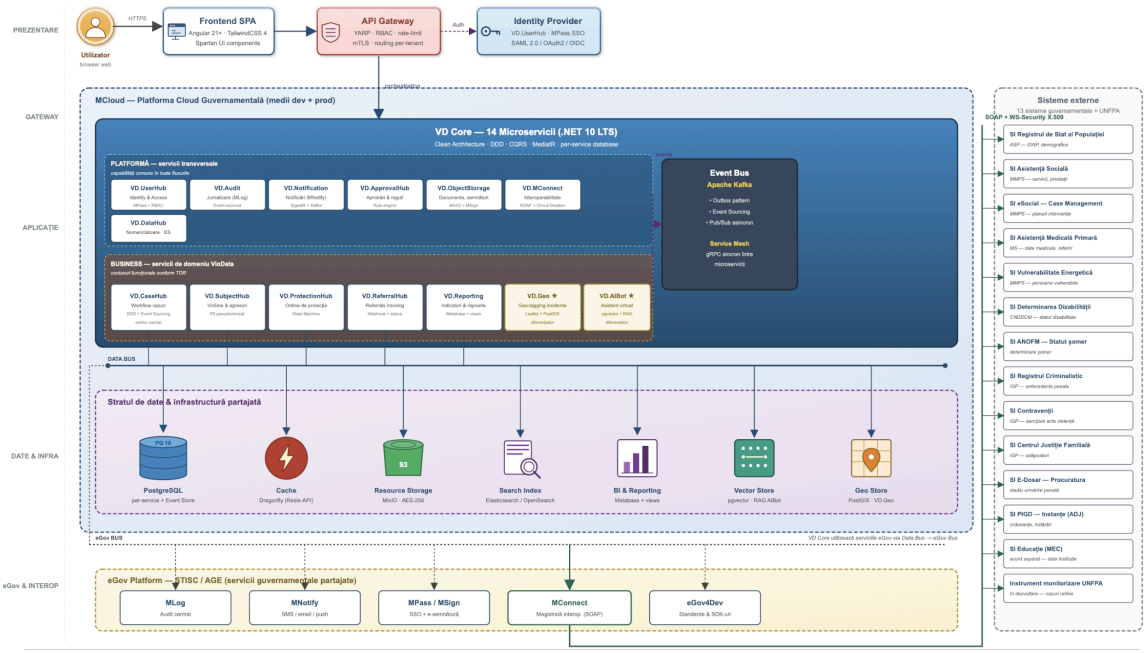

Figura 1 — Diagrama arhitectura SI RS VioData

Stratul de prezentare (interfața utilizator)

Vom dezvolta o interfața web moderna, de tip Single-Page Application (SPA), care va fi complet responsiva (320-1600px) și optimizată pentru eficiența operațională. Interfața va fi optimizată pentru fluxurile de lucru ale managerilor de caz, asistentilor sociali, ofiterilor de poliție, cadrelor medicale și juristilor, asigurand o experiență de utilizare intuitiva. Multilingva RO + RU (obligatoriu per clarif. 6) + EN. Conformitate WCAG 2.1 AA și Modelul Unitar de Design.

Stratul de aplicație (logica de business)
Acesta reprezintă nucleul sistemului și va cuprinde mai multe microservicii specializate, fiecare cu o responsabilitate clara — vezi secțiunea 3.2 pentru detalii.

Stratul de date
Vom adopta o abordare de persistenta poliglota, folosind cea mai potrivita tehnologie pentru fiecare nevoie:

- Stocare de obiecte (MinIO): Pentru managementul datelor nestructurate (documente atasate la cazuri, fisiere medicale, decizii instanțe).
- Motor de căutare (PostgreSQL Full-Text Search + Elasticsearch): Căutare avansata în toate datele stocate (cazuri, victime, agresori, documente).
- Baza de date relationala (PostgreSQL 18): Stocare principală pentru datele structurate despre cazuri, persoane, măsuri de protecție, referiri, planuri de intervenție.
- Stocare în memorie (DragonFly): Cache pentru datele accesate frecvent, sesiuni utilizator, rate limiting.
- Event streaming (Apache Kafka): Procesare evenimente MConnect, notificari interne asincrone, sincronizare între microservicii.

Stratul de integrare
Va facilita comunicarea cu sistemele externe prin API-uri standardizate. Implementarea va respectă principiile REST și va utiliza protocoale securizate. Integrare bidirectional cu:

- MConnect — pentru schimb de date cu cele 13 sisteme guvernamentale identificate
- MPass — autentificare și autorizare
- MSign — semnare electronică documente oficiale
- MLog — jurnalizare acțiuni utilizatori
- MNotify — notificari electronice utilizatori
- CNAJGS, UNFPA — prin acorduri bilaterale (integrări REST API directe)

Stratul de securitate
Va asigură protecția datelor și accesul controlat prin mecanisme de autentificare și autorizare robuste, criptarea datelor în tranzit (TLS 1.3) și în repaus (AES-256), și un audit complet al accesului. RBAC granular cu min. 5 roluri (SystemAdmin, Administrator, Manager de caz, Operator raportor, Consumator/Beneficiar).

Stratul de implementare (deployment)
Va gestiona implementarea și orchestrarea componentelor sistemului în MCloud, incluzand containerizarea aplicațiilor (Docker), orchestrarea (Kubernetes), managementul configuratiilor (Helm) și automatizarea proceselor de deployment (Azure DevOps Pipelines).

3.2 Microservicii Viodata (VD Core)
Sistemul VD Core este construit pe o arhitectură moderna bazată pe microservicii, care utilizează tehnologii open-source. Sistemul consta din 14 microservicii Viodata (.NET 10

(LTS)+) și un frontend Angular 21+, cu suport pentru caching și event streaming. Dintre acestea, 12 microservicii acoperă integral cele 9 contururi funcționale TOR + serviciile transversale obligatorii (Notification, Audit, MConnect, ObjectStorage), iar 2 microservicii sunt valoare adăugată INCLUSĂ fără costuri suplimentare: VD.Geo (geo-tagging conform clarificarea 16) și VD.AIBot (asistent virtual pentru utilizatori — diferențiator).

Componente principale:

Microserviciu Viodata	Responsabilitate	Tehnologie & pattern arhitectural
VD.UserHub	Identity & Access — autentificare MPass (SAML 2.0 + OAuth 2.0/OIDC), JWT tokens, ABAC/RBAC permisiuni cu attribute custom	.NET 10 (LTS), ASP.NET Core, Clean Architecture, MediatR; certificare X.509 pentru integrările guvernamentale
VD.CaseHub	Gestionare cazuri violență — workflow mulți-fază (deschidere → evaluare risc → plan intervenție → monitorizare → închidere); validare cu FluentValidation	DDD + CQRS + MediatR; PostgreSQL 18 cu Event Sourcing pentru tranziții stări; permission-based access via [VioAuthorize] attribute
VD.SubjectHub	Gestionare entitati victimă/agresor — date personale criptate, IDNP, audit complet trasabilitate	.NET 10 (LTS); PostgreSQL 18 cu TDE (Transparent Data Encryption); pseudonimizare în queries de raportare
VD.ReferralHub	Coordonare referiri inter-instituționale — adaposturi, asistență sociala, juridică, medicala (toate via MConnect)	.NET 10 (LTS); integrare MConnect adapter; webhook subscriptions pentru status referire
VD.ProtectionHub	Profil criza & evaluare risc/vulnerabilitate — severitate 1-5; planuri intervenție; status workflow Active → Assessment → Response → Resolved	DDD; State Machine pattern pentru tranziții status; integrare cu CaseHub via Kafka events
VD.ApprovalHub	Workflow aprobare planuri intervenție — aprobare în cascada mulți-nivel; notificare automata către stakeholderi	.NET 10 (LTS); rule engine cu reguli configurabile; Kafka publisher către Notification
VD.Notification	Comunicare mulți-canal — SMS, email, push notification, MNotify integration; WebSockets pentru notificari real-time	.NET 10 (LTS) + SignalR (WebSocket); Kafka consumer pentru evenimente; templates configurabile

VD.Audit	Trasabilitate completa — Event Sourcing; Kafka consumer pentru ingerare audit; transmitere log-uri centralizate via MLog	Kafka producer/consumer; Event Sourcing pattern; offset-based pagination pentru dataset-uri mari
VD.ObjectStorage	Document Management System — fisiere și imagini în MinIO; criptare la rest; versioning; access control rolual; semnătură electronică MSign	MinIO (S3-compatible); criptare AES-256; integrare MSign SDK pentru semnătură documente oficiale
VD.Reporting	Generare rapoarte standard și personalizate — dashboard interactiv; export PDF/CSV/Excel; integrare Metabase pentru BI avansat	.NET 10 (LTS); Metabase pentru analitice; PostgreSQL views materializate pentru rapoarte agregate
VD.MConnect	Adapter integrări guvernamentale — SOAP/WSDL; mutual TLS; certificate X.509; WS-Security. Toate integrările externe trec prin acest hub (NU point-to-point)	.NET 10 (LTS); SoapCore client; certificate management; circuit breaker pattern pentru reziliență
VD.DataHub	Platform Data Hub — date partajate inter-microservicii; ETL pentru raportare; agregari cross-domain	Kafka pentru evenimente; PostgreSQL că cache de read-models; Elasticsearch pentru căutare full-text
VD.Geo	Geo-etichetare GPS pentru incidente — vizualizare hartă; căutare proximitate adapostururi; geo-fence ordine de protecție	Frontend Leaflet 1.9+ (open-source); Backend PostGIS; OpenStreetMap tiles (open-source)
VD.AIBot	Asistent virtual conversational pentru cetățeni și lucratori sociali — multilingv RO/RU/EN (opțional)	Azure OpenAI cu pgvector pentru semantic search; streaming chat completions cu IAsyncEnumerable; Conversational history

Pe langa aceste microservicii backend, sistemul include:

- Frontend Angular 21+ cu TailwindCSS și componente Spartan UI — aplicații separate pentru back-office (utilizatori autorizati) și portal public (acces beneficiari)
- Common (NuGet packages): librarii cu entitati și utilitate comune între microservicii
- Reporting (Metabase): generare centralizata de rapoarte, tablouri de bord interactive, exporturi PDF/CSV/Excel

Data Storage:

- Object Storage — MinIO (date nestructurate)
- PostgreSQL 18 (baza de date relationala pentru date structurate)
- DragonFly (în-memory store pentru cache)
- Elasticsearch (căutare full-text și analiză logs)

Arhitectură de retea:

- Acces public — resurse accesibile din internet (HTTPS), portal beneficiari
- Acces pentru suport și mentenanță — resurse publice cu acces limitat
- Acces privat — retea internă pentru comunicarea între microservicii, baze date și componente terte

Monitorizare: Sistemul include monitorizarea resurselor (CPU, RAM, DISK) și a starii componentelor — Prometheus + Grafana + ELK Stack + Icinga2 + Node-exporter + Cadvisor.

CI/CD: Procesul de integrare continuă și livrare continuă utilizează Azure DevOps Pipelines + Harbor (registru Docker images), ambele integrate cu MCloud STISC.

3.3 Stiva tehnologică

Pentru a implementa arhitectură descrisa, propunem utilizarea unei stive tehnologice moderne, fiabile și cu un suport puternic din partea comunitatii. Selecția tehnologiilor a fost facuta pentru a garanta performanță, securitate și o mentenanță eficiența pe termen lung, fiind aliniata cu cerințele și recomandarile din Caietul de sarcini, cu clarificarile primite (stack flexibil — clarif. 5, 12, 13) și cu prevederile platformei eGov4Dev.

Categorie	Tehnologie	Descriere
Dezvoltare backend	.NET 10 (LTS)	Vom utiliza un ecosistem matur și robust pentru construirea de microservicii performanțe și securizate. Această alegere ofera un ciclu de dezvoltare rapid și o integrare excelenta cu restul tehnologiilor propuse. C# că limbaj principal.
Dezvoltare frontend	Angular 21+ (TypeScript)	Vom dezvolta o interfața de tip Single-Page Application utilizand un framework modern, care asigură o experiență de utilizare rapida, responsiva și intuitiva. TailwindCSS pentru styling, NgRx Signals pentru state management, Spartan UI pentru componente.
Baza de date	PostgreSQL 18	Sistem de gestiune a bazelor de date relationale open-source, renumit pentru fiabilitate, robustete și performanță, utilizat pentru stocarea datelor structurate. Extensia PostGIS pentru geo-etichetare (per clarif. 15).
Motor de căutare	PostgreSQL Full Text Search + Elasticsearch	Soluție pentru implementarea capabilitatilor de căutare

		avansata în timp real pentru cazuri, persoane și documente. Elasticsearch pentru centralizarea jurnalelor de sistem.
Stocare în memorie (cache)	DragonFly	Sistem de stocare în memorie utilizat pentru a accelera timpul de răspuns al aplicației prin caching-ul datelor frecvent accesate, imbunatatind performantele generale.
Stocare obiecte	MinIO	Server S3-compatibil pentru stocarea documentelor (decizii instanțe, fise medicale, dovezi) — open-source, scalabil, cu replicare nativa.
Containerizare	Docker	Standardul de facto pentru impachetarea aplicațiilor și a dependentelor lor în containere portabile și izolate, asigurand consistența între mediile de dezvoltare și producție.
Orchestrare	Kubernetes (k8s) + Helm	Platforma pentru automatizarea implementării, scalarii și gestionarii aplicațiilor containerizate la scara larga, fiind o cerința de arhitectură. Helm pentru deployment-uri reproducibile.
Broker de mesaje	Apache Kafka	Componentă ce faciliteaza comunicarea asincrona și decuplata între microservicii, esențială pentru procesarea evenimentelor în timp real (MConnect Events) și sincronizarea datelor.
Integrare continuă (CI/CD)	Azure DevOps Pipelines	Instrumente pentru crearea de fluxuri automate de integrare și livrare continuă, esențiale într-o metodologie de dezvoltare agile și pentru a asigură calitatea livrarilor.
BI / Raportare	Metabase	Platforma open-source pentru vizualizarea datelor și crearea de tablouri de bord (dashboards) interactive. Permite ANPCV să configureze rapoarte fără cunoștințe SQL.
Monitorizare	Prometheus + Grafana + ELK Stack	Colectare și vizualizare metrici. ELK (Elasticsearch +

		Logstash + Kibana) pentru agregare și analiză logs.
Reverse Proxy	Nginx	Server web și proxy invers pentru routing, terminare SSL, load balancing între instanțele microserviciilor.
Validare	FluentValidation	Validari declarative pentru cerințe business — utilizat pentru validarea formularelor de raportare cazuri și tranziții state machine (per clarif. 7).
Documentație API	Swashbuckle.AspNetCore (OpenAPI 3.0)	Generare automata documentație API interactiva (Swagger UI) pentru fiecare microserviciu.

Pe langa aceste componente, SI RS Viodata utilizează și o serie de servicii guvernamentale comune, oferite prin platforma AGE (Agenția de Guvernare Electronică) — vezi secțiunea 3.4.

3.4 Integrarea cu serviciile guvernamentale

Portalul VD Core, implementat pe baza REST API, ofera metode pentru integrarea serviciilor externe. Apelarea acestor metode se realizează de pe adrese autorizate, utilizand mecanisme de autentificare și autorizare. Unicitatea cererilor este asigurată prin token-uri de securitate asociate sesiunilor de lucru.

Integrarea cu serviciile externe guvernamentale oferite prin platforma AGE se bazează pe tehnologiile SOAP și REST API. Sistemul utilizează:

Serviciu eGov	Scop	Tehnologie integrare
MPass	Autentificarea și autorizarea utilizatorilor	OAuth 2.0/OIDC + SAML
MSign	Semnarea electronică a documentelor (decizii, ordonante, rapoarte oficiale)	REST API
MNotify	Notificarea electronică a utilizatorilor (email, SMS)	REST API
MLog	Înregistrarea acțiunilor și evenimentelor pentru audit	REST API
MConnect	Schimb de date cu sistemele externe (13 sisteme guvernamentale)	SOAP cu WS-Security + Kafka events
MCloud	Hosting infrastructură producție + dev (per clarif. 14)	Kubernetes containers

Lista completa a integrărilor (per clarificarea 4)

Domeniu	Sistem și Deținător	Tehnologie integrare	Flux date
Identitate persoană	Registrul de Stat al Populatiei (RSP) — ASP	MConnect (SOAP/WSDL + WS-Security X.509)	Validare IDNP, date demografice victimă/agresor
Documente identitate	Registrul de Stat al Actelor de Identitate — ASP	MConnect (SOAP)	Validare CI/pașaport

Stare civila	Registrul Stare Civila — ASP	MConnect (SOAP)	Statut familial, copii minori în familie
Adresa	Registrul Adreselor — ASP	MConnect (SOAP)	Verificare adresa victimei/agresorului
Servicii sociale	eSocial (ATAS/STAS) — MMPS	MConnect (SOAP — anexa tehnică MConnect Events)	Plan intervenție social, beneficii sociale
Servicii medicale primare	ȘI Asistență Medicala Primara (SIA AMP) — Compania Asigurari Medicale	MConnect (SOAP)	Confirmare istoric medical relevant, leziuni raportate
Asistență juridică garantată	ȘI CNAJGS (Asistență Juridică Garantată de Stat) — CNAJGS	MConnect (SOAP) — extindere prin MConnect după acord schimb date (clarificare 4)	Caz juridic, avocat desemnat — flux activat după integrarea CNAJGS în MConnect
Centre de criza și adaposturi	Registru Centre Justiție Familiala — IGP/MAI	MConnect (SOAP) — extindere prin MConnect după acord schimb date (clarificare 4)	Disponibilitate adapost, plasament victimă
Cadastru proprietati	Registru Bunuri Imobile — ASP	MConnect (SOAP)	Verificare proprietati comune (cazuri partaj)
Vehicule	Registru Vehicule — ASP	MConnect (SOAP)	Identificare auto în incidente domestice
Situație penală	Cazier Judiciar — Ministerul Justiției	MConnect (SOAP)	Antecedente agresor (ordin de protecție anterior)
Educatie	Sistem Informațional Educational — Ministerul Educatiei	MConnect (SOAP)	Statut copii în scoala (cazuri cu minori)
Notificare cetățeni	MNotify (SMS/email centralizat) — AGE	REST API (token JWT, mTLS)	Notificari victimă/agresor pentru ordine de protecție, audieri, programari
Autentificare	MPass (SSO guvernamental) — AGE	SAML 2.0 (primary) + OAuth 2.0/OIDC (secondary)	Autentificare profesioniști, lucratori sociali, victimă opt-în
Semnătură electronică	MSign (semnătură electronică autorizată) — AGE	REST API + integrare browser SDK	Semnare ordine, declarații, planuri intervenție
Logare centralizata	MLog — AGE	Kafka producer + REST API	Trasabilitate completa acțiuni utilizatori și evenimente sistem

Autentificare și autorizare

Portalul VD Core utilizează OAuth 2.0/OIDC că mecanism principal de autentificare și autorizare. Acest protocol permite utilizatorilor să isi acceseze datele din portal prin intermediul unor aplicații terte autorizate, fără a fi nevoie să isi imparta acreditatile de

autentificare cu aceste aplicații. Token-urile de acces și de reimprospatare sunt stocate în mod securizat, utilizand tehnici de criptare și de gestionare a cheilor. Durata de valabilitate a token-urilor este limitata, iar acestea pot fi revocate în orice moment.

Integrare SOAP (MConnect)

MConnect utilizează tehnologia SOAP cu WS-Security. Mecanismul de integrare:

7. Sistemul utilizează fisiere WSDL (Web Services Description Language) pentru a descrie interfața serviciilor SOAP cu care se integreaza. Aceste fisiere conțin informații despre metodele disponibile, tipurile de date utilizate și locatia endpoint-urilor.
8. Pe baza fisierelor WSDL, sistemul generează clienti SOAP care sunt utilizati pentru a apela metodele serviciilor terte.
9. Sistemul construieste mesaje SOAP conform specificațiilor definite în fisierele WSDL și le trimite către endpoint-urile serviciilor terte.
10. Sistemul primeste răspunsuri SOAP de la serviciile terte și le procesează conform specificațiilor.

Securitatea integrării SOAP:

- Autentificare: WS-Security cu certificate X.509 pentru mutual TLS
- Autorizare: politici de autorizare pentru a restrictiona accesul la metode
- Criptare: SSL/TLS pentru protejarea datelor în tranzit (certificate STISC per clarif. 16)

Capitolul 4: Conformitatea cu cerințele

4.1 Tabelul de conformitate cu cerințele funcționale

Tabelul de mai jos ofera o analiză detaliată a fiecarei cerințe funcționale din Caietul de sarcini (secțiunile 5.1 - 5.13). Pentru fiecare punct, nu doar confirmam conformitatea, ci și prezentam viziunea noastră tehnică privind modul de implementare.

Cod	Cerința funcțională	Viziune privind modul de implementare	Conform
F-01	5.1.1 Interfața utilizator multilingva — RO/RU/EN, RU obligatoriu (clarif. 6)	Vom implementa i18n cu resurse JSON. Limba implicita RO. Switch în UI pentru RU/EN. Toate textele, mesajele, formularele și rapoartele localizate.	DA
F-02	5.1.2 Accesibilitate WCAG (min nivel A)	Țintă noastră: WCAG 2.1 nivel AA (depășește cerința minimă). Audituri cu axe-core, lighthouse. Tastatura-friendly, screen reader compatible.	DA
F-03	5.1.3 Suport pentru dispozitive multiple (320-1600px)	Design adaptiv mobile-first. Testare în 7 viewport-uri. PWA capabilities pentru utilizare offline limitata.	DA
F-04	5.2.1 Administrare utilizatori și roluri	VD.UserHub cu CRUD utilizatori prin UI. Min 5 roluri (SystemAdmin, Administrator, Manager de caz, Operator raportor, Consumator). Integrare MPass. Drepturi acces granulare.	DA
F-05	5.2.2 Securitate, jurnalizare și audit	VD.Audit jurnalizeaza automat toate acțiunile (autentificari, accesari, modificări, schimbări stări, operatiuni admin). Integrare MLog. Audit logs filtrabile, exportabile.	DA
F-06	5.3.1 Înregistrare cazuri	VD.CaseHub generează ID unic UUID. Formular standardizat cu toate campurile din Concept HG 530/2025. Validare campuri obligatorii cu FluentValidation. Pentru cazuri online — link postare.	DA
F-07	5.3.2 Consimtamant și confidențialitate	Modul dedicat consimtamant cu înregistrare timestamp și IP. RBAC pe date sensibile (categorii speciale GDPR art. 9). Jurnalizare automata accesari date personale (GDPR art. 30).	DA

F-08	5.4.1 Ciclu de viață caz cu reguli configurabile (clarif. 7 — fără BRE)	State machine în cod cu reguli configurabile (workflow + roluri + date obligatorii + restricții active). Stare configurabila prin parametri/nomenclatoare/JSON config — FĂRĂ Business Rules Engine dedicat.	DA
F-09	5.4.2 Evaluare risc + plan intervenție	Modul evaluare risc cu criterii definite (letalitate, profil risc). Plan intervenție cu acțiuni, termene, responsabili. Import structuri date din eSocial — minim 5 câmpuri obligatorii conform clarificării 2: (1) ID plan / ID caz; (2) Statut caz; (3) Lista acțiuni; (4) Responsabil; (5) Termen de implementare.	DA
F-10	5.5.1 Gestionare referiri	VD.ReferralHub cu înregistrare referiri pentru servicii medicale, juridice, sociale, adapost. Tip serviciu selectabil din nomenclator. Statut actualizabil. Istoric complet vizibil per caz.	DA
F-11	5.5.2 Interoperabilitate referiri	Schimb date prin MConnect (sincron + asincron prin MConnect Events / Kafka). Structură date documentata (OpenAPI). Gestionare erori cu jurnalizare. Once-only principle.	DA
F-12	5.6.1 Evidență ordine restricție + ordonante protecție	VD.ProtectionHub cu campuri: autoritate emitenta, număr/data, perioadă, tipuri restricții, statut. Corelare cu cazul și agresorul. Alerte expirare prin VD.Notification + MNotify.	DA
F-13	5.6.2 Corelare măsuri protecție cu fluxul cazului	Vizualizare centralizata în fisa cazului. Blocare închidere caz cu măsuri active (cu exceptii pe roluri). Foreign keys + business rules tehnice.	DA
F-14	5.7.1 Rapoarte standard și personalizate	Rapoarte standard: Setul de indicatori naționali HG (clarif. 8). Rapoarte personalizate cu filtre. Export PDF/CSV/Excel. VD.Reporting via Metabase. Recipient pentru rezultate UNFPA (clarif. 9).	DA
F-15	5.7.2 Tablouri de bord configurabile (clarif. 10)	Dashboard-uri Metabase interactive cu filtre (perioadă, regiune, tip violență). Configurare prin filtre/indicatori/vizualizari — FĂRĂ dezvoltare custom	DA

		dashboard. Accesibile conform rolului.	
F-16	5.8 Nomenclatoare interne	VD.DataHub cu CRUD prin UI. Pentru fiecare nomenclator: denumire, descriere, lista valori, statut, data intrare în vigoare. Validari care previn introducerea de valori libere.	DA
F-17	5.9.1 Acces autorizat exclusiv prin MPass	Integrare nativa MPass via SAML 2.0 (mod implicit, conform majoritate sisteme guvernamentale MD) + OAuth 2.0/OIDC (secondary). Detalii: certificate X.509, mutual TLS, schimb metadata SAML cu IdP MPass. Implementare standard pe baza .NET 10 (LTS) ASP.NET Core SAML2 library; testare în MD-IAM staging înainte de producție.	DA
F-18	5.9.2 Acces public separat de date confidențiale	Aplicație portal public separata de back-office. Date publice strict separate. FĂRĂ acces public la date personale.	DA
F-19	5.10 Documente de baza (intrare/ieșire/tehnologice)	Sistem complet de Document Management conform Sec. 5.10.1-5.10.6 din Caietul de sarcini: 5.10.1 Clasificare: documente de intrare (sesizari victimă, rapoarte poliție), ieșire (ordine protecție, planuri intervenție, rapoarte ANPCV), tehnologice (audit, log-uri integrări). Tag-uri configurabile per tip. 5.10.2 Validare: ABAC reguli per tip document; semnătură MSign obligatorie pentru documente oficiale (ordine, decizii); validare schema metadata. 5.10.3 Aprobare: workflow mulți-nivel configurabil per tip document (lucrator social → coordonator → manager); semnături electronice secvențiale; istoric aprobare	DA

		cu timestamp și IP. 5.10.4 Arhivare: politica retentie configurabila per tip (75 ani cazuri grave, 25 ani standard); arhivare automata către MinIO Glacier/Cold tier; export StandardArchive moldovenesc. 5.10.5 Trasabilitate și audit: fiecare operație pe document generează eveniment în VD.Audit (Kafka); transmitere MLog. Istoric complet — cine, când, ce a vazut/modificat. 5.10.6 Acces controlat la arhiva: rol-based + ABAC; logging acces arhiva separat; export pentru subiectul datelor (drepturile GDPR). Stocare: MinIO (S3-compatible, open-source) cu criptare AES-256 la rest; versioning automat; retention policies.	
F-20	5.11 Obiecte informaționale (11 tipuri)	14 obiecte informaționale conform Sec. 5.11.1 din Caietul de sarcini: Obiecte de business (10): 1. Caz · 2. Victimă · 3. Agresor · 4. Incident · 5. Evaluare risc · 6. Plan intervenție · 7. Referire · 8. Serviciu furnizat · 9. Raport/Indicator · 10. Document Obiecte de infrastructură (4): 11. Utilizator · 12. Rol și permisiune · 13. Nomenclator/Clasificator · 14. Înregistrare audit Toate cele 14 obiecte sunt persistate în PostgreSQL 18 cu auditare completa via VD.Audit. Versioning și historic per obiect (Event Sourcing pe entitatile critice — Caz, Plan intervenție,	DA

		Evaluare risc, Ordin de protecție).	
F-21	5.12-5.13 Interoperabilitate sistemica	VD.MConnect microserviciu dedicat. Mecanisme sincron + asincron. Detectare și gestionare erori. Documentare API completa.	DA
F-22	6.4 Geo-etichetare GPS (opțional, clarif. 15)	Geo-etichetare GPS conform Sec. 6.4 — implementare 100% OPEN-SOURCE: Frontend: Leaflet 1.9+ (open-source, BSD-2 license) + OpenStreetMap tiles (gratuit, ODbL license). Alternative: MapLibre GL JS (fork open-source al Mapbox GL JS, BSD-3 license) pentru rendering vectorial avansat — selectat în funcție de cerințele de performanță. Backend: PostGIS extension pentru PostgreSQL 18 — indexare geo-spatiala B-tree + GiST. Stocare coordonate: lat/long că PostGIS POINT, cu indexare geo-spatiala pentru cautari de proximitate (adapost cel mai apropiat, geofencing ordin de protecție). NU folosim Mapbox proprietary (incompatibil cu cerința open-source din Sec. 6.1). Tile server: opțiune self-hosted (TileServer GL/MBTiles) pentru hartile cu trafic ridicat sau date sensibile.	DA

4.2 Tabelul de conformitate cu cerințele non-funcționale

Cod	Cerința non-funcțională	Viziune privind modul de implementare	Conform
NF-01	6.1 Tehnologii open-source și arhitectură modulară	Stack-ul propus este integral open-source. Arhitectură modulară cu microservicii interschimbabile. Conformitate Modelul Unitar	DA

		de Design (MUD) și eGov4Dev.	
NF-02	Arhitectură pe microservicii	Întreaga propunere tehnică este fundamentata pe o arhitectură moderna de microservicii — 11 servicii independențe containerizate (vezi 3.2).	DA
NF-03	Tehnologii moderne	Stiva tehnologică: .NET 10 LTS pentru backend, Angular 21+ pentru frontend, PostgreSQL 18+ pentru date, Kubernetes și Docker pentru infrastructură. Toate cu suport activ și pe termen lung.	DA
NF-04	Containerizare și orchestrare	Toate microserviciile vor fi impachetate în containere Docker și orchestrate cu Kubernetes în MCloud. Helm Charts pentru deployment-uri reproducibile.	DA
NF-05	API-uri REST cu OpenAPI/Swagger	Comunicarea între frontend și microservicii prin API-uri RESTful. Documentație auto-generata cu Swashbuckle (OpenAPI 3.0).	DA
NF-06	6.2 Hosting în MCloud (dev + prod, clarif. 14)	Atât mediul de dezvoltare cat și producția în MCloud. STISC asigură mediul de virtualizare. Nginx că reverse proxy. Configuratie via Helm.	DA
NF-07	6.3 Integrare e-Guvernare (MPass, MSign, MLog, MNotify, MConnect)	Microserviciu dedicat VD.MConnect. Integrări REST și SOAP. Vezi secțiunea 3.4.	DA
NF-08	6.5 Securitatea sistemului — OWASP, ISO 27001, HG 201/2017	OWASP Top 10 (2021) + ASVS Level 2. ISO 27001 (certificat ofertant). Conformitate HG 201/2017. Pen-testing trimestrial.	DA
NF-09	Criptare TLS 1.3 + AES-256	Toată comunicatia HTTPS (TLS 1.3) — certificate STISC (clarif. 16). Date sensibile criptate AES-256-GCM în repaus.	DA
NF-10	Protecție atacuri OWASP Top 10	Validari la nivel API. Mecanisme protecție CSRF/XSS. SonarQube pentru analiză statica. Code review obligatoriu.	DA
NF-11	Audit complet	VD.Audit + MLog. Fiecare operațiune importanta	DA

		jurnalizata în jurnal securizat. Trasabilitate completa.	
NF-12	6.6 Protecția datelor — GDPR + HG 1123/2010	DPIA în Etapă I. Drepturi persoane vizate. Data minimization. Pseudonymization. Consultare DPO ANPCV.	DA
NF-13	6.7 Scalabilitate — 500 utilizatori normal, 1000 în varf	Arhitectură orchestrata cu Kubernetes — scalare orizontala automata. Load balancer Nginx. Replicare PostgreSQL.	DA
NF-14	Disponibilitate 99.9%	Disponibilitate ≥ 99.95% (4.38h downtime/an), aliniat consistent cu RTO ≤ 4h pentru incidente P1. Calculul: o singura intervenție majora pe an consuma ~91% din bugetul de uptime → matematica consistența. Implementare: HA cluster Kubernetes 3-nodes, replicare PostgreSQL streaming replication + failover automat (Patroni); backup la 6h cu RPO ≤ 4h.	DA
NF-15	6.8 Performanță — încărcare caz <=2s, rapoarte <=5s, etc.	Ținte stricte: încărcare caz <=1.5s P95; rapoarte <=4s P95; latenta API intra <=30ms P95; API extern <=150ms P95. Caching DragonFly + indexare PostgreSQL + Elasticsearch FTS.	DA
NF-16	Volume — 1 milion+ înregistrări	PostgreSQL 18 cu indexare optimizată + sharding dacă necesar. Va fi validat prin teste de stres la 5 milioane înregistrări înainte de recepția finală (Etapa IV — Testare).	DA
NF-17	Monitorizare 24/7	Prometheus + Grafana + ELK + Icinga2. Alertare automata pentru incidente critice via PagerDuty/MS Teams.	DA
NF-18	6.9 Garanție 12 luni de la recepție finală (clarif. 19)	Etapă VI — 12 luni post-recepție finală. SLA P1 1h/4h, P2 4h/24h, P3 24h/5zl, P4 1sapt/urm.actualizare.	DA
NF-19	Mentenanță corectiva și adaptiva	Cele 4 categorii: actualizari API e-Guv, schimbări	DA

	~15% efort dezv (clarif. 18)	MCloud, patch-uri securitate, ajustari legislative minore.	
NF-20	Conformitate eGov4Dev	Respectare integrală a prevederilor https://egov-moldova.github.io/egov4dev/. MUD, principii arhitecturale, mecanisme integrare, ghiduri securitate.	DA

Capitolul 5: Securitate, monitorizare și SLA

5.1 Securitate

Securitatea sistemului VD Core este o prioritate absoluta, asigurand protecția datelor sensibile și a funcționalității platformei. Asigurarea securității sistemului se bazează pe mai multe aspecte:

A. Securitatea Aplicației

- Dezvoltare Sigură: Se utilizează limbaj de programare sigur (C#) cu funcții integrate de securitate.
- Validare strictă a tuturor intrarilor utilizatorului pentru a preveni atacurile de tip injection (SQL injection, XSS).
- Bibliotecile și framework-urile utilizate au istoric bun de securitate și sunt actualizate regulat.
- Instrumente de analiză statica a codului pentru a identifică potentialele vulnerabilitati înainte de implementare (SonarQube).
- Proces de revizuire a codului (code review obligatoriu) — minim 2 dezvoltatori verifică fiecare PR.
- Teste de penetrare și teste de vulnerabilitate trimestrial pentru a identifică și remedia slabiciunile de securitate.

B. Securitatea Infrastructurii

- Controlul Accesului — firewall configurat pentru a restrictiona accesul la sistem doar la adresele IP și porturile autorizate.
- Sistem de detectie a intruziunilor (IDS) pentru a monitoriza traficul și a detecta activități suspecte.
- Politici de securitate documentate, training echipă pe topic GDPR și security awareness.
- Background check pentru personal cu acces la date sensibile.
- NDA semnat de toată echipă.
- Acord procesare date GDPR semnat cu ANPCV (DPA).
- Incident response plan documentat — RTO 4h, RPO 1h.
- Disaster recovery testat anual.

C. Cadrul de conformitate

Standard / Reglementare	Aplicare în proiect
GDPR (UE) 2016/679	Procesare date personale (victime, agresori); DPIA; drepturile persoanelor vizate
HG nr. 1123/2010	Securitate date personale în sisteme informatice
HG nr. 201/2017	Cerințe minime obligatorii securitate cibernetica
HG nr. 530/2025	Conceptul SI Viodata — cerința originala
ISO/IEC 27001	Sistem management securitate informație (certificat ofertant)
ISO 9001	Sistem management calitate (certificat ofertant)

OWASP Top 10 (2021)	Eliminare 10 vulnerabilitati majore
OWASP ASVS Level 2	Țintă noastră pentru testare securitate
WCAG 2.1 nivel AA	Accesibilitate (depășește cerința minimă nivel A)
eGov4Dev	Standarde guvernamentale design și interoperabilitate

5.2 Monitorizare și logare

Pentru asigurarea functionarii optime și asigurarea securității sistemului VD Core, este implementat un sistem robust de monitorizare și logare. Acest sistem permite urmarirea performanței aplicației, identificarea rapida a erorilor și problemelor, precum și asigurarea unei piste de audit pentru acțiunile utilizatorilor și evenimentele de sistem.

Configurarea sistemului de monitorizare și logare:

- Instrumente: Prometheus + Grafana pentru metrici performanță. ELK Stack (Elasticsearch + Logstash + Kibana) pentru logs centralizate. Icinga2 pentru alerting. Node-exporter + Cadvisor pentru metrici hardware.
- Niveluri logare: Debug, Info, Warning, Error, Critical
- Centralizarea log-urilor: toate log-urile în Elasticsearch pentru căutare și corelare.
- Analiză log-urilor: identificare tendinte, detectare anomalii, generare alerte.
- Pastrarea log-urilor: 1 an pentru logs operaționale, 5 ani pentru logs de audit (cerința GDPR).

5.3 SLA (Acordul privind Nivelul de Serviciu)

Severitate incident	Definiție	Timp răspuns	Timp rezolvare
P1 — Critic	Sistem indisponibil; pierderea funcționalității principale; risc securitate datelor	1 ora	4 ore
P2 — Mare	Funcționalitate critica afectata; degradare semnificativa a performanței	4 ore	24 ore
P3 — Mediu	Funcționalitate non-critica afectata; problema cu workaround	24 ore	5 zile lucrătoare
P4 — Mic	Defect cosmetic sau sugestie de îmbunătățire	1 săptămână	Cu următoarea actualizare planificata

Procedura de escaladare a incidentelor:

- L1 — Service Desk Ofertant (24/7 pentru P1-P2)
- L2 — Echipă de dezvoltare specializată pe modul
- L3 — Arhitect IT + PM ofertant
- L4 — Conducerea ofertantului + PM ANPCV

Capitolul 6: Structură și managementul echipei de implementare

Succesul unui proiect de o asemenea anvergură depinde în mod direct de expertiza, coerenta și dedicarea echipei implicate. Abordarea noastră se bazează pe alocarea unei echipe de specialisti cu experiență vasta în livrarea de soluții software complexe pentru sectorul guvernamental, care vor lucra în strânsă colaborare cu ANPCV pe tot parcursul implementării.

6.1 Compozitia și structură echipei

Pentru implementarea acestui proiect, ASOCIEREA UPCODE GROUP S.R.L. și SMART ITWORKS S.R.L. aloca o echipă de 7 experți-cheie nominalizați conform cerințelor Caietului de sarcini Sec. 7. Fiecare expert este nominalizat individual cu CV-uri (Anexa 14.1) și depășește cerințele minime pentru rolul propus. Echipa este disponibilă pe toată durata contractului (32 luni: mai 2026 — decembrie 2028) și nu este nominalizată în alte oferte concurente.

Nr	Rol VioData	Expert nominalizat (zile + tarif)	Companie
1	**Manager de Proiect / Scrum Master**	Pavel Melinic — 250 zile alocate (tarif 5 700 MDL/zi)	SMART ITWORKS S.R.L. (ASOCIAT)
2	**Analist de Business**	Serghei Belyi — 190 zile alocate (tarif 6 900 MDL/zi — rol DUAL: BA principal + Tech Lead consultativ pentru integrările cu cele 13 sisteme guvernamentale; CTO ITW cu 25+ ani experiență, expertiza directă în arhitectura eGov: eSocial, mcabinet.gov.md, EVO, EcoVoucher)	SMART ITWORKS S.R.L. (ASOCIAT)
3	**Arhitect IT**	Valentin Gushan — 200 zile alocate (tarif 5 700 MDL/zi)	SMART ITWORKS S.R.L. (ASOCIAT)
4	**Dezvoltator Backend**	Aleksandr Dvortsov — 320 zile alocate (tarif 4 350 MDL/zi)	SMART ITWORKS S.R.L. (ASOCIAT)
5	**Dezvoltator Frontend**	Vladimir Tcaciuc — 230 zile alocate (tarif 5 700 MDL/zi)	UPCODE GROUP S.R.L. (LIDER)
6	**Specialist UX/UI**	Ana Brescher — 152 zile alocate (tarif 3 460 MDL/zi)	UPCODE GROUP S.R.L. (LIDER)
7	**Specialist QA / testare**	Andrei Lisnic — 230 zile alocate (tarif 3 460 MDL/zi)	SMART ITWORKS S.R.L. (ASOCIAT)

	TOTAL ECHIPĂ	**7 experți-cheie / 1 572 zile lucru / 7 900 720 MDL fără TVA**	**2 UPCODE + 5 ITW = ASOCIERE**

Total echipă: 7 experți-cheie conform Caietului de sarcini Sec. 7 (componența minimă obligatorie). Distribuția: 2 experți UPCODE GROUP S.R.L. (LIDER) + 5 experți SMART ITWORKS S.R.L. (ASOCIAT).

6.2 Rolurile și responsabilitatile

Fiecare membru al echipei va avea un rol clar definit pentru a asigură eficiența maximă a procesului de dezvoltare.

- Manager de Proiect / Scrum Master (Pavel Melinic, ITW): punct central de contact, supervizare logistica proiect, facilitare proces Agile/Scrum, eliminare impedimente, gestionare risc-uri, raportare către ANPCV. Min. 5 ani experiență în proiecte IT (caz Pavel Melinic: 8+ ani CEO & PM SMART ITWORKS, MBA Strategic Management) — depășește cerința tender.
- Analist de Business (Serghei Belyi, ITW — CTO): responsabil de elicitarea cerințelor, documentarea proceselor de afaceri (BPMN), elaborarea use-case-urilor SO-01..SO-09, modelelor de date și matricei de trasabilitate Concept—Cerință—Use case. Min. 5 ani experiență (caz Belyi: 25+ ani IT, ISO 9001 trained) — depășire substanțială.
- Arhitect IT (Valentin Gushan, ITW): responsabil de proiectarea arhitecturii sistemului, deciziile tehnologice (Clean Architecture, DDD, CQRS), supervizarea integrărilor cu sistemele guvernamentale (MConnect, MPass, MNotify, MSign, MLog). Min. 5 ani experiență IT + 3 ani rol arhitect (caz Gushan: 25+ ani IT, 12 ani titulatura Architect la DAAC System Integrator) — depășire substanțială.
- Dezvoltator Backend (.NET 10 LTS): proiectare, dezvoltare și integrare microservicii backend (.NET 10 (LTS), ASP.NET Core, Entity Framework, PostgreSQL 18). Min. 4 ani experiență backend (caz Dvortsov: 6+ ani Software Developer ITW + experiență CMS și REST API) — conform.
- Dezvoltator Frontend (Vladimir Tcaciuc, UPCODE — LIDER): dezvoltare UI Angular 21+ cu TailwindCSS și componente Spartan UI; integrare cu backend prin REST API; design responsive cross-device. Min. 3 ani experiență (caz Tcaciuc: 7+ ani Senior Frontend, lucrează acum pe sistem informațional similar) — depășire.
- Specialist QA / testare (Andrei Lisnic, ITW): garantarea calității produsului final — strategii testare unitară, integration, end-to-end, regression, automated (Selenium, Playwright); validare 5 milioane înregistrări (Etapa IV — Testare); securitate (OWASP Top 10). Min. 3 ani experiență testare (caz Lisnic: Senior QA 4+ ani C# .NET automation) — depășire.
- Specialist UX/UI (Ana Brescher, UPCODE — LIDER): proiectare fluxuri navigare, structură interfețe, prototipare cu Figma, conformitate WCAG 2.1 nivel A, accesibilitate, branding. Min. 3 ani experiență UX/UI (caz Brescher: 8+ ani design profesional + certificări UXClan + BangBangEducation, fost Art Director Simpals) — depășire.

Capitolul 7: Subcontractare

Ofertantul principal preia >=70% din scope-ul contractului. Subcontractarea, în limita maximă de 30% conform anuntului de participare cerința 15, este utilizata strategic pentru pachete unde expertiza specifică de la o companie specializată aduce valoare adăugată.

7.1 Pachete subcontractate

Pachet	Subcontractant nominalizat	% din contract	Valoare aproximativa fără TVA
UX/UI design specializat — wireframes, prototipuri, design system aliniat MUD	NU SE UTILIZEAZĂ — strategie ASOCIERE pură	0%	0 MDL
Securitate cibernetica și pen-test (OWASP Top 10, ASVS L2)	NU SE UTILIZEAZĂ — strategie ASOCIERE pură	0%	0 MDL
Instruire utilizatori (admin 16h + utilizatori 24h)	NU SE UTILIZEAZĂ — strategie ASOCIERE pură	0%	0 MDL
Traduceri profesionale RO/RU/EN și validare lingvistica	NU SE UTILIZEAZĂ — strategie ASOCIERE pură	0%	0 MDL

TOTAL subcontractare: maximum 17% — sub limita de 30% cu marja de siguranță substantiala.

Pentru fiecare subcontractant atasam la Anexa 15:

- Contract de subcontractare semnat (per pct. 32 alin 10 doc. standard)
- DUAE separat completat de subcontractant
- Toate documentele obligatorii din pct. 16 din anunțul de participare
- Acord NDA + Acord procesare date GDPR (DPA)
- Declarație pe propria răspundere: lipsă conflict interese (pct. 14 doc. standard), lipsă oferte multiple (pct. 66 doc. standard), conformitate art. 16(6) Legea 131/2015

Capitolul 8: Raport TCO (Total Cost of Ownership)

Conform clarificarii 1, raportul TCO este DISTINCT de ofertă financiară. Acest raport reflectă costurile reale ale ciclului de viață al sistemului pe minimum 3 ani.

8.1 Categorii de cost — sumar

Categorie cost	An 1 (2026)	An 2 (2027)	An 3 (2028)	Total 3 ani
1. Costuri inițiale (CAPEX)	2 550 000	3 550 000	0	6 100 000
Dezvoltare	1 800 000	2 700 000	0	4 500 000
Integrări	700 000	850 000	0	1 550 000
Setup infrastructură MCloud	50 000	0	0	50 000
2. Costuri operaționale (OPEX)	0	200 000	1 000 000	1 200 000
3. Costuri infrastructură — MCloud	0 (gratuit gov)	0	0	0
4. Costuri licentiere	0 (open-source)	0	0	0
5. Costuri interoperabilitate	100 000	150 000	0	250 000
6. Costuri securitate și conformitate	88 667	84 333	27 000	200 000
7. Costuri instruire	0	150 000	0	150 000
8. Costuri scoatere din exploatare	0	0	0	0
TOTAL TCO 3 ani	2 738 667	4 134 333	1 027 000	7 900 000

8.2 Asumari TCO

- Hosting MCloud — gratuit pentru instituții guvernamentale (politica AGE)
- Licențe open-source — fără costuri recurente (.NET, Angular, PostgreSQL, Docker, Kubernetes, Kafka, MinIO, etc. sunt toate open-source)
- Personal mentenanță — bazat pe ~15% din efortul de dezvoltare (clarif. 18)
- Inflatie estimată: 5%/an (conform prognoza BNM)
- Curs valutar: stabil MDL

8.3 Cost analysis

- Costul mediu anual TCO: 2 633 333 MDL/an fără TVA (= 7 900 000 / 3 ani)
- Cost per utilizator (la 500 utilizatori activi în 13 instituții guvernamentale, pe 3 ani): 5 267 MDL/utilizator/an fără TVA (= 7 900 000 / 500 / 3)
- Cost per caz gestionat (estimare 30 000 cazuri pe 3 ani conform statisticii naționale ~10 000 cazuri/an, vezi raport ANPCV 2024): 263 MDL/caz fără TVA (= 7 900 000 / 30 000)

Declarația ofertantului

Subsemnatul, în calitate de reprezentant legal al ofertantului, declar pe propria răspundere că:

11. Toate informațiile prezentate în această ofertă tehnică sunt corecte și conforme cu realitatea.
12. Asumăm integral și neconditionat îndeplinirea tuturor cerințelor din Caietul de sarcini și din clarificarile primite (24.03 și 02.04.2026).
13. Personalul nominalizat este disponibil pe durata contractului.
14. Subcontractantii nominalizați au fost informati și au acceptat rolul lor în proiect.
15. Avem capacitatea tehnică, operațională și financiară necesară pentru îndeplinirea contractului.
16. Vom menține valabilitatea ofertei pentru 90 zile calendaristice de la data limita de depunere.
17. Vom respectă termenul final de 25.12.2028 al contractului.

Data completării: 04 / 05 / 2026

Reprezentantul ofertantului:

Semnat: _____

Nume și prenume: Vadim Jeleascov

Functia în cadrul firmei: Administrator

Denumirea firmei: UPCODE GROUP S.R.L. (Lider al Asocierii cu SMART ITWORKS S.R.L.)

Stampila / Semnătură electronică calificata

3.5 Arhitectură modulară cu pattern-uri reutilizabile

Sistemul Viodata este construit pe o arhitectură modulară cu pattern-uri arhitecturale stabile și validate în producție pentru sisteme similare guvernamentale. Aceste pattern-uri formeaza fundamentul tehnic pentru toate cele 14 microservicii VD Core.

Pattern-uri arhitecturale aplicate:

- Clean Architecture (Robert C. Martin) — separare clara între Presentation, Application, Domain și Infrastructure layers; dependency rule respectată strict.
- Domain-Driven Design (DDD) — modele bogate de domeniu cu boundary clar; entitati, value objects, aggregate roots; bounded contexts pentru fiecare microserviciu.
- CQRS cu MediatR — separare commands/queries; handler-i specializati per operație; testabilitate ridicata.
- Event-Driven Architecture — comunicare inter-servicii via Kafka; pattern Outbox pentru consistența tranzactionala; event sourcing pe entitati critice (Caz, Plan intervenție).
- Database-per-Service — fiecare microserviciu cu instanță proprie PostgreSQL 18; date partajate via API sau evenimente, NU via shared database.
- Dependency Injection — IoC container .NET pentru toate componentele; testabilitate prin mock-uri și stub-uri.
- Circuit Breaker pattern (Polly) — pentru integrări externe (MConnect, MNotify, MPass) — toleranta la esecuri tranzitorii.
- API Gateway pattern — VD.MConnect că singur punct de ieșire către integrările guvernamentale (NU point-to-point).

Stiva tehnologică modulară — toate componentele open-source sau cu licența permisiva:

- Backend: .NET 10 (LTS)+ (Microsoft, MIT license), ASP.NET Core, Entity Framework Core, MediatR, FluentValidation. Conformitate eGov4Dev — https://egov-moldova.github.io/egov4dev/ (Tools and technologies — clarificarea 5 si 12).
- Frontend: Angular 21+ (Google, MIT), TailwindCSS 4+ (MIT), componente Spartan UI (MIT — selectat unic pentru consistența UI; NU PrimeNG mixed).
- Baze de date: PostgreSQL 18 (open-source, PostgreSQL License) cu extensions PostGIS, pgvector.
- Mesagerie: Apache Kafka (Apache 2.0 license).
- Cache: Dragonfly (BSL — open-source pentru utilizare non-comercială).
- Object Storage: MinIO (AGPL/comercial — selectabil; alternativa LakeFS).
- Search: Elasticsearch (SSPL — alternativa OpenSearch Apache 2.0 daca licentierea e issue).
- Containerization: Docker (Apache 2.0), Kubernetes (Apache 2.0).
- Monitoring: Prometheus + Grafana + ELK (toate Apache 2.0/MIT).
- Maps: Leaflet 1.9+ (BSD-2) + OpenStreetMap (ODbL) — exclus Mapbox proprietary.

Beneficiile abordarii modulare cu pattern-uri stabile:

- Reducere risc tehnic: pattern-urile sunt validate în industrie; comunitate larga de suport.
- Independență deployment: fiecare microserviciu poate fi deployat / scalat independent.
- Testabilitate: Clean Architecture + DI permite testare unit / integration / e2e cu acoperire ridicata.

- Mentenabilitate: structură predictibila → onboarding rapid pentru noi dezvoltatori.
- Open-source: zero vendor lock-în; conformitate cu cerința Sec. 6.1 din Caietul de sarcini.

3.6 Scoatere din exploatare (decommissioning)

Sistemul Viodata implementeaza un proces complet de scoatere din exploatare conform cerințelor finale ale Caietului de sarcini. Această secțiune detaliaza: export date, migrare, arhivare, oprire controlata și stergere ireversibila.

3.6.1 Export date către alte sisteme

- Endpoints REST API și SOAP cu autentificare ABAC pentru export programatic.
- Export incremental: webhooks Kafka pentru consumatori în timp real (utile pentru continuitate la migrare).
- Export bulk: endpoint /export/full cu generare async ZIP cu toate datele în formate standardizate (JSON, XML, CSV).
- Format de export: schema JSON-LD cu URI-uri persistente per obiect informațional; respectă StandardArchive moldovenesc.
- Validare integritate: SHA-256 checksums per fisier export; semnătură digitala MSign pe arhive.

3.6.2 Arhivare conform legislatiei

- Pastrare termen lung: 75 ani pentru cazuri grave (omor, lezuri grave) conform Legii MD; 25 ani pentru alte cazuri (în conformitate cu legislatia aplicabilă).
- Migrație automata din storage activ -> storage arhiva (MinIO Glacier/Cold tier) la termen.
- Index permanent — search by IDNP victimă/agresor pentru cercetare juridică ulterioară (acces controlat).
- Catalog StandardArchive Moldova — generare automata la export pentru transfer în arhive de stat.

3.6.3 Oprire controlata sistem

- Drain mode — sistemul refuză request-uri noi, finalizează cele în curs (timeout configurabil).
- Verificare integritate baza date înainte de închidere (CHECKSUM și BACKUP final pe MinIO + suport extern).
- Procedura de închidere documentata și testata anual cu echipă ANPCV.
- Preluare date către noul sistem (succesor) — perioadă de paralelizare configurabila pentru migrație soft.

3.6.4 Stergere ireversibila a datelor (când legal admisibil)

- Pentru date personale ale subiectilor care exercita dreptul GDPR de stergere: stergere logica + criptare cu aruncare cheie (criptografic shredding).
- Stergere fizică (data wipe DOD 5220.22-M sau echivalent) doar după confirmare audit + cerere oficiala ANPCV.
- Audit log al stergerii pastrat indefinit (cu pseudonimizare) — pentru conformitate trasabilitate.

3.7 Mapare use-cases SO-01..SO-09 pe microservicii

Fiecare use-case obligatoriu din Sec. 5.12 al Caietului de sarcini este mapat pe microserviciile VD Core și livrat în sprintul corespunzător. Această tabela este referința pentru evaluatori la verificarea conformității funcționale.

Cod use-case	Descriere	Microservicii VD livrate	Sprint livrare
SO-01	Înregistrare caz nou de violență	VD.CaseHub + VD.SubjectHub	Sprint 5-6 (Etapă III, lună 1-2 dezvoltare)
SO-02	Evaluare risc victimă și agresor	VD.ProtectionHub (Crisis Profile cu severitate 1-5)	Sprint 7-8
SO-03	Plan intervenție personalizat	VD.CaseHub + VD.ApprovalHub (workflow aprobare)	Sprint 8-9
SO-04	Monitorizare caz și evolutia intervenției	VD.CaseHub + VD.Audit (event sourcing)	Sprint 9-10
SO-05	Referire către servicii (adaposturi, juridic, medical)	VD.ReferralHub + VD.MConnect (integrări interinstituționale)	Sprint 10-11
SO-06	Monitorizare ordine de protecție	VD.ProtectionHub + VD.Geo (geofencing opțional)	Sprint 11-12
SO-07	Gestionare nomenclatoare (categorii violență, servicii)	VD.UserHub (extensia Registry)	Sprint 4 (early — pregătire pentru CaseHub)
SO-08	Închidere caz	VD.CaseHub (state transition Active -> Closed)	Sprint 12
SO-09	Generare rapoarte și indicatori	VD.Reporting + VD.DataHub	Sprint 13-14

Capitolul 9: Estimare efort om-zile (rol × etapă × activitate)

Conform Sec. 8 din Caietul de sarcini (Modalitatea de întocmire a ofertelor): 'Prestatorul trebuie să prezinte estimarea efortului în: om-zile sau om-ore; acesta trebuie să fie defalcat pe rol, pe etapă și pe activități.'

Tabelul de mai jos prezintă defalcarea completa a efortului estimat de 1.572 om-zile pe cele 7 roluri-cheie, 6 etape de implementare și activități specifice fiecarei etape. Total efort: 1.572 om-zile = ~75 om-luni la 21 zile/lună.

9.1 Defalcare efort total per rol și etapă (om-zile)

Rol	I Inițiere (2 luni)	II Proiectare (3 luni)	III Dezvoltare (9 luni)	IV Testare (3 luni)	V Lansare (3 luni)	VI Garanție (12 luni)	Total om-zile
Manager de Proiect / Scrum Master	13	38	113	25	25	36	250
Analist de Business	34	76	57	10	10	3	190
Arhitect IT	20	70	60	10	16	24	200
Dezvoltator Backend	6	32	176	32	16	58	320
Dezvoltator Frontend	5	23	127	23	12	40	230
Specialist UX/UI	8	84	41	6	7	6	152
Specialist QA / testare	5	12	46	92	30	45	230
TOTAL pe etapă	91	335	620	198	116	212	1572

9.2 Activități principale per rol și etapă

Manager de Proiect / Scrum Master

I: Plan proiect, kickoff stakeholder, baseline scope. II: Definire sprint-uri, ceremonii Scrum setup, risk register. III: Coordonare zilnică stand-up, sprint review, retrospectiva, raportare ANPCV. IV: Coordonare testare, sign-off livrabile. V: Plan rollout, instruire, recepție. VI: Coordonare suport L1-L2, raport mensual ANPCV.

Analist de Business
I: Elicitare cerințe, sesiuni cu ANPCV/IGP/MMPS, matrice trasabilitate cerințe → use cases. II: Specificații funcționale detaliate pentru cele 14 obiecte informaționale; modele BPMN pentru workflow-uri caz. III: Sprint planning input, validare incrementală cu utilizatorii. IV: User Acceptance Testing cu beneficiarul. V: Documentație utilizator, materiale instruire. VI: Triage incidente funcționale.

Arhitect IT
I: Analiză cerințe tehnice, validare integrări guvernamentale (MConnect, MPass, MNotify). II: Document arhitectură sistem; modele de date; specificații integrări; design API REST/SOAP. III: Code review arhitectural, decizii tehnice, intervenii pe issue-uri tehnice complexe. IV: Validare arhitecturala ramuri testare. V: Plan deployment producție. VI: Patch-uri securitate, ajustari tehnologice.

Dezvoltator Backend
I: Setup mediu dev, pipeline CI/CD inițial. II: Skeleton microservicii VD Core (14 servicii), modele entitati, repository pattern. III: Implementare logica business per microserviciu (CaseHub, SubjectHub, ProtectionHub, etc.); CQRS handlers; integrări MConnect. IV: Bug fixing post-testare, optimizari performanță. V: Suport go-live, hotfix-uri. VI: Bug-fix, mentenanță corectiva.

Dezvoltator Frontend
I: Setup proiect Angular 21+, componente UI baza Spartan UI. II: Wireframes interactive, prototip. III: Implementare ecrane back-office (lucratori sociali) și portal cetățeni; integrări API; state management NgRx. IV: Bug fixing UX, optimizari render. V: Documentație utilizator, training. VI: Mentenanță corectiva, ajustari adaptive.

Specialist UX/UI
I: Cercetare utilizator, persona definition (lucrator social, victimă, manager ANPCV). II: Wireframes, prototip Figma, design system, accesibilitate WCAG 2.1 A. III: Handoff componente către frontend, validare implementare. IV: User testing, ajustari UX. V: Documentație design. VI: Ajustari minore feedback utilizatori.

Specialist QA / testare
I: Test plan, framework testare (Selenium, Playwright). II: Test cases conform use cases SO-01..SO-09; setup automat. III: Testare unit + integration per sprint; regression testing. IV: Testare funcțională completa, performanță (load 5M înregistrări planificat), securitate (OWASP Top 10), interoperabilitate, pilotare cu utilizatori. V: Smoke testing după go-live. VI: Regression după fiecare patch garanție.

9.3 Rezumat efort total
- Total efort: 1.572 om-zile (echivalent ~75 om-luni la 21 zile lucrătoare/lună)
- Durata contract: 32 luni (mai 2026 — decembrie 2028)
- FTE mediu pe durata: 2,34 (echipă lucrează în medie la 33% capacitate fiecare expert pe perioadă contractului)
- Distribuție pe etape (pondere financiară conform Anexei 23 — Specificații preț): I=5%, II=13%, III=50%, IV=12%, V=7%, VI=13% (Total 100%; aliniat cu structura plăților lunare din Anexa 23 — Sheet 'Esalonare lunară'). Distribuția om-zile per etapă (conform Tabelei 15) diferă natural de pondere financiară: I=5,8%, II=21,3%, III=39,4%, IV=12,6%, V=7,4%, VI=13,5%. Diferența reflectă structura tarifelor zilnice per rol — Backend (4 350 MDL/zi) este alocat predominant în Etapa III, generând efort om-zile mai mare la cost financiar mediu pe lună similar cu alte etape.
- Detaliere zilnică pe sprint și activitate disponibilă în Anexa 23 Specificații de pret (Sheet 'Esalonare lunară')

Notă privind semnătura electronică:

Documentul este semnat electronic prin semnătură electronică autorizată conform Legii nr. 91/2014 privind semnătura electronică și documentul electronic.

Data întocmirii: 04.05.2026