Anexa nr. 22
la Documentația standard nr. ocds-b3wdp1-MD-1785752962918
din "_03_" _august__ 2026_

Specificaţii tehnice

[Acest tabel va fi completat de către ofertant în coloanele 2, 3, 4, 6, 7, iar de către autoritatea contractantă – în coloanele 1, 5]

Numărul procedurii de achiziție ocds-b3wdp1-MD-1785752962918 din 03.08.2026						
Obiectul achiziției: Servicii de elaborare a caietului de sarcini privind softul "EVIDENCE"						
Denumirea bunurilor/serviciilor	**Denumirea modelului bunului/serviciului**	**Ţara de origine**	**Produ-cătorul**	**Specificarea tehnică deplină solicitată de către autoritatea contractantă**	**Specificarea tehnică deplină propusă de către ofertant**	**Standarde de referinţă**
1	**2**	**3**	**4**	**5**	**6**	**7**
Servicii de elaborare a caietului de sarcini privind softul "EVIDENCE"	Servicii de dezvoltare software	Moldova	Akdev Solutions SRL	Conform caietului de sarcini	Conform caietului de sarcini, integral și fără rezerve. Soluție web 3-tier, 100% browser-based, construită pe tehnologii open-source fără costuri de licențiere: backend Java 21 LTS (OpenJDK) cu Spring Boot 3.3, bază de date PostgreSQL 16, frontend Angular 21 (SPA/PWA), API RESTful JSON peste HTTPS/TLS 1.3, containerizare Docker și orchestrare Kubernetes. Sunt acoperite toate cele 14 module funcționale (cap. 5), cerințele tehnice și de arhitectură (cap. 6), etapele și metodologia de execuție (cap. 7), precum și documentația, instruirea și mentenanța de 12 luni (cap. 8). Detalierea punct-cu-punct este prezentată în „Matricea de conformitate tehnică" anexată la prezentul formular, care constituie parte integrantă a propunerii tehnice.	Conform caietului de sarcini
TOTAL						

Semnat:_____ Numele, Prenumele: ___COLOSOV ALEXEI_____ În calitate de: _DIRECTOR_____

Ofertantul: _AKDEV SOLUTIONS SRL_____ Adresa: __Republica Moldova, mun. Chisinau, str. M. Sadoveanu 17, of. 321_____

Digitally signed by Colosov Alexei
Date: 2026.08.25 10:02:04 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

ANEXĂ LA ANEXA NR. 22
MATRICEA DE CONFORMITATE TEHNICĂ

Parte integrantă a propunerii tehnice

Procedura de achiziție: ocds-b3wdp1-MD-1785752962918 din 03.08.2026

Autoritatea contractantă: Inspectoratul General al Poliției, IDNO 1013601000495

Ofertant: „AKDEV SOLUTIONS” S.R.L., IDNO 1015600025259

Soluția tehnică propusă — sinteză

Sistemul EVIDENCE este propus ca aplicație web modulară, construită pe o arhitectură pe trei niveluri, cu următorul stack tehnologic, integral open-source și fără costuri de licențiere pentru Beneficiar, nici la implementare, nici ulterior:

- Nivel de prezentare: Angular 21 (SPA/PWA), Angular Material, interfață responsivă, funcționare offline pentru modulul CFL;
- Nivel de logică de business: Java 21 LTS (OpenJDK) cu Spring Boot 3.3 și Spring Security 6, API RESTful JSON documentat OpenAPI 3.1, comunicare peste HTTPS/TLS 1.3;
- Nivel de date: PostgreSQL 16, acces prin Spring Data JPA/Hibernate, integritate referențială, proceduri stocate PL/pgSQL, migrări versionate Flyway, particionare și replicare în flux;
- Infrastructură și exploatare: Docker, Kubernetes, Nginx, MinIO (stocare obiecte), Redis (cache), RabbitMQ (mesagerie), Jenkins și Maven (CI/CD), SonarQube (calitatea codului), Prometheus și Grafana (monitorizare);
- Servicii guvernamentale: conectori MPass și MSign, activabili prin configurare, fără a condiționa funcționarea sistemului, conform pct. 6.2 din Caietul de sarcini.

În tabelul de mai jos, fiecare cerință a Caietului de sarcini este prezentată alături de soluția tehnică propusă. Ofertantul confirmă conformitatea integrală cu cerințele solicitate, fără rezerve și fără abateri.

Nr.	Ref. Caiet de sarcini	Cerința autorității contractante	Confor-mitate	Soluția tehnică propusă de ofertant
A. MODULE FUNCȚIONALE ALE NOULUI SISTEM (cap. 5 din Caietul de sarcini)				
1	Modulul 1 (cap. 5)	Utilizatori, Identitate și Semnătură (MPass & MSign). Autentificare unică prin MPass, cu MFA, segmentare pe unități organizatorice și politici de expirare/reevaluare a accesului; funcționare autonomă prin conturi locale, fără dependență de servicii externe. Autorizare RBAC/ABAC cu granularitate până la nivel de câmp, acțiune și stare de flux. Semnare prin MSign cu marcă temporală și lanț de aprobare „patru ochi”; alternativ, semnătură internă cu mecanisme de integritate criptografică. Jurnale inviolabile (hash-uite), politici GDPR (minimizare, pseudonimizare, drepturile persoanei vizate). SLA configurabile per tranzacție critică, cu alerte la depășire. Administrarea personalului și a subdiviziunilor, inclusiv dosare personale (concedii, permise deținute, studii).	**Da, conform**	Serviciu dedicat Identity & Access Management construit pe Spring Boot 3.3 și Spring Security 6. Conector MPass (SAML 2.0 / OpenID Connect) activabil prin configurare, cu suport MFA delegat; mod autonom cu conturi locale, parole stocate prin Argon2id (Spring Security PasswordEncoder) și politici configurabile de complexitate, expirare, istoric și blocare după N încercări. Motor de autorizare RBAC/ABAC implementat prin Spring Security Method Security și reguli declarative evaluate pe atribute de utilizator, subdiviziune, tip document și stare de flux, aplicate la nivel de endpoint, de câmp (mascare prin filtre de serializare Jackson) și de tranziție de stare. Conector MSign prin API REST, cu marcă temporală RFC 3161 și stocarea dovezilor de integritate; alternativ, semnătură internă cu amprentă SHA-256, înlănțuire hash și sigilare la nivel de document. Flux de aprobare configurabil, inclusiv „patru ochi”. Jurnal append-only cu înlănțuire criptografică (fiecare înregistrare conține hash-ul precedentei), stocat separat de datele operaționale. Set de instrumente GDPR: pseudonimizare la export, registru de prelucrări, gestionarea cererilor persoanei vizate, politici de retenție. Motor SLA parametrizabil per tip de tranzacție, cu alerte și agregare către Modulul 12. Submodul HR: subdiviziuni ierarhice, dosare personale, concedii, permise deținute, studii și certificări, cu istoric și audit.
2	Modulul 2 (cap. 5)	CFL – Cercetare la Fața Locului. Interfețe orientate pe pași logici (deplasare, constituire echipă, constatări, colectare urme/obiecte, fotografiere, măsurători, închidere), cu validări contextuale. Captură automată a geolocației, timpului, condițiilor și participanților, cu legare la lanțul de custodie prin generarea imediată în teren a etichetelor cu coduri de bare. Lucru offline, cu reconciliere ulterioară și identificarea conflictelor. Semnarea documentelor de predare-primire, minutelor de închidere și anexelor foto. Timpii fiecărui pas configurabili și monitorizați, cu praguri și alerte. Încărcarea și păstrarea planșelor fotografice în format PDF.	**Da, conform**	Aplicație de teren de tip PWA construită pe Angular 17 cu Angular Service Worker, instalabilă pe tablete și laptopuri, cu persistență locală IndexedDB și coadă de sincronizare. Reconciliere la revenirea online prin versionare optimistă și marcare temporală a evenimentelor; conflictele sunt detectate automat și prezentate operatorului pentru rezolvare controlată, cu păstrarea ambelor versiuni în audit. Captură automată GPS, dată/oră, condiții meteo introduse și componența echipei. Generare imediată de etichete Code128/QR și tipărire pe imprimante mobile Bluetooth (limbaj ZPL/CPCL), cu asociere instantanee la lanțul de custodie din Modulul 7. Formulare pe pași („wizard”, Angular Reactive Forms) cu validări condiționale care blochează avansarea la date incomplete. Semnare a proceselor-verbale, minutelor și anexelor conform Modulului 1. Praguri de timp configurabile pe fiecare tranziție (ex. ridicare → etichetare), cu alerte și raportare. Încărcare planșe foto PDF, stocare în depozit de obiecte S3-compatibil (MinIO) cu amprentă de integritate.

Nr.	Ref. Caiet de sarcini	Cerința autorității contractante	Confor-mitate	Soluția tehnică propusă de ofertant
3	Modulul 3 (cap. 5)	AUP – Acțiuni de Urmărire Penală și Temeiuri Legale. Repertoriu codificat al infracțiunilor corelat cu un registru al temeiurilor (ordonanțe, solicitări, demersuri), care guvernează dinamica formularelor și obligativitatea câmpurilor. Păstrarea la nivel de structură de date a legăturilor dintre cauză, actul procesual, persoanele implicate și obiectele/urmele aferente, pentru corelări inter-caz. SLA pe stadii (propunere, avizare, emitere), cu alerte și rapoarte de conformitate.	**Da, conform**	Nomenclator versionat al infracțiunilor (cod, denumire, încadrare) și registru al temeiurilor legale, gestionate central în Modulul 14. Motor de formulare dinamice (Angular Reactive Forms generate din metadate) care determină, pe baza temeiului și a tipologiei faptei, câmpurile vizibile, obligatorii și regulile de validare, fără modificări de cod. Model relațional normalizat cauză ↔ act procesual ↔ persoană ↔ obiect/urmă, cu chei externe și integritate referențială gestionate prin JPA/Hibernate peste PostgreSQL, care permite interogări de corelare inter-caz și alimentează Modulul 11. Configurare SLA distinctă pe fiecare stadiu și pe unitate, cu alertare la depășire și includere automată în rapoartele de conformitate procedurală.
4	Modulul 4 (cap. 5)	Acțiuni Tehnico-Explozive (EOD). Taxonomii specializate (tipuri de dispozitive, procedee de neutralizare, nivel de risc), flux securizat notificare–dislocare–intervenție–raport, ancorare probatorie (etapizare procedurală, foto/video, consemnări semnate). Acces segregat pe profiluri EOD, documente finale validate prin MSign cu marcă temporală și jurnal criptografic. Timpi critici (dispecerizare, sosire, neutralizare) configurabili pe profiluri de risc, cu comparabile istorice. Evidența mașinilor de serviciu care deservesc personalul în cadrul acțiunilor.	**Da, conform**	Domeniu funcțional izolat, cu compartimentare a datelor (row-level security în PostgreSQL, aplicată prin context de sesiune Spring) și profiluri de acces EOD distincte; datele nu sunt vizibile utilizatorilor din alte domenii, inclusiv la nivel de căutare globală. Nomenclatoare dedicate pentru tipuri de dispozitive, procedee de neutralizare și niveluri de risc, versionate în Modulul 14. Flux de stare notificare → dislocare → intervenție → raport, implementat ca mașină de stări cu marcaje temporale automate la fiecare tranziție. Atașare foto/video cu amprentă de integritate la încărcare. Semnare a documentelor finale prin MSign (sau mecanism intern, conform pct. 6.2), cu jurnal criptografic separat. Profiluri de risc cu praguri proprii pentru dispecerizare, sosire și neutralizare, comparate automat cu seriile istorice și prezentate în tablourile de bord. Registru al autovehiculelor de serviciu (identificare, dotare, disponibilitate) cu alocare pe intervenție și istoric de utilizare.
5	Modulul 5 (cap. 5)	Trageri Experimentale și Marcarea Armelor. Trasabilitate completă a armelor de la recepție până la integrarea rezultatelor balistice. Gestionarea caracteristicilor tehnice (serie, calibru, marcaje) și asocierea cu loturi de tragere, mostre și rezultate; rapoarte standardizate semnate electronic. Câmp dedicat pentru stocarea unui identificator extern, introdus manual sau extras din EVOFINDER și TRAFFIC. În cazul disponibilității unor API, integrare bidirecțională și sincronizare automată a metadatelor și rezultatelor. Timpi ai operațiunilor (recepție–prelucrare–tragere–raportare) configurabili pe profilul laboratorului, cu alerte la stagnare și indicatori de randament.	**Da, conform**	Registru al armelor cu identificare univocă (serie, calibru, tip, marcaje, producător), legat de loturi de tragere, mostre prelevate și rezultate obținute, cu istoric complet al stărilor prin auditare Hibernate Envers. Entitatea Evidence include câmpuri dedicate pentru identificatorii externi EVOFINDER și TRAFFIC, editabile manual și populabile automat, cu validare de format și verificare de unicitate. Arhitectură de integrare pregătită (strat de conectori, contracte de date și mapări definite în Modulul 10) care permite activarea sincronizării bidirecționale imediat ce producătorii expun API; în lipsa acestora, corelarea funcționează integral la nivel de identificator și flux procedural, fără impact asupra funcționalității. Rapoarte standardizate generate din șabloane configurabile și semnate electronic. SLA pe etapele recepție–prelucrare–tragere–raportare, configurabile per laborator, cu alerte la stagnare și indicatori de randament al corelării și durate de procesare.
6	Modulul 6 (cap. 5)	Urme Papilare și Integrare AFIS. Gestionarea întregului ciclu de viață al urmelor: prelevare, evaluare calitativă, prelucrare, transmitere către sisteme externe, recepția rezultatelor, arhivare. Metadate standardizate (tip suport, tehnică de ridicare, parametri de calitate) și corelare cu dosarul, locul, obiectul și persoana. Corelare cu AFIS prin identificator extern și verificări de integritate; integrare automată prin API doar dacă acestea sunt disponibile. Rezultatele (pozitive/negative) încapsulate în documente oficiale semnate electronic sau validate intern. SLA configurabile per etapă, tablouri de bord cu timpi mediani și valori extreme.	**Da, conform**	Ciclu de viață al urmei modelat ca mașină de stări (prelevată → evaluată → prelucrată → transmisă → rezultat recepționat → arhivată), fiecare tranziție fiind jurnalizată și marcată temporal. Set de metadate standardizate: tip suport, tehnică de ridicare, parametri de calitate, condiții de prelevare, operator. Corelare relațională cu dosarul, locul faptei, obiectul și persoana. Identificator extern AFIS gestionat local, cu verificări de integritate și control al unicității; conectorul API este prevăzut arhitectural și se activează prin configurare atunci când interfața devine disponibilă. Rezultatele pozitive/negative sunt încapsulate în documente oficiale generate din șabloane și semnate conform Modulului 1. SLA configurabile la nivel de unitate pe fiecare etapă, cu tablouri de bord ce prezintă timpi mediani, percentile și valori extreme pentru intervenție managerială predictivă.
7	Modulul 7 (cap. 5)	Custodie & Probe. Identificatori unici pentru obiecte și pachete (coduri de bare/QR), compatibili cu imprimante mobile și reziliențI la condițiile de teren. Înregistrarea oricărei mișcări (ridicare, transport, depozit, laborator, arhivare) și semnalarea incongruențelor. Gestionarea scenariilor fără obiect fizic și a examinărilor complexe (comisii, interdisciplinare, suplimentare/repetate), cu responsabili, costuri și versionări ale concluziilor. Emiterea și semnarea în sistem a documentelor operaționale (procese-verbale, foi de traseu, fișe de depozit). Timpul dintre evenimentele cheie ca indicator de performanță configurabil, cu vizibilitate în timp real a depășirilor SLA.	**Da, conform**	Identificatori unici imuabili pentru obiecte și pachete, materializați în coduri Code128 și QR, cu redundanță de citire și etichete rezistente la condiții de teren; tipărire pe imprimante mobile și de birou. Fiecare mișcare este un eveniment imuabil în lanțul de custodie (cine, ce, de unde, unde, când, în ce scop), cu scanare la predare și la primire; discrepanțele (obiect nescanat la recepție, custodie dublă, pachet deschis fără autorizare) generează alerte imediate. Suport explicit pentru dosare fără obiect fizic. Modelare a examinărilor complexe: comisii cu membri și roluri, examinări interdisciplinare, suplimentare și repetate, cu responsabili nominali, evidența costurilor și versionarea concluziilor (fiecare revizie păstrată integral). Generare și semnare în sistem a proceselor-verbale, foilor de traseu și fișelor de depozit. Indicatori de performanță configurabili pe intervalele ridicare–etichetare, depozit–laborator, laborator–finalizare, cu vizibilitate în timp real și agregare pentru audit.
8	Modulul 8 (cap. 5)	Registru Digital al Expertizelor. Numerotare automată la nivel național, cu structurare pe prefixe configurabile (an, unitate,	**Da, conform**	Generator de numere de înregistrare cu unicitate garantată la nivel național prin secvențe atomice în PostgreSQL, cu șabloane de prefix configurabile (an, unitate, segment, tip expertiză) și fără risc de coliziune în regim concurent. Flux de

Nr.	Ref. Caiet de sarcini	Cerința autorității contractante	Confor-mitate	Soluția tehnică propusă de ofertant
		segment). Flux complet de înregistrare, verificare, distribuire și închidere a lucrărilor, cu validare prin mecanisme configurabile de asumare și semnare. Corelarea înregistrărilor cu pachetele, subdiviziunile, executorii, obiectele și rapoartele aferente. Export controlat către alte sisteme prin interfețe API definite, documentate și securizate. Timpi de circulație configurabili diferențiat pe tip de expertiză, cu evidențierea blocajelor recurente. Încărcarea, gestionarea și arhivarea rapoartelor de expertiză, planșelor fotografice și altor documente justificative în format PDF.		stare înregistrare → verificare → distribuire → executare → închidere, cu validare prin MSign sau mecanism intern, conform configurației. Legături relaționale către pachete (Modulul 7), subdiviziuni, executori, obiecte și rapoarte. API REST versionat, documentat OpenAPI 3.1 (springdoc-openapi), securizat prin OAuth 2.0 / mTLS cu Spring Security Resource Server, cu drepturi granulare de export și jurnalizarea fiecărei cereri. SLA de circulație configurabile separat pe tip de expertiză (intrare→alocare, alocare→preluare, preluare→închidere), cu identificarea automată a blocajelor recurente și suport pentru realocare operativă. Încărcare, indexare și arhivare a rapoartelor de expertiză și planșelor fotografice în PDF, cu amprentă de integritate și căutare full-text.
9	Modulul 9 (cap. 5)	Corespondență și Flux Documentar. Registru al comunicărilor oficiale între experții criminaliști și organele judiciare: intrări/ieșiri, expeditor/destinatar, obiect, termene, anexe. Normalizarea metadatelor pentru documentele generate intern sau recepționate extern; semnare și contrasemnare prin MSign, cu conservarea urmelor de audit. Căutare inter-modulară (după dosar, persoană, locație, termen). Notificări privind scadențele aliniate SLA-urilor configurate; depășirile înregistrate și vizibile în rapoartele de conformitate procedurală.	**Da, conform**	Registru unic de intrări/ieșiri cu numerotare automată, metadate normalizate (expeditor, destinatar, tip, obiect, termen de răspuns, anexe) și legare la dosarul, persoana sau expertiza de referință. Semnare și contrasemnare conform Modulului 1, cu păstrarea integrală a urmelor de audit pentru fiecare tranzacție. Motor de căutare inter-modulară implementat pe indexare full-text PostgreSQL (tsvector) cu filtre combinate pe dosar, persoană, locație, interval de timp și subdiviziune. Notificări de scadență (în aplicație și pe e-mail) generate din SLA-urile configurate în Modulul 14 prin sarcini programate Spring Scheduler, cu escaladare la depășire și înregistrarea automată a abaterilor în rapoartele de conformitate.
10	Modulul 10 (cap. 5)	Interoperabilitate și Conectori (EVOFINDER, TRAFFIC, AFIS). Contracte de date stabile (mapări câmp-la-câmp, reguli de transformare, mecanisme de validare), orchestrarea fluxurilor de tip eveniment (create/update/delete), politici de rezolvare a conflictelor și jurnal inviolabil al schimburilor, utilizabil pentru audit și litigii. Corelare implicită prin stocarea și gestionarea locală a identificatorilor externi, introduși manual sau preluați din sistemele partenere. La disponibilitatea unor API, activarea sincronizărilor automate bidirecționale. Supraveghere operațională cu vizibilitate asupra latențelor, erorilor și mecanismelor de reîncercare; SLA de integrare declarate distinct per sistem partener.	**Da, conform**	Strat de integrare dedicat, izolat de logica de business, construit pe modelul adaptoarelor: fiecare sistem partener are un conector propriu, cu contract de date declarat (schemă JSON/XSD), mapări câmp-la-câmp, reguli de transformare și validare aplicate înainte de persistare. Orchestrare pe evenimente (create/update/delete) printr-o coadă de mesaje (RabbitMQ / Kafka, la opțiunea Beneficiarului), cu livrare garantată, reîncercare exponențială (Spring Retry) și coadă de erori pentru intervenție manuală. Politici configurabile de rezolvare a conflictelor (prioritate sursă, ultima modificare, escaladare la operator). Jurnal inviolabil al schimburilor, append-only și înlănțuit criptografic, cu păstrarea cererii și răspunsului pentru audit și litigii. Regimul implicit de funcționare este cel prin identificatori externi gestionați local, complet operațional fără dependență de terți; conectorii REST/JSON și SOAP cu autentificare mutuală pe certificate se activează prin configurare atunci când partenerii expun interfețe. Tablou de bord de integrare cu latențe, rate de eroare, reîncercări și SLA declarate separat pentru fiecare sistem partener.
11	Modulul 11 (cap. 5)	Forensic Intelligence și Clasificări. Cadru taxonomic multi-criterial (tip, gramaj, serie, metodă de falsificare, proveniență, infracțiune, infractor, victimă, localitate etc.) și mecanisme analitice pentru identificarea patternurilor, seriilor, rutelor și relațiilor între cazuri. Clasificările guvernate printr-un dicționar central versionat și auditat (Modulul 14); calitatea datelor monitorizată prin reguli de completitudine și consistență. Analizele (rețele de corelații, serii temporale) materializate în produse consumabile de management și operativ.	**Da, conform**	Model de clasificare multi-criterial, extensibil fără modificări de cod, alimentat exclusiv din dicționarul central versionat al Modulului 14, astfel încât modificarea unei taxonomii să nu invalideze datele istorice (fiecare înregistrare reține versiunea de clasificare aplicată). Motor analitic care identifică serii și patternuri prin corelarea atributelor comune între cazuri, cu vizualizare a rețelelor de relații (graf de legături persoană–obiect–loc–caz) și analiza seriilor temporale pe intervale configurabile. Reguli de calitate a datelor (completitudine, consistență, valori aberante) executate periodic, cu raport de conformitate și listă de înregistrări de corectat. Rezultatele sunt expuse ca produse analitice reutilizabile în Modulul 12.
12	Modulul 12 (cap. 5)	Rapoarte și Analitică. Concentrarea la nivel instituțional a tuturor rapoartelor: operaționale (CFL, AUP, EOD, Trageri, AFIS, Custodie, Registru, Corespondență, experți etc.), statistice, de conformitate și performanță. Filtrare avansată, export în PDF/XLSX și semnare electronică prin MSign pentru rapoartele oficiale, native. Consumarea de modele semantice curate din întregul sistem, astfel încât graficele și tabelele să fie consecvente și verificabile; cronologia generării rapoartelor.	**Da, conform**	Motor de raportare unic, alimentat dintr-un strat semantic definit peste modelul operațional (vizualizări materializate în PostgreSQL, reîmprospătate programat), astfel încât aceeași metrică returnează aceeași valoare indiferent de raportul care o consumă. Bibliotecă de rapoarte operaționale acoperind toate modulele, plus rapoarte statistice, de conformitate procedurală și de performanță SLA. Filtrare avansată combinată (perioadă, unitate, executor, tip, stare, taxonomie) cu salvarea filtrelor ca rapoarte personale sau instituționale. Export nativ PDF (JasperReports) și XLSX (Apache POI), cu semnare electronică prin MSign pentru rapoartele oficiale. Fiecare generare este înregistrată (cine, când, cu ce filtre, ce versiune de date), asigurând reproductibilitatea și verificabilitatea rezultatelor.
13	Modulul 13 (cap. 5)	Calitate, Audit. Controale organizaționale automate în punctele critice ale fluxurilor: validarea concluziilor de expertiză, predarea probelor, închiderea cazurilor complexe. Jurnale read-only protejate criptografic; orice abatere (ex. încercare de închidere fără	**Da, conform**	Motor de reguli de control aplicat la nivel de tranziție de stare, care blochează operațiunea neconformă înainte de persistare (nu doar o semnalează ulterior) și înregistrează tentativa în jurnalul de audit cu context complet. Controalele sunt configurabile pe puncte critice: validarea concluziilor, predarea probelor, închiderea cazurilor complexe. Jurnalele sunt stocate append-only, fără drept de modificare sau ștergere pentru niciun rol, inclusiv administrator, protejate prin înlănțuire

Nr.	Ref. Caiet de sarcini	Cerința autorității contractante	Confor-mitate	Soluția tehnică propusă de ofertant
		contrasemnătură) este blocată și semnalată. Măsurarea calității: rate de respingere la verificare, timpi de reverificare, cauze tipice ale neconformităților, vizibile în tablouri de bord și disponibile pentru audit intern sau extern.		de amprente SHA-256 și verificate periodic automat. Set de metrici de calitate: rata de respingere la verificare, timpul mediu de reverificare, clasificarea cauzelor de neconformitate, evoluția în timp pe unitate și executor, expuse în tablouri de bord și exportabile pentru audit intern sau extern.
14	Modulul 14 (cap. 5)	Administrare, Nomenclatoare și Configurații. Registru centralizat de taxonomii și liste controlate, cu versionare, ferestre de valabilitate, publicare etapizată și evaluare de impact. Gestionarea unităților, rolurilor, regulilor de formulare (câmpuri obligatorii per context), șabloanelor de documente și politicilor de timp/SLA aferente pașilor de flux din fiecare modul. Orice modificare produce urme de audit și note de publicare, iar acolo unde impactul este ridicat, necesită aprobări în logica „patru ochi”.	**Da, conform**	Registru central de nomenclatoare cu versionare completă: fiecare valoare are versiune, fereastră de valabilitate (valid de la / până la) și stare (ciornă, publicat, retras); înregistrările istorice păstrează versiunea aplicată la momentul creării, astfel încât rapoartele retroactive rămân corecte. Publicare etapizată cu mediu de pregătire și evaluare de impact automată (numărul de înregistrări afectate, module dependente) prezentată administratorului înainte de confirmare. Administrare a unităților organizatorice ierarhice, rolurilor și permisiunilor, regulilor de formulare per context (câmpuri obligatorii, vizibile, validări), șabloanelor de documente și politicilor SLA pe fiecare pas de flux din fiecare modul — toate configurabile prin interfață, fără dezvoltare. Fiecare modificare generează urmă de audit și notă de publicare; pentru modificările cu impact ridicat se aplică obligatoriu aprobarea „patru ochi”.
B. CERINȚE TEHNICE ȘI DE ARHITECTURĂ (cap. 6 din Caietul de sarcini)				
15	pct. 6.1	Arhitectură pe trei niveluri (3-tier) – interfață utilizator, logică de business, strat de date – cu separare strictă a componentelor pentru mentenanță, extindere și testare independentă. Comunicare între module prin servicii RESTful JSON, peste HTTPS/TLS 1.3.	**Da, conform**	Arhitectură 3-tier cu frontieră strictă între niveluri: prezentare (Angular 17, SPA/PWA), logică de business (Spring Boot 3.3 pe Java 21 LTS, cu separare pe straturi controller / service / domeniu, fără acces direct la persistență din controllere) și strat de date (Spring Data JPA și repository pattern peste PostgreSQL 16). Comunicarea integral prin API RESTful JSON, versionat și documentat OpenAPI 3.1 prin springdoc-openapi, exclusiv peste HTTPS cu TLS 1.3, cu HSTS activat și suite de cifruri restricționate. Fiecare nivel este testabil independent: teste unitare pe domeniu (JUnit 5), teste de integrare pe API cu baze de date reale efemere (Testcontainers) și teste end-to-end pe interfață (Cypress).
16	pct. 6.1	Sistem 100% web-based, accesibil prin browser, fără instalare locală, compatibil cu infrastructura beneficiarului. Funcționare optimă pe Chrome, Edge, Firefox și suport pentru rezoluții variate și dispozitive mobile (tablete și laptopuri de teren).	**Da, conform**	Aplicație integral web, fără componente instalabile pe stațiile de lucru. Compatibilitate testată pe ultimele două versiuni majore Chrome, Edge și Firefox. Interfață responsivă construită pe Angular Material și CDK Layout, proiectată mobile-first, validată pe rezoluții de la 1024×768 până la 4K și pe tablete de teren; controalele critice sunt dimensionate pentru utilizare tactilă cu mănuși. Livrarea ca PWA prin Angular Service Worker permite lucrul offline în modulul CFL fără instalare clasică. Testarea compatibilității se execută automat în pipeline-ul CI pe fiecare livrare.
17	pct. 6.1	Logica aplicației pe platformă enterprise robustă (ex. .NET 8 / Java EE / Python FastAPI), cu persistență într-un SGBD relațional performant (PostgreSQL / Oracle / MS SQL Server), optimizat pentru cerințe tranzacționale și de raportare. Utilizarea procedurilor stocate și a mecanismelor de integritate referențială. Utilizarea de platforme OpenSource care, la final, să nu includă costuri adiționale de tip licențe.	**Da, conform**	Backend pe platformă enterprise Java: Java 21 LTS (OpenJDK, licență GPLv2 cu Classpath Exception, fără costuri de licențiere) și Spring Boot 3.3 (Apache License 2.0), platformă enterprise matură, cu ciclu lung de suport și ecosistem stabil. Bază de date PostgreSQL 16 (licență PostgreSQL, open-source), optimizată separat pentru sarcina tranzacțională și pentru raportare. Integritate referințială impusă la nivel de schemă (chei externe, constrângeri CHECK și UNIQUE, tranzacții cu nivel de izolare adecvat, gestionate declarativ prin Spring Transaction Management); proceduri stocate și funcții PL/pgSQL pentru operațiunile critice de consistență (alocare numere de înregistrare, tranziții în lanțul de custodie, agregări de raportare). Migrări de schemă versionate și auditabile prin Flyway. Întregul stack propus este open-source: Java 21 / OpenJDK, Spring Boot 3.3, PostgreSQL 16, Angular 17 (MIT), Docker, Kubernetes, Nginx, MinIO, Redis, Keycloak (opțional), Grafana/Prometheus. Beneficiarul nu suportă niciun cost de licențiere nici la implementare, nici ulterior.
18	pct. 6.2	Respectarea cerințelor standardelor ISO/IEC 27001, 27002 și 27005 privind securitatea informațiilor și managementul riscurilor. Protejarea tuturor comunicațiilor prin criptare cu algoritmi puternici (de tip AES-256). Guvernarea accesului la funcționalități și date prin politici de autentificare și autorizare cu granularitate pe roluri și atribute (RBAC/ABAC).	**Da, conform**	Proiectarea, dezvoltarea și exploatarea sistemului se realizează în conformitate cu controalele ISO/IEC 27001 și 27002, iar analiza și tratarea riscurilor urmează metodologia ISO/IEC 27005; livrabilele includ registrul riscurilor, declarația de aplicabilitate a controalelor și politicile de securitate aferente sistemului. Criptare în tranzit prin TLS 1.3 și în repaus prin AES-256 (date sensibile la nivel de coloană, fișiere atașate, copii de siguranță). Gestionarea cheilor separat de date. Autorizare RBAC/ABAC prin Spring Security 6, aplicată consecvent pe API, interfață și interogări de date, conform Modulului 1.
19	pct. 6.2	Administrarea locală a utilizatorilor interni, cu autentificare pe bază de nume de utilizator și parolă și politici configurabile de complexitate, expirare și blocare a conturilor. Opțional, integrarea cu servicii externe de identitate (MPass) pentru SSO și, după caz, MFA, fără a condiționa funcționarea sistemului. Semnarea documentelor prin MSign sau prin mecanisme interne de validare și asumare, cu stocarea controlată a marcajelor temporale și a dovezilor de integritate.	**Da, conform**	Sistemul este pe deplin funcțional în regim autonom, cu administrare locală a conturilor: politici configurabile de complexitate, istoric al parolelor, expirare, blocare temporară și permanentă, deblocare controlată de administrator. Integrarea MPass este implementată ca modul opțional (Spring Security SAML2 / OAuth2 Client), activabil prin configurare, fără refactorizare și fără indisponibilitate în cazul în care serviciul extern nu este accesibil. Semnarea documentelor funcționează dual: prin MSign (semnătură electronică calificată, marcă temporală RFC 3161) sau prin mecanism intern de asumare (amprentă SHA-256, sigilare, lanț de integritate), opțiunea fiind stabilită de Beneficiar. Marcajele temporale și dovezile de integritate sunt stocate în arhivă digitală securizată, separată de documentul semnat.

Nr.	Ref. Caiet de sarcini	Cerința autorității contractante	Confor-mitate	Soluția tehnică propusă de ofertant
20	pct. 6.2 pct. 6.5	Fiecare acces, modificare, validare sau semnare generează urme de audit criptate și nealterabile, cu jurnalizare completă (identitate utilizator, acțiune, dată/oră, rezultat). Evenimentele critice marcate cu identificatori unici și agregate în rapoarte de integritate verificabile. Orice acțiune (introducere, modificare, ștergere, semnare, export, sincronizare) însoțită de urmă de audit inviolabilă, stocată criptat, accesibilă doar persoanelor autorizate, conținând utilizatorul, operațiunea, data, durata, rezultatul și sursa IP. Generarea automată de alerte de integritate la anomalii (tentative de ștergere, autentificări multiple, acces neautorizat) și rapoarte periodice către administratorul de securitate.	**Da, conform**	Subsistem de audit independent, cu stocare append-only și înlănțuire criptografică a înregistrărilor (fiecare intrare conține amprenta celei precedente), ceea ce face detectabilă orice alterare sau ștergere ulterioară. Captarea modificărilor la nivel de entitate se realizează prin Hibernate Envers, completată de interceptoare Spring AOP pentru operațiunile de citire, export și sincronizare. Fiecare înregistrare conține: identificator unic al evenimentului, identitatea utilizatorului, rolul efectiv, operațiunea, entitatea afectată, valorile anterioare și noi, data/ora cu precizie de milisecundă, durata, rezultatul și adresa IP sursă. Datele de audit sunt criptate în repaus și accesibile exclusiv rolurilor de audit și securitate, fără drept de modificare pentru niciun rol. Detectare automată a anomaliilor (tentative de ștergere, autentificări multiple eșuate, acces în afara programului, escaladare de privilegii) cu alertare imediată și rapoarte periodice programate către administratorul de securitate. Verificare automată de integritate a lanțului de audit, cu raport de conformitate.
21	pct. 6.3	Timp de răspuns sub 3 secunde pentru 95% dintre interogările uzuale și disponibilitate minimă de 99,5% în intervalele de lucru instituțional. Optimizarea bazei de date prin indexări, particionare și politici de arhivare automată a datelor istorice. Mecanisme de cache inteligent, gestionare a conexiunilor și limitare a resurselor. Proceduri automate de failover și replicare în timp real între instanțele active.	**Da, conform**	Obiectivele de performanță sunt asumate contractual și verificate prin teste de încărcare (k6/JMeter) executate în Etapa III și repetate înainte de recepția finală: P95 < 3 s pe interogările uzuale, la volumul și concurența convenite cu Beneficiarul. Optimizare prin indexare țintită (inclusiv indici parțiali și GIN pentru căutare full-text), particionare pe intervale temporale a tabelelor cu creștere mare (audit, custodie, corespondență) și politici automate de arhivare a datelor istorice, astfel încât performanța să nu se degradeze odată cu volumul. Cache distribuit Redis prin Spring Cache pentru nomenclatoare și rezultate de raportare, cu invalidare pe eveniment. Pool de conexiuni HikariCP, completat de PgBouncer la nivel de infrastructură; limitare de resurse și rate limiting pe API pentru a preveni degradarea. Replicare PostgreSQL în flux (streaming replication) cu instanță de rezervă sincronizată și failover automat; aplicația rulează în minimum două replici Kubernetes în spatele unui echilibrator de sarcină, cu sonde de sănătate Spring Boot Actuator (liveness/readiness) și reluare automată. Disponibilitatea este măsurată și raportată lunar prin Prometheus/Grafana (Micrometer).
22	pct. 6.4	Mecanisme de interoperabilitate configurabile pentru corelarea cu EVOFINDER, TRAFFIC și AFIS, bazate prioritar pe gestionarea locală a identificatorilor externi. La disponibilitatea unor API, activarea unor conectori standardizați prin REST/JSON sau SOAP, cu autentificare mutuală pe bază de certificate digitale. Documentarea completă a mapării câmpurilor și regulilor de sincronizare, incluzând definirea evenimentelor (create/update/delete), tratarea erorilor, reconcilierea datelor și arhivarea schimburilor. Jurnalizarea tuturor schimburilor într-un registru de audit; detectarea și gestionarea diferențelor de versiune și neconcordanțelor, automat sau cu intervenție umană controlată.	**Da, conform**	Implementare conform Modulului 10. Regimul implicit este cel prin identificatori externi gestionați local, care asigură funcționalitate completă fără dependență de disponibilitatea partenerilor. Conectorii REST/JSON (Spring WebClient) și SOAP (Spring Web Services) sunt prevăzuți arhitectural și se activează prin configurare, cu autentificare mutuală TLS pe bază de certificate digitale și rotație controlată a acestora. Livrabilele includ documentația completă de mapare câmp-la-câmp, regulile de transformare și validare, definirea evenimentelor create/update/delete, matricea de tratare a erorilor, procedura de reconciliere periodică și politica de arhivare a schimburilor. Toate schimburile sunt jurnalizate în registrul de audit inviolabil; neconcordanțele de date și diferențele de versiune sunt detectate automat, fiind rezolvate conform politicii configurate sau escaladate către operator atunci când impactul operațional ori juridic o impune.
23	pct. 6.6	Livrarea sistemului împreună cu un plan de continuitate și proceduri de recuperare în caz de dezastru (Disaster Recovery Plan). Copii de siguranță ale bazelor de date și fișierelor atașate realizate zilnic, criptate și păstrate în locații distincte. Menținerea a cel puțin șapte versiuni consecutive de backup. Restaurarea completă a sistemului în cel mult 6 ore de la incident. Verificări periodice de integritate ale backupurilor, automate și auditate.	**Da, conform**	Plan de continuitate a activității și Disaster Recovery Plan livrate ca documente distincte, cu RTO ≤ 6 ore și RPO stabilit de comun acord cu Beneficiarul (implicit ≤ 24 ore prin copie completă zilnică, reductibil la minute prin arhivarea continuă a jurnalelor WAL). Copii de siguranță zilnice ale bazei de date (pgBackRest) și ale depozitului de fișiere, criptate AES-256, replicate în minimum două locații distincte. Retenție de minimum 7 versiuni consecutive, cu politică extinsă (zilnic/săptămânal/lunar) configurabilă. Verificare automată de integritate după fiecare copie și restaurare de test programată periodic într-un mediu izolat, cu raport auditabil al rezultatului. Procedura de restaurare completă este documentată, cronometrată și demonstrată practic Beneficiarului în cadrul Etapei V.
C. ETAPELE DE IMPLEMENTARE ȘI METODOLOGIA DE EXECUȚIE (cap. 7 din Caietul de sarcini)				
24	pct. 7.1	Implementare etapizată, conform unei metodologii agile-controlate (Agile with gated milestones), pentru livrări iterative și verificabile, în strânsă colaborare cu Beneficiarul. Fiecare etapă încheiată printr-o recepție parțială documentată și un raport de validare ce confirmă atingerea obiectivelor.	**Da, conform**	Metodologie Agile cu jaloane controlate: sprinturi de două săptămâni cu demonstrație funcțională la finalul fiecăruia, grupate în șase etape delimitate prin porți de calitate. Trecerea la etapa următoare este condiționată de recepția parțială semnată de Beneficiar și de raportul de validare care confirmă atingerea obiectivelor și criteriilor de acceptanță convenite în prealabil. Reprezentantul Beneficiarului participă la planificarea și la demonstrația fiecărui sprint, având vizibilitate permanentă asupra progresului.
25	pct. 7.2 Etapa I	Analiza detaliată a cerințelor și modelarea de business: interviuri și workshop-uri cu structurile operative (criminalistică, balistică, EOD, AFIS, AUP etc.), documentarea proceselor existente și identificarea nevoilor. Livrabile: modelul AS-IS, analiza disfuncțiilor, modelul	**Da, conform**	Program de interviuri și workshop-uri structurate cu fiecare structură operativă vizată, conduse de analistul de business și de managerul de proiect, cu minute aprobate de participanți. Livrabile: modelul AS-IS al proceselor, analiza disfuncțiilor cu prioritizare, modelul TO-BE, dicționarul de date inițial, diagramele BPMN 2.0 pentru fluxurile principale și planul de integrare inter-sistem. Toate livrabilele sunt supuse reviziei formale și aprobate de Beneficiar înainte de închiderea etapei.

Nr.	Ref. Caiet de sarcini	Cerința autorității contractante	Confor-mitate	Soluția tehnică propusă de ofertant
		TO-BE, dicționarul de date inițial, diagrama de procese BPMN și planul de integrare inter-sistem.		
26	pct. 7.2 Etapa II	Arhitectură software și design detaliat: proiectarea arhitecturii logice și fizice, a modelelor de date, regulilor de securitate, schemelor de flux, API-urilor și structurii interfețelor. Aprobarea de către Beneficiar a prototipurilor UI/UX și a fluxurilor principale (CFL, Custodie, Trageri, AFIS, Rapoarte etc.).	**Da, conform**	Documentul de arhitectură (logică și fizică, diagrame de componente și de desfășurare), modelul de date detaliat, matricea de securitate pe roluri și atribute, schemele fluxurilor de stare, specificația API în OpenAPI 3.1 și biblioteca de componente Angular reutilizabile (design system intern bazat pe Angular Material). Prototipuri UI/UX interactive (Figma) pentru fluxurile principale, prezentate și aprobate de Beneficiar înainte de începerea dezvoltării, pentru a elimina reproiectările tardive.
27	pct. 7.2 Etapa III	Dezvoltare, integrare și testare internă: implementarea modulelor conform designului aprobat, cu testare unitară, integrare continuă și jurnalizare completă. Realizarea testelor de performanță, securitate și interoperabilitate, precum și a testelor de semnare MSign.	**Da, conform**	Dezvoltare iterativă cu integrare continuă (Jenkins, build Maven), analiză statică a codului (SonarQube) și verificare automată a dependențelor pentru vulnerabilități (OWASP Dependency-Check) la fiecare livrare. Acoperire prin teste unitare JUnit 5 și teste de integrare cu Testcontainers pe logica de business, cu prag minim de acoperire convenit cu Beneficiarul. Teste de performanță (k6/JMeter) pentru validarea pragurilor de la pct. 6.3, teste de securitate (SAST, DAST, scanare de dependențe și configurații) și teste de interoperabilitate pe conectorii Modulului 10. Testele de semnare se execută atât pe fluxul MSign, cât și pe mecanismul intern de asumare, pentru a valida ambele regimuri de exploatare.
28	pct. 7.2 Etapa IV	Testare de acceptanță la beneficiar (UAT): efectuarea testelor de conformitate și acceptanță pe baza scenariilor și datelor de probă convenite. Generarea rapoartelor UAT, documentarea neconformităților și corectarea iterativă până la obținerea acceptanței finale.	**Da, conform**	Mediu de acceptanță dedicat, identic ca structură cu producția, populat cu date de probă anonimizate convenite cu Beneficiarul. Scenarii de testare elaborate în comun și acoperind fiecare modul funcțional. Neconformitățile sunt înregistrate în sistemul electronic de management al proiectului, clasificate pe severitate, remediate iterativ și reverificate, cu raport UAT la fiecare ciclu. Acceptanța finală se acordă numai după închiderea tuturor neconformităților blocante și critice.
29	pct. 7.2 Etapa V	Implementare pilot și tranziție în producție: implementarea unei versiuni pilot într-o unitate de referință, analiza timpilor reali de flux, a performanței și uzabilității, cu alimentarea optimizării sistemului final. După validare, implementarea la scară națională.	**Da, conform**	Pilot într-o unitate de referință stabilită de Beneficiar, cu sprijin la fața locului și colectarea sistematică a indicatorilor reali: timpi efectivi pe fiecare pas de flux, performanță observată, incidente și observații de uzabilitate. Concluziile pilotului sunt consolidate într-un raport de optimizare, iar ajustările sunt implementate înainte de extinderea națională. Tranziția în producție se face conform unui plan de punere în funcțiune cu ferestre de mentenanță convenite, plan de revenire (rollback) documentat și verificare post-implementare.
30	pct. 7.2 Etapa VI	Suport post-implementare și transfer de cunoștințe: asigurarea suportului tehnic pe 12 luni, monitorizarea performanței și remedierea deficiențelor, precum și transferul complet de cunoștințe către echipa beneficiarului.	**Da, conform**	Suport tehnic asigurat 12 luni de la recepția finală, conform pct. 8.3. Monitorizare continuă a performanței și disponibilității prin Prometheus/Grafana, cu rapoarte lunare transmise Beneficiarului. Transfer de cunoștințe structurat către echipa IT a Beneficiarului: sesiuni tehnice practice, parcurgerea codului sursă și a arhitecturii, proceduri de exploatare, administrare, backup și restaurare, astfel încât Beneficiarul să poată prelua operarea integral la finalul perioadei.
31	pct. 7.3	Menținerea unui plan de management al calității bazat pe standardul ISO 9001, cu rapoarte periodice, registru de neconformități, evidența reviziilor și aprobărilor. Supunerea oricărui livrabil (documentație, cod, raport, test) reviziei formale și aprobării prin fluxul „patru ochi". Utilizarea unui sistem electronic de management al proiectului (JIRA / Redmine / Azure DevOps), accesibil beneficiarului, pentru urmărirea sarcinilor, erorilor și progresului.	**Da, conform**	Plan de management al calității elaborat conform principiilor ISO 9001, cu rapoarte periodice de calitate, registru al neconformităților și evidența completă a reviziilor și aprobărilor. Niciun livrabil nu este predat fără revizie formală: codul trece prin revizuire obligatorie de către un al doilea inginer înainte de integrare, iar documentația și rapoartele sunt aprobate prin fluxul „patru ochi", cu trasabilitate în sistem. Managementul proiectului se realizează în JIRA (sau Redmine / Azure DevOps, la opțiunea Beneficiarului), cu cont de acces acordat reprezentanților Beneficiarului pentru vizibilitate permanentă asupra sarcinilor, erorilor, sprinturilor și progresului.
D. DOCUMENTAȚIE, INSTRUIRE ȘI MENTENANȚĂ (cap. 8 din Caietul de sarcini)				
32	pct. 8.1	Documentație completă și actualizată, în format digital și tipărit: arhitectura generală a sistemului cu diagrame logice și fizice, fluxuri de date și integrare; manualul de instalare și configurare; manualul de administrare (utilizatori, roluri, securitate, backup, audit); manualul de utilizare pentru fiecare modul funcțional; ghidul de operare în teren și protocoalele de lucru offline; documentația API și specificațiile de interoperabilitate (EVOFINDER, TRAFFIC, AFIS); politicile de securitate și confidențialitate, inclusiv procedurile GDPR; planul de testare și rezultatele testelor de performanță; codul sursă în format CD. Redactare în limba română, cu terminologie tehnică și juridică adecvată, proprietate exclusivă a Beneficiarului.	**Da, conform**	Se livrează integral setul de documente solicitat, în format digital (PDF cu semnătură electronică) și tipărit: documentul de arhitectură cu diagrame logice și fizice și fluxuri de date și integrare; manualul de instalare și configurare; manualul de administrare acoperind utilizatori, roluri, securitate, backup și audit; manualul de utilizare separat pentru fiecare dintre cele 14 module; ghidul de operare în teren și protocoalele de lucru offline; documentația API (OpenAPI 3.1) și specificațiile de interoperabilitate pentru EVOFINDER, TRAFFIC și AFIS; politicile de securitate și confidențialitate, inclusiv procedurile GDPR; planul de testare și rezultatele testelor de performanță; codul sursă complet, comentat, pe suport optic, împreună cu istoricul depozitului de cod și scripturile de migrare a schemei. Toată documentația este redactată în limba română, cu terminologie tehnică și juridică adecvată, și devine proprietatea exclusivă a Beneficiarului.

Nr.	Ref. Caiet de sarcini	Cerința autorității contractante	Confor-mitate	Soluția tehnică propusă de ofertant
33	pct. 8.2	Sesiuni de instruire pentru toate categoriile de utilizatori: instruire generală pentru personalul criminalistic de teren privind utilizarea tuturor modulelor; instruire avansată pentru coordonatori privind gestionarea rapoartelor, fluxurilor și configurarea timpilor de execuție; instruire administrativă și tehnică pentru personalul IT privind instalarea, backupul și securitatea; instruire pentru management și analiză strategică privind modulele Rapoarte și Forensic Intelligence. Materiale de instruire incluzând prezentări, fișe de lucru, tutoriale video și ghiduri de bune practici.	**Da, conform**	Program de instruire structurat pe cele patru categorii solicitate, livrat în grupe, la sediul Beneficiarului sau în format mixt, cu exerciții practice pe mediul de instruire populat cu date de probă. Instruire generală pentru personalul de teren pe toate modulele operaționale; instruire avansată pentru coordonatori pe rapoarte, fluxuri și configurarea timpilor de execuție; instruire tehnică pentru personalul IT pe instalare, configurare, backup, restaurare și securitate; instruire pentru conducere pe modulele Rapoarte și Forensic Intelligence. Materialele livrate includ prezentări, fișe de lucru, tutoriale video înregistrate în limba română și ghiduri de bune practici, rămânând în proprietatea Beneficiarului pentru instruiri ulterioare proprii. Se organizează sesiuni de recapitulare după implementarea pilot.
34	pct. 8.3	Perioadă de mentenanță de minimum 12 luni după implementarea finală. Remedierea incidentelor în termen de maximum 24 h pentru cele critice și 5 zile lucrătoare pentru cele minore; actualizări periodice de securitate și optimizare a performanței; asistență tehnică online/telefonică în intervalul de lucru al beneficiarului; canal securizat de raportare a problemelor (portal suport / ticketing). La încheierea perioadei de mentenanță, beneficiarul deține toate drepturile asupra codului sursă, bazei de date, documentației și licențelor aferente.	**Da, conform**	Mentenanță asigurată 12 luni de la recepția finală, cu SLA asumat: incidente critice remediate în maximum 24 de ore, incidente minore în maximum 5 zile lucrătoare, cu confirmare de primire a sesizării în cel mult 4 ore lucrătoare. Actualizări periodice de securitate (inclusiv corectarea vulnerabilităților identificate în dependențe, monitorizate automat) și optimizări de performanță. Asistență tehnică online și telefonică în intervalul de lucru al Beneficiarului, cu persoane de contact nominalizate. Canal securizat de raportare prin portal de ticketing cu acces autentificat, evidența completă a sesizărilor, a termenelor și a soluțiilor, și raport lunar de respectare a SLA. La încheierea perioadei de mentenanță — și, de fapt, de la recepția finală — Beneficiarul deține integral drepturile asupra codului sursă, bazei de date, documentației și licențelor aferente; stack-ul propus fiind integral open-source, nu există licențe cu costuri recurente care să fie transferate.
35	Anunț de participare, pct. 12	Depunerea unei declarații pe proprie răspundere prin care să fie confirmată disponibilitatea de efectuare a ajustărilor tehnice pe o perioadă de 2 ani după finalizarea contractului.	**Da, conform**	Confirmăm disponibilitatea de a efectua ajustările tehnice necesare pe o perioadă de 2 ani după finalizarea contractului, inclusiv adaptarea la modificările cadrului normativ, corectarea deficiențelor constatate, optimizări de performanță și actualizări de securitate. Declarația pe proprie răspundere aferentă este depusă separat, ca document distinct al ofertei.

Data completării: 25.08.2026

Semnat: _____ (semnătură electronică avansată calificată)

Nume, prenume: COLOSOV Alexei

Funcţia în cadrul firmei: Director

Denumirea firmei: „AKDEV SOLUTIONS” S.R.L.

IDNO: 1015600025259

Adresa: Republica Moldova, mun. Chișinău, str. M. Sadoveanu 17, of. 321

Digitally signed by Colosov Alexei
Date: 2026.08.25 10:02:24 EEST
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ