# Caiet de sarcini
# privind achiziționarea serviciilor de dezvoltare a SIA ”Urmărire penală: E-Dosar”

1. **Autoritatea contractantă:** Procuratura Generală a Republicii Moldova
2. **Adresa:** mun. Chișinău, bd. Ștefan cel Mare și Sfânt, 73
3. **IDNO:** 1006601003865
4. **Tip procedură achiziție:** Licitație deschisă
5. **Obiectul achiziției:** Servicii de dezvoltare a SIA ”Urmărire penală: E-Dosar”
6. **Sursa alocațiilor bugetare:** buget de stat
7. **Cod CPV:** 72212900-8
8. Caietul de sarcini este întocmit în scopul achiziționării Serviciilor de dezvoltare a SIA ”Urmărire penală: E-Dosar”.

Digitally signed by Dimitraș Marcel
Date: 2020.10.01 15:44:59 EEST
Reason: MoldSign Signature
Location: Moldova

| Nr. d/o | Cod CPV | Denumirea serviciilor | Un. de măs. | Canti-tatea | Specificarea tehnică deplină solicitată, Standarde de referință |
|---|---|---|---|---|---|
| 1 | 72212900-8 | Servicii de dezvoltare a SIA ”Urmărire penală: E-Dosar” | buc | 1 | **Cerințe funcționale a SIA ”Urmărire penală: E-Dosar”:**<br>- Migrarea SIA ”Urmărire penală: E-Dosar” pe una din bazele de tip Enterprise MS SQL, Oracle, PostgreSQL cu opțiunile disponibile de clusterizare, care nu presupune un cost de licență sau costul de licență va fi inclus în oferta ca poziție separata;<br>- Crearea unei baze de date noi optimizată pentru citire și exportul în arhivă;<br>- Configurarea unui proces/flux de restabilire a dosarelor din arhivă, pentru consultare, sau reluarea urmăririi penale;<br>- Ajustarea fluxurilor curente prin exportul automat a dosarului și tuturor documentelor aferente;<br>- Exportul log-urilor (evenimentele jurnalizate) mai vechi de un an în arhivă;<br>- Integrarea cu sistemele terțe relevante SIA RSUD (Registrul de stat al unităților de drept), SIA RSP (Registrul de stat al populației), SIA RST (Registrul de stat al transporturilor), SIA ECCRPP (Sistemul informatic de evidență a cauzelor contravențiilor, amenzilor și a persoanelor care le-au desfășurat), SIA IGPF (Sistemul informațional al Departamentului Poliție de Frontieră), etc., prin intermediul MConect;<br>- Integrarea cu serviciile MPass/MSign/ MNotify/ MLog, cu posibilitatea prelungirii certificatelor de tip server pentru utilizarea MPass/MSign;<br>- Adăugarea certificatelor de tip server pentru criptarea traficului browser-server.<br>- Reconfigurarea de pe HTTP pe HTTPS;<br>- Automatizarea infrastructurii pe o scalare orizontală prin containerizarea sistemului SIA ”Urmărire penală: E-Dosar” cu posibilitatea utilizării soluției de orchestrare a containerelor (Kubernetes);<br>- Configurarea formularelor tipizate prin intermediul instrumentelor grafice care sunt prevăzute în SIA ”Urmărire penală: E-Dosar”, cu opțiunea de configurare a formularelor de documente (șabloane) din interfața grafică;<br>- Crearea bazei de date externe pentru arhivă și migrarea tuturor dosarelor cu o soluție finală în această bază;<br>- Exportul evenimentelor mai vechi de 1 an sau 6 luni într-un sistem extern/bază de date specializată pentru monitorizarea și analiza evenimentelor (log monitoring analysis tools);<br>- Crearea unei baze de date suplimentare pentru informația analitică (data warehouse/analytics platform), sau crearea unor tabele separate în baza de date de „arhivă” și reconfigurarea rapoartelor statistice;<br>- Configurarea proceselor resurse umane și transferul automatizat al drepturilor de vizualizare/accesare a dosarelor de transfer, detașare, delegare a angajaților în altă subdiviziune, promovare în funcție sau retrogradare, etc.<br>**Cerințe non-funcționale a SIA ”Urmărire penală: E-Dosar”:**<br>- Aplicarea în medii containerizate a diferitor componente ale sistemului de operare, *middleware, baze de date, etc*., cu utilizarea tehnologiilor informaționale de ultima generație.<br>- Includerea în ofertă a informației detaliate privind platforma tehnologică recomandată ținând cont de necesitățile Procuraturii stabilite în acest caiet de sarcini.<br>**Cerințe de interoperabilitate cu alte sisteme informatice:**<br>- Interfețele, fluxurile de mesaje expuse în SIA ”Urmărire penală: E-Dosar”, trebuie să fie bazate pe standarde deschise.<br>- Interacționarea interfețelor din SIA ”Urmărire penală: E-Dosar” cu alte aplicații externe atît în regim real, cat și în regim off-line.<br>- Integrarea mecanismelor bidirecționale de integrare prin API bine structurate, securizate și documentate.<br>- Posibilitatea generării de documente noi, schimb de informații între subdiviziunile Procuraturii, etc. cu accesarea tuturor funcțiilor ale sistemului.<br>- Interfețe standard pentru exportul datelor în cadrul instrumentelor de tipul *Data Warehouse*.<br>**Cerințe de performanță a SIA ”Urmărire penală: E-Dosar”:**<br>- Timpul de răspuns la o solicitare utilizator/serviciu extern nu trebuie să depășească o secundă.<br>- Gestionarea 1000 de sesiuni concurente (conexiuni utilizatori autorizați și sisteme externe).<br>- Includerea în ghidurile de administrare și operare a sistemului informație privind procesele ce pot diminua performanța SIA ”Urmărire penală: E-Dosar” și recomandările sale privind rularea concurentă a acestor procese (*exemplu: nu se recomanda rularea procesului X de generare a rapoartelor zilnice, simultan cu procesul Y de generare a copiei de rezervă*).<br>- Generarea rapoartelor și accesarea informației în scopul analizei fără afectarea performanței operaționale a sistemului la nivel de procesare.<br>- În documentația sistemului vor fi identificate rapoartele cu impact semnificativ asupra performanței și formulate recomandările furnizorului privind generarea rapoartelor respective astfel încât să nu influențeze indicii de performanță a SIA ”Urmărire penală: E-Dosar”.<br>- Indicarea în ofertă a valorilor minime garantate pentru caracteristicele de performanță ale sistemului, cu referință la platforma tehnologica recomandată. Valorile minime garantate nu vor fi mai mici decît cele minime solicitate.<br>- Deținerea capacității de a procesa cel puțin 100000 de operațiuni pe zi. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | **Cerințe pentru mentenanță a SIA ”Urmărire penală: E-Dosar”:**<br>- Deținerea mecanismelor de monitorizare a nivelului de încărcare și funcționare pentru toate componentele cheie.<br>- Generarea notificări în cazul în care performanța componentelor sale degradează (exemplu: timpul de răspuns la interpelările utilizatorilor depășește 2 secunde).<br>- Ofertantul va enumera mijloacele ce vor fi utilizate la depanarea tehnică a sistemului.<br>- Elaborarea mecanismelor de către ofertant, care ar facilita funcțiile de administrare a sistemului cum ar fi: pornirea, resetarea, crearea copiei de rezervă a bazei de date și fișierelor de conținut, restaurarea funcționalității sistemului în baza copiei de rezervă, arhivare date istorice, pregătire date pentru rapoarte complexe, etc.)<br>- Posibilitatea implementării noilor versiuni livrate de furnizor fără a afecta configurările și componentele existente a arhitecturii SIA ”Urmărire penală: E-Dosar”, pentru interacțiunea cu sisteme informatice externe și interne ale Procuraturii.<br>- Posibilitatea de testare și dezvoltare a SIA ”Urmărire penală: E-Dosar” în vederea asigurării proceselor solicitate.<br>- Înregistrarea erorilor și excepțiilor în funcționarea sistemului nominalizat cu expunerea utilizatorilor în timpul de lucru cu SIA ”Urmărire penală: E-Dosar”, clar și explicit.<br>- Posibilitatea prelucrării a tuturor erorilor generate cu înregistrarea și posibilitatea analizei.<br>**Cerințe de scalabilitate a SIA ”Urmărire penală: E-Dosar”:**<br>- Configurarea sistemului pentru scalare automată la nivelul componentelor cheie (lag sensitive), atât pe verticală, cât și pe orizontală, fără a întrerupe funcționarea capacității de procesare*:* adăugarea automata de noi containere și efectuare balansare a încărcării.<br>**Cerințe pentru asigurarea securității SIA ”Urmărire penală: E-Dosar”:**<br>- Ofertantul va asigura securizarea sistemului conform politicii de securitate aprobate de către Procuratura Generală.<br>- Posibilitatea accesării funcțiilor sale doar după autentificarea cu succes a utilizatorului/administratorului.<br>- Ofertantul va oferi suport sistemului pentru cel puțin următoarele metode de autentificare: în bază de ID și parolă cu dublu factor de autentificare, M-Pass în calitate de mecanism de autentificare a utilizatorilor prin intermediul certificatului digital sau identității mobile.<br>- Înregistrarea utilizatorilor și a informației de profil aferentă acestora*:* ID, parola, nume, prenume, Email etc..<br>- Parolele utilizatorilor trebuie să fie protejate. Metoda de protejare a parolelor trebuie să asigure imposibilitatea interceptării, deducerii sau recuperării acestora.<br>- Definirea și implementarea seturilor de politici de utilizare a parolelor. Politicile trebuie să permită setarea cerințelor cel puțin pentru: complexitatea parolei; obligativitatea schimbării parolei; durata de viață a parolei; utilizarea repetată a parolelor; numărul de încercări de autentificare eșuată; dicționar de parole interzise.<br>- Sistemul informatic va furniza utilizatorului în timp util informație cu privire la aplicarea politicilor de utilizare a parolelor (exemplu: mesaj de expirare a parolei în **n** zile).<br>- Aplicarea diferențiată a politicilor de utilizare a parolelor pentru diferite grupuri de utilizatori.<br>- Blocarea, dezactivarea sau suspendarea conturilor utilizatorilor la nivel de aplicație.<br>- Integrarea cu servicii externe de tipul „ISP” (*Identity Services Providers*). Metodele de autentificare ce trebuie să fie susținute cu implicarea unui ISP extern sunt: ID și parola cu dublu factor de autentificare; Certificate X.509.<br>- Aplicarea diferențiată a metodelor de autentificare, în funcție de resursele accesate.<br>- Setarea numărului de conexiuni simultane ce pot fi inițiate de un utilizator.<br>- Setarea timpului de expirare a sesiunilor utilizatorilor în caz de inactivitate.<br>- Elaborarea mecanismelor eficiente de prevenire a preluării neautorizate a sesiunilor active inițiate de utilizatorii legitimi.<br>- Sesiunea de lucru în SIA ”Urmărire penală: E-Dosar” va fi blocată la solicitarea utilizatorului sau automat, la expirarea sesiunii utilizatorului.<br>**Cerințe față de mecanismul de autorizare în SIA ”Urmărire penală: E-Dosar”:**<br>- Posibilitatea gestiunii granulare a drepturilor de acces la toate obiectele sistemului informatic și acțiunile posibile asupra acestora*:* entități, proprietăți ale entităților, formulare electronice, meniuri, rapoarte, acțiuni de creare/vizualizare/actualizare/ eliminare.<br>- Definirea de grupuri de utilizatori și roluri în cadrul sistemului și asocierea utilizatorilor la aceste grupe și roluri.<br>- Acordarea drepturilor de acces la nivel de utilizator explicit, grup și rol. Un grup de utilizatori va putea conține mai multe subgrupuri/roluri. Un utilizator poate fi asociat unuia sau mai multor grupuri și roluri, drepturile sale de acces fiind determinate cumulativ.<br>- Acordarea drepturilor de acces bazate pe reguli de procese: modificarea documentului, stare, context dacă utilizatorul este autor sau dacă operațiunea se face într-un anumit interval de timp<br>- Permisiunea atribuiri temporare a drepturilor deținute de un utilizator, către un alt utilizator. Atribuirea va putea fi efectuată cu păstrarea sau suspendarea drepturilor deținute de utilizatorul către care se deleagă drepturile.<br>- Permisiunea ștergerii activităților administrative de către administrator.<br>- Furnizarea vizualizări și rapoarte privind drepturile de acces configurate. Acestea vor putea fi parametrizate în funcție de cel puțin următoarele criterii: grup de utilizatori/rol în, ID utilizator, entitate de business, proprietate aferentă entității de business, acțiuni admise.<br>**Cerințe față de mecanismul de validare a datelor de intrare/ieșire:**<br>- Deținerea mecanismelor pentru a preveni manipularea datelor de intrare (date de intrare parvenite de la utilizatorii autorizați, date de intrare parvenite de la aplicații externe) atât la nivel de aplicație cât și la nivel de bază de date.<br>- Acțiunile de modificare a datelor critice și sensibile în cadrul sistemului, vor fi efectuate prin intermediul formularelor, conform fluxului de lucru stabilit pentru aceste date critice.<br>- Efectuarea validării complete și independente a datelor pe partea de nivelul de prezentare, logicii, nivelul de date, în scopul asigurării integrității, completitudinii și corectitudinii datelor.<br>- Datele confidențiale nu vor fi stocate și accesate nesecurizat în fișiere log, caching, etc.<br>- Deținerea mecanismelor de protejare adițională a datelor confidențiale (exemplu: afișarea mascată a datelor, stocarea datelor în formă criptată, autentificarea repetată a utilizatorului etc.). |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | - Deținerea proceduri de rutină pentru verificarea și detectarea posibilelor coruperi a relațiilor de integritate a datelor, mecanisme adecvate pentru a preveni manipularea datelor stocate.<br>**Cerințe față de mecanismul de jurnalizare și audit a SIA "Urmărire penală: E-Dosar":**<br>- Deținerea componentelor de audit care vor colecta și gestiona centralizat înregistrările de audit la nivelul fiecărui modul al sistemului informatic.<br>- Componenta de audit va permite configurarea granulară a politicilor de audit.<br>- Posibilitatea stabilirii politicilor de audit la nivel de obiect/entitate/eveniment jurnalizat.<br>- Stabilirea caracteristicilor specifice evenimentelor ce trebuie să fie jurnalizate (exemplu: produse într-un anumit interval de timp, o anumita valoare a proprietarii entității de business).<br>- Fiecare înregistrare de audit va conține cel puțin: momentul în timp al producerii evenimentului; subiectul evenimentului (ID utilizator); obiectul sau entitatea afectată; evenimentul produs; adresa IP a sursei ce a inițiat evenimentul.<br>- Înregistrările de audit nu vor conține informație de proces confidențială.<br>- Jurnalizarea erorilor de audit nu trebuie să afecteze funcționarea normală a sistemului.<br>- Componenta de audit va utiliza ceasul de sistem setat la nivelul sistemului de operare în care rulează componenta de audit.<br>- Componenta de audit va deține un mecanism de arhivare a înregistrărilor de audit istorice. Procesul de arhivare va conține: frecvența, vechime date, format arhivare, destinație etc.).<br>- Generarea automată a notificări către persoanele responsabile la producerea anumitor evenimente de securitate, conform configurațiilor setate.<br>- Componenta de audit va putea fi integrată în baza standardelor deschise cu soluții de tipul SIEM (*Security Incident and Event Management*) în vederea preluării înregistrărilor de audit produse în cadrul sistemului, de către soluțiile respective.<br>- Fixarea versiunilor istorice ale datelor, ce vor fi considerate deosebit de senzitive.<br>- Activitățile de schimbare stări și responsabili înregistrări vor fi jurnalizate.<br>- Elaborarea mecanismelor pentru accesarea și procesarea evenimentelor jurnalizate, inclusiv filtrarea înregistrărilor de audit după orice câmp deținut și exportul acestora în format uzual. Instrumentele de audit ale sistemului vor putea fi utilizate și în scopul importului arhivelor cu fișiere de audit pentru activități de analiza ocazionale.<br>- Posibilitatea jurnalizării evenimentelor de proces în paralel și sincron prin intermediul sistemului guvernamental de jurnalizare *MLog*, mecanisme de configurare a evenimentelor de proces care vor fi jurnalizate alternativ și prin intermediul serviciului *MLog*.<br>**Cerințe față de mecanismul de gestiune a excepțiilor și erorilor:**<br>- Înregistrarea centralizată la toate excepțiile și erorile generate de componentele sale.<br>- La producerea unei erori, SIA "Urmărire penală: E-Dosar" va afișa utilizatorului un mesaj de eroare generic. Acesta poate conține un cod de eroare și un identificator unic al erorii, pentru a facilita implicarea serviciilor de suport.<br>- Toate erorile care vor expuse utilizatorilor în timpul de lucru cu SIA "Urmărire penală: E-Dosar" vor fi suficient de clare și sugestive.<br>- Deținerea instrumentelor necesare pentru analiza și procesarea înregistrărilor aferente excepțiilor și erorilor.<br>- Generarea automată a notificărilor către persoanele responsabile la producerea anumitor erori în funcționarea a componentelor sale.<br>**Cerințe de reziliență și continuitate a SIA "Urmărire penală: E-Dosar":**<br>- Implementarea instrumentelor pentru executarea procedurilor de generare automată a copiilor de rezervă și gestiune a copiilor de rezervă istorice.<br>- Deținerea mecanismelor de asigurare a integrității datelor în cazul căderilor la nivelul oricăror componente, restabilirea operativă a disponibilității și accesibilității în cazul unor incidente de continuitate, asigurarea a integrității datelor în cazul unor căderi accidentale la nivelul oricăror componente ale sale.<br>- Arhitectura SIA "Urmărire penală: E-Dosar" trebuie să fie rezistentă la căderi de componente și să nu dețină puncte singulare de cădere (SPOF).<br>**Cerințe fata ofertant:**<br>- Capacitatea organizațională și resurse umane (nr. specialiștilor TI angajați min. 15 persoane);<br>- Experiență de minim 7 ani în dezvoltarea sistemelor informatice<br>- Reputația profesională a organizației și a echipei, minim 5 scrisori de recomandare sau referințe de la beneficiari privind implementarea de sisteme informatice complexe;<br>- Proiecte de complexitate similare în sectorul public din Republica Moldova, cu prezentarea descrierilor activităților specifice, cu accent pe migrarea datelor (minim 2 proiecte); integrarea cu serviciile de platforma e-Gov (minim 2 proiecte); interoperabilitatea cu sistemele terțe enumerate prin intermediul MConnect (minim 2 proiecte); containerizarea și orchestrarea sistemelor prin intermediul docker si Kubernetes (minim 2 proiecte).<br>- Experiența în elaborarea și implementarea soluțiilor bazate pe PHP, PostgreSQL, MS SQL, My SQL, docker, Kubernetes.<br>- Copiile certificatelor: ISO 9001:2015; ISO 20000-1:2018; ISO 27001:2013; ISO 37001:2016;<br>- Certificat de conformitate al Sistemului de management al serviciilor în domeniul tehnologiei informației ISO/IEC 20000-1:2011 (sau similar) – copie – confirmată prin semnătură și ștampilă;<br>- Manager de Proiect, certificat PMI.<br>- Arhitect de sistem, min. 5 ani experiență, certificate în domeniul cloud, CV atașat cu descrierea activităților conform CPI.4.<br>- Inginer-programator x 2, min. 5 ani experiență in utilizarea tehnologiile specificate CPI.5.<br>- Inginer Devops, min. 2 ani experiență în utilizarea tehnologiilor docker, Kubernetes. |
| | | | | | ***Valoarea estimativă a lotului fără TVA 1 500 000,00 lei*** |

**Președintele grupului de lucru pentru achiziții _____ L.Ș**