JUDEȚUL MEHEDINȚI
CONSILIUL LOCAL AL MUNICIPIULUI DROBETA TURNU SEVERIN
DIRECȚIA DE ASISTENȚĂ SOCIALĂ
Str. Decebal nr.40, bl. A1, tel. 0252/329577, fax 0352/401029
E-mail:dasdts@dasdts.ro, Web:dasdts.ro

Nr. 3584 / 07.04.2026

Aprobat,
Director Executiv,
Alisa-Bianca Alstani

Alisa-Bianca Alstani
Semnat digital de Alisa-Bianca Alstani
Data: 2026.04.22 12:32:45 +03'00'

CAIET DE SARCINI

Achiziție servicii privind licențe, instalare, configurare și punere în funcțiune, pregătirea personalului, inclusiv pentru securitate cibernetică

în cadrul proiectului „Digitalizarea proceselor de asistență socială la nivelul Municipiului Drobeta-Turnu Severin”

Autoritatea Contractantă: Direcția de Asistență Socială Drobeta-Turnu Severin

Sursa de finanțare: Programul Regional Sud-Vest Oltenia 2021-2027

FIȘA ACHIZIȚIEI

Denumire beneficiar	Direcția de Asistență Socială Drobeta-Turnu Severin
Sediu beneficiar	Strada Decebal 40, Bloc A1, Drobeta-Turnu Severin, județul Mehedinți, România
Obiectul procedurii de achiziție	Servicii privind licențe, instalare, configurare și punere în funcțiune, pregătirea personalului, inclusiv pentru securitate cibernetică
Descrierea cheltuielii	Se solicită implementarea unei soluții informatice tip ERDP (Electronic Registered Delivery Platform) ce cuprinde (1) componentă de subscripție/servicii licențiere acces la soluție cloud SAAS pentru digitalizarea proceselor și a relației cu terții, produs de tip comercial disponibil prestatorului la momentul depunerii ofertei care include în mod nativ infrastructura de găzduire, actualizările de securitate și funcționale, precum și suportul tehnic standard; (2) componentă de servicii de parametrizare (personalizare) a soluției SAAS la nevoile Direcției de Asistență Socială Drobeta-Turnu Severin și subordonatelor raportat la procesele administrative și serviciile electronice specifice (inclusiv instalare și punere în funcțiune); și (3) componentă de servicii de pregătire a personalului, inclusiv pentru securitate cibernetică.
Cod CPV	Principal: 72260000-5 Servicii de software (Rev.2) Secundare: 72212900-8 Diverse servicii de dezvoltare de software si sisteme informatice (Rev.2); 80530000-8 - Servicii de formare profesionala
Tipul contractului	Servicii/Servicii în afara celor cuprinse în Anexa II
Investiția	Programul Regional Sud-Vest Oltenia 2021-2027, Acţiunea A - „Digitalizare în folosul cetățenilor”, Prioritatea 2 - „Digitalizare în beneficiul cetățenilor și al firmelor”
Durata de implementare	7 luni
Contract de finanțare	numărul 653 din 15.07.2025
Activități eligibile vizate	CAPITOLUL 2. Cheltuieli pentru operaționalizarea obiectivului de investiții IT&C (investiția de bază): 2.2 Licențe; 2.3.1. Instalare, configurare și punere în funcțiune licență/soft; CAPITOLUL 4 Cheltuieli pentru pregătirea personalului: 4.1 Pregătirea personalului, inclusiv pentru securitate cibernetică

CUPRINS

1 INTRODUCERE

Prezentul Caiet de Sarcini stabilește cerințele tehnice, funcționale, non-funcționale și de servicii pentru achiziția soluției informatice din cadrul proiectului **„Digitalizarea proceselor de asistență socială la nivelul Municipiului Drobeta-Turnu Severin”**. Ca parte a Documentației de Atribuire, acest document definește cerințele minimale și obligatorii pe baza cărora fiecare Ofertant își va elabora Propunerea tehnică și Oferta financiară.

În cadrul acestei proceduri, termenii de mai jos au următorul înțeles:

- **Autoritatea Contractantă/Achizitor**: **Direcția de Asistență Socială Drobeta-Turnu Severin**, instituția publică ce organizează procedura și va încheia contractul.
- **Beneficiar**: **Direcția de Asistență Socială Drobeta-Turnu Severin**, alături de cetățeni, mediul de afaceri și personalul propriu, care vor utiliza soluția implementată.
- **Prestator**: Orice operator economic care depune o ofertă și, în cazul desemnării drept câștigător, va implementa soluția și va presta serviciile solicitate.

Nerespectarea integrală a cerințelor specificate în acest document atrage după sine considerarea ofertei ca neconformă și respingerea acesteia în etapa de evaluare. Nu se acceptă depunerea de oferte alternative sau parțiale.

Orice referire la o anumită origine, marcă, brevet, standard sau similar va fi interpretată ca având mențiunea **„sau echivalent”**.

Ofertanții pot propune soluții tehnice superioare cerințelor minime, fără costuri suplimentare pentru Achizitor. Acestea vor fi luate în considerare doar dacă demonstrează un nivel calitativ superior.

2 CONTEXTUL REALIZĂRII ACESTEI ACHIZIȚII

2.1 Informații despre Autoritatea contractantă

Prezenta achiziție se realizează în cadrul proiectului „Digitalizarea proceselor de asistență socială la nivelul Municipiului Drobeta Turnu-Severin” (Cod SMIS: 327211), finanțat prin Programul Regional Sud-Vest Oltenia 2021-2027. Proiectul este implementat printr-un parteneriat între Municipiul Drobeta Turnu Severin, în calitate de Lider de proiect, și Direcția de Asistență Socială Drobeta Turnu-Severin, în calitate de Partener și Beneficiar al soluției informatice. În contextul prezentei proceduri, Direcția de Asistență Socială Drobeta Turnu-Severin acționează în calitate de Autoritate Contractantă.

2.1.1 Descrierea autorității contractante (partener – Direcția de Asistență Socială Drobeta Turnu-Severin)

Direcția de Asistență Socială (DAS) Drobeta Turnu-Severin este instituția publică aflată în subordinea Consiliului Local al municipiului Drobeta Turnu-Severin. Misiunea sa principală este aplicarea politicilor sociale în domeniul protecției copilului, familiei, persoanelor vârstnice, persoanelor cu dizabilități și altor persoane sau comunități aflate în dificultate. Instituția funcționează în baza prevederilor Legii asistenței sociale nr. 292/2011.

Principalele activități desfășurate de DAS vizează acordarea de servicii sociale destinate: a) Prevenirii și combaterii sărăciei și riscului de excluziune socială, adresate persoanelor și familiilor fără venituri sau cu venituri reduse, persoanelor fără adăpost și victimelor traficului de persoane. b) Prevenirii și combaterii violenței domestice, prin centre de primire în regim de urgență, centre de recuperare, locuințe protejate, centre de consiliere și centre destinate agresorilor. c) Sprijinirii persoanelor cu dizabilități, prioritizând serviciile de îngrijire la domiciliu, centrele de zi, asistență și suport. d) Asistării persoanelor vârstnice, prin servicii de îngrijire personală la domiciliu sau în centre rezidențiale pentru persoanele vârstnice dependente sau singure. e) Protecției și promovării drepturilor copilului, incluzând servicii de prevenire a separării copilului de părinți și consiliere familială.

2.1.2 Descrierea liderului de proiect (Municipiul Drobeta Turnu-Severin)

Unitatea Administrativ Teritorială Municipiul Drobeta Turnu-Severin este persoană juridică de drept public, funcționând în baza Codului Administrativ (O.U.G. nr. 57/2019). Instituția se concentrează pe gestionarea urbană și dezvoltarea durabilă. Primăria Municipiului Drobeta Turnu-Severin deține o vastă experiență în atragerea și implementarea fondurilor europene (începând din 2005, cu peste 100 de proiecte implementate în ultimii 15 ani), demonstrând capacitatea de a administra resursele și de a coordona diversele părți interesate pentru atingerea obiectivelor comune de dezvoltare durabilă și inovație socială.

2.1.3 Contextul achiziției și activități afectate de rezultatele serviciilor

Pentru o înțelegere corectă a necesității acestei achiziții de către potențialii ofertanți, este important cunoașterea contextului operațional actual al Autorității Contractante. Direcția de Asistență Socială Drobeta Turnu-Severin nu a făcut subiectul unui proces consolidat și integrat de transformare digitală.

În prezent, instituția nu dispune de capabilități digitale elementare, precum registratură electronică, arhivă electronică, management de documente electronice, management de fluxuri electronice sau capabilități de semnare și sigilare electronică calificată. Drept consecință, întreaga activitate a DAS se desfășoară predominant pe suport de hârtie.

De asemenea, instituția nu dispune de interconectivitate cu alte instituții publice, acționând în mod insular. Această situație generează nevoia de a transpune în format de hârtie toată corespondența, conducând la o fragmentare a serviciilor publice furnizate și la o sarcină administrativă semnificativă.

Rezultatele serviciilor ce vor fi achiziționate (implementarea unui sistem informatic integrat) vor afecta în mod direct și fundamental modul de desfășurare a tuturor activităților administrative și de furnizare a serviciilor sociale. Implementarea soluției va transforma modul în care sunt furnizate serviciile publice și va îmbunătăți eficiența administrativă.
Activitățile care vor fi afectate includ digitalizarea fluxurilor de lucru interne la nivelul tuturor structurilor DAS Drobeta-Turnu Severin, cum ar fi:

- **Management (Director Executiv):** Emiterea dispozițiilor, notelor de serviciu, constituirea comisiilor de concurs și evaluare.
- **Serviciul de Asistență Socială:** Gestionarea cererilor privind venitul minim de incluziune, referate de înhumare, dosarele beneficiarilor Cantinei de ajutor social, gestionarea ajutoarelor de urgență/înmormântare și a stimulentelor educaționale (tichete sociale pentru grădiniță).
- **Serviciul Protecție Specială și Monitorizare:** Gestionarea dosarelor beneficiarilor de indemnizații, efectuarea și gestionarea anchetelor sociale pentru evaluare/reevaluare conform Legii nr. 448/2006, monitorizarea activității asistenților personali.
- **Serviciul Protecția Persoanelor Vârstnice:** Gestionarea dosarelor electronice de îngrijire la domiciliu, contracte de furnizare servicii, anchete sociale pentru instituționalizare, rapoarte de monitorizare.
- **Serviciul Protecția Drepturilor Copilului:** Gestionarea electronică a dosarelor de plasament, anchete sociale pentru centre de zi, verificarea minorilor aflați în situații de risc social.
- **Resurse Umane, Financiar-Contabil și Juridic:** Gestionarea electronică a dosarelor de personal, cererilor de concediu, planului anual al achizițiilor publice, facturilor, angajamentelor bugetare, ordonanțărilor de plată, precum și a acțiunilor și întâmpinărilor juridice.
- **Secretariat, Administrativ, Arhivă, Registratură:** Întregul proces de primire a corespondenței externe, transpunerea în format electronic și transmiterea pe fluxuri digitale către structurile specializate.

Prin această achiziție, Autoritatea Contractantă urmărește standardizarea modului de lucru, asigurarea conformității legale în generarea actelor administrative în format electronic, reducerea birocrației prin eliminarea proceselor redundante bazate pe hârtie și asigurarea interconectivității și interoperabilității sistemelor publice.

2.2 Informații despre contextul care a determinat achiziționarea serviciilor

Achiziționarea acestor servicii este determinată de un context strategic european și regional care vizează accelerarea transformării digitale, aliniat la Programul de politică Deceniul Digital 2030 al Uniunii Europene. Oportunitatea specifică este dată de lansarea Programului Regional Sud-Vest Oltenia 2021-2027, apelul „Digitalizare în beneficiul cetățenilor".
Prezenta achiziție reprezintă componenta esențială a proiectului de investiții „Digitalizarea proceselor de asistență socială la nivelul Municipiului Drobeta Turnu-Severin". Scopul achiziției este implementarea unei soluții informatice integrate care să adreseze decalajele semnificative existente în digitalizarea serviciilor publice locale.

2.2.1 Contextul general și regional

Contextul actual este marcat de întârzieri în adoptarea tehnologiilor digitale. Conform Indicelui economiei și societății digitale (DESI) 2022, România se situează pe ultimul loc în UE la dimensiunea Servicii publice digitale. În regiunea Sud-Vest Oltenia, utilizarea serviciilor de e-guvernare este foarte scăzută (9%). Această situație este cauzată de probleme sistemice precum lipsa de interoperabilitate a sistemelor IT, nivelul redus de integrare al bazelor de date, ceea ce conduce la fragmentarea serviciilor publice și la o sarcină administrativă semnificativă.

2.2.2 Identificarea problemelor și constrângerilor autorității contractante

Pentru a elabora o propunere optimă, ofertanții trebuie să înțeleagă problemele și constrângerile specifice cu care se confruntă Direcția de Asistență Socială (DAS) Drobeta Turnu-Severin. Instituția nu a făcut niciodată subiectul unui proces consolidat și integrat de transformare digitală, iar capacitatea instituțională de a concepe tranziția către fluxuri operaționale digitale este limitată.
Constrângerile majore care au condus la necesitatea achiziționării acestor servicii sunt:

1. **Activitate desfășurată integral pe suport de hârtie:** Instituția nu dispune de capabilități digitale elementare. Lipsesc instrumentele precum: registratură electronică, arhivă electronică, managementul documentelor și fluxurilor electronice, precum și capabilități de semnare și sigilare electronică calificată. Dependența de hârtie generează ineficiențe și o povară administrativă considerabilă.
2. **Lipsa interconectivității și operarea insulară:** Instituția acționează în mod insular, fără interconectivitate electronică cu alte instituții publice. Această constrângere impune transpunerea în format de hârtie a întregii corespondențe interinstituționale.
3. **Complexitatea proceselor și volumul mare de lucru:** Autoritatea Contractantă gestionează procese interne și interinstituționale complexe, deservind un număr semnificativ de cetățeni (5341 de beneficiari de asistență socială). Gestionarea acestui volum prin metode tradiționale, pe hârtie, afectează eficiența și timpul de răspuns al instituției.
4. **Absența serviciilor publice online:** Serviciile publice aflate în competența DAS nu sunt disponibile cetățenilor prin intermediul unei platforme online, operând exclusiv în regim de back-office.

Achiziția serviciilor de digitalizare este esențială pentru a depăși aceste constrângeri, pentru a standardiza modul de lucru, a reduce birocrația și a asigura tranziția către un sistem digital eficient și interoperabil.

2.3 Informații despre beneficiile anticipate de către Autoritatea Contractantă

Prin achiziționarea și implementarea serviciilor de digitalizare, Autoritatea Contractantă anticipează o transformare fundamentală a modului său de operare. Rezultatele serviciilor achiziționate vor influența direct performanța instituțională, vizând creșterea eficienței administrative, asigurarea conformității legale și îmbunătățirea semnificativă a calității serviciilor publice furnizate. Beneficiile sunt anticipate pentru instituție, angajați, precum și pentru cetățeni și mediul de afaceri.

2.3.1 Beneficii anticipate la nivel instituțional (îmbunătățirea performanței)

Autoritatea Contractantă se așteaptă la îmbunătățiri substanțiale ale eficienței operaționale și ale capacității decizionale:

1. **Creșterea productivității și eficienței:** Se anticipează o creștere a productivității la nivelul instituției de 50%, prin economii de timp și creșterea randamentului angajaților. Aceasta se va realiza prin eliminarea activităților manuale repetitive (precum colectarea, sortarea, clasificarea, indexarea, capturarea manuală a datelor, stocarea și distribuirea fizică) și prin standardizarea modului de lucru.
2. **Îmbunătățirea procesului decizional și a vitezei de reacție:** Se estimează o creștere a vitezei de reacție instituțională cu aproximativ 60%. Acest beneficiu va fi generat de automatizări precum preluarea continuă a cererilor, repartizarea automatizată a solicitărilor și automatizarea procesului de colectare a semnăturilor (necondiționat de prezența fizică a semnatarilor). De asemenea, se anticipează un nivel de acces la date îmbunătățit cu circa 80%, facilitând analiza rapidă și luarea deciziilor informate.
3. **Reducerea costurilor operaționale:** Se estimează o scădere de minim 70% a costurilor anuale cu hârtia, consumabilele și expedierea corespondenței (în anul 3 de exploatare). Se vor eficientiza și costurile prin reducerea nevoii de mentenanță pentru sisteme informatice disparate.
4. **Reducerea birocrației:** Eliminarea proceselor administrative redundante sau perimate determinate de modul de lucru tradițional pe hârtie.

2.3.2 Beneficii privind conformitatea, interoperabilitatea și securitatea

Implementarea soluției va asigura alinierea la standardele digitale și de securitate:

1. **Conformitate legală:** Asigurarea conformității legale în generarea actelor administrative în format electronic și respectarea condițiilor de valabilitate ale acestora.
2. **Interconectivitate și Interoperabilitate:** Asigurarea schimbului eficient de date între sistemele publice, facilitând o mai bună colaborare și partajare rapidă a informațiilor între instituții.
3. **Aplicarea Principiului „O singură dată” (Once Only):** Interoperabilitatea instituțională va crea condițiile fundamentale pentru respectarea acestui principiu în relația cu cetățeanul.
4. **Securitate cibernetică avansată:** Protejarea integrată a datelor, aplicațiilor și rețelelor; gestionarea securizată a accesului la resurse; prevenirea atacurilor cibernetice și minimizarea timpului de reacție prin automatizarea proceselor, notificărilor și reacțiilor.

2.3.3 Beneficii pentru angajați

Se așteaptă o îmbunătățire semnificativă a competențelor digitale ale angajaților. Accesul la instrumente de lucru inovative va facilita munca, va crește productivitatea și va îmbunătăți satisfacția acestora în exercitarea atribuțiilor curente de serviciu.

2.3.4 Beneficii pentru cetățeni și mediul de afaceri (digitalizarea relației cu terți)

Proiectul va genera o creștere semnificativă a calității actului administrativ și a ratei de adopție a serviciilor digitale:

1. **Accesibilitate sporită:** Asigurarea unui punct de acces centralizat la serviciile publice. Administrația va fi accesibilă prin cloud, permițând solicitarea și primirea documentelor de oriunde și oricând.
2. **Servicii de calitate superioară:** Upgrade-ul sistemic al serviciilor publice la gradul 5 de sofisticare digitală (automatizate, personalizate și centrate pe utilizator).
3. **Economie de timp:** Eliminarea cozilor și a necesității deplasărilor fizice la instituție.
4. **Trasabilitate:** Cetățeanul va avea un istoric clar al interacțiunilor sale cu administrația.

2.4 Factori interesați și rolul acestora

Implementarea serviciilor de digitalizare implică interacțiunea și gestionarea așteptărilor unui număr semnificativ de factori interesați. Conștientizarea rolurilor și așteptărilor acestora este esențială pentru ofertanți în vederea înțelegerii complexității activităților și a relațiilor care trebuie gestionate pe perioada derulării contractului.
Principalii factori interesați identificați sunt:

2.4.1 Beneficiarul final al serviciilor și utilizatorii

- **Direcția de Asistență Socială (DAS) Drobeta Turnu-Severin (Autoritatea Contractantă):** Este beneficiarul principal al investiției.
    - *Rol:* Definirea cerințelor strategice și operaționale, asigurarea cadrului necesar implementării și adoptarea soluției la nivel instituțional.

- *Așteptări:* Implementarea unei soluții informatice funcționale, conforme cu specificațiile tehnice și legale, care să conducă la standardizarea proceselor, creșterea eficienței administrative și asigurarea interoperabilității.

- **Personalul DAS (utilizatori direcți):** Cei 54 de angajați ai DAS (personal de conducere și de execuție) care vor utiliza sistemul informatic în activitatea curentă.
  - *Rol:* Utilizarea zilnică a platformei, participarea la sesiuni de instruire și furnizarea de feedback în fazele de testare.
  - *Așteptări:* Un sistem intuitiv și stabil, care să simplifice sarcinile administrative, să reducă munca manuală și să ofere acces la instrumente de lucru inovative.
- **Cetățenii și mediul de afaceri (utilizatori indirecți):** Inclusiv cei 5341 de beneficiari de asistență socială ai municipiului Drobeta Turnu-Severin.
  - *Rol:* Utilizarea platformei online pentru accesarea serviciilor publice, depunerea solicitărilor și comunicarea cu Autoritatea Contractantă.
  - *Așteptări:* Accesibilitate sporită (de oriunde, oricând), economie de timp, eliminarea deplasărilor fizice și trasabilitatea interacțiunilor.

2.4.2 Factori interesați implicați în managementul și aprobarea rezultatelor

Acești factori vor interacționa direct cu Contractantul pe perioada derulării contractului.

- **Unitatea de implementare a proiectului (UIP) din cadrul DAS și al Primăriei Drobeta-Turnu Severin :** Echipa internă formată din Manager de Proiect, Responsabil Comunicare, Responsabil IT, Responsabil Manager Financiar, Responsabil Achiziții Publice și Responsabil Consilier Juridic.
  - *Rol:* Coordonarea generală a implementării, monitorizarea activităților Contractantului, asigurarea conformității tehnice și juridice, validarea și aprobarea livrabilelor și a rapoartelor de progres. UIP este principalul punct de contact pentru Contractant și reprezintă interesele Beneficiarului în relația cu acesta.
  - *Așteptări:* Respectarea riguroasă a termenelor, calității și obiectivelor contractuale; comunicare proactivă și profesionalism.
- **Municipiul Drobeta Turnu-Severin (Lider de proiect):**
  - *Rol:* Supervizarea generală a proiectului în parteneriat și asigurarea sustenabilității financiare.
  - *Așteptări:* Implementarea cu succes a investiției în conformitate cu Contractul de Finanțare și atingerea indicatorilor asumați.

2.4.3 Autorități implicate în gestionarea asistenței financiare nerambursabile

Deciziile acestor factori pot influența activitatea Contractantului și fluxul financiar al proiectului.

- **Agenția pentru Dezvoltare Regională Sud-Vest Oltenia (ADR Sud-Vest Oltenia) – Autoritatea de Management (AM):**
  - *Rol:* Monitorizarea implementării proiectului, verificarea conformității achizițiilor și a eligibilității cheltuielilor, aprobarea cererilor de rambursare/plată.
  - *Așteptări:* Respectarea strictă a legislației privind fondurile europene și a cerințelor finanțatorului, raportare transparentă și corectă.

2.4.4 Alți factori interesați (parteneri instituționali)

- **Instituții subordonate (ex. Creșa Drobeta):**
  - *Rol:* Adoptarea și utilizarea sistemului informatic standardizat pentru serviciile specifice (ex. educaționale).
  - *Așteptări:* O soluție care să răspundă nevoilor specifice, menținând interoperabilitatea cu DAS.
- **Autorități publice centrale și locale (ex. ANAF, RECOM, Primărie, DGASPC, Trezorerie):**
  - *Rol:* Parteneri de interoperabilitate pentru schimbul electronic de date.
  - *Așteptări:* Schimb de date securizat, eficient și conform cu standardele naționale de interoperabilitate.

Complexitate și potențiale conflicte de așteptări

Complexitatea proiectului derivă din necesitatea de a alinia așteptări diverse. Un potențial conflict poate apărea între așteptările personalului DAS (care în prezent lucrează exclusiv pe hârtie) privind ușurința în utilizare și timpul necesar pentru adaptarea organizațională, și cerințele stricte de conformitate tehnică și termenele de implementare impuse de UIP și AM. Contractantul va trebui să gestioneze aceste dinamici prin comunicare eficientă și un plan de management al schimbării robust.

3 DESCRIEREA SERVICIILOR SOLICITATE

3.1 Descrierea situației actuale la nivelul Autorității Contractante

Situația actuală la nivelul Direcției de Asistență Socială (DAS) Drobeta Turnu-Severin, în legătură cu serviciile care fac obiectul prezentului contract, a fost determinată printr-o analiză detaliată documentată în Studiul de Fezabilitate și Proiectul Tehnic aferente proiectului. Această analiză a stabilit că Autoritatea Contractantă nu a făcut anterior subiectul unui proces consolidat și integrat de transformare digitală.

3.1.1 Infrastructura de aplicații și soluții în uz

În prezent, la nivelul instituției nu există servicii publice disponibile cetățenilor prin intermediul unei platforme online (front-office).
Singura soluție software utilizată constă într-o licență pentru un modul informatic dedicat exclusiv utilizării interne (back-office). Acest modul gestionează informațiile despre beneficiarii de venit minim garantat, ajutor pentru încălzirea locuinței și ajutor pentru susținerea familiei, limitându-se la calculul cuantumului ajutoarelor și emiterea dispozițiilor aferente. Nivelul de digitalizare a activităților de front-office și back-office este, prin urmare, scăzut și neuniform.

3.1.2 Capabilități digitale și procese operaționale

Instituția nu dispune de capabilități digitale elementare, iar întreaga activitate operațională și administrativă se desfășoară pe suport de hârtie.
În mod specific, la nivelul DAS lipsesc următoarele sisteme esențiale care urmează a fi implementate prin prezentul contract:

- Registratură electronică;
- Arhivă electronică;
- Sistem de management al documentelor electronice;
- Sistem de management al fluxurilor electronice de lucru (workflow management);
- Capabilități de semnare și sigilare electronică calificată.

3.1.3 Interconectivitate și Securitate

Instituția operează în mod insular, nefiind interconectată electronic cu nicio altă instituție publică. Acest lucru necesită transpunerea pe suport de hârtie a întregii corespondențe interinstituționale. De asemenea, instituția nu dispune de mijloace electronice integrate pentru asigurarea securității cibernetice, a protecției datelor cu caracter personal sau pentru managementul identității electronice a cetățenilor.

3.1.4 Infrastructura hardware și de comunicații

Autoritatea Contractantă dispune de infrastructura de comunicații (rețea locală) și de echipamentele necesare (dispozitive fixe și mobile) care vor permite personalului accesarea și exploatarea în condiții de securitate a viitoarei soluții informatice de tip SaaS (Software as a Service).

3.1.5 Abilități digitale ale personalului

Modul de lucru actual, bazat integral pe hârtie, impune necesitatea îmbunătățirii competențelor digitale ale angajaților pentru a asigura tranziția eficientă către utilizarea sistemelor informatice care fac obiectul prezentului contract.

3.2 Obiectivul general la care contribuie realizarea serviciilor

Realizarea serviciilor incluse în prezentul Caiet de Sarcini contribuie direct la atingerea obiectivului general al proiectului „Digitalizarea proceselor de asistență socială la nivelul Municipiului Drobeta Turnu-Severin". Acest obiectiv este aliniat la Obiectivul Specific 1.2 al Programului Regional Sud-Vest Oltenia 2021-2027 și vizează transformarea digitală a administrațiilor publice locale.
Obiectivul general strategic la care contribuie serviciile este valorificarea avantajelor digitalizării, în beneficiul cetățenilor, al companiilor, al organizațiilor de cercetare și al autorităților publice.

3.2.1 Impactul Contractului de servicii

Serviciile care fac obiectul acestui contract sunt instrumentul principal prin care Autoritatea Contractantă (Direcția de Asistență Socială Drobeta Turnu-Severin) va realiza tranziția de la modul de lucru actual, bazat integral pe hârtie și caracterizat de lipsa interoperabilității (așa cum a fost descris în capitolul Context), la o administrație digitală eficientă.
În mod operațional, impactul contractului se va concretiza prin punerea la dispoziția cetățenilor și persoanelor juridice din cadrul Municipiului Drobeta-Turnu Severin a unui punct de acces centralizat la toate serviciile sociale aflate în responsabilitatea instituțiilor publice din cadrul municipiului.
Prin realizarea acestor servicii și atingerea obiectivului general, Direcția de Asistență Socială Drobeta Turnu-Severin își asumă rolul de lider la nivel local pentru atingerea obiectivelor programului regional și se constituie ca un contribuitor la atingerea țintelor asumate de România la nivel european în domeniul digitalizării.

3.3 Obiectivele specifice la care contribuie realizarea serviciilor

Serviciile achiziționate trebuie să asigure transformarea digitală a Direcției de Asistență Socială Drobeta Turnu-Severin și a instituțiilor subordonate. Obiectivul strategic este realizarea unui upgrade sistemic al tuturor serviciilor publice aflate în responsabilitatea instituției la gradul 5 de sofisticare digitală, caracterizat prin servicii online automatizate, personalizate și centrate pe utilizator. Această cerință acoperă integral serviciile publice specifice domeniului asistenței sociale (servicii și beneficii sociale) și relațiilor publice (ex. petiții, audiențe).
Serviciile achiziționate vor asigura atingerea obiectivului general prin realizarea următoarelor obiective specifice:

1. **Adoptarea de noi tehnologii:** Implementarea soluțiilor tehnice necesare în vederea îmbunătățirii semnificative a calității serviciilor publice aflate în competența Autorității Contractante.
2. **Standardizarea proceselor:** Uniformizarea modului de lucru la nivelul Direcției de Asistență Socială, al instituțiilor subordonate și al partenerilor instituționali cu care aceasta colaborează în mod regulat.

3. **Creșterea interoperabilității:** Asigurarea unui grad sporit de interconectivitate și interoperabilitate cu toate entitățile publice și private care dețin atribuții în buna desfășurare a serviciilor publice la nivel local.
4. **Dezvoltarea de servicii electronice avansate:** Crearea de funcționalități noi în legătură cu serviciile publice electronice puse la dispoziția cetățenilor, mediului de afaceri și altor autorități sau instituții publice.
5. **Dezvoltarea de funcționalități noi:** Crearea de funcționalități noi în legătură cu serviciile publice electronice puse la dispoziția cetățenilor și mediului de afaceri.

Pentru a atinge nivelul 5 de sofisticare, soluția trebuie să implementeze capabilități tehnice care asigură automatizarea proceselor, incluzând (dar nelimitându-se la):

- Automatizarea proceselor de convertire în format PDF a documentelor.
- Automatizarea proceselor de preluare, înregistrare și repartizare a solicitărilor.
- Automatizarea completă a proceselor de colectare a semnăturilor.
- Automatizarea proceselor de arhivare electronică și de expediere a conținutului.
- Automatizarea proceselor de notificare a utilizatorilor.
- Automatizarea completă a creării identității electronice a utilizatorilor.
- Personalizarea accesului la serviciile publice în funcție de atribute specifice ale utilizatorilor.

Prin realizarea acestor servicii, DAS Drobeta-Turnu Severin contribuie la atingerea țintelor asumate de România la nivel european în cadrul Deceniului Digital, vizând atingerea nivelului de 100% servicii publice digitale până în decembrie 2029.

3.4 Activitățile ce vor fi realizate.

Se solicită implementarea unei soluții informatice tip Platformă de distribuție electronică înregistrată - ERDP (Electronic Registered Delivery Platform) ce cuprinde (1) componentă de subscripție/servicii licențiere acces la soluție cloud SAAS pentru digitalizarea proceselor și a relației cu terții, produs de tip comercial disponibil prestatorului la momentul depunerii ofertei care include în mod nativ infrastructura de găzduire, actualizările de securitate și funcționale, precum și suportul tehnic standard; (2) componentă de servicii de parametrizare (personalizare) a soluției SAAS la nevoile Direcției de Asistență Socială Drobeta-Turnu Severin și subordonatelor raportat la procesele administrative și serviciile electronice specifice (inclusiv instalare și punere în funcțiune); și (3) componentă de servicii de pregătire a personalului, inclusiv pentru securitate cibernetică, după cum urmează:

3.4.1 Servicii de licențiere acces la soluție cloud SAAS.

În vederea eficientizării activității beneficiarului va fi implementată o soluție informatică interinstituțională, interconectată și interoperabilă, produs de tip comercial disponibil prestatorului la momentul depunerii ofertei, înțelegând prin aceasta o arhitectură distribuită de instanțe diferite având la bază un nucleu comun, fiecare instanță fiind capabilă să asigure guvernanța specifică contextului funcțional particular și să acționeze interconectată și în mod interoperabil cu toate celelalte, beneficiind de propriile instrumente și interfețe de lucru.

Având în vedere nivelul foarte ridicat de complexitate al soluției informatice, ansamblul extrem de variat de nevoi specifice fiecărui participant, provocările ridicate de diversitatea de resurse software și hardware pe care fiecare dintre entitățile implicate le dețin, precum și riscurile ce decurg din acestea cu privire la posibilitatea de a influența succesul proiectului, Autoritatea Contractantă apreciază că abordarea potrivită pentru prezentul proiect reprezintă o infrastructură de tip cloud care să nu depindă de resursele tehnice și umane existente ale nici unuia dintre participanți. Astfel, va fi asigurată deopotrivă eficientizarea activității de la nivelul actorilor interni instituției și subordonatelor, precum și al celor externi (cetățeni, mediu de afaceri, instituții) prin accesibilitate (de oriunde, oricând și de pe orice dispozitiv), reducerea costurilor operaționale asociate, fluidizarea circulației informațiilor și documentelor specifice între participanți, creșterea gradului de trasabilitate operațională și asigurarea unui nivel crescut de transparență decizională.

Soluția va include un mediu de lucru colaborativ sigur care va permite și va facilita:

- digitalizarea fluxurilor interne specifice și instituționale (suport) / digitalizarea proceselor;
- digitalizarea interacțiunii cu terți (prin terț se înțeleg diferite entități cu care Direcția de Asistență Socială Drobeta-Turnu Severin intră în contact: cetățeni, societăți comerciale, instituții etc);
- pregătirea sistemului pentru interoperabilitate cu alte instituții/unități (integrare/consolidare și replicare date),

oferind accesul la serviciile electronice specifice activității instituției și asigurând prin elementele arhitecturale integrate atât canale de comunicare interne și cu terți, cât și funcționalități adecvate lucrului în mediul digital.

Concret, soluția digitală implementată va asigura cumulativ:

- un mediu de lucru colaborativ digital intern, integrând și subordonatele;
- un mediu de lucru colaborativ digital interoperabil între instituție și terți;
- acoperirea completă a serviciilor publice digitale ce implică în mod tradițional prezența la instituție;
- transparență, predictibilitate și trasabilitate în operare;
- conformitate cu reglementările europene și naționale relevante în vigoare.

Utilizatorul final al soluției implementate trebuie să poată accesa, exploata soluția și transmite feedback cu privire la experiența avută, independent de tehnologie și respectând principiile orizontale prevăzute în reglementările europene și naționale, în conformitate cu prevederile legale și independent de aspectele de dizabilitate, sex, origine, religie sau orientare sexuală.

Soluția ofertată va integra funcționalități pentru managementul identităților electronice, înregistrarea operațiunilor administrative (registratură, managementul fluxurilor, formulare tipizate), interconectare și interoperabilitate, arhivare electronică, semnare și sigilare electronică, securitate și audit.
Având în vedere că Autoritatea Contractantă:

- are actualmente 54 funcționari cu atribuții operaționale efective în activitatea curentă,
- estimează la nivelul unui an aplicarea sigiliului electronic pe un număr maxim de 15000 documente,
- își exercită competențele în colaborare cu entități juridice,

în vederea realizării livrabilelor și atingerii rezultatelor așteptate ale Proiectului, Prestatorul asumă în sarcina sa prin costul ofertat următoarele:

- ➢ acordarea licenței de acces la soluția cloud SAAS ofertată pe durata a 5 ani începând cu data recepției/acceptanței, pentru instituție, funcționari, cetățeni și reprezentanți persoane juridice, fără a limita numărul acestora (livrabil 1), inclusiv asigurarea continuității serviciului (găzduire/comunicații/interconectări), dreptul de actualizare la noile versiuni (update/upgrade/parametrizare) și suport tehnic;
- ➢ parametrizarea soluției propuse raportat la structura organizației, procesele administrative și serviciile electronice specifice Direcției de Asistență Socială Drobeta-Turnu Severin și subordonatelor (inclusiv instalare și punere în funcțiune; livrabil 2);
- ➢ instruirea personalului, inclusiv pentru securitate cibernetică pentru 54 utilizatori-funcționari (livrabil 3);
- ➢ punerea în funcțiune: soluția configurată este livrată oficial, testată și acceptată de beneficiar, fiind gata de a intra în producție.

În afara serviciilor solicitate și fără a majora prețul prestației, Prestatorul poate dezvolta și implementa în soluția ofertată noi funcționalități adițional celor cuprinse în Caietul de sarcini.
Asigurarea serviciilor operaționale în perioada de sustenabilitate post garanție este asumată de Autoritatea Contractantă.

Activitatea de formare/instruire va fi furnizată pentru numărul de funcționari/personal contractual solicitat în baza unui program ce va fi agreat de părți, înaintea demarării activității, pe baza unei metodologii ce va cuprinde cel puțin următoarele condiții:

- Obiectivul programului va viza îmbunătățirea nivelului de cunoștințe și abilități digitale ale cursanților (formare profesională) în vederea folosirii corecte și eficiente la locul de muncă a soluției informatice implementate în cadrul proiectului;
- Durata activității de formare/instruire va include 2 componente:
    - una de învățare teoretică, sesiuni de maxim 6 ore / zi;
    - una de învățare practică - sesiuni de 4 ore /zi.

Ofertanții vor prezenta programa de curs, alcătuită astfel încât să cuprindă aspecte cu privire la riscurile de securitate și la modul în care își pot proteja dispozitivele și datele. Acest lucru include instruirea privind recunoașterea e-mailurilor de tip „phishing", utilizarea parolelor puternice și alte bune practici de securitate.
Cursanții vor primi un certificat de participare emis de entitatea care furnizează programul de formare/instruire.
Pentru adopția eficientă a personalului, contractantul va pune la dispoziția achizitorului, pe întreaga durată de prestare a serviciilor, un mediu de învățare cu aceleași funcțiuni implementate pe mediul de producție.

3.5 Rezultatele care trebuie obținute în urma prestării serviciilor. Livrabilele contractului.

Implementarea Contractului în conformitate cu prevederile prezentului Caiet de Sarcini trebuie să conducă cel puțin la atingerea următoarelor rezultate finale măsurabile așteptate, realizate în termenele prezentate raportat la data semnării contractului (corelate cu cele de finalizare ale activităților proiectului și structura serviciilor solicitate), după cum urmează:

Nr. crt.	Activitate (Etapă) / Servicii prestate	Livrabil / Rezultat așteptat Termen
1	Licențiere acces la soluție cloud SAAS pentru digitalizarea proceselor și a relației cu terții.	Licența de acces la soluția IT pentru digitalizarea proceselor și a relației cu terții este acordată, pentru instituție și subordonate fără a limita numărul funcționarilor ori numărul de cetățeni / reprezentanți persoane juridice ce pot accesa sistemul, respectiv: ● Structura departamentelor instituției este definită, rolurile, registrele și grupele de documente sunt parametrizate și active operațional; ● Activitățile specifice administrării sistemului (alte parametrizări, roluri) sunt realizate, și conturile pentru numărul de utilizatori funcționari solicitat sunt activate; ● Funcționalitățile specifice soluției digitale (front-office și back-office) sunt realizate și disponibile cetățenilor și firmelor; ● Funcționalitățile specifice fluxurilor back-office sunt implementate și disponibile

		operațional interconectat la nivel interinstituțional (se testează capabilitatea în sine raportat la funcționalitățile solicitate, respectiv transportul de date și trasabilitatea manifestată interactiv la nivelul fluxului din perspectivele actorilor); *termen: 3 luni de la semnarea contractului*
2	Parametrizarea soluției SAAS la nevoile Direcției de Asistență Socială Drobeta-Turnu Severin și subordonatelor raportat la procesele administrative și serviciile electronice specifice.	Funcționalitățile specifice proceselor administrative și serviciilor electronice ale Direcției de Asistență Socială Drobeta-Turnu Severin și subordonatelor (front-office și back-office) sunt parametrizate la nivelul structurilor și disponibile cetățenilor și firmelor. *termen: 5 luni de la semnarea contractului*
3	Servicii de pregătirea personalului, inclusiv pentru securitate cibernetică.	Serviciile de pregătirea personalului, inclusiv pentru securitate cibernetică pentru 54 utilizatori-funcționari sunt prestate. *termen: 6 luni de la semnarea contractului*

3.6 Atribuțiile și responsabilitățile părților

3.6.1 Atribuțiile prestatorului

Prestatorul este pe deplin responsabil pentru:

1. Asigurarea tuturor resurselor care sunt în sarcina sa pentru buna derulare a Contractului;
2. Asigurarea planificării resurselor în raport cu graficul estimat prezentat pentru derularea Contractului;
3. Îndeplinirea obligațiilor sale cu respectarea celor mai bune practici din domeniu, a prevederilor legale și contractuale, urmărind asigurarea îndeplinirii obiectivelor stabilite;
4. Prestarea serviciilor în conformitate cu cerințele prezentului Caiet de sarcini;
5. Asigurarea garanției, continuității serviciului (găzduire/comunicații/interconectări), dreptul de actualizare la noile versiuni (update/upgrade/parametrizare) și suport tehnic;
6. Colaborarea cu personalul Achizitorului pentru serviciile desfășurate conform Contractului (monitorizarea progresului activităților în cadrul Contractului, coordonarea activităților în cadrul Contractului, feedback).

3.6.2 Atribuțiile achizitorului

Achizitorul este responsabil pentru:

1. Asigurarea tuturor resurselor care sunt în sarcina sa pentru buna derulare a Contractului;
2. Punerea la dispoziția Prestatorului a tuturor informațiilor disponibile pentru obținerea rezultatelor așteptate;
3. Exercitarea responsabilităților privitoare la rezultatele proiectului: recepția și verificarea rezultatelor, furnizarea rezultatului evaluării către Prestator în termenul prevăzut în documentația de atribuire.

3.7 Garanție

Pentru soluția IT de digitalizare (componenta software/SaaS), garanția de funcționare, mentenanța și suportul tehnic se acordă pe o perioadă de 5 ani, calculată de la data semnării procesului-verbal de recepție finală și punere în funcțiune, acoperind întreaga perioadă de subscripție contractată. Pentru serviciile de implementare, garanția privind viciile ascunse este conformă prevederilor legale.
Prin asigurarea garanției se înțelege că ofertantul asumă în sarcina sa prin costul ofertat realizarea operațiunilor de suport tehnic și remediere a oricărei disfuncționalități față de cerințele caietului de sarcini sau agreate formal de părți pe perioada implementării, ori la disfuncționalități care împiedică funcționarea, în întreg sau în afara parametrilor acceptabili, a uneia sau mai multor componente ale sistemului.
În vederea asigurării conformității cu cerințele privind disponibilitatea serviciilor (SLA), subscripția include actualizările legislative, tehnice și funcționale relevante.

Pentru semnalarea în perioada de garanție a defectelor identificate pe parcursul utilizării soluției ofertate, prestatorul va pune la dispoziția beneficiarului cel puțin următoarele modalități de comunicare:

- Acces la o aplicație web specializată de tip helpdesk pentru raportarea disfuncționalităților / Alternativ o soluție pentru raportarea disfuncționalităților încorporată în sistem;
- Un responsabil dedicat pentru suport tehnic, disponibil în zilele lucrătoare în intervalul orar 8-17.

Fiecare incident de suport este caracterizat de un nivel de prioritate, care va evidenția impactul acestuia asupra funcționalităților produsului.
Nivelele de prioritate sunt:

- Critic - incidentul are impact major asupra utilizatorilor produsului. Problema împiedică desfășurarea activității Autorității Contractante;

- Mare - impact semnificativ asupra utilizatorilor produsului. Problema împiedică desfășurarea în condiții normale a activității Autorității Contractante. Nici o soluție alternativă nu este disponibilă, activitatea autorității contractante poate totuși continua, însă într-un mod restrictiv;
- Mediu - impact mediu asupra desfășurării activității Autorității Contractante. Problema afectează minor funcționalitățile produsului. Impactul reprezintă un inconvenient care necesită soluții alternative pentru refacerea funcționalităților;
- Minor - impact minim asupra desfășurării activității Autorității Contractante. Problema nu afectează funcționalitățile produsului. Rezultatul este o eroare minoră care nu împiedică desfășurarea în bune condiții a activității Autorității Contractante.

Prestatorul trebuie să asigure disponibilitatea serviciilor de suport tehnic. În cazul incidentelor cu prioritate „critic" intervenția va fi asigurată 24x7, din momentul primirii sesizării și până la remedierea definitivă a problemei și asigurarea funcționalității integrale a produsului. Prestatorul va trebui să respecte următorii timpi de răspuns, corelați cu nivelul de prioritate a incidentului:

Nivel prioritate	Timp de răspuns	Timp de rezolvare
Critic	o oră	o zi
Mare	2 ore	2 zile
Mediu	4 ore	2 zile lucrătoare
Minor	4 ore	3 zile lucrătoare

Înainte de efectuarea operațiunilor de mentenanță, prestatorul comunică autorității contractante lista operațiunilor de mentenanță care trebuie efectuate.
Operațiunile de mentenanță vor fi realizate în afara orelor normale de lucru (Luni-Vineri 08:00-17:00) sau în sărbători legale.

3.8 Principii generale

care trebuie respectate în implementarea și parametrizarea soluției propuse:

- ❖ Principiul legalității, care presupune crearea și exploatarea sistemului informațional în conformitate cu legislația națională în vigoare, a normelor și standardelor internaționale recunoscute în domeniu;
- ❖ Principiul datelor sigure, presupune introducerea datelor în sistem doar prin canale autorizate, autentificate și criptate;
- ❖ Principiul securității informaționale, presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și de acces nesancționat;
- ❖ Principiul accesibilității informației cu caracter personal, care presupune implementarea procedurilor de asigurare a accesului solicitanților la informația cu caracter care îi privește și care este stocată de soluția informatică;
- ❖ Principiul transparenței, presupune proiectarea și implementarea sistemului conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informaționale și de telecomunicații;
- ❖ Principiul expansibilității, stipulează posibilitatea extinderii și completării sistemului informațional cu noi funcții sau îmbunătățirea celor existente;
- ❖ Principiul integrării cu produsele de program existente, presupune posibilitatea soluției informatice de a se integra și interacționa cu aplicațiile, serviciile și bazele de date implementate în cadrul autorităților publice și instituțiilor din România;
- ❖ Principiul simplității și comodității utilizării, presupune proiectarea, realizarea și implementarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor sistemului, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție;
- ❖ Principiul neutralității și adaptării tehnologice, presupune că sistemul trebuie să se orienteze pe cerințele funcționale, asigurând accesul la serviciul informatic public independent de tehnologii sau produse specifice;
- ❖ Principiul îmbinării publicității și confidențialității, prevede publicarea informației general accesibile, cu excepția informației recunoscute ca fiind confidențială, în modul stabilit de legislația națională în vigoare;
- ❖ Principiul protecției datelor cu caracter personal și al datelor sensibile, prevede crearea și exploatarea sistemului de evidentă a serviciilor publice în conformitate cu acordurile și convențiile internaționale, precum și cu legislația națională în vigoare în domeniul protecției datelor cu caracter personal;
- ❖ Principiul identificării unice, prevede faptul că toate obiectele informaționale de evidentă trebuie să aibă un număr unic de identificare;
- ❖ Principiul controlului, prevede controlul măsurilor ce asigură calitatea, fiabilitatea resurselor și sistemelor informaționale, precum și păstrarea și utilizarea rațională a acestora.

4 CERINȚE GENERALE PRIVIND SOLUȚIA TEHNICĂ

4.1 Aspecte generale

Proiectul TIC ce se dorește a fi implementat în activitatea curentă a Direcției de Asistență Socială Drobeta-Turnu Severin și a instituțiilor subordonate urmărește asigurarea accesului cetățenilor și mediului de afaceri la toate serviciile publice oferite de instituție, alături de interconectarea și interoperabilitatea între Direcția de Asistență Socială Drobeta-Turnu Severin și toate instituțiile subordonate în vederea digitalizării complete a fluxurilor de comunicare interne și interinstituționale.
Soluția ofertată trebuie să permită un management integrat al sarcinilor de serviciu zilnice în cadrul instituției și în relația cu alte entități publice sau private, cetățeni sau persoane juridice.

Soluția este destinată să asigure:

- Deplina conformitate cu legislația națională și europeană în ceea ce privește activitățile administrației publice și gestionarea serviciilor publice aflate în responsabilitate.
- Standardizarea și uniformizarea proceselor interne și a instrumentarului digital utilizat la nivelul tuturor instituțiilor vizate.
- Interconectarea și interoperabilitatea între instituții la nivel local/județean/regional pentru a se asigura schimbul de date și documente.
- Asigurarea pentru cetățeni și mediul de afaceri a unui punct de acces centralizat la serviciile publice gestionate de instituțiile din subordinea Direcției de Asistență Socială Drobeta-Turnu Severin
- Scăderea poverii administrative determinată de modul de lucru tradițional pe hârtie.

Sub aspect tehnic soluția informatică va îndeplini cerințele unei **Platforme de distribuție electronică înregistrată** (*ERDP – Electronic Registered Delivery Platform*) care va include următoarele 6 componente logice arhitecturale: (1) managementul identităților electronice și autentificarea, (2) înregistrarea operațiunilor administrative și managementul documentelor, (3) interconectarea și interoperabilitatea inter și intra-instituțională, (4) arhivarea și îndosarierea electronică, (5) semnarea și sigilarea electronică calificată și (6) securitatea și auditul platformei. Soluția trebuie să integreze în mod unitar funcționalitățile componentelor antemenționate.
Notă: Structura componentelor arhitecturale prezentată nu este una impusă soluției propuse, ci urmărește să ofere ofertanților, pentru claritate și o bună înțelegerea nevoilor, o perspectivă structurată a cerințelor funcționale raportat la nevoile instituției și scopul urmărit prin implementarea proiectului. Arhitectura software a soluției informatice este la latitudinea ofertantului iar acesta va prezenta în propunerea sa tehnică arhitectura propusă.

Soluția ofertată trebuie să fie de tip „web-based", accesibilă și „responsive" front-office și back-office pe orice dispozitiv (desktop, tabletă, telefon), utilizând minim următoarele soluții de navigare internet (browser) precum Google Chrome, Microsoft Edge, Mozilla Firefox, Safari. Soluția ofertată trebuie să fie disponibilă pe orice tip de dispozitiv mobil de largă răspândire (android) prin aplicație nativă.

Având în vedere faptul că soluția propusă va stoca date personale ale rezidenților UE, ofertantul va prezenta informații relevante care să dovedească stocarea și gestionarea acestora sub incidența Regulamentului (UE) 679 din 27 aprilie 2016 - GDPR - privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestora.
Prestatorul trebuie să demonstreze că are implementată o procedură de management al incidentelor de securitate. În cazul unei breșe de securitate care afectează datele cu caracter personal, Prestatorul are obligația de a notifica Autoritatea Contractantă fără întârzieri nejustificate, și, dacă este posibil, în termen de maximum 24 de ore de la momentul constatării incidentului. Prestatorul va oferi asistență tehnică și organizațională Autorității Contractante pentru a putea răspunde cererilor venite din partea persoanelor vizate (dreptul la acces, rectificare, ștergere, portabilitate etc.

Soluția tehnică propusă va fi utilizată atât pentru operațiunile interne ale instituției și subordonatelor, cât și pentru a furniza servicii digitale. Având în vedere prevederile Directivei (UE) 2022/2555 privind măsurile pentru un nivel comun ridicat de securitate cibernetică în Uniune, precum și obligațiile ce îi revin în temeiul Ordonanței de Urgență nr. 155 din 30 decembrie 2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, Autoritatea Contractantă apreciază că asigurarea securității este o obligație justificată rezonabil pe care fiecare dintre ofertanți trebuie să și-o asume alături de costurile generate, cu caracter periodic, independent de cadrul ofertei.
Pe baza documentării anterioare realizată cu privire la aplicațiile informatice, Autoritatea Contractantă apreciază că în 12 luni o aplicație de acest tip poate suferi modificări substanțiale la nivelul codului sursă, motiv pentru care un nou audit este necesar pentru a reconfirma că nu există breșe de securitate în aplicație.
În același sens, având în vedere obligațiile Autorității Contractante de a fi conformă operațional cu cadrul național de interoperabilitate, se impune ca soluția informatică ce va fi implementată să respecte bunele practici de securitate cibernetică, asigurând astfel o precondiție minimă a interconectării cu alte sisteme.

Raportat la aceste aspecte, Autoritatea Contractantă solicită ofertanților să facă dovada auditării de securitate (test de penetrare sau echivalent) a soluției tehnice propuse și să fie în măsură să prezinte raportul final al auditului, atât la momentul depunerii ofertei cât și la intervale regulate de cel mult 12 luni pe durata prestării serviciilor.
Auditul trebuie să respecte bunele practici din industrie și să fie realizat de o terță parte, o entitate certificată în acest sens de către Autoritatea pentru Digitalizarea României (listă disponibilă la adresa web https://www.adr.gov.ro/lista-auditorilor-it) și să fie realizat cu nu mai mult de 12 luni vechime înainte de momentul ofertării. Acreditarea auditorilor de securitate de către Autoritatea pentru Digitalizarea României se face în baza OMCSI 553 din 2019.
În acest sens ofertantul va menționa în propunerea tehnică numele auditorului folosit și va anexa Raportul de audit întocmit de acesta.

Având în vedere că soluția tehnică propusă va presupune prelucrarea datelor unui număr mare de persoane, inclusiv prin corelarea seturilor de date și utilizarea de tehnologii avansate, Autoritatea Contractantă consideră că aceste operațiuni sunt susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice. Autoritatea Contractantă consideră de importanță critică asigurarea conformității legale privind riscurile legate de datele personale și implementarea măsurilor de protecție adecvate, protejarea confidențialității cetățenilor privind riscurile de acces neautorizat, scurgere de date sau utilizare abuzivă a informațiilor raportat la angajamentul instituției față de protecția datelor personale ale cetățenilor care utilizează sistemul. În conformitate cu Art. 35 din GDPR, se impune în mod obligatoriu realizarea unei Evaluări a Impactului asupra Protecției Datelor (DPIA).
Prin urmare, se solicită ofertanților să se angajeze la următoarele:
a) Prezentarea unei DPIA, cel târziu la momentul punerii în funcțiune a soluției.
b) Reevaluarea și prezentarea unei DPIA actualizate la intervale regulate, care nu vor depăși 12 luni, pe întreaga durată a contractului.
Se subliniază că DPIA este un proces continuu. Costurile aferente elaborării și actualizărilor periodice cad în sarcina exclusivă a ofertantului și trebuie asumate independent de cadrul ofertei.

Ofertantul va pune la dispoziția autorității contractante pe o perioadă de 10 zile lucrătoare de la data limită de depunere a ofertelor un mediu de testare funcțional al soluției informatice ofertate pentru a permite verificarea unui subset de patru funcționalități de bază solicitate prin Caietul de sarcini, respectiv va include componentele/funcționalitățile de registratură electronică, management al identității electronice, semnare și sigilare electronică și comunicare între funcționari și cetățeni/reprezentanții mediului de afaceri.
Pentru respectarea principiului proporționalității și pentru a nu angaja operatorii economici la cheltuieli suplimentare majore în faza de ofertare, mediul de testare solicitat presupune exclusiv punerea la dispoziție a unei instanțe a produsului comercial (SaaS) deja existent în portofoliul ofertantului. Această probă practică se limitează strict la demonstrarea funcționalităților critice de bază (out-of-the-box), fără a necesita dezvoltare software personalizată (care face obiectul Livrabilului 2) și nu reprezintă realizarea în avans a unei părți din contract.
În ceea ce privește interconectările necesare testării cu succes a acestora de către comisia de evaluare a ofertelor (altele decât cele obiect al personalizărilor proceselor în instituție solicitate în cadrul implementării), pentru a nu angaja costuri suplimentare sau realizarea unei părți din contract înainte de atribuire, demonstrația va respecta următoarele condiții:

1. Interconectări funcționale (live): Se vor prezenta funcțional integrările care confirmă maturitatea tehnică a soluției, respectiv și care nu necesită protocoale instituționale prealabile (având API și documentație de integrare sunt disponibilă gratuit și nerestricționat), respectiv:
    - Integrarea cu un furnizor de servicii de încredere (pentru validarea semnăturii/sigiliului);
    - Interconectarea tehnică cu ONRC/ANAF (pentru preluarea datelor persoanelor juridice), utilizând mecanisme standardizate/API-uri publice sau de test disponibile.
2. Interconectări simulate (mock-up): Pentru interconectările care depind strict de semnarea unor acorduri de colaborare sau tuneluri VPN securizate cu instituții terțe, se acceptă prezentarea prin simulare sau scenarii predefinite, pentru a demonstra capacitatea logică de procesare a fluxurilor, fără a fi necesară conexiunea operațională în timp real la momentul ofertării.

Scopul acestei cerințe rezidă în nevoia autorității contractante de a evita riscul implementării unei soluții experimentale, respectiv una care nu a atins nivelul de maturitate minim adecvat și pentru a se asigura că ofertanții au înțeles corect nevoile instituției și dețin soluții potrivite pentru adresarea eficientă a acestora.
Mediul de testare va constitui element suport în evaluarea conformității ofertelor, respectiv asigură aprecierea obiectivă a faptului că soluția propusă implementează cerințele funcționale/fluxurile minime ale celor patru funcționalități de bază solicitate - ceea ce nu poate reieși nemijlocit doar din conținutul teoretic al propunerii tehnice și al tabelului de corespondență al cerințelor cu oferta tehnică prezentate. Nivelul de conformitate al acestor funcționalități de bază cu cerințele funcționale corespondente acestora din documentația de atribuire va fi evaluat la momentul depunerii ofertei. Neîndeplinirea acestora de către soluția propusă atrage neconformitatea ofertei.
Principiul de testare va fi „așa cum e", în consecință nu sunt permise modificări sau dezvoltări de funcționalități pe parcursul etapei de atribuire a contractului. Pentru că se urmărește testarea unor funcționalități și nu a performanței, infrastructura tehnică în care este pus la dispoziție mediul de testare poate fi una oarecare și nu una echivalentă mediului de exploatare live.
Raportat la cerință, ofertantul va menționa în propunerea tehnica: URL-ul de acces al mediului de testare, și credențiale de acces pentru: un Administrator de sistem; două conturi de utilizator-funcționar și câte un cont de utilizator persoană fizică și utilizator persoană juridică.

4.2 Principii și opțiuni tehnologice

Soluția propusă trebuie să adere la următoarele principii tehnologice care definesc arhitectura și modelul de livrare a serviciilor:
Soluția va fi furnizată exclusiv într-un **model Soluție de tip Software as a Service (SaaS)**, fiind găzduită într-o infrastructură de tip cloud. Prestatorul este integral responsabil pentru managementul, mentenanța, securitatea, scalabilitatea și actualizarea infrastructurii hardware și software necesare funcționării optime a platformei. Beneficiarul nu va fi responsabil pentru achiziția sau administrarea de servere, sisteme de operare, baze de date sau alte componente de infrastructură.
Prestatorul va asigura disponibilitatea platformei conform indicatorilor de performanță (SLA), realizarea copiilor de siguranță (backup), implementarea măsurilor de securitate cibernetică la nivel de infrastructură și aplicație, managementul actualizărilor și al corecțiilor de securitate.
Beneficiarul va asigura infrastructura de comunicații la sediile proprii și la punctele de lucru, precum și a echipamentelor necesare utilizatorilor finali (stații de lucru, laptopuri, dispozitive mobile).
Prezentul Caiet de Sarcini definește cerințele funcționale, de performanță și de securitate. Alegerea tehnologiilor specifice (limbaje de programare, platforme de dezvoltare, sisteme de gestiune a bazelor de date etc.) este la latitudinea ofertantului, cu condiția obligatorie ca acestea să fie soluții stabile, mature și actualizate.

4.3 Implementarea principiului „Do No Significant Harm" (DNSH)

Ofertantul va avea în vedere în cadrul ofertei tehnice aderența soluției și a modelului de livrare la principiul „a nu prejudicia în mod semnificativ" mediul. Aceasta implică, dar nu se limitează la:

- Eficiența energetică: Utilizarea unei infrastructuri care operează în centre de date moderne, cu un management avansat al consumului de energie și un indicator PUE (Power Usage Effectiveness) cât mai redus.
- Dezvoltare software sustenabilă: Soluția software va fi optimizată pentru a minimiza consumul de resurse computaționale (CPU, memorie), contribuind astfel la reducerea amprentei de carbon.

Cerințe pentru ofertant:

- Ofertantul va prezenta „Declarație privind respectarea aplicării principiului DNSH", asumând angajamentul pe durata prestării serviciilor;

4.4 Funcționalități specifice tehnologiilor avansate

Proiectul are în vedere implementarea următoarelor tehnologii avansate:

- Cloud computing (îndeplinită prin modelul solicitat);
- Automatizarea de procese (RPA);
- Instrumente de analiză a textului și procesare a vorbirii.

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică tehnologiile avansate (automatizarea de procese (RPA) și/sau instrumente de analiză a textului și procesare a vorbirii) ce vor fi implementate în soluția propusă, precum și modalitatea de implementare.

4.5 Principii fundamentale de securitate cibernetică

Având în vedere responsabilitatea instituției în cazul unui potențial incident, securitatea cibernetică a soluției urmărite se bazează pe următoarele principii fundamentale care ghidează eforturile de protejare a sistemelor, rețelelor și datelor împotriva amenințărilor cibernetice:

A. **Confidențialitatea**: Asigurarea că informațiile sensibile sunt accesibile doar persoanelor autorizate. Acest lucru implică utilizarea de criptare, controlul accesului și alte măsuri de protecție a datelor.
B. **Integritatea**: Garantarea că datele și informațiile rămân exacte și nealterate. Acest lucru se realizează prin utilizarea de mecanisme de detectare a modificărilor, cum ar fi sumele de control și semnăturile digitale.
C. **Disponibilitatea**: Asigurarea că sistemele, rețelele și datele sunt accesibile și funcționale atunci când este nevoie. Acest lucru implică implementarea de măsuri de redundanță, backup și recuperare în caz de dezastru.
D. **Autentificarea**: Verificarea identității utilizatorilor, sistemelor sau dispozitivelor înainte de a le acorda acces la resurse. Aceasta se realizează prin utilizarea de parole, token-uri, certificate digitale sau biometrie.
E. **Autorizarea**: Determinarea drepturilor și permisiunilor pe care le are un utilizator, sistem sau dispozitiv după ce a fost autentificat. Aceasta implică definirea și implementarea de politici de control al accesului.
F. **Non-repudierea**: Asigurarea că acțiunile și tranzacțiile nu pot fi negate ulterior de către părțile implicate. Acest lucru se realizează prin utilizarea de semnături digitale și înregistrarea jurnalelor de audit.
G. **Apărarea în profunzime**: Implementarea mai multor straturi de securitate pentru a proteja sistemele și datele. Acest lucru include utilizarea de firewall-uri, software antivirus, sisteme de detectare a intruziunilor și alte măsuri de securitate.
H. **Principiul celui mai mic privilegiu**: Acordarea utilizatorilor, sistemelor sau dispozitivelor doar a privilegiilor necesare pentru a-și îndeplini funcțiile. Acest lucru reduce riscul ca un atacator să obțină acces neautorizat la resurse sensibile.

I. **Actualizarea constantă**: Menținerea sistemelor, software-ului și dispozitivelor la zi cu cele mai recente patch-uri și actualizări de securitate. Acest lucru ajută la eliminarea vulnerabilităților cunoscute care pot fi exploatate de atacatori.

J. **Educarea utilizatorilor**: Informarea și instruirea utilizatorilor cu privire la riscurile de securitate și la modul în care își pot proteja dispozitivele și datele. Acest lucru include instruirea privind recunoașterea e-mailurilor de tip „phishing", utilizarea parolelor puternice și alte bune practici de securitate.

Principiile fundamentale ale securității cibernetice antemenționate vor fi implementate în cadrul soluției SaaS printr-un model de responsabilitate partajată („shared responsibility model"), specific mediilor cloud:

i. Ofertantul devenit Prestator este responsabil pentru securitatea la nivel de aplicație (cod sigur, managementul vulnerabilităților aplicației, configurarea securizată a componentelor software) și pentru securitatea datelor gestionate direct de aplicație (mecanisme de criptare la nivel de aplicație, controlul accesului la date în cadrul aplicației).

ii. Administratorii infrastructurii de găzduire cloud sunt responsabili pentru securitatea infrastructurii fizice a centrelor de date, a rețelei, a platformelor de virtualizare și a serviciilor de platformă (PaaS) și infrastructură (IaaS) oferite. Aceasta include protecția perimetrală, detecția intruziunilor la nivel de rețea, și managementul securității sistemelor de operare de bază.

iii. Beneficiarul Direcția de Asistență Socială Drobeta-Turnu Severin este responsabil pentru managementul corect și securizat al accesului utilizatorilor săi la aplicația SaaS (definirea rolurilor și permisiunilor, gestionarea parolelor, instruirea utilizatorilor privind practicile sigure) și pentru respectarea politicilor de securitate și a procedurilor interne.

Implementarea acestor principii trebuie să fie aliniată cu Strategia Națională de Securitate Cibernetică a României și cu reglementările specifice domeniului (Legea nr. 58/2023, Directiva NIS2).

5 CERINȚELE FUNCȚIONALE ALE SOLUȚIEI INFORMATICE

5.1 Interfața cu utilizatorul și accesibilitatea

Pentru a asigura o interfață cu utilizatorul care să fie ușor de utilizat, intuitivă și eficientă pentru toți utilizatorii, indiferent de nivelul lor de experiență sau de abilitățile lor tehnice, soluția ofertată trebuie să respecte următoarele cerințe:

Accesibilitate și ușurință în utilizare:

- Accesibilă tuturor utilizatorilor: Interfața trebuie să fie ușor de utilizat și accesibilă pentru toate categoriile de utilizatori, inclusiv pentru cei cu dizabilități, respectând nivelul AA de conformitate WCAG 2.1. Aceasta include asigurarea unui contrast suficient între text și fundal, navigarea prin tastatură, prezentarea de alternative text pentru imagini, o structură și semantică clare, precum și evitarea conținutului care poate declanșa crize.
- Multilingvă: Interfața va fi disponibilă în limba română și cel puțin o altă limbă de circulație europeană.
- Ușor de navigat și de înțeles: Utilizatorii ar trebui să poată găsi și accesa cu ușurință informațiile și funcțiile dorite, cu un efort minim. Interfața trebuie să fie proiectată logic și previzibil, utilizând iconografie și terminologie familiare, și să ofere un flux de lucru eficient, cu un număr minim de pași.
- Rapidă și receptivă: Interfața trebuie să ofere timpi de răspuns rapizi și feedback clar utilizatorilor.

Personalizare și feedback:

- Personalizabilă: Interfața trebuie să ofere opțiuni de personalizare, cum ar fi numele, prenumele, poza de profil și preferințele de limbă.
- Comunicare clară: Soluția informatică trebuie să ofere notificări în timp real și feedback clar cu privire la starea operațiunilor și a acțiunilor utilizatorului.
- Gestionarea erorilor: Mesajele de eroare trebuie să fie clare, informative și să ofere soluții sau instrucțiuni pentru remedierea erorilor. Utilizatorii ar trebui să aibă posibilitatea de a reveni la pagina anterioară și să fie avertizați cu privire la modificările nesalvate înainte de a părăsi o pagină.
- Feedback: Interfața trebuie să ofere utilizatorilor posibilitatea de a transmite opinii de îmbunătățire și de a semnala disfuncționalități.

Validări și opțiuni:

- Validări relevante: Formularele și câmpurile trebuie să aibă validări adecvate pentru toate tipurile de date introduse (de exemplu, formatul adresei de e-mail, numărul de telefon, data nașterii etc) pentru a preveni erorile și a asigura integritatea datelor.
- Opțiuni clare și contextuale: Opțiunile disponibile utilizatorilor trebuie să fie clare, concise și relevante pentru contextul actual. Meniurile și listele derulante trebuie să fie organizate logic și să ofere opțiuni ușor de înțeles.

Atractivitate și personalizare operațională:

- Aspect atrăgător: Interfața trebuie să aibă un aspect plăcut și modern, utilizând culori și elemente grafice adecvate.
- Terminologie specifică: Terminologia utilizată trebuie să fie adaptată tipului de utilizator (persoană fizică, persoană juridică, funcționar) și să fie ușor de înțeles.
- Număr optim de opțiuni: Numărul de opțiuni prezentate utilizatorului trebuie să fie optimizat pentru a evita supraîncărcarea și a facilita luarea deciziilor. Opțiunile trebuie să fie filtrate contextual în funcție de tipul de utilizator, rol și contextul specific.

- Explicații contextuale: Interfața trebuie să ofere explicații contextuale și sfaturi pentru a ajuta utilizatorii să înțeleagă funcționalitățile și să le utilizeze corect.

5.2 Cerințe fundamentale pentru platformele de distribuție electronică înregistrată (ERDP)

Soluția informatică va face posibilă transmiterea datelor între expeditor și destinatar prin mijloace electronice și va furniza dovezi referitoare la manipularea datelor transmise (inclusiv dovada trimiterii și primirii datelor) și care protejează datele transmise împotriva riscului de pierdere, furt, daune sau orice modificări neautorizate.
Datele generate în interiorul platformei care dovedesc ca un anumit eveniment a avut loc la un anumit moment dat se constituie ca dovezi asociate conținutului transferat între expeditor și destinatar și trebuie să fie auditabile. Cerințele generale privind platformele de distribuție electronică pentru a asigura securitatea, integritatea și legalitatea serviciilor oferite derivă în principal din Regulamentul (UE) nr. 910/2014 (eIDAS2) și din standardele tehnice ETSI asociate care definesc cerințele funcționale (ex. ETSI EN 319 521 V1.1.1 din februarie 2019).
Platforma trebuie să implementeze mecanisme tehnice (ex. criptare, controlul accesului) care protejează datele transmise împotriva riscului detectabil de pierdere, furt, daune sau orice modificări neautorizate pe durata ciclului de viață al datelor în platformă.
Datele generate ca dovezi trebuie să fie auditabile, să ateste momentul exact al evenimentelor și să fie corelate univoc cu conținutul transferat.

5.2.1 Cerințe privind integritatea și confidențialitatea conținutului utilizatorului

- Platforma trebuie să mențină disponibilitatea, integritatea (ex. prin hashing/sigilare) și confidențialitatea (prin criptare și RBAC) a 100% din conținutul utilizatorului și metadatele asociate, atât în tranzit, cât și în repaus (stocare).
- Accesul la identitatea utilizatorului trebuie restricționat strict pe bază de roluri și permisiuni (RBAC), prevenind accesul neautorizat direct sau indirect.
- Dacă sunt necesare modificări ale conținutului utilizatorului, platforma trebuie să notifice utilizatorul în mod explicit în timp real și să stocheze automat o dovadă imuabilă a conținutului inițial.
- Platforma trebuie să ofere capabilitatea tehnică de a proteja conținutul utilizatorului astfel încât să înlăture posibilitatea ca datele să fie schimbate într-o manieră nedetectabilă, fie prin semnături electronice calificate (QES) și/sau sigilii electronice calificate (QSeal), fie printr-un mecanism alternativ făcut disponibil de un furnizor de servicii de încredere calificat (QTSP) integrat în platformă.
- Platforma trebuie să valideze automat (1) validitatea semnăturii electronice / sigiliului electronic / mecanismului alternativ și (2) caracterul „calificat” al acestuia, prin interogarea listelor de încredere (Trusted Lists) relevante.

Cerințe pentru ofertant:

- ofertantul va detalia protocoalele criptografice (ex. TLS 1.3, AES-256), algoritmii de hashing și mecanismele de management al cheilor utilizate;
- ofertantul va detalia modelul de control al accesului (RBAC) implementat;
- ofertantul va prezenta descrierea procesului de aplicare și validare automată a unei semnături electronice/sigiliu electronic/mecanism alternativ, inclusiv verificarea în raport cu listele de încredere;

5.2.2 Cerințe privind identificarea și autentificarea

Identificarea - Platforma trebuie să dețină mijloacele tehnice necesare pentru a asigura identificarea utilizatorilor atât direct, cât și prin intermediul furnizorilor de servicii de încredere calificați.
Mijloacele de stabilire a identității electronice vor fi:

- Prin prezența fizică a individului (în cazul persoanelor) sau a reprezentantului autorizat al persoane juridice (în cazul persoanelor juridice).
- La distanță, folosind mijloace de identificare electronice care asigură respectarea nivelurilor de încredere substanțial sau ridicat așa cum sunt definite în Regulamentul (UE) 910/2014 (eIDAS).
- Cu ajutorul unui certificat calificat emis de un furnizor de servicii de încredere calificat în conformitate cu prevederile regulamentului.
- Alte metode de identificare recunoscute la nivel național care furnizează garanții similare prezenței fizice.

Procesul de stabilire a identității electronice a utilizatorului trebuie parcurs într-un mediu sigur și controlat, toate dovezile rezultate în urma acestuia (inclusiv consimțământul persoanei) trebuie capturate și stocate la nivelul platformei.
Toate evenimentele referitoare la identitatea inițială a utilizatorului și a autentificărilor ulterioare trebuie jurnalizate.
În cazuri speciale în care stabilirea identității electronice a utilizatorului nu poate fi constituită respectând cerințele menționate anterior deși identificarea fizică a avut loc (ex. persoana refuză constituirea identității electronice la nivelul platformei) se vor reține la nivelul sistemului indicii preliminare de identitate precum și dovezi clare ce stabilesc răspunderea operatorului care a procesat informațiile (ex. log-uri de sistem).
Autentificarea - Platforma trebuie să îi permită autentificarea utilizatorul înainte ca acestuia să i se acorde acces la conținutul din platformă.
Mijloacele de autentificare pot fi:

- Mecanisme de autentificare multi-factor;

- Semnătură digitală calificată emisă de un furnizor de servicii de încredere autorizat.

Soluția informatică propusă trebuie să dispună de o singură pagină de înregistrare și autentificare pentru toate tipurile de utilizatori (persoane fizice, persoane juridice, funcționari).

Autentificarea în soluția informatică se va face securizat folosind un strat suplimentar de securitate de tip 2FA („two factor authentication") asigurând nu doar autentificarea utilizatorului, ci și identificarea certificată a acestuia.

Platforma va folosi una din metodele de autentificare:

- Credențiale de acces (utilizator și parolă), caz în care se va aplica unul din următoarele nivele suplimentare:
- Dispozitiv de autentificare hardware cu doi factori de autentificare (2FA);
- OTP via SMS sau email;
- Dispozitiv de autentificare software cu doi factori de autentificare (2FA);
- Notificări transmise către dispozitivul mobil (de tip „push") cu doi factori de autentificare (2FA);
- Alte forme de autentificare cu doi factori (2FA) bazate pe infrastructura de autentificare a dispozitivului utilizat (ex. recunoaștere voce, facială sau amprentă)
- Semnătură electronică calificată.

Pagina principală („homepage") a sistemului trebuie includă funcționalitățile de:

- Validarea identității;
- Validarea parolei;
- Confidențialitatea parolei;
- Vizualizare parolă;
- Recuperare nume de utilizator;
- Recuperare parolă;
- Validare cu doi factori de autentificare (2FA);
- Revalidare cu doi factori de autentificare (2FA).

În oricare circumstanță trebuie să prezinte mesaje personalizate de notificare tip eroare pentru fiecare eroare pe care utilizatorul o poate genera în procesul de autentificare.

Pagina principală („homepage") a platformei trebuie să permită inițierea procesului de înrolare („onboarding") la înregistrarea utilizatorilor persoane fizice și persoane juridice și să prezinte cumulativ, în mod transparent potențialilor utilizatori:

- Acordul de prelucrare a datelor cu caracter personal;
- Termenii și Condițiile de utilizare ai soluției informatice;
- Politica de confidențialitate.

5.2.3 Cerințe privind evenimentele din cadrul platformei și dovezile acestora

Platforma trebuie să stocheze evenimentele și dovezi cu privire la evenimentele ce au avut loc cu privire la conținutul utilizatorilor. Categorii de informații care trebuie stocate / arhivate:

- Datele de identificare a utilizatorilor;
- Datele de autentificare a utilizatorilor;
- Dovada că identitatea expeditorului a fost verificată inițial;
- Log-uri de sistem privind verificarea identității expeditorului și destinatarului;
- Log-uri de sistem privind comunicarea;
- Dovezi cu privire la conținutul utilizatorului, dacă a fost modificat sau nu a fost modificat în timpul transmiterii;
- Dovezi corespunzătoare datei și orei încărcării, expedierii și recepționării conținutului utilizatorului, după caz.

Platforma trebuie să garanteze confidențialitatea, integritatea și disponibilitatea log-urilor de sistem și arhivarea acestora pentru scopuri legale în conformitatea cu prevederile naționale.

5.3 Managementul identităților electronice și autentificarea

Cerințele detaliate în acest capitol sunt determinate de nevoile fundamentale ale Direcției de Asistență Socială Drobeta-Turnu Severin (Beneficiarul investiției) de a realiza o transformare digitală sigură, legală și centrată pe cetățean, în contextul implementării platformei ERDP.

Aceste nevoi instituționale se axează pe asigurarea acurateței datelor, securității, conformității legale, trasabilității, schimbului de date standardizat și eficientizarea interacțiunilor cu cetățenii și funcționarii.

Managementul identităților electronice este fundația digitală a platformei. Fără un management riguros și legal al identităților, instituția nu ar putea atinge obiectivele de standardizare, securitate și oferire de servicii publice electronice sofisticate (grad 5), deoarece nu ar exista mecanisme sigure pentru a ști cine accesează sistemul, ce drepturi are și când a efectuat o anumită acțiune.

5.3.1 Identitatea electronică

5.3.1.1 Introducere și context

Managementul identităților electronice și autentificarea reprezintă pilonul central al soluției, asigurând un cadru de încredere robust și auditabil pentru interacțiunea digitală dintre instituție/subordonate și cetățeni, mediul de afaceri, alte instituții. Arhitectura funcțională a acestei componente logice este direct fundamentată pe cerințele obligatorii stipulate de două regulamente europene majore, care definesc atât nivelul de încredere, cât și protecția datelor personale: Regulamentul eIDAS și Regulamentul General privind Protecția Datelor (GDPR).

Procesul de stabilire a identității electronice a utilizatorilor (cetățeni, persoane juridice, funcționari) va fi pe deplin compatibil cu / va prioritiza utilizarea serviciilor oferite de sistemul național de identitate electronică ROeID, așa cum acesta este integrat și disponibil în cadrul Cloudului Privat Guvernamental. Nivelurile de asigurare a identității (scăzut, substanțial, ridicat), conform Regulamentului eIDAS, vor fi aliniate cu implementarea specifică din ROeID și cu cerințele de acces la diferitele tipuri de servicii publice.

5.3.1.2 Procesul auditabil de creare a identității (model „root of trust")

Cerințe generale și definiții

Soluția informatică propusă trebuie să includă un proces riguros și auditabil al managementului identităților electronice (persoane fizice, persoane juridice, funcționari). Pentru a evita orice neclaritate, prin termenul *auditabil* se înțelege capabilitatea soluției informatice de a crea și stoca în mod agregat (pe model „root of trust") înregistrări exacte pentru fiecare pas descris în procesul de creare a identității electronice, înregistrări care să nu poată fi șterse de niciun utilizator.

Metode și reguli de creare

Identitățile electronice rezidente în soluția informatică vor putea fi create prin prezența fizică la ghișeele instituției a solicitantului sau direct prin mediul online.

Regulile de creare sunt diferențiate în funcție de rol:

- Identitățile persoanelor fizice și juridice se vor putea crea de toți funcționarii.
- Identitățile funcționarilor vor fi create doar de administratorii de sistem.

Pașii auditabili (root of trust)

Mecanismele de auditare vor cuprinde minim următoarele elemente:

- **colectarea datelor:** colectarea corectă și completă a atributelor identității - validarea acestora trebuie să fie efectuată la momentul introducerii, corelat la nivelul întregului set de atribute;
- **capturarea acordului:** capturarea și salvarea acordului de procesare a datelor cu caracter personal;
- **identificare la ghișeu (prezența fizică a persoanei):** cererea de înregistrare semnată olograf, înregistrată în registratura electronică a instituției;
- **identificare video (online):** identificarea video (la identificarea online) salvată în cloud și asociată solicitării care a stabilit cadrul procedural auditabil pentru identificarea online - fișierul video va fi asociat identității persoanei în cauză;
- **acordarea nivelului de încredere:** nivelul de încredere acordat identității (scăzut, substanțial, ridicat);
- **semnătura funcționarului:** semnătura electronică calificată a funcționarului;
- **sigiliul instituției:** sigiliul electronic al instituției.

Fluxul de validare și activare

Identitatea electronică va fi în prealabil verificată/validată și ulterior inițiată de funcționarul care a realizat identificarea.

Toate atributele verificate și validate care au stat la baza unei identități electronice (indiferent că este personală sau profesională, persoană fizică sau juridică) vor fi asumate personal de funcționarul care a realizat validarea atributelor prin semnarea electronică calificată a acestora, acestea dobândind astfel caracter irefutabil.

Activarea efectivă a identității se va face de către titularul de drept al acesteia. Fiecare identitate electronică (personală/profesională) va fi confirmată de titular pe un canal extern soluției informatice (ex. e-mail, sms etc.) și asupra căruia are controlul personal deplin, urmând ca ea să devină complet operațională ulterior momentului confirmării. Canalul extern folosit trebuie să fie în afara controlului fizic și logic al autorității contractante.

Robustețe, trasabilitate și cerințe tehnice

Operațiunile de creare/modificare a identităților se vor face în regim de tranzacție și trebuie să aibă implementate proceduri de recuperare din eroare și revenire în starea precedentă consistentă în cazul în care apar erori.

Soluția informatică va dispune de mecanisme de protecție față de editarea concurentă de către mai mulți utilizatori a unei înregistrări.

Pentru integrarea cu ROeID se vor utiliza API-urile oficiale puse la dispoziție prin intermediul ADR și/sau STS pentru acest scop, respectând protocoalele de comunicație și standardele de securitate impuse.

Jurnalele detaliate de acces la datele de identitate și de modificare a acestora vor fi păstrate și protejate conform cerințelor de audit și securitate ale HG 98/2020CPG.

Cerințe pentru ofertant:

- Ofertantul va descrie în detaliu procesul de colectare, păstrare și protejare a înregistrărilor privind trasabilitatea succesiunii de operațiuni efectuate în sistem („audit trail") integrat în soluția informatică propusă;

- Ofertantul va prezenta procedura de realizare, modificare/corectare/actualizare, ștergere online a identităților electronice atât pentru persoane fizice, cât și pentru persoane juridice;
- Ofertantul va prezenta procedura de realizare, modificare/corectare/actualizare, ștergere la ghișeu a identităților electronice atât pentru persoane fizice, cât și pentru persoane juridice;
- Ofertantul va descrie în detaliu cum asigură procesul de confirmare a identității electronice nou create, precum și parametrii de utilizare a identității în perioada cât identitatea sa nu este încă confirmată (deci nu este efectivă).

5.3.1.3 Tipologia identităților

Conceptul de bază: identități unice și interdependente

Identitățile electronice (personale sau profesionale) trebuie să fie unice și interdependente. Vor fi definite prin atribute specifice fiecărui tip de identitate și vor fi agregate sub un identificator unic (ID) care va include identitatea creată în forma sa evolutivă (inclusiv toate modificările făcute de-a lungul existenței sale).

Ofertantul va atașa la propunerea tehnică descrierea conceptului de identitate electronică (eID) folosit de soluția informatică propusă.

Modelul fundamental: identitate personală (master) vs. profesională

1. **Identitatea personală (Master):** Reprezintă entitatea **cetățean (persoană fizică)**.
    - o persoană poate deține **o singură** identitate electronică personală;
    - aceasta este identitatea „părinte" obligatorie pentru orice altă identitate;
    - identitatea personală va permite utilizatorului deținerea controlului asupra existenței identităților profesionale;
    - *atribute vizate (persoană fizică):*
        - datele din actele de identitate (CNP și toate actele de identitate);
        - adresa de e-mail;
        - număr de telefon;
        - semnătura electronică calificată;
        - credențiale (utilizator și parolă) - pentru identitățile electronice efective.
2. **Identitatea profesională:** Reprezintă o persoană fizică acționând în numele unei entități (o **instituție publică** sau o **firmă**).
    - o persoană poate deține un **număr nelimitat** de identități electronice profesionale;
    - identitățile electronice profesionale (ex. funcționar, reprezentant legal etc.) nu pot exista în cadrul soluției informatice în lipsa identității electronice personale, ci doar asociate acesteia;
    - dezactivarea/ștergerea identității personale va genera și dezactivarea/ștergerea tuturor identităților profesionale asociate;
    - *tip 1: reprezentant al entității „firmă" (persoană juridică):*
        - *atribute vizate (identitatea profesională a reprezentantului firmei):*
            - denumirea organizației reprezentante;
            - denumirea departamentului;
            - informația despre funcția deținută;
            - adresa de e-mail profesională;
            - număr de telefon;
            - persoana care a inițiat identitatea;
            - valabilitatea identității profesionale;
            - credențiale (utilizator și parolă) - pentru identitățile electronice efective.
    - *tip 2: reprezentant al entității „instituție publică" (funcționar):*
        - atributele specifice sunt definite prin politicile interne, suprapunându-se parțial cu cele ale reprezentantului de firmă, dar cu reguli de creare și stări logice distincte.
3. **Entitatea „firmă" (persoană juridică):** O entitate pasivă, gestionată prin reprezentanți.
    - identitatea persoanei juridice nu va putea exista în lipsa unui reprezentant legal (direct sau prin împuternicit) cu identitate electronică de nivel de încredere substanțial / ridicat;
    - *atribute vizate (persoană juridică):*
        - datele persoanei juridice - CUI;
        - extras constatator ONRC sau alte doveditoare (certificate, autorizații, licențe etc.);
        - datele reprezentantului persoanei juridice sau ale împuternicitului acestuia;

Managementul colaborativ al persoanei juridice (firmă)

Managementul spațiului virtual al persoanelor juridice se va realiza în mod colaborativ de către reprezentantul legal (administratorul persoanei juridice / împuternicit) și funcționari (reprezentanții instituției):

- **responsabilități ale funcționarului (instituția):**
    - verificarea corectitudinii și integrității datelor despre persoana juridică;
    - verificarea corectitudinii și integrității datelor despre reprezentantul legal;
    - activarea identității profesionale a reprezentantului legal;

- activarea identității persoanei juridice.

- **responsabilități ale reprezentantului legal (firma):**
  - inițierea, activarea, ștergerea, dezactivarea sau suspendarea identităților profesionale ale altor funcționari (angajați ai firmei);
  - stabilirea serviciilor publice la care aceștia au acces;
  - menținerea datelor despre persoana juridică la un nivel de acuratețe curent.

Credențiale și SSO (Single Sign On)

Fiecare identitate (personală sau profesională) va dispune de un set distinct de credențiale care va identifica în mod unic o singură identitate.

Fiecare identitate efectivă va dispune de un set unic de credențiale, care vor constitui mijlocul principal de autentificare a identității respective.

Identitățile aparținând unei singure persoane vor fi integrate prin SSO (Single Sign On), aceasta putând comuta între identități fără o autentificare suplimentară.

Roluri și modele de guvernanță digitală

Identitățile (inclusiv cele personale) vor putea avea asociate unul sau mai multe roluri, guvernate de modele de guvernanță digitală specifice. Rolurile asociate vor putea fi accesate și utilizate în baza credențialelor identității la care sunt asociate (fără autentificări suplimentare).

- *definiție model de guvernanță digitală:* un ansamblu de reguli / proceduri care definesc identitatea / rolul, vizând cumulativ cel puțin:
  - persoanele responsabile cu configurarea identității / rolului;
  - operațiunile specifice pe care identitatea / rolul le poate face;
  - consecințele juridice generate.
- *atribute vizate (roluri):*
  - titulatura rolului;
  - identitatea căreia îi este asociat;
  - persoana care a generat rolul;
  - valabilitatea rolului.

Grade de operaționalizare

Raportat la gradul de operaționalizare, identitățile pot fi:

1. **Identitatea efectivă:** îndeplinește cumulativ 4 condiții: (1) identificator unic, (2) set complet de atribute specifice, (3) asumată conștient de titular, (4) exercitată activ.
2. **Identitatea neefectivă:** toate identitățile care includ obligatoriu CNP sau CUI/CIF, dar nu îndeplinesc cumulativ condițiile identității efective. (exemplu: până la confirmarea de către titular). Vor putea deveni efective doar după ce vor fi complete, asumate și exercitate.
3. **Indiciile preliminare de identitate:** datele cu privire la un solicitant (ex. adresa de e-mail, număr de telefon etc.) care nu au asociat un CNP/CI/CIF. Vor fi asumate de angajatul care le-a introdus în sistem și supuse auditării. Soluția trebuie să poată captura, salva și operaționaliza parțial aceste indicii, care vor genera consecințe juridice limitate.

Indiferent de gradul de operaționalizare, soluția trebuie să implementeze modele de guvernanță digitală contextuală pentru toate cele trei categorii.

Stări logice ale identităților

Soluția propusă trebuie să poată gestiona ciclul de viață complet al unei identități digitale, respectiv să stocheze și operaționalizeze prin modele de guvernanță digitală specifice următoarele stări logice:

- **pentru persoanele fizice (cetățean) și juridice (firmă):**
  - perioada de inactivitate;
  - perioada între momentul inițializării și momentul activării;
  - perioada de activitate;
  - perioada de suspendare (ex. suspiciuni de fraudă, detașare, indisponibilitate);
  - perioada ulterioară dezactivării.
- **pentru funcționari (instituție):**
  - perioada de inactivitate;
  - perioada între momentul inițializării și momentul confirmării;
  - perioada de activitate;
  - perioada în concediu;
  - perioada de suspendare;
  - perioada ulterioară dezactivării.
- **stări logice agregate (pentru modelele de guvernanță)***:* inactivă (neefectivă); inițiată / neconfirmată (neefectivă); activă (efectivă); suspendată (efectivă); în concediu (efectivă, specifică funcționarilor); dezactivată (neefectivă); șterasă.

Cerințe pentru ofertant:

1. Privind tipologie și guvernanță, ofertantul va prezenta în propunerea tehnică:
    - descrierea detaliată a modului în care gestionează atributele identităților (personale și profesionale);
    - descrierea detaliată a modului cum asigură relația de interdependență (personală-profesională);
    - descrierea detaliată a modului cum asigură asocierea de roluri la fiecare tip de identitate;
    - descrierea detaliată a modului cum asigură modele de guvernanță particularizată pe fiecare rol;
    - descrierea detaliată a modului cum gestionează procesul de actualizare a atributelor fără a afecta consistența versiunilor anterioare (istoricul);
    - detalierea modelelor de guvernanță digitală contextuală pentru cele 3 grade de operaționalizare (efectivă, neefectivă, indicii preliminare);
    - detalierea modelelor de guvernanță digitală specifice fiecărei stări logice a identităților.
2. Privind conformitate GDPR Ofertantul va descrie în detaliu:
    - anonimizarea: modalitatea de anonimizare a datelor în interfețele de lucru curente (expuse riscului de vizualizare);
    - acuratețea: modalitatea de asigurare a nivelului maxim de acuratețe a datelor personale;
    - consimțământul: modalitatea de capturare și stocare a acordului de procesare a datelor cu caracter personal;
    - motivul accesului: modalitatea de capturare a motivului de acces la datele personale ale utilizatorului (din interfața de lucru);
    - dreptul de a fi uitat: modul în care asigură solicitantului respectarea „dreptului de a fi uitat”.
3. Privind conformitate eIDAS ofertantul trebuie să detalieze:
    - niveluri de încredere: modalitatea de asigurare a nivelurilor de încredere (scăzut, substanțial și ridicat) și modelul de guvernanță digitală ce definește fiecare nivel;
    - tranziția între niveluri: procesul de tranziție de la un nivel la altul;
    - identificarea video: modalitatea de identificare online a utilizatorilor, capturarea și salvarea în cloud a identificării video și integrarea acesteia în „audit trail”;
    - integrarea serviciilor de încredere: descrierea detaliată a modului în care soluția propusă integrează și utilizează servicii de încredere calificate (furnizate de un QTSP) pentru a asigura crearea, verificarea și validarea semnăturilor electronice calificate, sigiliilor electronice calificate și mărcilor temporale calificate.

5.3.1.4 Interfața utilizator („Contul meu”)

Informațiile privind identitatea electronică vor fi disponibile și accesibile fiecărui utilizator într-o secțiune de tip „Contul meu”.

Interfață - utilizator persoană fizică (cetățean)

Interfața grafică trebuie să afișeze minim:

- datele personale ale titularului identității electronice personale;
- poza de profil;
- actele de identitate ale titularului actualizate;
- date privind funcționarul care a creat identitatea electronică;
- semnătura olografă a utilizatorului (dacă este înregistrată);
- semnătura electronică calificată a titularului (cu detalii: furnizor, valabilitate etc.);
- modificarea parolei de acces la sistem.

Interfață - utilizator persoană juridică (reprezentant firmă)

Interfața grafică trebuie să afișeze minim:

- datele personale ale titularului identității electronice profesionale;
- datele specifice identității profesionale;
- poza de profil;
- semnătura olografă a utilizatorului (dacă este înregistrată);
- semnătura electronică calificată a titularului identității;
- modificarea parolei de acces la sistem.

Interfață - utilizator funcționar (reprezentant instituție)

Interfața grafică trebuie să afișeze minim:

- datele personale ale titularului identității electronice profesionale;
- datele specifice identității profesionale;
- poza de profil;
- semnătura olografă a utilizatorului (dacă este înregistrată);
- semnătura electronică calificată a titularului identității;
- modificarea parolei de acces la sistem.

Notă: Se vor avea în vedere cerințele cu privire la coerența interfeței grafice.

Managementul propriilor date (self-service)

Atributele identității electronice care nu sunt considerate ca având grad mare de sensibilitate (e-mail, număr de telefon, poza de profil, semnătura olografă) vor putea fi editate/actualizate de utilizator fără o validare explicită a funcționarilor.
Pentru restul informațiilor se va cere validarea de către funcționar și, acolo unde există posibilitatea, semnarea lor electronică calificată de către titularul identității electronice.

5.3.1.5 Managementul datelor de către funcționari (back-office)

Principii de acces (privilegii funcționari)
Informațiile despre toți utilizatorii (persoane fizice, persoane juridice sau funcționari) vor fi făcute disponibile și accesibile tuturor funcționarilor în baza principiului „nevoii de a cunoaște". Informațiile vor putea fi accesate doar individual și condiționat de existența unui motiv temeinic. Motivul accesului va fi capturat în sistem pentru a asigura conformitatea cu prevederile GDPR.
Pentru a evita orice dubiu, soluția ofertată nu va permite niciunui tip de utilizator funcționar vizualizarea tuturor identităților personale din sistem sub formă de listă și fără un motiv exprimat și capturat la momentul accesului.
Instrumente de management (back-office)
Funcționarii vor dispune de instrumente destinate managementului datelor utilizatorilor, precum:

- inițierea procesului de resetare a parolei de acces;
- vizualizarea istoricului / versiunilor anterioare ale datelor personale ale utilizatorului;
- editarea datelor personale ale utilizatorilor.

5.3.2 Autentificarea

Autentificarea multi-factor (2FA) va fi implementată ca mecanism obligatoriu pentru funcționarii publici și va fi oferită ca opțiune robustă de securitate pentru cetățeni și reprezentanții persoanelor juridice, utilizând mecanisme de autentificare aprobate și validate pentru utilizare în CPG (Cloudul Privat Guvernamental).
Pentru a asigura un proces de autentificare sigur și ușor de utilizat, soluția ofertată trebuie să respecte următoarele cerințe funcționale:

- Autentificare unică: O singură pagină de înregistrare și autentificare (SSO) pentru toate tipurile de utilizatori (persoane fizice, persoane juridice, angajați).
- Integrare cu ROeID: Posibilitatea de autentificare prin Sistemul Național de Identitate Electronică (ROeID).
- Autentificare cu doi factori (2FA): Implementarea unui strat suplimentar de securitate prin 2FA.
- Metode de autentificare 2FA posibile: Dispozitiv hardware, OTP prin SMS/e-mail, dispozitiv software, notificări push, autentificare biometrică (opțional).
- Funcționalități ale paginii de autentificare:
    - Validare identitate/parolă
    - Confidențialitate parolă
    - Vizualizare parolă
    - Recuperare nume utilizator/parolă
    - Validare și revalidare 2FA
    - Cerințe (de securitate) privind parola:
        - Lungime minimă a parolei (de exemplu, 8 caractere)
        - Complexitatea parolei (combinație de litere mari, litere mici, cifre și caractere speciale)
        - Expirarea parolei după o anumită perioadă (de exemplu, 90 de zile)
        - Blocarea contului după un anumit număr de încercări de autentificare nereușite
        - Prevenirea reutilizării parolelor anterioare
- Mesaje de eroare personalizate: Mesaje clare și informative pentru fiecare eroare posibilă în procesul de autentificare.
- Înrolare (Onboarding) utilizatori: Prezentarea acordului de prelucrare a datelor, termenilor și condițiilor și politicii de confidențialitate.
- Canal de comunicare destinat suportului pentru înrolare securizat și protejat împotriva atacurilor cibernetice.

5.4 Înregistrarea operațiunilor administrative

Cerințele detaliate în acest capitol sunt determinate de o serie complexă de nevoi instituționale ale Direcției de Asistență Socială Drobeta-Turnu Severin, care vizează transformarea digitală a activității administrative, asigurarea conformității legale și stabilirea unui cadru robust de gestionare a documentelor ca dovezi (*Records Management*), convergând către patru piloni esențiali:
(1) **Asigurarea conformității legale** stricte, atât cu standardele de guvernanță a înregistrărilor (ISO 15489), cât și cu legislația națională, în special în cadrul procedural administrativ;
(2) **Garantarea securității juridice și a non-repudierii**, printr-un control absolut asupra numerelor de înregistrare, care trebuie să fie unice, inalterabile și acordate lucrărilor și actelor administrative finalizate și semnate electronic calificat;
(3) Nevoia de **structurare logică a informației** conform modelului relațional LUCRARE – ACT – DOSAR, pentru a asigura trasabilitatea completă și managementul metadatelor;
(4) **Asigurarea flexibilității operaționale** prin gestionarea dual a fluxurilor, integrând atât o registratură fizică digitalizată, cât și o registratură online automatizată.

Înregistrarea riguroasă a operațiunilor administrative reprezintă fundația procedurală și legală a întregului sistem. Fără un mecanism standardizat de captare a dovezilor activității, instituția nu ar putea atinge obiectivele de standardizare, interconectivitate și oferire de servicii publice de grad 5, deoarece actele administrative produse digital nu ar avea garanția autenticității, trasabilității și valorii legale (non-repudiere) în fața legii, a unui audit sau în relația cu cetățeanul.

5.4.1 Introducere și context

Înregistrările sunt atât dovezi ale activității instituțiilor publice, cât și bunuri informaționale. Ele pot fi diferențiate de alte active informaționale prin rolul lor ca dovezi în operațiunile administrative și prin dependența lor de metadate. Metadatele pentru înregistrări sunt utilizate pentru a indica și păstra contextul și pentru a aplica reguli adecvate pentru gestionarea înregistrărilor, acestea fiind în strânsă legătură cu evaluarea condițiilor de valabilitate și oportunitate/necesitate a actului administrativ.
Gestionarea înregistrărilor cuprinde următoarele:

- Crearea și înregistrarea înregistrărilor pentru a îndeplini cerințele de evidență a activității curente administrative.
- Luarea de măsuri adecvate pentru a le proteja autenticitatea, fiabilitatea, integritatea și capacitatea de utilizare întrucât contextul administrativ și cerințele pentru managementul acestora se modifică în timp.

Alinierea modului de lucru la prevederile privind crearea, captarea și gestionarea înregistrărilor bazate pe conceptele și principiile ISO 15489-1 din 2016 (privind managementul înregistrărilor în sistemele de Records Management) asigură că dovezile autorizate ale activității sunt create, capturate, gestionate și făcute accesibile celor care au nevoie de ele, atâta timp cât este necesar.
Implementarea acestor cerințe sprijină direct obiective strategice, precum asigurarea transparenței și responsabilității operațiunilor administrative, luarea deciziilor în cunoștință de cauză, managementul riscurilor, protecția și sprijinul în litigii și, nu în ultimul rând, protecția memoriei instituționale, personale și colective.
Necesitatea administrativă de gestiune a fluxurilor în cadrul Direcției de Asistență Socială Drobeta-Turnu Severin impune nevoia de trasabilitate riguroasă a operațiunilor administrative, centrată pe beneficiar, precum și flexibilitatea necesară perspectivelor structurilor organizației (ex. protecția copilului, protecția persoanelor vârstnice, asistenți personali). Fundamentul acestui sistem este distincția conceptuală clară între proces și rezultat.
Pilonul central operațional al instituției este **procesul administrativ în sine** (de exemplu, soluționarea unei cereri de ajutor social/venit minim, procesarea dosarului pentru ajutorul de încălzire sau gestionarea unei cereri pentru cantina socială). Un proces administrativ gestionează întregul context operațional: intrările (dovezile, fie ele fișiere atașate precum Adeverință de venit a membrului familiei, înscrisuri de tip mesaj sau simple comunicări), participanții și toate elementele de context auditabile.
Finalizarea cu succes a unui proces administrativ generează **un rezultat de ieșire validat**, născut exclusiv din acel proces (de exemplu, un act precum Dispoziția de acordare/respingere a ajutorului social, înscrisuri de tip mesaj sau simple comunicări).
Pentru o gestionare eficientă, este nevoie de un **mecanism flexibil de grupare (agregare)**, care să îndeplinească două funcții distincte:
(1) Gruparea proceselor administrative în dosare operaționale, relevante pentru diverse perspective și competențe ale structurilor (ex. un Dosar de Beneficiar, care referă toate lucrările asociate acestuia de-a lungul timpului – cererea inițială, reevaluările anuale, cererile punctuale);
(2) Gruparea rezultatelor finale pentru a satisface cerințe specifice de evidență și raportare (ex. Registrul beneficiarilor de ajutor social pe luna curentă sau Evidența dispozițiilor de plată).

5.4.2 Funcțiile registraturii

Soluția informatică va dispune de o componentă de registratură instituțională care va fi organizată ținând cont de competența materială a acestei funcții instituționale, respectiv:

1. Primirea și repartizarea actelor intrate în instituție.
2. Expedierea actelor către entități externe instituției.
3. Circulația actelor de uz intern.

5.4.3 Instrumentarul administrativ

Registratura va fi structurată ținându-se cont de instrumentarul relațional clasic administrativ, respectiv LUCRARE (procesul administrativ) - ACT (rezultatul) – DOSAR (mecanismul de grupare), asigurând managementul auditabil al dovezilor privind operațiunile asupra înregistrărilor, înțelegând prin aceasta asigurarea colectării probelor (metadatelor) de audit în mod trasabil cronologic.
Astfel:

- LUCRAREA va include unul sau mai multe acte ce au legătură cu aceeași solicitare precum și toate elementele de context care definesc lucrarea respectivă, respectiv comunicări, participanți (fiecare cu rolul lui, conexări, referințe, etc.).
- un ACT va putea face parte din una sau mai multe lucrări/dosare electronice în același timp, diferențierea făcându-se contextual pe baza numărului de înregistrare unic primit la fiecare asociere - un act nu va putea exista de sine stătător, ci doar în structura unei lucrări.
- un DOSAR va include întotdeauna mai multe lucrări asociate în jurul unui subiect comun.

5.4.4 Tipuri de registratură

Având în vedere nevoile specifice administrației publice, Autoritatea Contractantă urmărește implementarea unei soluții informatice care să adreseze într-o manieră standardizată și integrată următoarele componente specifice activității de registratură:

- Activitatea de registratură fizică digitalizată - respectiv intrările de solicitări și ieșirea de corespondență prin ghișeele instituției;

- Activitatea de registratură online automatizată - intrările și ieșirile realizate direct prin mediul virtual.

Pentru a înlătura orice dubiu cu privire la sensul termenilor folosiți în prezenta documentație și pentru a asigura o bună înțelegere de către ofertanți a nevoilor instituției menționăm că sensul terminologic al celor două tipuri de registraturi este următorul:

- Registratura fizică digitalizată - capabilitățile oferite de soluția informatică de a prelua actele recepționate pe suport de hârtie prin ghișeele instituției și de a le introduce pe fluxurile de lucru digitalizate
- Registratură online automatizată - capabilitățile oferite de soluția informatică de a prelua actele recepționate pe canalul online și de a le introduce pe fluxurile de lucru preconfigurate sau configurabile

Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la registratura fizică digitalizată, respectiv registratura online automatizată. Pentru fiecare cerință funcțională se va furniza un URL.

5.4.4.1 Cerințe privind registratura online automatizată

Registratura online automatizată trebuie:

- Să efectueze recepționarea automatizată (atât în format tichet cât și pe formulare tipizate) online a solicitărilor de la alte entități, fie ele persoane fizice sau juridice, cu colectarea tuturor metadatelor relevante pentru lucrarea respectivă;
- Să includă o funcție (ca opțiune) de repartizare automatizată a lucrărilor recepționate prin mediul online, configurabilă în funcție de cel puțin următoarele criterii:
    - gradul de încărcare al funcționarului;
    - criteriul ierarhic (repartizarea automată către șeful de structură);
    - competența teritorială a funcționarului;
    - competența materială a funcționarului.
- Să permită funcționarului vizualizarea istoricului de solicitări al solicitantului în vederea evitării dublării solicitărilor;
- Să permită funcționarului vizualizarea tuturor solicitărilor care i-au fost repartizate pentru procesare, și să-i permită să le filtreze după cel puțin următoarele criterii:
    - nume solicitant;
    - CNP / CUI;
    - număr de lucrare;
    - subiect;
    - conținut;
    - data recepționării;
    - data înregistrării;
    - starea lucrării.
- Să permită funcționarului să repartizeze lucrări, fie către un alt funcționar din cadrul instituției, fie către o altă instituție atunci când este cazul. Repartizarea trebuie să poată fi individuală (lucrare cu lucrare) sau în loturi (mai multe lucrări expediate printr-o singură operațiune către funcționarul responsabil);
- Să permită funcționarului să organizeze consultări cu alți funcționari pentru a întocmi răspuns la cererile venite de la cetățeni;
- Să permită funcționarului să conexeze mai multe lucrări într-un dosar - conexarea trebuie să fie posibilă atât cu o lucrare deja existentă în instituție, cât și cu o lucrare care să fie inițiată ad-hoc din cea curentă;
- Să permită funcționarului să comunice online cu solicitanții în vederea solicitării de detalii suplimentare cu privire la solicitarea trimisă;
- Să permită funcționarului să finalizeze / soluționeze solicitările primite prin una din modalitățile de finalizare disponibile în sistem. Finalizarea trebuie să poată fi individuală (lucrare cu lucrare) sau în serii/loturi (mai multe lucrări finalizate printr-o singură operațiune);
- Să permită funcționarului să arhiveze lucrările finalizate. Arhivarea lucrărilor trebuie să poată fi individuală (lucrare cu lucrare) sau în serii/loturi (mai multe lucrări arhivate printr-o singură operațiune).

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă.

5.4.4.2 Cerințe privind registratura fizică digitalizată

Registratura fizică digitalizată trebuie:

- Să permită recepționarea solicitărilor de la alte entități fie ele persoane fizice sau juridice cu colectarea tuturor metadatelor relevante pentru lucrarea respectivă;
- Să permită preluarea în format e-mail/mesagerie electronică sau prin formulare tipizate a solicitărilor. Toate formularele tipizate existente și utilizate în cadrul instituției vor fi disponibile pentru preluarea solicitărilor de către funcționarii din registratură;
- Să asigure recepționarea solicitărilor în toate cele 3 ipoteze de identitate în care solicitantul se poate afla:
    - solicitant cu identitate efectivă;
    - solicitant cu identitate neefectivă;
    - solicitant care prezintă doar indicii preliminare de identitate (ex. petițiile venite pe e-mail).

- Să permită repartizarea lucrărilor pe fluxurile de resoluționare și ulterior către persoanele responsabile cu soluționarea acestora, capturând integral tot fluxul instituțional parcurs de lucrare;
- Să dispună de o secțiune de ciorne destinată salvării lucrărilor care sunt în curs de editare și din diverse motive nu au putut fi expediate;
- Să permită comunicarea actelor de ieșire atunci când titularul solicitării/împuternicitul acestuia se prezintă la ghișeu. În cazul comunicării către împuterniciți sistemul trebuie să condiționeze comunicarea de încărcarea în sistem a împuternicirii;
- Să permită căutarea lucrărilor și vizualizarea conținutului acestora în registrul unic la solicitarea beneficiarului (persoana fizica, juridică sau funcționar), accesarea lor cu respectarea condițiilor impuse de GDPR, tipărirea și transmiterea actelor din lucrare solicitantului prezentat la ghișeu;
- Să permită funcționarului să vizualizeze toate solicitările pe care le-a repartizat, și să-i permită să le filtreze după cel puțin următoarele criterii:
    - nume solicitant;
    - număr de lucrare;
    - nume destinatar;
    - subiect;
    - conținut;
    - CNP / CUI;
    - data recepționării;
    - data înregistrării.

  Selecția va putea fi făcută prin aplicarea de filtre simple sau conjugate astfel încât timpul de căutare să fie limitat la maxim.
- Să permită funcționarului să arhiveze lucrările repartizate după ce acestea au fost finalizate. Arhivarea lucrărilor trebuie să poată fi individuală (lucrare cu lucrare) sau în serii/loturi (mai multe lucrări arhivate printr-o singură operațiune).

Cerințe pentru ofertant:

- Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la registratura fizică digitalizată. Pentru fiecare cerință funcțională se va furniza un URL.

5.4.5 Cerințe detaliate privind lucrările, actele și dosarele

5.4.5.1 Cerințe conceptuale despre actele electronice

Pentru a asigura o corectă înțelegere a termenilor de către toți ofertanții interesați, prin act electronic se înțelege un document electronic care prezintă cumulativ cel puțin următoarele caracteristici:

1. Are un autor (cu o identitate efectivă / neefectivă / indicii preliminare de identitate).
2. Are un conținut care reflectă ceva ce a fost spus, făcut sau agreat.
3. Este semnat și asumat în nume personal sau în numele altei persoane.
4. A făcut obiectul unui proces de avizare/aprobare conform unui cadru procedural intern.
5. A făcut sau nu a făcut obiectul unui proces de înregistrare (are număr de înregistrare).
6. Poate fi original într-un sistem electronic sau reprezintă o copie semnată electronic calificat pentru conformitate cu originalul a unui document pe hârtie.

Actele electronice pot fi emise de persoane fizice, persoane juridice sau de instituții.

Actele emise de către persoanele fizice și persoanele juridice (altele decât instituții) pentru a avea relevanță într-un context instituțional trebuie să facă obiectul unui proces de înregistrare / luare în evidență.

Documentele emise de instituții pot constitui acte electronice doar în măsura în care îndeplinesc cumulativ următoarele condiții:

1. Prezintă indicii clare ale autorului documentului.
2. Poartă identitatea vizuală a instituției emitente.
3. A parcurs un proces de semnare, avizare și aprobare agreat formal la nivelul instituției emitente.
4. A fost înregistrat cu număr de înregistrare unic în evidențele instituției emitente.

5.4.5.2 Cerințe specifice privind actele electronice

Soluția informatică propusă trebuie să asigure minim următoarele capabilități ce privesc documentele / actele electronice ce vor fi gestionate la nivelul instituției:

- Să asigure încărcarea de fișiere în sistem individual sau prin serii/loturi, atât prin butoane de încărcare, cât și prin operațiuni tip „drag and drop” și „copy-paste” - încărcarea trebuie să se poată face din arhiva electronică la care are acces și din calculator;
- Să asigure ștergerea fișierelor electronice din sistem cu excepția celor care au fost arhivate electronic și a căror ștergere nu este permisă;
- Să asigure conversia (automat și manual) în format pdf a fișierelor din surse externe sistemului încărcate în sistem și a celor redactate în sistem (minim următoarele formate de fișiere electronice .jpg, .jpeg, .bmp, .png, .doc, .docx, .odf);
- Conversia în format pdf trebuie să poată fi făcută atât individual cât și în loturi;

- Să aibă integrată o procedură electronică de conformare cu originalul prin semnarea electronică calificată de către funcționar;
- Conformarea cu originalul prin semnare electronică calificată trebuie să poată fi făcută atât individual cât și în loturi;
- Să asigure versionarea documentelor electronice aflate în proces de a deveni acte (aflate pe fluxurile de avizare, aprobare, înregistrare);
- Să poată asigura colectarea cu ușurință a tuturor metadatelor relevante în funcție de contextul în care se află utilizatorul (arhivă personală, instituțională);
- Să permită redenumirea fișierelor electronice fără să fie nevoie de descărcarea lor din sistem;
- Să permită o evidență riguroasă a actelor principale și a anexelor acestora - relația „act principal-anexă" fiind stocată la nivelul sistemului;
- Să asigure vizualizarea documentelor / actelor electronice în sistem fără a fi nevoie de descărcarea lor;
- Să permită semnarea electronică atât prin trimiterea documentului/actului electronic pe un flux electronic, cât și static;
- Procesul de semnare electronică trebuie să permită inserarea de elemente vizuale în formate .jpg, .jpeg, .png, cum ar fi sigla, imaginea semnăturii olografe etc. De asemenea, funcționalitatea de semnare electronică calificată trebuie să fie disponibilă atât individual, cât și în serii/loturi;
- Să permită utilizatorului amplasarea semnăturii electronice calificate astfel încât să nu se suprapună cu textul. Dacă documentul încărcat în sistem are factor de rotire amplasarea semnăturii electronice trebuie să țină cont de acest element;
- Să dispună de facilități de arhivare electronică, precum și facilități de stocare;
- Să aibă implementate politici de control al dimensiunii fișierelor;
- Să dispună de capabilități de separare a paginilor unui document și salvarea ca documente diferite, de ordonare / reordonare a paginilor în cadrul aceluiași document, de concatenare a mai multor fișiere;
- Să implementeze servicii de încredere în înțelesul regulamentului UE nr. 910/2014, respectiv să asigure crearea, verificarea și validarea semnăturilor electronice, a sigiliilor electronice dintr-un document și să certifice validitatea semnăturilor și sigiliilor electronice dintr-un document;
- Să se asigure că actele electronice vor fi unice la nivel de sistem;
- Să asigure capabilitatea de face referințe electronice actelor electronice către un număr nelimitat de dosare electronice;
- Actele electronice vor putea fi salvate pe grupe acte specifice activității fiecărui structuri din organigramă;
- Să permită configurarea drepturilor de acces la nivel de grupă și document;
- Să asigure capabilități de configurare a drepturilor de acces la grupe atât pentru scriere cât și pentru citire. Configurarea se va putea face individual sau ca grup predefinit de utilizatori ai sistemului;
- Actele electronice vor putea fi mutate între grupele arhivistice asociate aceluiași registru. Mutarea în grupe asociate altui registru decât cel în care a fost înregistrat este interzisă;
- În relația lor cu dosarele electronice actele electronice vor putea face obiectul următoarelor operațiuni:
    - salvarea în dosar;
    - ștergere din dosar;
    - mutare în alt dosar;
    - creare referință în alt dosar;
    - comparare fișiere.
- Să permită gruparea actelor pe grupe care vor putea face obiectul următoarelor tipuri de operațiuni:
    - crearea și editarea grupei;
    - ștergerea grupei;
    - stabilirea drepturilor de acces la grupe;
    - asocierea de tipuri de procese specifice.

Toate cerințele formulate mai sus vor fi disponibile integrat pe toate fluxurile de lucru din sistem.
Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru verificarea cerinței funcționale. Pentru fiecare cerință funcțională se va furniza un URL.

5.4.5.3 Cerințe conceptuale privind lucrările electronice

Soluția informatică trebuie să trateze lucrările ca structuri logice caracterizate de minim următoarele atribute:

- tipul lucrării;
- numărul de înregistrare al lucrării (pentru cele înregistrate);
- denumirea lucrării;
- data și ora creării;
- data și ora înregistrării;
- data și ora primirii;
- data finalizării;
- modalitatea de finalizare;
- cronologia lucrării - succesiunea de acțiuni și evenimente consemnate în conținutul lucrării marcate temporal;

- datele despre participanții la lucrare, rolurile pe care aceștia îl au în lucrare și starea acestora;
- conținutul lucrării - poate include mesaje, idei, sugestii, argumente, puncte de vedere, etc.;
- documentele/actele lucrării;
- informații despre eventuale conexări;
- guvernanța lucrării - setul particular de reguli și acțiuni care guvernează lucrarea în funcție de tipul ei;
- starea lucrării (ex. de stări - fără a fi obligatorii sau limitate la acestea - neînregistrată, în lucru, finalizată, etc.);
- orice alt eveniment sau obiect consemnat la nivelul lucrării și care poate contribui la colecția de metadate evolutivă a lucrării (ex. rapoarte de citire, notificări, anunțuri, contor de mesaje, durata, etc).

Cerințe pentru ofertant:

Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru verificarea cerinței funcționale. Pentru fiecare cerință funcțională se va furniza un URL.

5.4.5.4 Cerințe specifice privind lucrările electronice

Soluția informatică propusă trebuie să asigure minim următoarele capabilități ce privesc lucrările electronice ce vor fi gestionate la nivelul instituției:

Fundamente și configurare sistem:

- Să dispună de nomenclator de procese cu guvernanță predefinită care să permită filtrarea în pagina utilizatorului doar a acelor tipuri de procese conforme cu competența sa materială sau teritorială;
- Să implementeze în activitatea funcționarilor conceptul de „manager de cont" - titular unic pentru rezolvarea lucrării;
- Să aibă definită la nivel de sistem o procedură de predare-primire a lucrărilor;

Inițierea și crearea lucrării:

- Să permită crearea / editarea / semnarea / configurarea și expedierea lucrărilor pe fluxurile de lucru în funcție de tipul lor;
- Să permită configurarea lucrării prin operațiuni precum crearea conținutului lucrării, stabilirea rolurilor și responsabilităților fiecărui participant, modelarea / remodelarea fluxului de semnare al documentelor lucrării, etc;

Procesarea și editarea lucrării:

- Să dispună de editoare de fișiere / mesaje text online ce includ elementele de formatare text standardizate la nivelul platformelor web;
- Să permită încărcarea de fișiere din calculator și din arhivele electronice aflate la dispoziția utilizatorului;
- Să integreze nomenclatorul arhivistic electronic pentru a permite utilizatorului să salveze fișierele pe grupe și dosare electronice;
- Să dispună în procesul de editare al unei lucrări de toate capabilitățile sistemului prezentate la actele electronice;
- Să permită salvarea ca ciornă a lucrării în curs de editare, precum și posibilitatea de a relua o lucrare salvată astfel;

Flux de lucru și automatizare:

- Să implementeze capabilități de automatizare a executării cursului lucrărilor - odată configurată lucrarea, executarea operațiunilor să se succeadă fără o intervenție explicită a utilizatorului.

Finalizare și expediere:

- Să permită expedierea atât în interiorul sistemului, cât și în afara lui;
- Să permită semnarea multiplă de lucrări cu toate fișierele atașate (ex. Pachete de lucrări) și expedierea automatizată a acestora pe fluxurile prestabilite;
- Să asigure expedierea ca tranzacție și aibă implementate proceduri de recuperare din eroare și revenire în starea precedentă consistentă în cazul în care apar erori în procesul de prelucrare și expediere;
- Să permită expedierea automată a lucrărilor electronice către destinatari în serii mari (fără a limita numărul lucrărilor din serie) - expedierea trebuie să tranziteze lucrările din serie prin operațiunea de sigilare electronică calificată și să permită destinatarilor să revină cu răspuns către instituție;

Vizualizare, raportare și istoric:

- Să dispună de o secțiune de evidență a lucrărilor la care participă funcționarul;
- Să permită vizualizarea tuturor lucrărilor la care utilizatorul participă în format listă / tabel;
- Să permită filtrarea / sortarea / căutarea lucrărilor în funcție de atributele menționate la secțiunea „cerințe conceptuale despre lucrări";
- Să dispună de un contor de lucrări care să se actualizeze funcție de filtrele aplicate în lista de lucrări;
- Să furnizeze rapoarte de progres de expediere și, în cazul în care în procesul de expediere au apărut erori, acestea sa fie capturate pentru a permite funcționarilor analizarea lor;
- Să permită vizualizarea istoricului detaliat al fiecărei lucrări la care a participat;

Integrări

- Să integreze secțiunea de evidență a lucrărilor să fie integrată cu registratura electronică a instituției, arhiva electronică a instituției, componenta de semnare și sigilare electronică calificată;

- Să se integreze cu componenta de management al identităților astfel încât să poată consuma cu ușurință informațiile / atributele furnizate de aceasta: ex. identitățile electronice profesionale, starea specifică la momentul redactării lucrării celorlalți participanți (activ, în concediu, suspendat, etc);

Cerințe pentru ofertant:

- Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru verificarea cerinței funcționale. Pentru fiecare cerință funcțională se va furniza un URL.
- Ofertantul va prezenta în detaliu procedura de predare-primire a lucrărilor între funcționari.
- Ofertantul va prezenta în detaliu modalitatea de implementare la nivelul lucrărilor a conceptului de „titular unic al lucrării".
- Ofertantul va prezenta în detaliu modalitatea de automatizare a executării lucrărilor.

5.4.5.5 Cerințe conceptuale privind dosarele electronice

Pentru a asigura o acurată înțelegere a nevoilor instituțiilor menționăm că la nivelul instituției au fost identificate 2 tipuri de dosare:

- Dosare de lucrări electronice/dosare operaționale - acest tip de dosare reunește mai multe lucrări în jurul unui topic comun - ele apar ca urmare a conexării mai multor lucrări;
- Dosare de acte electronice - acest tip de dosare agregă în același loc actele ce privesc un proces specific din activitatea instituției (ex. dosare de personal, dosare de achiziții publice, dosare de proiecte, etc).

Cerințe pentru ofertant:

- Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru verificarea cerinței funcționale. Pentru fiecare cerință funcțională se va furniza un URL.

5.4.5.6 Cerințe specifice privind dosarele de lucrări electronice

Soluția informatică propusă trebuie să asigure minim următoarele capabilități ce privesc dosarele electronice ce vor fi gestionate la nivelul instituției:

- Să dispună de o procedura de configurare a guvernanței digitale a dosarului de lucrare electronică care trebuie să cuprindă informații despre minim următoarele aspecte:
    - crearea și ștergerea dosarului
    - editarea atributelor dosarului
    - adăugarea și ștergerea de lucrări electronice în dosar
    - stabilirea drepturilor de acces la dosarul de lucrare electronică

Cerințe pentru ofertant:

- Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru verificarea cerinței funcționale. Pentru fiecare cerință funcțională se va furniza un URL.
- Ofertantul va detalia modalitatea de configurare a guvernanței dosarelor de lucrări electronice.

5.4.5.7 Cerințe specifice privind dosarele de acte electronice

Soluția informatică propusă trebuie să asigure minim următoarele capabilități ce privesc dosarele electronice ce vor fi gestionate la nivelul instituției:

- Să dispună de un mecanism de creare / editare a dosarelor de acte electronice care să stabilească ce funcționari și în ce condiții vor putea utiliza funcționalitatea
- Să permită o arhitectură de tip arbore („tree") cu dosare și sub dosare în care relațiile de subordonare între dosare la nivelul soluției să poată fi modificate

Cerințe pentru ofertant:

- Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru verificarea cerinței funcționale. Pentru fiecare cerință funcțională se va furniza un URL.
- Ofertantul va detalia modalitatea de configurare a guvernanței dosarelor de acte electronice.

5.4.6 Registre electronice

Registratura instituției va include un singur registru de lucrări la nivel de instituție, denumit Registrul Unic, și având următoarele responsabilități:

- Va asigura o evidență centralizată, astfel încât toate lucrările realizate în activitatea curentă să se regăsească într-o singură interfață.
- Va asigura numere unice de înregistrare lucrărilor.
- Va include atât lucrările de intrare și de ieșire, cât și lucrările interne.

Pe lângă Registrul Unic, sistemul va include Registre de acte (fără a limita numărul acestora) destinate structurilor din organigrama instituției (serviciu, birou, compartiment etc.).

Aceste registre au următoarele responsabilități:

- Vor asigura numere de înregistrare unice actelor (specifice activității structurii respective).

- Soluția informatică trebuie să permită posibilitatea ca mai multe structuri din instituție cu competențe similare să utilizeze același registru de acte.

Întregul sistem de registratură (incluzând Registrul Unic și Registrele de acte) trebuie să respecte următoarele cerințe funcționale:

- Configurabilitate: Soluția informatică trebuie să permită crearea și configurarea registrelor instituției.
- Integrare: Registrele trebuie să fie integrate cu arhiva electronică curentă.
- Gestiune multianuală (automatizarea închiderii de an): Registratura trebuie să permită gestiunea multianuală a registrelor, generarea automată a registrelor la începutul anului, arhivarea automată a registrelor din anul încheiat și conexarea registrelor din ani succesivi.

Cerințe pentru ofertant:

- Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la:
    - vizualizarea Registrului Unic de lucrări
    - vizualizarea Registrelor de acte
    - pagina de generare și parametrizare a registrelor (toate)
- Ofertantul va descrie modalitatea de integrare a registrelor cu arhiva electronică curentă furnizând URL-ul la care integrarea poate fi vizualizată.
- Ofertantul va face dovada automatizării procesului de regenerare a registrelor pentru anul următor, de arhivare automată a registrelor din anul tocmai încheiat și de conexare a registrelor din ani succesivi.

5.4.7 Înregistrarea lucrărilor și actelor – Termeni și Condiții

Numărul de înregistrare reprezintă contextul particular în care lucrarea / actul a luat naștere (la lucrările interne și cele de ieșire) sau a fost luat în evidența instituției (la lucrările de intrare).

Din acest motiv modalitatea de acordare a numerelor trebuie să fie riguros controlată și să reflecte întocmai realitatea.

Acordarea numerelor de înregistrare trebuie să țină cont de următorii Termeni și Condiții esențiali pentru a avea o evidență legală, corectă și transparentă a lucrărilor și actelor electronice din instituție:

- Numerele de înregistrare date lucrărilor se vor acorda automat de sistem respectând ordinea cronologică a creării lucrărilor;
- Acordarea numerelor de înregistrare se va face incremental;
- Pentru lucrările de intrare numerele de înregistrare se vor acorda la momentul luării lor în evidență, deci la momentul intrării;
- Pentru lucrările interne și cele de ieșire numerele de înregistrare se vor acorda în momentul în care lucrarea a parcurs fluxul de avizare și aprobare, respectiv a fost semnată electronic calificat de toți semnatarii și sigilată electronic calificat cu sigiliul electronic al instituției;
- Acordarea numerelor de înregistrare trebuie fie securizată și auditabilă;
- Soluția informatică trebuie să poată aloca numere lucrărilor atât în format individual, cât și în serii mari de lucrări (zeci de mii de lucrări consecutiv);
- Numerele de înregistrare acordate lucrărilor și actelor vor fi unice;
- Numerele de înregistrare vor fi inserate în structura actului în format pdf împreună cu toate metadatele autorului, semnatarilor și instituției;
- Numerele de înregistrare vor fi vizibile atât pe act, cât și în panoul de semnături al actului alături de toate celelalte metadate;
- Soluția informatică trebuie să permită funcționarului ca, la nevoie, acesta sa poată stabili amplasarea în cadrul documentului a numărului de înregistrare - locul unde va fi vizibil pe document fiind important pentru a evita suprapunerea numărului de înregistrare peste conținutul actului;
- Soluția trebuie să permită tipărirea la nevoie a numărului de înregistrare pentru lucrările primite și luate în evidență la ghișeu;
- Soluția informatică trebuie să permită, în cazuri agreate la nivel instituțional, ca lucrările (inclusiv actele pe care acestea le includ) sa fie marcate ca fiind clasate;
- Soluția informatică nu va permite ștergerea numerelor de înregistrare.

5.5 Interconectare, interoperabilitate și colaborare intra-/interinstituțională

5.5.1 Operaționalizarea canalelor de comunicare inter și intra-instituționale

Soluția propusă trebuie să asigure transportul datelor între structurile interne ale Direcției de Asistență Socială Drobeta-Turnu Severin cât și între instituțiile vizate pentru interconectare prin proiect, respectiv să permită încărcarea, transmiterea bidirecțională și livrarea către destinatar a conținutului personalizat (fișiere și date structurate), asigurând garanțiile specifice de livrare înregistrată.

Notă: instituțiile vizate pentru interconectare sunt prezentate în secțiunea dedicată a cap. „Cerințe de parametrizare a soluției informatice”.

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă sau va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată.

5.5.2 Operaționalizarea canalelor de comunicare între funcționari și cetățeni/reprezentanții mediului de afaceri

Soluția propusă trebuie să includă o platforma multi-instituțională de interacțiune și comunicare bidirecțională între funcționari și cetățeni. Prin această platformă cetățenii vor dobândi acces de oriunde, de pe orice tip de dispozitiv fix sau mobil și în orice moment la serviciile publice oferite de Direcția de Asistență Socială Drobeta-Turnu Severin și de instituțiile subordonate. Platforma de interacțiune cu cetățenii va asigura un punct centralizat de acces al cetățenilor la serviciile sociale aflate în competența Direcției de Asistență Socială Drobeta-Turnu Severin. Soluția va trebuie să fie disponibilă tuturor utilizatorilor persoane fizice, persoane juridice și funcționari și să fie personalizată în funcție de specificul de utilizare al fiecărui tip de utilizator.

Mărimea fișierelor trebuie să fie controlată prin politici de restricționarea a documentelor și de menținere a conținutului pentru o perioadă determinată de timp.

Pentru persoane fizice și juridice, soluția de mesagerie electronică trebuie să adreseze următoarele cerințe funcționale specifice digitalizării proceselor alături de cele specifice tuturor soluțiilor de tip „e-mail client", respectiv:

- Structură de comunicări: Să dispună de structura clasică a clienților de email: Primite, Trimise, Ciorne, Șterse, Arhivate.
- Mesagerie: Să permită schimbul de mesaje bidirecțional cu instituția, instituțiile subordonate și cu cele vizate pentru interconectare, incluzând destinatar, subiect, conținut mesaj și atașamente.
- Standardizarea formatului: Să aibă integrate capabilități de conversie automată și manuală în PDF a atașamentelor cel puțin din formatele txt, doc/docx/odt, xls/xlsx/ods, jpg/jpeg/bmp/tiff.
- Protejarea conținutului: Să aibă integrate capabilități integrate de semnare electronică calificată a fișierelor atașate.
- Gestiunea fluxului de date și documente: Soluția trebuie să asigure procedurile complete și sigure pentru întregul ciclu de viață al conținutului (date și documente), incluzând: încărcarea, transportul securizat (transfer), livrarea către utilizatori/module, vizualizarea conținutului în interfață.

Pentru funcționari, soluția de mesagerie electronică trebuie să adreseze următoarele cerințe funcționale specifice digitalizării proceselor alături de cele specifice tuturor soluțiilor de tip „e-mail client", respectiv:

- Structură de comunicări: Să dispună de structura clasică a clienților de email: Primite, Trimise, Ciorne, Șterse, Arhivate.
- Mesagerie: să permită schimbul de mesaje bidirecțional între funcționari și toate tipurile de utilizatori, incluzând destinatar, subiect, conținut mesaj și atașamente.
- Comunicare cu non-utilizatori: Să permită schimbul bidirecțional de mesaje (trimitere și primire) cu orice parte terță (persoane fizice sau reprezentanți ai persoanelor juridice) care nu e utilizator înregistrat în sistem.
- Integrare cu registratura: Să fie integrată cu registratura online automatizată pentru a permite transformarea unui mesaj în lucrare când aceasta întrunește condițiile cerute de instituție. Se dorește astfel evitarea transferului manual între soluții diferite de mesagerie a conținutului solicitărilor.
- Standardizarea formatului: Să aibă integrate capabilități de conversie automată și manuală în PDF a atașamentelor cel puțin din formatele txt, doc/docx/odt, xls/xlsx/ods, jpg/jpeg/bmp/tiff.
- Protejarea conținutului: Să aibă integrate capabilități integrate de semnare electronică calificată a fișierelor atașate.
- Instrumente de lucru colaborativ și asistare digitală: Soluția trebuie să pună la dispoziție o suită de instrumente integrate pentru colaborare în timp real și asincron, incluzând:
    - mesagerie instant: schimb bidirecțional de mesaje (text), comunicare individuală (1-la-1) și în grupuri (canale), posibilitatea de a atașa și partaja fișiere.
    - conferințe și partajare: audio conferință, video conferință (individuală și de grup), partajare de ecran.
    - editare colaborativă: crearea și editarea simultană (colaborativă) a documentelor (de tip text).
- Gestiunea fluxului de date și documente: Soluția trebuie să asigure procedurile complete și sigure pentru întregul ciclu de viață al conținutului (date și documente), incluzând: încărcarea, transportul securizat (transfer), livrarea către utilizatori/module, vizualizarea conținutului în interfață.

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă sau va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată.

5.5.3 Comunicarea prin intermediul formularelor electronice inteligente

Soluția trebuie să implementeze un constructor de formulare care să permită personalizarea/parametrizarea oricărui tip de formular necesar în activitatea curentă a instituției, precum și comunicare pe bază de formulare inteligente pentru uzul utilizatorilor externi (cetățeni) și pentru uzul intern al funcționarilor.

Formularele inteligente implementate trebuie:

- să fie grupate pe tipuri de utilizatori;
- să asigure colectarea datelor în format structurat și validat la nivelul introducerii datelor;
- să furnizeze contextual documentele justificative specifice aferente fiecărui tip de formular;
- să dispună de o zonă de administrare care sa permită instituției să configureze fiecare formular în parte;
- să dispună de posibilitatea de a fi salvate în Ciorne pentru cazurile în care editarea nu a putut fi finalizată și va trebui reluată la un moment ulterior;

- să dispună de capabilități integrate de semnare electronică calificată;
- să fie interconectate cu arhiva utilizatorului pentru a permite încărcarea de documente atât din calculator, cât și din arhiva electronică.

Sistemul informatic va permite exploatarea tuturor formularelor prin registratura instituției și va permite configurarea lor pentru a tranzita fluxurile electronice de lucru și a asigura exportul de date în formate standardizate către destinatari (ex. formulare pentru cetățeni, formulare pentru activitatea internă a instituției, formulare destinate comunicării inter-instituționale, etc.)
Cerințele funcționale menționate la secțiunea documente / acte electronice se vor aplica întocmai și în cazul formularelor.
Sistemul va dispune de motoare de căutare și selectare a formularelor inteligente folosite cu o frecventă mai mare într-o zonă de „Favorite".
Utilizatorii trebuie să aibă la dispoziție o secțiune în care vor putea vizualiza toate solicitările trimise/primite prin formulare inteligente. Secțiunea va implementa mecanisme de filtrare, sortare, căutare după metadatele colectate și relevante în fiecare context.
Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă sau va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată.

Configurarea de fluxuri predefinite
Configurarea fluxurilor electronice predefinite în soluția informatică trebuie să fie condiționată de următorii factori ce țin de guvernanța electronică a instituției:

- Competența materială și teritorială a funcționarilor;
- Structura organizatorică a instituției (structura de compartimente și relațiile ierarhice dintre acestea);
- Gradul de încărcare al funcționarilor;
- Procedurile interne ale instituției;
- Modelarea fluxurilor de lucru trebuie să fie facilă și să nu necesite un nivel ridicat de expertiză it;
- Trecerea la un flux de lucru ajustat nu trebuie să influențeze structurile de date create de versiunile anterioare ale fluxului;
- Modelarea fluxului să includă cel puțin următoarele caracteristici:
    - denumirea fluxului creat;
    - capabilități de creare de conținut structurat (text, inputuri, validări, etc);
    - procesul la care se referă (competența materială);
    - date despre inițiator;
    - date despre semnatari;
    - date despre destinatar;
    - parcursul instituțional pe care îl poate avea;
    - eventuale condiționări specifice determinate de guvernanța instituțională (ex. competență teritorială);
    - condiționări cu privire la semnarea electronică a documentelor;
    - termenii și condițiile înregistrării, procesării, finalizării și arhivării electronice a lucrărilor astfel generate.
- Fluxurile predefinite relevante să fie disponibile tuturor categoriilor de utilizatori (persoane fizice, juridice, funcționari - atât pe canalul offline - prezență fizică, cât și pe canalul online).

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă sau va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată.

Modelarea contextuală a fluxurilor electronice
Soluția informatică propusă trebuie să dispună de capabilități de modelare și execuție de fluxuri de lucru, documente și informații în cadrul instituției cu respectarea următoarelor cerințe funcționale:

- posibilitatea de modelare trebuie sa fie disponibilă tuturor funcționarilor;
- odată modelat fluxul, acesta se va executa automat fără intervenția funcționarului;
- să fie implementat un mecanism de revenire în starea inițială în mod tranzacțional („rollback") care să poată fi apelat motivat de oricare dintre participanții la flux.

Modelarea fluxului să includă cel puțin următoarele caracteristici:

- denumirea fluxului creat;
- capabilități de creare de conținut structurat (text, intrări de date, validări, etc);
- procesul la care se referă (competența materială);
- date despre inițiator;
- date despre semnatari;
- date despre destinatar;
- monitorizarea executării fluxului;
- eventuale condiționări specifice determinate de guvernanța instituțională (ex. competență teritorială);

- condiționări cu privire la semnarea electronică calificată și sigilarea electronică calificată a documentelor, precum: desemnarea semnatarilor, stabilirea ordinii semnării, stabilirea motivului semnării pentru fiecare semnatar în parte, poziționarea semnăturilor, poziționarea sigiliului, versionarea documentelor în procesul de semnare, anularea semnării, revizuirea semnării;
- termenii și condițiile înregistrării, procesării, finalizării și arhivării electronice a lucrărilor astfel generate.

Modelarea fluxurilor electronice va respecta următoarele reguli:

- Contextualitate: Fluxurile vor putea fi adaptate la contextul specific al fiecărui proces de lucru și tip de document.
- Automatizare: Cât mai multe etape ale fluxurilor vor putea fi automatizate pentru a reduce timpul de procesare și a minimiza erorile.
- Transparență: Fluxurile vor fi transparente și ușor de urmărit de către utilizatori.
- Flexibilitate: Fluxurile vor fi flexibile și ușor de modificat în funcție de schimbările din procesele de lucru.

Managementul fluxurilor electronice

Fluxurile electronice reprezintă traseul pe care îl parcurg acțiunile, documentele și informațiile prin diferitele etape ale procesului de lucru, de la creare până la arhivare.

Sistemul va suporta următoarele tipuri de fluxuri electronice:

- Fluxuri de lucru (workflow-uri): Reprezintă succesiunea de etape și acțiuni necesare pentru finalizarea unei sarcini sau a unui proces. De exemplu, fluxul de lucru pentru aprobarea unei comunicări.
- Fluxuri de documente: Reprezintă traseul pe care îl parcurg documentele electronice prin diferite etape de avizare, semnare și înregistrare. De exemplu, fluxul de documente pentru o factură.
- Fluxuri de informații: Reprezintă circulația informațiilor între diferite sisteme și utilizatori. De exemplu, fluxul de informații privind numărul lucrărilor în lucru.

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă sau va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată.

Automatizarea proceselor de expediere a conținutului

Soluția informatică trebuie să fie capabilă să execute în regim automatizat procese operaționale complexe care includ:

- Colectarea semnăturilor electronice;
- Înregistrarea documentelor;
- Sigilarea electronică calificată;
- Arhivarea electronică;
- Expedierea;
- Finalizarea lucrării.

5.5.4 Parametrizarea de notificări de sistem în funcție de tipul de utilizator

Soluția informatică propusă trebuie să dispună de capabilități de notificare pentru toate tipurile de utilizatori, respectiv:

- Notificări pe e-mail;
- Notificări în contul personal;
- Notificări de tip „push” în aplicația mobilă;

Pe durata prestării serviciilor, transmiterea de notificări nu va fi limitată de Prestator cantitativ (cum ar fi spre exemplu pachete numărul de notificări), și nici calitativ (cum ar fi spre exemplu pachete de notificări adresate cetățenilor dintr-o arie de acoperire).

Notificări pe e-mail

Soluția informatică propusă trebuie să poată trimite notificări pe e-mail ori de câte ori este nevoie pentru a semnaliza utilizatorului ceva de interes.

Notificări în contul personal și notificări pe dispozitivele mobile

Soluția informatică trebuie să poată trimite notificări de tip „push” către dispozitivele mobile ale utilizatorului, instantaneu sau în „coadă”, cu respectarea următoarelor cerințe funcționale:

- Notificările să poată fi trimise către utilizatori / grupuri de utilizatori minim către:
    - un utilizator individual persoana fizică, juridică sau funcționar;
    - administratorii persoanelor juridice;
    - toți reprezentanții unei persoane juridice;
    - toți funcționarii;
    - toți funcționarii dintr-o anumită instituție;
    - toți reprezentanții persoanelor juridice;
    - toți utilizatorii asociați unei adrese poștale.
- Să permită parametrizarea mesajului de trimis (număr de caractere);
- Să furnizeze informații de progres cu privire la trimiterea de notificări în serii/loturi mari;

- Să aibă implementate proceduri de recuperare din eroare și revenire în starea precedentă consistentă în cazul în care apar erori în procesul de trimitere.

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă sau va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată.

5.5.5 Sincronizarea cu managementul identităților, înregistrarea, arhivarea și îndosarierea electronică

Sincronizarea cu componenta de management al identităților, cu cea de înregistrare, precum și cu cea de arhivare și îndosariere electronică.

Cerințe pentru ofertant:

- Ofertantul va descrie în detaliu, în Propunerea Tehnică, modul în care a fost proiectată arhitectura soluției pentru a îndeplini sincronizarea funcțională, incluzând descrierea arhitecturii logice: Se va prezenta modul în care fluxurile de comunicare (din componenta de interconectivitate) consumă în timp real informații și atribute de la celelalte componente.

5.5.6 Interconectări cu alți furnizori de servicii

Soluția Informatică trebuie să dispună de integrări prin API-uri sau Web Services cu sisteme digitale existente la nivel național și european care furnizează capabilități tehnice de interconectare:

- Sistemele instituțiilor care gestionează registrele critice care dispun de astfel de instrumente de comunicare, respectiv ANAF și ONRC;
- Sistemul național de identitate electronică ROeID;
- Furnizorul de servicii de încredere STS (Serviciul de Telecomunicații Speciale);
- Administratorul la nivel european al European Union Trusted Lists (EUTL - furnizori de servicii de încredere acreditați pentru a oferi cele mai nivelurile de conformitate cu Regulamentul UE privind semnătura electronică (eIDAS).

Raportat la soluțiile de interoperabilitate prin care sistemele informatice ce fac obiectul proiectului pot asigura transferul facil al datelor cu alte sisteme informatice trebuie menționat că acestea vor fi menționate de fiecare ofertant în procedura de ofertare. Instituția lasă la latitudinea potențialilor ofertanți soluțiile tehnice de interoperabilitate cu amendamentul că acestea trebuie să fie conforme prevederilor legii 242 din 2022.

Cerințe pentru ofertant:

- Ofertantul va prezenta în Propunerea Tehnică documentația tehnică a serviciilor API pentru realizarea interconectivității. Structurile de date menționate în documentație trebuie să fie complete și să respecte cerințele referitoare la lucrări și acte.

5.6 Arhivarea și îndosarierea electronică

Arhivarea electronică vizează asigurarea următoarelor funcționalități:

- Asigurarea procedurilor de creare și parametrizare multianuală a nomenclatorului arhivistic (grupele de documente);
- Gestionarea structurilor de metadate pentru documentele arhivate;
- Asigurarea procedurilor de creare și parametrizare multianuală a structurii de îndosariere a actelor (dosarele de acte);
- Automatizarea arhivării electronice a documentelor;
- Întreținerea listelor de documente;
- Asigurarea procedurilor de acces la arhiva electronică istorică;
- Asigurarea mecanismelor de mutare a documentelor între grupele de arhivă;
- Asigurarea motoarelor de căutare în grupele arhivistice;
- Implementarea mecanismelor de sortare a documentelor în vederea distrugerii;
- Implementarea măsurilor de auditare a accesului la documente;
- Parametrizarea de rapoarte specifice arhivării electronice și stabilirea drepturilor de acces la rapoarte.

Soluția informatică propusă trebuie să pună la dispoziția fiecărui tip de utilizator (persoană fizică, persoană juridică sau angajat):

- Arhivă electronică de documente/acte - destinată să permită utilizatorului accesul rapid la toate documentele sale (atât documente personale, cât și acte emise de instituție);
- Arhivă electronică de lucrări - destinată arhivării solicitărilor trimise către instituție și care au fost deja finalizate.
- Cerințe pentru ofertant:
- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă.

5.6.1 Cerințe specifice privind arhiva electronică de documente / acte a persoanelor fizice și juridice

Soluția informatică propusă trebuie să dispună de următoarele capabilități tehnice:

- Să fie integrată cu componenta de management a identităților electronice și permită accesul la documente în funcție de nivelul de încredere (scăzut / substanțial sau ridicat);
- Să fie integrată cu componenta de formulare electronice și cu soluția de comunicare electronică a sistemului astfel încât utilizatorul să poată încărca individual sau în loturi documente direct din arhiva sa electronică;
- Să permită utilizatorilor autorizați vizualizarea, descărcarea și tipărirea documentelor / actelor;

- Să permită vizualizarea tuturor metadatelor stocate la nivelul sistemului pentru fiecare document / act în parte;
- Să dispună de capabilități de filtrare, sortare și căutare în funcție de metadate relevante (ex. Denumire fișier, număr de înregistrare, data, etc);
- Să permită utilizatorului ștergerea documentelor / actelor din arhiva personală;
- Să nu permită utilizatorului ștergerea actelor transmise lui de către instituții;
- Să permită utilizatorului să vizualizeze lucrarea din care a făcut parte actul emis și transmis lui de către instituție;
- Să dispună de mecanisme de colectare nativă și implicită (fără ca utilizatorul să facă un efort suplimentar în acest sens) a metadatelor prin inputuri controlate, validate și parametrizate în vederea asigurării unui nivel superior de acuratețe a acestor informații.
- Să dispună de o politică de management a documentelor încărcate în sistem cel puțin din perspectiva:
    - formatelor de fișiere acceptate;
    - parametrii denumirilor fișierelor;
    - mărimea fișierelor;
    - scanarea documentelor;
    - accesului la fișiere (în cazul persoanelor juridice care au mai mulți reprezentanți soluția trebuie să stabilească drepturile de acces ale fiecăruia la fișiere).

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă sau va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată;
- Ofertantul va descrie în detaliu mecanismul de colectare a metadatelor implementat în soluția ofertată;
- Ofertantul va descrie în detaliu politica de management a documentelor implementată în soluția ofertată.

5.6.2 Cerințe specifice privind arhiva electronică de lucrări a cetățenilor și persoanelor juridice

Soluția informatică propusă trebuie să dispună de următoarele capabilități tehnice:

- Să permită utilizatorilor autorizați vizualizarea lucrărilor și a documentelor asociate;
- Să permită vizualizarea tuturor metadatelor stocate la nivelul sistemului pentru fiecare lucrare;
- Să dispună de capabilități de filtrare, sortare și căutare în funcție de metadate relevante (ex. denumire, conținut, număr de înregistrare, data, etc);
- Să nu permită utilizatorului ștergerea lucrărilor transmise lui de către instituții.

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă sau va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată;
- Ofertantul va descrie în detaliu mecanismul de colectare a metadatelor implementat în soluția ofertată.

5.6.3 Cerințe specifice privind arhiva de documente electronice a instituției

Soluția informatică oferită trebuie să dispună de capabilități de arhivare electronică instituțională care să îndeplinească minim următoarele condiții:

- Să permită crearea nomenclatorului arhivistic electronic (conform prevederilor legale) și managementul arhivei electronice instituționale;
- Să fie integrată la nivelul soluției informatice propuse în toate mijloacele de comunicare relevante ce produc consecințe juridice;
- Să fie integrată cu componenta de management a identităților pentru a colecta actele de identitate ale utilizatorului direct din procedura de înrolare („onboarding”);
- Să dispună de mecanisme auditabile (log-uri) explicite cu privire la orice modificare, acces sau operațiune ce are impact în arhiva electronică;
- Să fie sincronizată cu registrele instituției pentru a asigura o bună trasabilitate și transparență în gestiunea actelor;
- Să salveze toate metadatele relevante ale actelor în structura pdf a acestora;
- Să poată exporta la cererea beneficiarului, în format structurat și fără costuri pentru beneficiar, toate actele existente în sistem și datele colectate ca obligație legală a instituției. Datele care există în sistem în vederea personalizării experienței de utilizare nu fac subiectul acestei obligații.

Soluția informatică ofertată trebuie să dispună de capabilități de:

- configurare de fluxuri de arhivare predefinite;
- modelare contextuală de fluxuri de arhivare.

Pentru arhivarea pe termen lung cu valoare legală, soluția trebuie să fie capabilă să transfere în mod securizat documentele electronice și metadatele arhivistice asociate către un serviciu de arhivare electronică acreditat de ADR ca „administrator de arhivă electronică”, sau este interconectat în mod sigur cu acesta.

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă sau va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată.
- Ofertantul va prezenta în propunerea tehnică capabilitatea de export a datelor și documentelor arhivate în formate standard, deschise și interoperabile (de exemplu, PDF/A, XML cu scheme asociate), pentru a asigura reversibilitatea, portabilitatea datelor și accesul pe termen lung la arhivă, independent de continuitatea serviciului SaaS respectiv.

5.6.4 Cerințe specifice privind arhiva de lucrări electronice a instituției

Soluția informatică propusă trebuie să dispună de următoarele capabilități tehnice:

- Să permită funcționarilor autorizați vizualizarea lucrărilor și a documentelor asociate;
- Să permită vizualizarea tuturor metadatelor stocate la nivelul sistemului pentru fiecare lucrare;
- Să dispună de capabilități de filtrare, sortare și căutare în funcție de metadate relevante (ex. Denumire, conținut, număr de înregistrare, data, etc);
- Să nu permită utilizatorului ștergerea lucrărilor transmise lui de către instituții.

Cerințe pentru ofertant:

- Ofertantul va prezenta în propunerea tehnică modalitatea de îndeplinire a cerințelor în soluția propusă sau va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată.

5.7 Semnarea și sigilarea electronică calificată

5.7.1 Semnarea electronică calificată

Soluția informatică ofertată va putea utiliza fără niciun fel de restricționare certificate calificate emise de orice furnizor de servicii de încredere acreditat la nivelul Uniunii Europene, în conformitate cu prevederile regulamentului eIDAS.

Documentele încărcate în sistem vor putea fi semnate electronic cu orice tip de instrument criptografic cu certificat calificat stocat pe token sau în cloud, emis de furnizor de servicii de încredere acreditat la nivel european.

Certificatele calificate cu chei criptografice stocate în cloud se vor putea sincroniza cu sistemul oferind posibilitatea realizării unui management riguros al acestuia: ex. import, ștergere, vizualizare detalii certificat, etc.

Soluția informatică trebuie să dispună de integrare cu minim 2 furnizori de servicii de încredere acreditați la nivel european și cu STS.

Din perspectiva semnării electronice calificate Autoritatea Contractantă urmărește realizarea următoarelor cerințe funcționale:

- Să permită sincronizarea / desincronizarea certificatului calificat de semnare electronică cu sistemul;
- Să permită, opțional, integrarea semnăturii olografe în semnătura electronică calificată;
- Să dispună de integrarea semnăturii electronice calificate pe toate fluxurile de comunicare implementate la nivelul sistemului;
- Să permită semnarea simplă (1 document) și semnarea mai multor documente în serii tuturor utilizatorilor sistemului, în plus, salariaților semnarea de tip „queue” (coadă);
- Să permită un management contextual al motivelor de semnare;
- Să permită semnarea în interiorul sau independent de existența unui flux de semnare;
- Să permită verificarea și validarea semnăturilor electronice calificate aplicate pe documente / acte, respectiv:
    - validarea tipului de semnătură;
    - verificarea lanțului de încredere al certificatului;
    - data și ora semnării;
    - identitatea celui care a semnat;
    - dacă documentul a fost sau nu modificat după semnare;
    - date privind valabilitatea certificatului calificat;
    - emitentul certificatului;
    - motivul de semnare.
- Să permită poziționarea semnăturii electronice calificate vizibile pe document la libera alegere a utilizatorului - dacă documentul suport va avea factor de rotație inserat aplicarea va ține cont de acesta;
- Să permită operațiuni precum anularea semnării, revizuirea semnării, reluarea semnării;
- Să permită vizualizarea listingului de solicitări de semnare și gestionarea cererilor / invitațiilor de semnare;
- Să permită salariaților semnarea multiplă a mai multor lucrări odată, cu posibilitatea de selectare a lucrărilor care vor face obiectul semnării;
- Să permită previzualizarea documentelor ce urmează a fi semnate fără să fie nevoie de descărcarea lor.

Cerințe pentru ofertant:

- Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată. Pentru fiecare cerință funcțională se va furniza un URL.
- Ofertantul va indica cel puțin 2 furnizori de servicii de încredere acreditați integrați în sistem (în afară de STS).

5.7.2 Sigilarea electronică calificată

Soluția informatică ofertată va putea utiliza fără niciun fel de restricționare sigilii electronice calificate găzduite în cloud emise în conformitate cu prevederile regulamentului eIDAS de orice furnizor de servicii de încredere acreditat de pe teritoriul Europei.
Accesul soluției informatice propuse la sigiliul electronic găzduit în cloud se va face securizat și auditabil.
Soluția informatică trebuie să dispună de integrare cu minim 2 furnizori de servicii de încredere acreditați la nivel european și cu STS.
Din perspectiva sigilării electronice calificate, Autoritatea Contractantă urmărește realizarea următoarelor cerințe funcționale:

- Să permită sigilarea electronică calificată atât în regim de aplicare automată, cât și în regim de aplicare manuală;
- Să permită sigilarea electronică calificată simultană a mai multor documente și sigilarea de tip „queue" (coadă);
- Să permită gestionarea a multiple cozi de sigilare pentru a asigura o viteză de aplicare sporită când sistemul execută sigilarea electronică calificată a unui număr foarte mare de acte;
- Să fie integrat cu mecanismul de acordare a numerelor de înregistrare tuturor actelor originale sau luate în evidență în sistem;
- Să permită poziționarea vizibilă a sigiliului electronic în orice loc pe document - dacă documentul suport va avea factor de rotație inserat, aplicarea va ține cont de acesta;
- Să dispună de mecanisme de revenire în starea precedentă pentru cazurile în care documentele lansate spre sigilare electronică calificată prezintă erori structurale și nu pot fi sigilate, necesitând intervenția unui operator tehnic în acest sens.

Cerințe pentru ofertant:

- Ofertantul va pune la dispoziție URL-ul la care funcționalitatea poate fi accesată sau detalii relevante de navigare pentru a ajunge la funcționalitatea implementată. Pentru fiecare cerință funcțională se va furniza un URL;
- Ofertantul va indica cel puțin 2 furnizori de servicii de încredere acreditați integrați în sistem (în afară de STS);
- Ofertantul va descrie modalitatea securizată prin care platforma va avea acces la sigiliul electronic stocat în infrastructura cloud a furnizorului QSEAL.

5.8 Securitatea și auditul platformei

Cerințe de securitate cibernetică și conformitate
Soluția informatică propusă trebuie să fie protejată împotriva amenințărilor cibernetice și să asigure conformitatea cu legislația națională și europeană în vigoare, incluzând **Regulamentul GDPR (UE) 679/2016** și **Directiva NIS2 (UE) 2555/2022**.
Implementarea soluției comportă respectarea cel puțin a următoarelor cerințe privind măsuri asiguratorii de securitate cibernetică:

5.8.1 A. Confidențialitate

Soluția trebuie să implementeze criptarea end-to-end a datelor sensibile și să protejeze datele împotriva accesului neautorizat.

- **Date în tranzit (Securitatea comunicațiilor):**
  - Accesul la soluția informatică se va face prin URL securizat cu certificat site-SSL.
  - Toate comunicațiile externe și interne care transportă date sensibile (inclusiv API-uri, interfețe web, transferuri „browser to server" și „server to server") vor fi securizate utilizând protocoale de criptare moderne și standardizate (ex: TLS v1.2 sau ulterior), cu suite de cifrare robuste.
  - Platforma trebuie să utilizeze certificate de autentificare TLS sau echivalent.
- **Date în repaus (Criptarea informației):**
  - Toate bazele de date, stocarea de fișiere (inclusiv volumele de stocare persistente) și orice alte medii de stocare care conțin date sensibile vor fi criptate folosind algoritmi de criptare robuști (ex: AES-256).
  - Comunicarea, atât între componentele arhitecturale ale soluției, cât și între acestea și cele de stocare, se va face criptat.
- **Managementul cheilor:**
  - Cheile de criptare vor fi gestionate de Prestator în conformitate cu bune practici (ex: utilizarea unui key management service - KMS).
  - Responsabilitatea gestionării și înlocuirii periodice a cheilor de criptare revine prestatorului.
- **Conformitate GDPR:**
  - Soluția trebuie să descrie modalitatea de anonimizare a datelor în interfețele de lucru curente.
  - Trebuie implementată modalitatea de capturare și stocare a acordului de procesare a datelor cu caracter personal.
- **Acces autorizat:** Se va asigura accesul la date strict pe baza autorizației (detaliat la secțiunea D).

5.8.2 B. Integritate

Soluția va implementa mecanisme pentru a preveni și detecta modificările neautorizate ale datelor și ale codului.

- **Protecția conținutului:**
  - Integritatea conținutului utilizatorului și a metadatelor asociate trebuie protejate pe toată durata stocării și transmiterii.
  - Dacă se impun modificări, acestea trebuie aduse la cunoștința utilizatorului în mod transparent, platforma stocând dovezi despre forma inițială.

- **Validarea datelor:** La toate punctele de intrare și procesare, vor fi aplicate reguli stricte de validare și standardizare a datelor (inclusiv verificări de tip, format, lungime și conținut) pentru a preveni injecțiile de cod și coruperea datelor.
- **Mecanisme de control (Semnarea și sigilarea):**
    - Semnătura electronică calificată și sigiliul electronic calificat constituie măsuri de control de securitate care asigură integritatea, autenticitatea și non-repudierea.
    - Vor fi utilizate mecanisme de hashing și semnături digitale (acolo unde este cazul) pentru a verifica autenticitatea și integritatea datelor critice pe parcursul ciclului de viață (ex: la transfer, arhivare).
- **Piste de audit:** Orice modificare a datelor critice trebuie să fie înregistrată într-un jurnal de audit (log) ne-modificabil (detaliat la secțiunea E).

5.8.3 C. Disponibilitate

Soluția trebuie să asigure o funcționare continuă (înaltă disponibilitate), o recuperare rapidă în caz de defecțiune și o infrastructură robustă.

- **Infrastructură și certificări:**
    - Conform cap. „Cerințe ale infrastructurii cloud".
- **Redundanță și SLA:**
    - Arhitectura soluției va include redundanță la nivel de componente critice (aplicație, baze de date, rețea).
    - Sistemul trebuie să asigure mecanisme automate de disponibilitate continuă (failover) pentru a minimiza timpul de nefuncționare.
    - Operațiunile intensive de backup se vor programa automatizat în intervalul orar 00:00 – 05:00 pentru a nu afecta performanța.
    - Sistemul trebuie să asigure o disponibilitate a serviciilor (**SLA**) de minim **99,9%** pe durata programului de lucru în decursul unui an.
- **Monitorizare:** Vor fi implementate sisteme de monitorizare proactive a stării de funcționare, performanței și capacității sistemului, cu alerte automate, pentru a menține SLA-ul contractual.
- **Backup și recuperare (Disaster Recovery):**
    - Va fi implementată o politică/procedură de backup regulată și testată (inclusiv a datelor criptate), capabilă să restabilească serviciile în termenele RTO și RPO specificate.
    - Prestatorul este responsabil pentru asigurarea soluției de backup în caz de dezastre (DR).
    - Soluția de backup trebuie să asigure copii de siguranță pentru mai multe versiuni ale aceleiași entități logice (restaurări selective).

5.8.4 D. Autentificare, autorizare și principiul celui mai mic privilegiu

Soluția va folosi mecanisme de control al accesului robuste și granulare.

- **Autentificare:**
    - Utilizatorii trebuie să fie autentificați înainte de a li se permite accesul.
    - Sistemul trebuie să poată determina univoc identitatea utilizatorului.
    - Se va utiliza o soluție de identitate bazată pe standarde deschise (ex: OAuth 2.0, OpenID Connect, SAML).
- **Autentificare Multi-Factor (MFA/2FA):**
    - Soluția trebuie să asigure un strat suplimentar de securitate de tip autentificare cu doi factori (2FA), obligatoriu cel puțin pentru administratori și utilizatori cu drepturi extinse.
    - Metodele acceptate includ cel puțin: dispozitive hardware/software 2FA (ex. cartea electronică de identitate + IDPLUGMANAGER), OTP via SMS sau email sau notificări push.
- **Autorizare (RBAC) și principiul celui mai mic privilegiu:**
    - Va fi implementat un model granular de autorizare bazată pe roluri (RBAC).
    - Sistemul trebuie să restricționeze drepturile de acces ale utilizatorului la funcționalitățile și datele sistemului pe baza rolului desemnat acestuia.
    - Atât utilizatorii, cât și componentele sistemului (conturi de servicii) vor primi doar acele permisiuni strict necesare (principiul celui mai mic privilegiu).
    - Accesul funcționarilor la informațiile utilizatorilor trebuie să se facă doar individual și condiționat de existența unui motiv temeinic (principiul „nevoii de a cunoaște"). Motivul accesului va fi capturat în sistem.
    - Sistemul nu va permite niciunui funcționar vizualizarea tuturor identităților personale din sistem sub formă de listă și fără un motiv capturat la momentul accesului.
- **Gestionarea credențialelor:** Sistemul va avea reguli parametrizate privind politica de securitate (complexitatea parolei, perioada de valabilitate, număr de încercări eșuate).

5.8.5 E. Non-repudiere (Audit și jurnalizare)

Soluția trebuie să asigure înregistrarea necontestabilă a acțiunilor critice efectuate de utilizatori, pentru toate accesele la date (în special cele cu caracter personal), pentru modificările de configurație ale sistemului și pentru toate evenimentele de securitate detectate, prin logare detaliată și protejată.

- **Logare și audit:**
    - Toate activitățile derulate în sistem trebuie înregistrate (jurnale de audit / log-uri) pentru a permite auditarea ulterioară.
    - Va fi implementat un sistem de logare centralizat (ex: SIEM) care să înregistreze detaliat și trasabil toate evenimentele de securitate și acțiunile critice (ex: login, modificări de permisiuni, acces la date sensibile, modificări privind identitatea electronică).
    - Toate evenimentele referitoare la identitatea inițială și autentificările ulterioare trebuie jurnalizate.
    - Componenta de securitate trebuie să asigure crearea și întreținerea dinamică a sistemului de log-uri.
- **Imuabilitate și protecție:**
    - Log-urile și jurnalele de audit trebuie să fie protejate împotriva modificărilor sau ștergerilor.
    - Platforma trebuie să garanteze confidențialitatea, integritatea și disponibilitatea log-urilor de sistem și arhivarea acestora pentru scopuri legale în conformitatea cu prevederile naționale, iar aceste jurnale de audit vor fi stocate în conformitate cu politicile de retenție și securitate specificate în normele metodologice aferente OUG 89/2022 (de exemplu, HG 70/2023 și HG 112/2023). Jurnalele trebuie să asigure trasabilitatea completă a acțiunilor, non-repudierea și să fie disponibile pentru audituri de conformitate și investigații de securitate, protejate împotriva modificărilor neautorizate.
- **Corelare:** Sistemul de logare trebuie să permită corelarea acțiunilor cu identitatea utilizatorului (sau a serviciului) care le-a inițiat.

5.8.6 F. Apărare în profunzime (Managementul incidentelor și vulnerabilităților)

Soluția va integra controale de securitate stratificate și va dispune de proceduri clare de răspuns la incidente.

- **Stratificare și măsuri complementare:**
    - Securitatea va fi implementată pe multiple straturi: securitatea rețelei (ex. firewall-uri), securitatea sistemului de operare, securitatea aplicației (validarea la nivel de cod) și securitatea datelor (criptare).
    - Se vor utiliza măsuri complementare, astfel încât eșecul unui control să nu compromită întregul sistem (ex: un web application firewall - WAF în fața aplicației).
- **Managementul vulnerabilităților și actualizărilor:**
    - Se va asigura managementul vulnerabilităților, inclusiv prin scanare regulată.
    - Menținerea sistemelor și software-ului la zi cu cele mai recente patch-uri și actualizări de securitate este obligatorie.
- **Managementul incidentelor de securitate:**
    - **Monitorizare și răspuns:** Trebuie implementate instrumente de monitorizare și măsuri de detectare a indicatorilor unor potențiale incidente de securitate.
    - **Limitarea impactului:** Trebuie implementate măsuri pentru a realiza intervenția la timp și în mod coordonat în scopul limitării impactului breșelor de securitate.
    - **Notificare:** Trebuie implementate proceduri de notificare a organelor competente și a persoanelor fizice afectate în situația identificării unui incident de securitate.

5.8.7 Notificări (privind incidente de securitate)

Notificarea privind incidentele de securitate se face către Directoratul Național de Securitate Cibernetică (DNSC) și este un proces în mai multe etape:

- Alertă timpurie: În termen de 24 de ore de la momentul la care a luat cunoștință de un incident semnificativ. Această alertă indică doar dacă incidentul este suspectat a fi cauzat de un atac cibernetic.
- Notificare privind incidentul: În termen de 72 de ore de la luarea la cunoștință. Această notificare actualizează alerta timpurie și oferă o evaluare inițială a gravității, impactului și, dacă există, a indicatorilor de compromitere.
- Raport final: În termen de o lună de la notificarea incidentului.

Notificarea privind incidentele de securitate se face către ANSPDCP (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal) și este un proces în mai multe etape:

i) Notificarea Autorității Competente (cf. Art. 33)

- Când: Fără întârzieri nejustificate și, dacă este posibil, în termen de 72 de ore de la data la care operatorul a luat cunoștință de breșă.
- Ce: Trebuie să descrie natura breșei, categoriile și numărul persoanelor vizate, consecințele probabile și măsurile luate (inclusiv cele de limitare a impactului).

ii) Notificarea Persoanelor Fizice Afectate (cf. Art. 34)

- Când: Se face „fără întârzieri nejustificate”, dar numai dacă breșa este „susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice”.
- Scop: Permiterea persoanelor afectate să ia măsuri de precauție (de ex., schimbarea parolelor, monitorizarea conturilor bancare).

Cerințe pentru ofertant (privind principii B, C, D, F cf. cap 4.5 Principii fundamentale de securitate cibernetică, care nu se regăsesc în altă secțiune a caietului de sarcini:
Ofertantul va include în propunerea tehnică descrieri detaliate pentru următoarele aspecte:

1. **Validarea și standardizarea datelor (din principiul B. Integritate)**
    - Ofertantul va descrie regulile și mecanismele tehnice stricte de validare și standardizare a datelor implementate la toate punctele de intrare (ex. API-uri, formulare web) pentru a preveni în mod specific atacurile de tip injecție de cod (cum ar fi SQL Injection, Cross-Site Scripting - XSS) și coruperea datelor.
2. **Obiectivele de recuperare (din principiul C. Disponibilitate)**
    - Deși politica de backup este solicitată, ofertantul trebuie să specifice în mod clar în propunerea tehnică obiectivele de timp și de punct de recuperare pe care le garantează contractual:
        - **RTO** (Recovery Time Objective) – Timpul maxim acceptabil în care serviciul trebuie restabilit complet după un dezastru.
        - **RPO** (Recovery Point Objective) – Punctul maxim acceptabil în timp la care datele trebuie să poată fi recuperate (adică, cantitatea maximă de date care pot fi pierdute).
        - Ofertantul va specifica **serviciile native cloud sau mecanismele tehnice** utilizate pentru realizarea copiilor de siguranță (ex: snapshot-uri automate la nivel de volum, replici de baze de date, versionare S3, servicii native de backup ale furnizorului de cloud)

    Notă: dacă informațiile sunt prezentate în politica de backup, se va indica referința.
3. **Utilizarea standardelor deschise de autentificare (din principiul D. Autentificare)**
    - Pe lângă integrarea solicitată cu ROeID, ofertantul va descrie modul în care soluția de management al identității utilizează standarde deschise (ex: OAuth 2.0, OpenID Connect, SAML) pentru a asigura interoperabilitatea, securitatea și facilitarea integrărilor viitoare ale proceselor de autentificare.
4. **Arhitectura de apărare în profunzime (din principiul F. Apărare în profunzime)**
    - Ofertantul va descrie arhitectura de securitate stratificată (apărare în profunzime) a soluției. Această descriere trebuie să includă modul de implementare a măsurilor tehnice complementare, cum ar fi utilizarea unui Web Application Firewall (WAF), securizarea la nivel de aplicație (validarea la nivel de cod) și securizarea sistemului de operare (hardening).
5. Ofertantul va confirma asumarea activităților privind notificările în caz de incident, alături de timpii de răspuns.

6 CERINȚE DE PARAMETRIZARE A SOLUȚIEI INFORMATICE

Cerințele din acest capitol se referă la serviciile de instalare, configurare și parametrizare a soluției propuse pentru a satisface nevoile personalizate ale Direcției de Asistență Socială Drobeta-Turnu Severin, urmărind adoptarea de noi tehnologii în vederea îmbunătățirii semnificative a calității serviciilor publice și standardizarea modului de lucru la nivelul tuturor instituțiilor subordonate și a partenerilor instituționali.

6.1 Personalizarea structurală și a identității

6.1.1 Obiectivul și scopul parametrizării

Scopul serviciilor de instalare, configurare/parametrizare pentru soluția SAAS la nivelul Instituției Beneficiare Centrale și al entităților subordonate este de a asigura digitalizarea proceselor și a relației cu terții. Aceste servicii sunt destinate să asigure interconectarea și interoperabilitatea între instituții la nivel local și central, crearea de funcționalități noi în legătură cu serviciile publice electronice și standardizarea modului de lucru la nivelul tuturor instituțiilor subordonate și a partenerilor instituționali.

6.1.2 Cadrul de referință și cerințe de configurare structurală

Identitatea instituțională și vizuală:

- Se solicită parametrizarea identității vizuale a instituției emitente. Actele electronice emise de instituție pot constitui acte electronice doar în măsura în care îndeplinesc condiția de a purta identitatea vizuală a instituției emitente.
- Parametrizarea trebuie să asigure uniformizarea documentelor de ieșire.

Managementul identităților funcționarilor, configurarea și parametrizarea trebuie să includă**:**

- Crearea identităților electronice profesionale pentru toți salariații. Identitățile funcționarilor vor fi create doar de administratorii de sistem.
- Configurarea nomenclatorului categoriilor de personal (nomenclator de funcții), stabilirea meta descriptorilor specifici (inclusiv pregătirea profesională), și maparea poziției angajaților în structura organizațională.
- Implementarea planificării activității personalului (pentru repartizarea automatizată a lucrărilor).
- Parametrizarea modelelor de guvernanță digitală contextuală pentru toate cele șapte stări logice agregate ale identităților funcționarilor, respectiv: inactivă (neefectivă); inițiată / neconfirmată (neefectivă); activă (efectivă); suspendată (efectivă); în concediu (efectivă, specifică funcționarilor); dezactivată (neefectivă); ștearsă.

Configurarea registrelor și a arhivei, care trebuie să includă:

- Parametrizarea Registrului Unic de lucrări (un singur registru la nivel de instituție). Acesta va asigura o evidență centralizată a tuturor lucrărilor și va include lucrările de intrare, ieșire și cele interne.
- Parametrizarea Registrelor de acte (fără a limita numărul acestora), destinate structurilor din organigrama instituției (serviciu, birou, compartiment, etc.), care vor asigura numere de înregistrare unice actelor.
- Parametrizarea Nomenclatorului Arhivistic electronic.

Configurarea nomenclatoarelor generale, care trebuie să includă:

- Parametrizarea nomenclatoareloror de obiecte necesare managementului identităților (ex. nomenclator stradal, nomenclatorul unităților administrativ teritoriale, nomenclatorul instituțiilor publice, nomenclatorul tipurilor de persoane juridice)

6.1.3 Lista entităților subordonate vizate

Locația proiectului este la sediile Direcției de Asistență Socială și ale instituțiilor subordonate. Entitățile subordonate vizate includ amplasamentele Creșei Drobeta.

6.2 Nevoi de parametrizare din perspectiva instituției beneficiare centrale

6.2.1 Modelarea fluxurilor administrative interne (back-office)

În procesul de parametrizare a soluției, Prestatorul va implementa modelarea fluxurilor de lucru identificate în tabelul de mai jos, utilizând două paradigme de configurare distincte, în funcție de gradul de predictibilitate și standardizare al activității aplicabil la realitatea operațională dinamică a DAS Drobeta-Turnu Severin. În acest sens, prestatorul nu va modela fluxuri automate rigide (hard-coded pe utilizatori nominali), ci va implementa o arhitectură de proces bazată pe management de caz adaptabil și alocare pe baze de competență sau încărcare.

Soluția informatică trebuie să permită coexistența și interacțiunea dintre cele două tipuri de fluxuri:

A. Fluxuri de tip „ad-hoc/manual" (definite de inițiator)

Acest tip de flux se aplică proceselor administrative non-standardizate, ocazionale sau care necesită o flexibilitate decizională maximă. Ruta de circulație a lucrării nu este „prestabilită" în sistem. Inițiatorul sau deținătorul curent al sarcinii decide, la fiecare pas, cine este următorul destinatar sau care este următoarea acțiune, selectând dintr-un nomenclator de utilizatori/grupuri sau acțiuni disponibile.

Cerință de implementare: Pentru aceste fluxuri, sistemul va oferi utilizatorului interfața de modelare contextuală solicitată la cerințele funcționale, permițând selectarea destinatarilor, a semnatarilor și a acțiunilor (avizare, aprobare, informare) în timp real, fără intervenția administratorului de sistem.

B. Fluxuri semi-automatizate și automatizate (predefinite/bazate pe reguli)

Acest tip de flux se aplică proceselor operaționale standardizate (care au un cadru procedural intern riguros și inflexibil), repetitive, cu volum mare.

Circulația documentelor este guvernată de un motor de proces (workflow engine/RPA) pe baza unor reguli prestabilite care au în vedere parametri precum competența materială, teritorială, ierarhică și modalitatea de repartizare a sarcinilor (nivelul de încărcare).

Cerințe de implementare:

- Pentru a asigura continuitatea în condiții de fluctuație a personalului, distribuirea în aceste fluxuri NU se va face către utilizatori nominali, ci către grupuri de sarcini (Task pools / Queues).
    - *Semi-automatizare:* Sistemul plasează lucrarea în coșul comun al serviciului competent, de unde poate fi repartizată de șeful ierarhic sau preluată de utilizatori.
    - *Automatizare completă:* Sistemul execută pași fără intervenție umană acolo unde este posibil (ex: alocarea automată, expedierea notificărilor, repartizarea automată bazată pe gradul de încărcare și/sau competență teritorială).
- Flexibilitate (Override): Chiar și în cazul fluxurilor automatizate, sistemul trebuie să permită intervenția umană pentru excepții (ex. reasignare manuală de către șeful ierarhic), conform cerințelor de flexibilitate organizațională.

Strategia de implementare evolutivă: „Process discovery" și standardizare progresivă

Având în vedere situația actuală a DAS Drobeta-Turnu Severin, caracterizată prin operarea exclusivă pe suport de hârtie și lipsa unor fluxuri digitale anterioare, modelarea proceselor nu va fi tratată ca o acțiune unică și definitivă la momentul lansării („Go-live"), ci ca un proces iterativ.

Prestatorul va configura soluția pentru a susține o abordare de tip „Process discovery", respectând următoarele etape de maturizare a fluxurilor în perioada de implementare și suport:

- Etapa 1 - Flexibilitate (lansare):

Configurarea inițială va privilegia Fluxurile de tip A (ad-hoc/manual) pentru majoritatea proceselor interne care nu au o reglementare legislativă strictă privind traseul documentelor sau aceasta nu este aplicabilă operațional din motive obiective. Acest lucru va permite utilizatorilor să definească dinamic traseul lucrărilor în funcție de realitatea operațională, fără a bloca activitatea în proceduri rigide care nu au fost încă validate în mediul digital.

- Etapa 2 - Analiza tiparelor (monitorizare):

Soluția informatică trebuie să permită administratorilor să vizualizeze traseele reale parcurse de documente în Etapa 1, utilizând jurnalele de audit și istoricul fluxurilor („audit trail" / „logs").

Analiza informațiilor despre procese exportate din sistem (ex: hărți termice de proces sau frecvența rutelor) vor permite autorității contractante identificarea tiparelor repetitive de lucru, a punctelor de aglomerare, etc.

- Etapa 3 - Standardizare (optimizare):

Pe baza tiparelor identificate în Etapa 2, Beneficiarul (după caz, asistat de Prestator) va transforma fluxurile recurente din Tip A (Manual) în Tip B (Semi-automatizat/Automatizat). Soluția permite (conform cerințelor formulate la cap. Configurarea de fluxuri predefinite) crearea de șabloane de flux automatizate fără dezvoltare de cod sau cunoștințe avansate, permițând instituției să standardizeze procesele treptat, pe măsură ce cadrul procedural intern este actualizat la realitatea digitală, precum și evolutiv pe întreaga durată de exploatare.

Configurarea va include pentru ambele tipuri de fluxuri cerințele privind stabilirea ordinii de semnare electronică calificată, motivul semnării și poziționarea vizibilă a semnăturii/sigiliului pe document.

Se prezintă tabelul fluxurilor de lucru ce urmează a fi digitalizate (lucrări) pe Direcție/Serviciu:

Direcție / Serviciu / Compartiment	**Flux de lucru digital ca urmare a implementării proiectului**
Director executiv	Dispozițiile emise de către Directorul Executiv; Dispoziții și note de serviciu cu privire la constituirea comisiilor de concurs, evaluarea ofertelor, promovarea în grad profesional, încadrările.
Serviciul de asistență socială	Cererile privind venitul minim de incluziune (depunere, înregistrare, arhivare); Dosarele beneficiarilor de servicii sociale gratuite/contra cost prestate de Cantina de ajutor social; Cereri și adeverințe eliberate beneficiarilor de venit minim de incluziune; Corespondență cu alte instituții și ONG-uri privind beneficiarii.
Serviciul Protecție Specială	Liste de inventar și procese-verbale de predare-primire a dosarelor; Corespondență persoane fizice și/sau juridice referitoare la anchete sociale conform Legii nr. 448/2006; Cereri ale solicitanților pentru efectuarea anchetei sociale privind evaluarea/reevaluarea socio-medicală.
Serviciul Monitorizare	Corespondență cu persoanele fizice și instituțiile publice: adrese, invitații, petiții; Corespondență internă (adrese, note de serviciu și/sau de informare, rapoarte de monitorizare); Adrese, tabele, invitații cu privire la monitorizarea persoanelor cu handicap grav și monitorizarea asistenților personali.
Serviciul Protecția persoanelor vârstnice	Dosare electronice ale beneficiarilor de servicii sociale de îngrijire la domiciliu; Contracte de furnizare a serviciilor sociale; Decizii privind acordarea serviciului social de îngrijire la domiciliu; Anchete sociale, dovezi și grile medico-sociale pentru instituționalizare.
Serviciul Resurse Umane	Raportări către Agenția Națională a Funcționarilor Publici; Dosare personale ale funcționarilor publici și personalului contractual în format electronic; Cereri ale angajaților privind acordarea concediului de odihnă, eliberarea adeverințelor și acordarea tichetelor de vacanță.
Serviciul Protecția Drepturilor Copilului	Dosarele de plasament gestionate în format electronic; Anchetele sociale de instituire / reevaluare (inclusiv pentru Centrul de zi); Sesizări primite de la persoane fizice și instituțiile statului.
Serviciul Facilități Asistență Socială	Corespondență – cereri privind acordarea cardurilor de călătorie; Corespondență (adrese, situații centralizatoare) privind certificarea contractelor, acordarea alocației, acordarea tichetelor valorice pentru nou-născuți.
Serviciul Financiar Contabilitate	Planul anual al achizițiilor publice; Referate și comenzi către ofertanți; Facturi – luare în evidență, înregistrare, semnare și sigilare electronică calificată, arhivare electronică; Angajamentele bugetare, Ordonanțările de plată.
Serviciul Secretariat Administrativ, Arhivă, Registratură	Primire corespondenței externe fizic sau electronic; Transpunerea corespondenței externe primite fizic în format electronic și transmiterea pe fluxuri digitale.

6.3 Parametrizarea serviciilor publice electronice (front-office)

Prestatorul va configura toate serviciile publice ale instituției (apreciate ca fiind „noi" din punct de vedere digital) la gradul 5 de sofisticare digitală, materializat prin automatizarea proceselor de gestiunea a identității electronice, de preluare, generare și conversie documentară (în format PDF), înregistrare și repartizare a solicitărilor, de colectare a semnăturilor, de arhivare electronică și de expediere a conținutului, de notificare a utilizatorilor cu privire la informații relevante despre solicitările lor, și personalizarea accesului la serviciile publice în funcție de atribute specifice ale utilizatorilor.

Lista completă (21 de elemente) a serviciilor publice digitale care urmează a fi implementate:

1. Înscriere în educația timpurie (antepreșcolar).
2. Acordarea ajutorului de urgență.
3. Acordarea Venitului Minim de Incluziune.
4. Acordarea indemnizației de creștere a copilului.

5. Acordare alocație de stat.
6. Acordare stimulent de inserție.
7. Acordare servicii sociale - urgență.
8. Cerere acordare îngrijire la domiciliu.
9. Cerere instituționalizare.
10. Cerere indemnizație persoană cu dizabilități.
11. Cerere referat pentru scutire de la plata tarifului de utilizare a rețelelor de drumuri naționale.
12. Cerere acordare tichete sociale pentru grădiniță.
13. Cerere acordare abonament transport public local (donatori).
14. Cerere acordare abonament transport public local (pensionari).
15. Cerere acordare abonament transport public local (persoane cu dizabilități).
16. Cerere acordare abonament transport public local (veterani).
17. Cerere acordare trusou nou-născut.
18. Cerere aprobare / încetare indemnizație persoană cu dizabilități.
19. Solicitare efectuare anchetă socială privind evaluarea sau reevaluarea încadrării în grad de handicap.
20. Depunerea și soluționarea petițiilor.
21. Programări și audiențe online.

6.4 Parametrizarea automatizării registraturii online

Repartizarea automatizată a lucrărilor recepționate prin mediul online trebuie să fie configurabilă în funcție de cel puțin următoarele criterii:

- gradul de încărcare al funcționarului;
- criteriul ierarhic (repartizarea automată către șeful de structură);
- competența teritorială a funcționarului;
- competența materială a funcționarului.

6.5 Parametrizarea interconectării (fluxuri interinstituționale)

Interconectarea și interoperabilitatea vor fi operaționalizate prin intermediul serviciului de distribuție electronică înregistrată (ERDP). Soluția informatică trebuie să permită transportul datelor bidirecțional și livrarea conținutului personalizat (fișiere și date structurate).

Modelarea fluxului interconectat DAS Drobeta-Turnu Severin ↔ Primăria Drobeta-Turnu Severin

Actorul A (DAS Drobeta-Turnu Severin)	Fluxuri și Acte Schimbate (Direcționalitate)	Actorul B (Primăria Drobeta-Turnu Severin)
A → B (Rapoarte și Solicitări)	↔	**B → A** (Decizii și Acte de Aprobare)
Transmiterea referatului de acordare a beneficiilor sociale însoțit de modelul de dispoziție de acordare a beneficiilor sociale.	↔	Transmiterea Dispoziției de primar de acordare a beneficiilor sociale către DAS.
Transmiterea confirmării de începere a activității privind munca în folosul comunității în vederea semnării.	↔	Solicitări, petiții, adrese transmise către DAS Drobeta-Turnu Severin a căror soluționare se află în competența Primăriei.
Transmiterea adeverințelor de efectuare a orelor în folosul comunității.	↔	
Transmiterea contractelor individuale de muncă ale asistenților personali (întocmite de DAS) spre semnare.	↔	

Modelarea fluxului interconectat DAS Drobeta-Turnu Severin ↔ DGASPC Mehedinți

Actorul A (DAS Drobeta-Turnu Severin)	Fluxuri și Acte Schimbate (Direcționalitate)	Actorul B (DGASPC Mehedinți)
A → B (Rapoarte și Solicitări)	↔	**B → A** (Decizii și Acte de Aprobare)
Transmiterea lunară a situațiilor intrărilor și ieșirilor privind indemnizația de handicap aferentă gradului grav cu asistent personal	↔	Transmiterea dosarelor persoanelor cu handicap pentru evaluare/reevaluare.
Anchetele sociale efectuate de către DAS la solicitarea DGASPC privind protecția copilului	↔	

Situații statistice pentru copii cu părinți plecați la muncă în străinătate	↔	

6.5.1 Modelarea fluxurilor cu partenerii locali/centrali

Interconectarea efectivă cu soluția nou propusă se va realiza cu sistemele informatice ale autorităților sau instituțiilor publice centrale și locale, în măsura în care documentația de interconectare va fi disponibilizată de instituția vizată, după cum urmează:

Instituție vizată de interconectare	Acte și date ce vor face obiectul interconectării
ANAF / Trezorerie	Adrese deschidere/închidere conturi
RECOM	Integrări necesare pentru asigurarea unor identități acurate.
ROeID	Sistem Național de Identitate Electronică.
ONRC	Oficiul Național al Registrului Comerțului.
Furnizori de servicii de încredere (minim 2) și STS	Asigurarea și mentenanța API-urilor de interconectare. Integrare cu minim 2 furnizori acreditați la nivel european și cu STS.

6.5.2 Nevoi de parametrizare pentru fluxurile inter-instituționale cu entitățile subordonate

Modelarea fluxurilor inter-instituționale (Entități subordonate ↔ Instituția centrală)

Prestatorul va modela fluxurile de lucru bidirecționale necesare comunicării dintre Instituția Centrală (DAS Drobeta-Turnu Severin) și entitățile subordonate, utilizând serviciul ERDP. Entitatea subordonată vizată este Creșa Drobeta.

Instituție subordonată	Fluxuri și acte schimbate (Expeditor Creșa Drobeta → Destinatar: DAS Drobeta-Turnu Severin Central)
Creșa Drobeta	Rapoartele financiare trimestriale
	Cererile de deschidere de credite
	Adrese, informări, raportări
	Solicitări, petiții, adrese care se află în competența DAS Drobeta-Turnu Severin

6.5.3 Datele ce vor face obiectul interconectării și formatul acestora

Datele schimbate prin fluxurile de lucru interconectate interne și interinstituționale vor fi:

1. Date structurate: cele specifice solicitării și procesării solicitării, fiind specifice formularelor tipizate.
2. Documente (date nestructurate) - cele specifice documentelor doveditoare și documentelor cu caracter general, care includ metadate structurate și documentul în format electronic.

În ambele situații de mai sus (1 și 2), datele tehnice specifice identității digitale, managementului înregistrărilor (ERDS), semnării și sigilării electronice calificate se vor colecta în format structurat în acte/documente

6.6 Parametrizarea formularisticii și a colaborării

Configurarea formularisticii

Se vor configura punctele de acces și formularele electronice specifice de interacțiune directă între instituție/instituțiile subordonate și beneficiari. Formularele trebuie să fie grupate pe tipuri de utilizatori și să asigure colectarea datelor în format structurat și validat la nivelul introducerii datelor. De asemenea, formularele trebuie să poată fi salvate în „Ciorne" pentru reluarea ulterioară a editării.

Configurarea colaborării

Se vor configura mijloacele colaborative de lucru pentru funcționari, incluzând:

- schimb bidirecțional de mesaje;
- atașare de fișiere;
- comunicarea individuală sau în grup;
- audio conferință;
- video conferință;
- partajare de ecrane;
- documente colaborative (crearea și editarea simultană de documente de tip text).

6.7 Parametrizarea elementelor transversale (e-guvernanță)

- Semnare și Sigilare:
    - Configurarea cerințelor privind Semnarea electronică calificată în regim de aplicare automată și manuală.
    - Configurarea Sigilării electronice calificate în regim de aplicare automată și manuală.
    - Soluția va permite semnarea simplă (1 document) și semnarea în serii mari („batchuri").
    - Se va permite sigilarea electronică calificată simultană a mai multor documente și gestionarea a multiple cozi de sigilare (tip „queue").
    - Se solicită integrarea semnăturii olografe în semnătura electronică calificată.

- Automatizare: Configurarea cerințelor pentru automatizarea proceselor operaționale complexe (RPA). Procesele automatizate includ: colectarea semnăturilor electronice, înregistrarea documentelor, sigilarea electronică calificată, arhivarea electronică, expedierea și finalizarea lucrării.
- Notificări: Configurarea sistemului de notificare trebuie să includă notificări pe e-mail, în contul personal și notificări de tip push în aplicația mobilă. Sistemul trebuie să dispună de proceduri de recuperare din eroare (*fallback*) implementate pentru gestionarea situațiilor când apar erori în procesul de trimitere în serii mari („batchuri") de notificări.

Acces și Securitate: Se va realiza parametrizarea rolurilor de securitate (RBAC) și a accesului la date pe baza principiului „nevoii de a cunoaște". Accesul la informații se va face doar individual și condiționat de existența unui motiv temeinic, care va fi capturat în sistem. Soluția nu va permite niciunui tip de utilizator funcționar vizualizarea tuturor identităților personale din sistem sub formă de listă și fără un motiv capturat la momentul accesului.

7 CERINȚE NEFUNCȚIONALE

În cadrul Propunerii Tehnice se vor prezenta cel puțin următoarele informații, din care să rezulte îndeplinirea cerințelor nefuncționale solicitate:

7.1 Flexibilitatea și funcționalitatea sistemului

Arhitectura sistemului va trebui să fie deschisă și bazată pe standarde larg acceptate în industrie. Aceasta va asigura cuplarea slabă cu aplicațiile cu care comunică, precum și suport UTF-8/16.
Din punct de vedere tehnologic atât produsele ofertate, cât și personalizările, vor trebui să fie grupate astfel încât sistemul informatic ofertat să fie unul unitar, configurabil și ușor administrabil.
Sistemul va trebui să fie configurat pentru a răspunde tuturor cerințelor funcționale specificate în caietul de sarcini.
Caracteristicile flexibilității arhitecturii trebuie să fie exprimate minim prin:

- posibilitatea de a modifica parametrii aplicației;
- oferirea unor mecanisme flexibile de introducere și validare, import export date și interogare a bazei de date;
- posibilitatea definirii de noi fluxuri de lucru direct în aplicație, de către utilizatorii sistemului;
- folosirea de standarde tehnice deschise recunoscute și acceptate precum XML/HTTP/HTTPS/SSL etc.;
- utilizarea unei arhitecturi modulare care permite modificarea anumitor componente fără impact major în restul soluției;
- interfața ergonomică, ușor de utilizat și coerentă din punct de vedere al elementelor de design al interfeței.

7.2 Proprietatea datelor

Datele rezultate din exploatarea soluției informatice de către utilizatorii interni (funcționari ai Autorității Contractante) sunt proprietatea exclusivă a Achizitorului, iar datele introduse de către utilizatorii externi sunt proprietatea exclusivă a acestora.

7.3 Drepturi de proprietate intelectuală

În conformitate cu OUG 41/2016, art. 12, drepturile de autor asupra oricărui programe informatice dezvoltate la solicitarea instituției în cadrul contractului, sunt transferate autorității contractante la finalizarea contractului. Această prevedere nu se aplică produselor software disponibile în mod comercial prestatorului și incluse în ofertă.
Codul sursă care face obiectul acestei prevederi va fi predat de către Contractant la finalul contractului, în versiunea actualizată de la momentul predării, necriptat, pe suport fizic (ex: CD), împreună cu documentația și un hash SHA. Codul sursă trebuie să conțină comentarii în română și să respecte standardele de programare, fără a fi ascuns. Proprietatea codului sursă revine beneficiarului după validare, cu drept de acces, modificare și distribuire către terți, cu drepturi perpetue de exploatare.

7.4 Cerințe ale infrastructurii cloud

Infrastructura cloud în care se va pune în producție soluția informatică ofertată trebuie să îndeplinească minim condițiile pentru centrele de date menționate de Ordinul MCSI nr. 489 din 2009 la art. 6, 8-12, privind:

- asigurarea funcționării echipamentelor în condiții de securitate specifice și la parametrii optimi prevăzuți de producătorii acestora;
- asigurarea redundanței și realizarea backup-ului;
- asigurarea unei infrastructuri scalabile de echipamente și transport;
- asigurarea securității și integrității datelor, la nivel de securitate fizică și acces prin mijloace informatice;
- disponibilitatea serviciului de arhivare electronică și backup-ul informațiilor stocate;
- asigurarea managementului, controlului și a securității sistemelor pe baza unor strategii, politici și proceduri bine determinate.

Îndeplinirea condițiilor prevăzute în Ordinul MCSI nr. 489 din 2009 la art. 6, 8-12 se va face prin certificări/autorizări ale autorităților competente sau prin rapoarte de audit ale unor terțe părți avizate.

În vederea asigurării conformității depline cu prevederile Regulamentului (UE) 679/2016 și a protejării datelor împotriva accesului neautorizat din țări terțe, Ofertantul va asigura cumulativ următoarele:

- Toate datele cu caracter personal gestionate prin soluție (inclusiv datele de producție, metadatele, jurnalele de sistem și toate copiile de siguranță) vor fi stocate exclusiv în centre de date localizate fizic pe teritoriul Uniunii Europene (UE) sau al Spațiului Economic European (SEE).
- Ofertantul va garanta prin măsuri tehnice și organizatorice adecvate că activitățile de procesare a datelor (incluzând, dar fără a se limita la, operațiunile de administrare, mentenanță la distanță și suport tehnic) sunt realizate exclusiv de către personal localizat fizic pe teritoriul UE/SEE.

În cadrul propunerii tehnice, Ofertantul va descrie detaliat arhitectura soluției cloud și politicile de management al accesului prin care demonstrează îndeplinirea ambelor condiții, specificând locațiile fizice (țara) ale centrelor de date primare și secundare (pentru recuperare în caz de dezastru).
Neîndeplinirea condițiilor privind infrastructura cloud va face ca oferta să fie neconformă.

8 IPOTEZE ȘI RISCURI

În pregătirea Ofertei, ofertanții trebuie să aibă în vedere cel puțin riscurile și ipotezele descrise în continuare. În acest sens, la întocmirea ofertei, ofertantul trebuie să ia în considerare resursele necesare (de timp, financiare și de orice altă natură), pentru reducerea riscurilor identificate.
Ipotezele avute în vedere la momentul începerii procedurii de achiziție:

- conținutul serviciilor solicitate este descris în mod explicit în Caietul de Sarcini;
- corelația dintre resursele necesare și rezultatele așteptate este realistă;
- începerea serviciilor se va realiza în perioada preconizată;
- nu se prevăd schimbări ale cadrului instituțional și legal care să afecteze major implementarea și desfășurarea în bune condiții a Contractului;
- toate informațiile relevante și disponibile la nivelul Autorității Contractante pentru realizarea serviciilor vor fi puse la dispoziția Contractantului;

Contractantul va semna un acord de confidențialitate la momentul semnării Contractului și va respecta toate instrucțiunile privind utilizarea informațiilor confidențiale (după cum este aplicabil).

9 ABORDARE ȘI METODOLOGIE ÎN CADRUL CONTRACTULUI

Autoritatea Contractantă solicită Ofertantului să propună abordarea și metodologia care urmează să fie utilizate în prestarea serviciilor, la libera sa alegere.
În cadrul Propunerii Tehnice se vor prezenta cel puțin următoarele informații:

- Rezumat / Viziunea asupra contractului, care prezintă modul în care ofertantul înțelege contextul, scopul proiectului, obiectivele contractului și sarcinile stabilite de Autoritatea Contractantă;
- Descrierea soluției propriu-zise propuse, cel puțin la nivelul diagramei de arhitectură.
- Abordarea propusă ce corespunde rezultatelor intermediare și rezultatului final al contractului, în raport cu serviciile și responsabilitățile stabilite prin caietul de sarcini, relevând aspectele-cheie privind îndeplinirea obiectivelor contractului și atingerea rezultatelor așteptate;
- Metodologia propusă pentru realizarea activităților în scopul obținerii rezultatelor așteptate;
- Prevederile legale avute în vedere în cadrul prestației, specifice domeniului de activitate aferent obiectului contractului ce urmează a fi atribuit, ce pot avea incidență asupra derulării/implementării acestuia,

având în vedere respectarea cerințelor minime și într-o formă care conduce la obținerea rezultatelor așteptate.

Riscurile identificate privind derularea contractului:
Organizatorice

1. Dificultăți tehnice neprevăzute susceptibile să determine întârzierea unor activități.
   - Măsuri de gestionare/mitigare: Realocarea anumitor resurse pe direcțiile/activitățile unde sunt întâlnite dificultăți tehnice. Monitorizarea regulată a progresului, replanificarea resurselor.
   - Impactul pentru riscul identificat - moderat.
   - Probabilitate: scăzută.
2. Întârzieri în realizarea livrabilelor.
   - Măsuri de gestionare/mitigare: Planificarea timpurie a livrabilelor și structurii conținutului acestora, monitorizarea progresului realizat. Redistribuirea efortului (dacă este necesar) în vederea atingerii obiectivelor propuse.
   - Impactul pentru riscul identificat - foarte scăzut.
   - Probabilitate: scăzută.

3. Interes scăzut al beneficiarilor pentru rezultatele proiectului.
    - Măsuri de gestionare/mitigare: Realizarea măsurilor de informare și publicitate și promovarea rezultatelor proiectului pe tot parcursul implementării, cu evidențierea beneficiilor generate de utilizarea soluțiilor implementate.
    - Impact pentru riscul identificat - foarte scăzut.
    - Probabilitate: foarte scăzută.

Tehnice

4. Dificultăți tehnice neprevăzute susceptibile să determine întârzierea unor activități.
    - Măsuri de gestionare/mitigare: Realocarea anumitor resurse pe direcțiile/activitățile unde sunt întâlnite dificultăți tehnice. Monitorizarea regulată a progresului, replanificarea resurselor.
    - Impactul pentru riscul identificat - foarte scăzut.
    - Probabilitate: foarte scăzută.

privind Resursa umană

5. Schimbări de personal în poziții cheie pentru proiect.
    - Măsuri de gestionare/mitigare: identificarea persoanelor potrivite să preia sarcinile, pregătirea acestora în ritm accelerat pentru îndeplinirea sarcinilor.
    - Impactul pentru riscul identificat - foarte scăzut.
    - Probabilitate: foarte scăzută.

Financiare

6. Riscul de neplată sau plăți întârziate.
    - Măsuri de gestionare/mitigare: prevederea din timp a sumelor necesare în bugetul autorității contractante; angajarea sumelor cel mai târziu la plata primei facturi către contractant.
    - Impactul pentru riscul identificat - ridicat.
    - Probabilitate: moderat.

Riscuri specifice implementării soluției IT

Tehnice

7. Lipsa de capacitate (inclusiv lățime de bandă) a infrastructurii de transport date/conexiune internet la beneficiar.
    - Măsuri de gestionare/mitigare: Încheierea unui contract de furnizare de servicii de internet care să asigure o lățime de banda cât mai mare.
    - Impactul pentru riscul identificat - risc asumat de Autoritatea Contractantă.
    - Probabilitate: foarte scăzută.

Legislative

8. Numeroase și/sau frecvente actualizări/modificări ale legilor și/sau procedurilor administrative cu privire la procedurile pentru gestionarea și controlul sistemului.
    - Măsuri de gestionare/mitigare: identificarea rapidă a nevoilor reale de reconfigurare a traseelor documentelor, inclusiv a livrabilelor tipizate și implementarea noilor configurări.
    - Impactul pentru riscul identificat - moderat.
    - Probabilitate: foarte scăzută.

privind Resursa umană

9. Posibilitatea ca personalul tehnic, prin acțiunile sale, să afecteze/producă daune datelor arhivate în sistem.
    - Măsuri de gestionare/mitigare: trecerea în revistă a tipurilor de erori identificabile și a modalităților de evitare a acestora; asigurarea unui control foarte riguros al accesului la date
    - Impactul pentru riscul identificat - ridicat.
    - Probabilitate: foarte scăzută.

În cadrul Propunerii Tehnice ofertanții vor prezenta cel puțin următoarele informații, din care să rezulte:

- ➔ Că ofertantul a luat cunoștință și avea în vedere riscurile prezentate de Autoritatea Contractantă;
- ➔ Ajustările considerate / observații asupra riscurilor prezentate de Autoritatea Contractantă după caz, și riscuri identificate și detaliate inclusiv pe baza experienței proprii din proiecte similare, prezentând și măsuri de gestionare/mitigare a acestora.

10 PLAN DE LUCRU PENTRU ACTIVITĂȚILE/SERVICIILE SOLICITATE

Autoritatea Contractantă solicită Ofertantului să propună Planul de lucru pentru realizarea serviciilor care urmează să fie utilizate în prestarea serviciilor.

În cadrul Propunerii Tehnice se vor prezenta cel puțin următoarele informații:

- Planul de lucru, incluzând detalierea graficului de execuție după cum urmează:
    - denumirea, durata și descrierea activităților și etapelor (pachetelor de activități) din cadrul contractului, așa cum sunt acestea prezentate la capitolul „ABORDARE ȘI METODOLOGIE ÎN CADRUL CONTRACTULUI";
    - succesiunea și interrelaționarea activităților;
    - punctele-cheie de control („jaloanele" proiectului);

- graficul de planificare în timp al activităților / subactivităților (graficul Gantt);
- Modul de luare și ierarhizare a deciziilor, cu indicarea deciziilor care se iau de Prestator cu deplină autoritate și a deciziilor care se iau de către Beneficiar, pe baza propunerilor făcute de Prestator,

prezentând activitățile pe care ofertantul le consideră necesare și într-o formă care conduce la obținerea rezultatelor așteptate în termenele solicitate.
După semnarea contractului, în perioada de început a acestuia, există posibilitatea modificării planului de lucru doar cu acordul Autorității Contractante.

11 LOCUL ȘI DURATA DESFĂȘURĂRII ACTIVITĂȚILOR

11.1 Locul desfășurării activităților

Activitățile proiectului se vor desfășura atât la sediul Beneficiarului cât și la sediul Prestatorului, precum și în alte locații, după caz, în funcție de particularitățile activităților proiectului și de nevoile identificate.
În funcție de situația existentă atât la nivel local la momentul dat al derulării activităților de teren, Prestatorul va asigura măsurile de protecție a persoanelor implicate și va lua în considerare derularea activităților prin mijloace online conform metodologiilor de lucru propuse în cadrul ofertei.

11.2 Data de început și data de încheiere a prestării serviciilor sau durata prestării serviciilor

Activitățile din cadrul contractului vor fi demarate la primirea ordinului de începere din partea Achizitorului în urma semnării contractului de achiziție publică de ambele părți. Ordinul de începere va fi emis în maxim 10 zile de la data semnării contractului.
Durata contractului este de 7 luni.

12 RESURSELE NECESARE/EXPERTIZA NECESARĂ PENTRU REALIZAREA ACTIVITĂȚILOR ÎN CONTRACT ȘI OBȚINEREA REZULTATELOR

În vederea implementării cu succes a contractului de servicii, Ofertantul va organiza și va pune la dispoziția Achizitorului o echipă de experți care, prin atribuțiile și pregătirea lor, vor realiza execuția tuturor activităților în cadrul contractului.
Ofertantul se obligă să păstreze, atât el cât și resursele umane propuse, confidențialitatea asupra informațiilor primite de la Achizitor pe parcursul derulării contractului și asupra rezultatelor obținute în executarea contractului.
Ofertantul este responsabil în exclusivitate și integral pentru stabilirea componenței echipei de proiect, pentru organizarea tuturor experților propuși, precum și pentru depunerea efortului necesar desfășurării în bune condiții a tuturor activităților solicitate prin prezentul caiet de sarcini. Experții non-cheie vor lucra sub îndrumarea experților cheie.
În cazul necesității de implicare a unor asemenea experți, este în răspunderea ofertanților:

- Să furnizeze orice personal suport necesar, pentru asigurarea îndeplinirii corespunzătoare a obligațiilor contractuale pe toată durata de execuție a contractului;
- Să prezinte în cadrul propunerii tehnice rolul și responsabilitățile deținute în vederea execuției contractului, precum și orice alte informații relevante din cadrul cărora să rezulte pregătirea și experiența/competențele profesionale ale acestora;

Ofertantul trebuie să asigure folosirea echipamentelor adecvate pentru toți experții, inclusiv consumabilele necesare și facilitățile mobile operaționale/comunicaționale necesare pentru fiecare expert nominalizat (cum ar fi laptop cu software aferent, voce, date), precum și orice alte resurse materiale necesare. Ofertantul:

- Va descrie în cadrul propunerii tehnice, modalitatea în care va asigura sprijinul necesar întregii echipei de experți, atât în ceea ce privește experții, personalul suport, cât și în ceea ce privește logistica și infrastructura tehnică necesară (echipamente/dotări);
- Are obligația asigurării resurselor financiare necesare pentru a sprijini activitățile experților în cadrul acestui proiect, scop în care în măsura în care oferta va fi declarată câștigătoare va trebui să procedeze la plata acestora în mod regulat (la perioade de timp corespunzătoare) astfel încât să existe premisele optime pentru buna îndeplinire a contractului și finalizarea acestuia fără incidente;
- Sunt considerate ca fi incluse în prețul total ofertat pentru execuția contractului, orice costuri cu cheltuielile conexe necesare desfășurării activităților acestui contract, inclusiv:
- Eventuale deplasări ale personalului propriu (cum ar fi dar fără a se limita la acestea diurnă, transport, cazare, masă);
- Cele legate de redactarea, multiplicarea și/sau circularea documentației de contract/livrabilelor de contract elaborate în scopul realizării contractului precum și cele vizând elaborarea diferitelor materialele necesare/de realizarea oricăror activități conexe. (cum ar fi, dar fără a se limita la managementul de proiect, expertiza furnizată prin intermediul experților externi, etc).

Definiții de termeni:

1) Prin „a face dovada" se înțelege prezentarea de scrisori de recomandare de la colaboratori anteriori / certificate de predare-primire / recomandări / procese-verbale de recepție / certificate constatatoare sau orice alte documente doveditoare ale participării expertului în un proiect/contract similar ca anvergură și complexitate.
2) Prin „experiența specifică" solicitată se înțelege, îndeplinirea în cadrul proiectului/contractului similar ca anvergură și complexitate, de către persoana propusă, a aceluiași tip de activități ca cele pe care urmează să le îndeplinească în viitorul contract.
3) Prin „proiect similar ca anvergură și complexitate", se înțelege un proiect/contract care inclus servicii de dezvoltare, implementare sau extindere a unor sisteme informatice integrate sau soluții software de nivel enterprise, având o complexitate comparabilă sau superioară cu cea a contractului ce urmează a fi atribuit.
Având în vedere complexitatea contractului care va fi atribuit, specificul activității Achizitorului și al soluției tehnice solicitate, precum și necesitatea ca prestatorul să gestioneze metodologic procesul de implementare, Autoritatea Contractantă a formulat cerințele tehnice minimale și obligatorii cu privire la componența și responsabilitățile echipei de proiect a prestatorului.
Ofertanții vor dovedi că dispun de experții-cheie solicitați prin Caietul de sarcini și că aceștia îndeplinesc cerințele stabilite.
În cadrul Propunerii Tehnice se vor prezenta cel puțin următoarele informații, din care să rezulte:
La nivelul echipei de experți:

1. Diagrama organizațională a echipei de experți propusă, care relevă modalitatea de organizare a echipei propuse, incluzând rolurile, responsabilitățile solicitate și, adițional, considerate de ofertant;
2. Lista experților propuși, prezentând pentru fiecare expert cheie solicitat:

- CV format Euro Pass;
- În cazul în care persoana propusă nu este angajat al prestatorului, o declarație de disponibilitate și o declarație de confidențialitate, semnate, prin care expertul își exprimă disponibilitatea pentru ducerea la îndeplinire a responsabilităților aferente poziției pentru care este propus, conform cerințelor;
- Documente doveditoare ale cerințelor privind calificarea educațională și/sau profesională, dacă acestea au fost solicitate persoanei propuse: diploma de licență sau echivalent / studii postuniversitare / studii de masterat / doctorat / alte cursuri care s-au finalizat cu certificări recunoscute la nivel național/internațional. Personalului nerezident i se permite să prezinte certificări și autorizări corespunzătoare echivalente emise în țara de rezidență.
- Documente doveditoare ale cerințelor privind competențele specifice, dacă acestea au fost solicitate persoanei propuse: studii absolvite în specializarea respectivă, diploma de licență/absolvire sau echivalent / studii postuniversitare / studii de masterat / doctorat / alte cursuri care s-au finalizat cu certificări recunoscute la nivel național/internațional, ori printr-o experiență profesională relevantă în raport cu specializarea solicitată, conform art. 7 alin. (3) din Instrucțiunea ANAP nr. 1/2017. Personalului nerezident i se permite să prezinte certificări și autorizări corespunzătoare echivalente emise în țara de rezidență;
- Documente doveditoare care probează experiența specifică. Dacă aceasta a fost solicitată persoanei propuse, documente care trebuie să îndeplinească cumulativ următoarele condiții:
  Să precizeze obiectivul contractului din care să rezulte că acesta îndeplinește caracteristicile unui proiect similar.
  Din documente să reiasă clar:
  - ➔ numele și prenumele persoanei propuse;
  - ➔ perioada în care persoana propusă a desfășurat activități în cadrul proiectului;
  - ➔ rolul (poziția) ocupată de persoana nominalizată în cadrul proiectului similar și activitățile îndeplinite de persoana nominalizată în cadrul proiectului similar

Un expert cheie nu poate ocupa simultan mai multe poziții.
Înlocuirea experților cheie propuși de ofertant, precum și suplimentarea numărului acestora față de numărul prevăzut în ofertă (în cazul necesității unui astfel de demers pentru asigurarea bunei desfășurări a contractului ce urmează să fie atribuit) se realizează cu aprobarea autorității contractante și numai în condițiile reglementate prin prevederile art. 162 din H.G. nr. 395/2016. Astfel, pe toată perioada de derulare a contractului, Prestatorul se obligă să ia toate măsurile pentru a asigura în mod continuu disponibilitatea personalului cheie specializat pentru îndeplinirea în mod eficient a sarcinilor acestora.
Ofertantul poate să prevadă în propunerea tehnică și alți experți non-cheie, fără să îi nominalizeze și fără să includă pentru ei documentele solicitate persoanelor propuse în rolurile solicitate prin caietul de sarcini.
Rolurile experților care trebuie să compună echipa de implementare a prestatorului sunt prezentate în continuare împreună cu atribuțiile principale ale acestora în cadrul contractului:

12.1 Profilul experților principali (cheie)

12.1.1 Manager de proiect (expert-cheie - 1 persoană)

Managerul de proiect răspunde de coordonarea activităților contractului, monitorizarea rezultatelor obținute și raportarea acestora către beneficiar, asigurând implementarea acestora, (întocmai și la timp), în conformitate cu cerințele caietului de sarcini, propunerea tehnică și contractul semnat.
Necesitățile specifice aferente procesului de implementare a proiectului impun acordarea suportului/asistenței tehnice din partea acestui expert, în proporții variabile, pe întreaga durată a contractului (incluzând perioada de garanție).
Responsabilitățile managerului de proiect includ următoarele activități specifice:

- Managementul proiectului, un ansamblu care presupune activități de organizare a proiectului, planificare, execuție, monitorizare, control și închidere a proiectului;
- Coordonarea din punct de vedere operațional a echipelor tehnice implicate în procesul de implementare a proiectului, respectiv experții cheie/non-cheie din cadrul echipei de proiect;
- Menținerea relației cu beneficiarul ca punct principal de contact;
- Alocarea resurselor proiectului și urmărirea realizării activităților;
- Urmărirea respectării tuturor termenelor limită;
- Rezolvarea diferitelor situații în scopul evitării situațiilor de criză;
- Identificarea riscurilor, evaluarea și propunerea de soluții în vederea evitării și diminuării riscurilor aferente implementării proiectului;
- Raportarea rezultatelor obținute în urma derulării activităților specifice pe parcursul procesului de implementare a proiectului, elaborarea proceselor-verbale de recepție/rapoartelor de activitate precum și a altor documente de raportare a progresului către beneficiar, ori care derivă din necesitățile proiectului.

Expertul propus trebuie să îndeplinească minim următoarele cerințe de calificare educațională și/sau profesională, privind deținerea de competențe specifice, experiență profesională generală și experiență profesională specifică:

- Calificare educațională și/sau profesională: Studii superioare absolvite, finalizate cel puțin cu diplomă de licență/absolvire (minim ciclul 1 de studii) sau echivalent;
- Experiență profesională specifică dobândită în minim un proiect/contract în care a desfășurat activități similare (de coordonare).

12.1.2 Expert e-guvernare (expert-cheie - 3 persoane)

Experții e-guvernare planifică și monitorizează parcurgerea etapelor de implementare a fluxurilor digitale (proiectare, implementare), aplicând metodologii standardizate ale analizei de business, potrivit uzanțelor, metodelor și instrumentelor de lucru recunoscute la nivel național și internațional. Activitatea se raportează la situația specifică a instituției, realizând implementarea personalizată a serviciilor electronice expuse de instituție, a fluxurilor de lucru pentru funcționari (back-office) și beneficiari (front-office), precum și a specificațiilor de interconectare.

Pentru a acoperi volumul și complexitatea sarcinilor din proiect, la nivelul contractului se disting trei direcții de acțiune ce se vor desfășura în paralel, fiecare dintre acestea fiind asignată în mod distinct și individual unui expert, după cum urmează:

1. Expert e-guvernare 1 (responsabil arhitectură operațională, organizatorică și interoperabilitate): Are ca atribuții exclusive definirea și parametrizarea structurii organizaționale la nivelul instituției și subordonatelor (identități, roluri, registre și grupe de documente, activități specifice administrării sistemului). De asemenea, implementează fluxurile specifice interoperabilității și realizează evaluarea și implementarea interconectărilor și a transportului de date către/din aplicațiile și sistemele în uz.
2. Expert e-guvernare 2 (responsabil implementarea fluxurilor administrative de bază - componente transversale): Are responsabilitatea directă privind implementarea și îmbunătățirea fluxurilor administrative de bază, vizând în mod specific funcționalitățile de registratură, management al documentelor, arhivare, identitate și comunicare.
3. Expert e-guvernare 3 (responsabil digitalizarea serviciilor specifice de front-office și back-office): Gestionează implementarea fluxurilor administrative specifice din perspectiva instituției beneficiare centrale, vizând digitalizarea fluxurilor interne de lucru (back-office) și parametrizarea fluxurilor specifice serviciilor electronice expuse către cetățeni și mediul de afaceri (front-office și back-office).

Având în vedere că activitățile tuturor celor 3 experți vizează predominant proiectarea, implementarea și îmbunătățirea fluxurilor digitale de lucru (workflow), precum și realizarea interoperabilității, competențele profesionale necesare acestora sunt comune și corespund profilului de Expert e-guvernare (cod COR 242234) sau oricărei alte ocupații echivalente din domeniul analizei de business / analizei de sisteme informatice (ex. Analist, Proiectant sisteme informatice etc.).

În virtutea principiului transferabilității competențelor consacrat de art. 9 alin. (1) din Instrucțiunea ANAP nr. 1/2017, pentru asigurarea unei competiții extinse și respectarea principiului proporționalității, nu este obligatoriu ca ocupația/experiența să conțină explicit termenul de „e-guvernare" sau să provină exclusiv din sfera administrației publice. Sunt considerate echivalente și deplin acceptate ocupații care se aliniază cu responsabilitățile de reinginerie a proceselor descrise în Caietul de Sarcini, specifice implementării de sisteme informatice complexe în orice domeniu de activitate (public sau privat).

La nivelul direcției asignate, responsabilitățile operaționale ale fiecărui expert includ următoarele activități specifice:

- Analiza, proiectarea, redesign-ul și reingineria fluxurilor administrative și a serviciilor de tip e-guvernare.
- Facilitarea modelării rapoartelor și a realizării interoperabilității electronice, a schimbului de date și documente electronice.
- Colaborarea cu echipele tehnice.
- Suport în definirea ecranelor utilizator și documentarea activităților efectuate.
- Evaluarea progresului activității și raportarea către managerul de proiect.

Pentru a asigura o abordare integrată, experții au obligația să colaboreze regulat sub coordonarea managerului de proiect pentru a garanta uniformitatea și standardizarea rezultatelor la nivelul tuturor componentelor de front-office și back-office.

Necesitățile specifice aferente procesului de implementare impun acordarea suportului tehnic din partea acestor experți preponderent în etapele de implementare și parametrizare/personalizare, având o tendință descrescătoare spre fazele de testare, lansare și instruire

a utilizatorilor. O eventuală contribuție din partea acestui expert ulterior momentului punerii în producție poate fi anticipată în cazul intervenției uneia sau mai multor solicitări de modificare/schimbare a fluxurilor de lucru personalizate sau a realizării unor noi interconectări.
Dinamica volumului de muncă, încadrarea în timp, zilele/orele expert și succesiunea operațiunilor nu sunt predefinite fix, ci revin în sarcina ofertantului, care trebuie să le detalieze și să le coreleze corespunzător în Planul de lucru și graficul Gantt.
Fiecare din experții propuși trebuie să îndeplinească minim următoarele cerințe de calificare educațională și profesională:

- Calificare educațională: Studii superioare absolvite, finalizate cel puțin cu diplomă de licență/absolvire (minim ciclul 1 de studii) sau echivalent.
- Competențe profesionale: Expert e-guvernare, cod COR 242234 sau echivalent. În virtutea principiului transferabilității competențelor, sunt acceptate ocupații echivalente din domeniul analizei de business / analizei de sisteme informatice (ex. Analist, Proiectant sisteme informatice etc.), nefiind obligatoriu ca ocupația să conțină explicit termenul de „e-guvernare”.
- Experiență profesională specifică: dobândită în minim un proiect/contract similar ca anvergură și complexitate.

12.2 Infrastructura Contractantului necesară pentru desfășurarea activităților Contractului

Pentru îndeplinirea cu succes a activităților descrise, Prestatorul va pune la dispoziția echipei de proiect proprii toate resursele materiale necesare (echipamente de lucru, licențe, mijloace de transport, consumabile).
În cazul întâlnirilor de lucru de oricare natură la sediul Beneficiarului sau, după caz, ai partenerilor săi instituționali implicați în proces, acesta va dispune personalul și mijloacele adecvate scopului întâlnirii (sală ședințe, mijloace de prezentare, consumabile).

13 CADRUL LEGAL CARE GUVERNEAZĂ RELAȚIA DINTRE AUTORITATEA CONTRACTANTĂ ȘI CONTRACTANT (INCLUSIV ÎN DOMENIILE MEDIULUI, SOCIAL ȘI AL RELAȚIILOR DE MUNCĂ)

Prestatorul va desfășura activitățile, presta serviciile și va furniza produsele și documentele specifice Contractului având în vedere toate prevederile legale și strategice naționale, europene și internaționale relevante existente la momentul semnării Contractului, precum și cele emise ulterior, pe parcursul derulării acestuia, incluzând ansamblul reglementărilor subsecvente, enumerarea următoare nefiind limitativă:

- Legea nr. 98/2016 privind achizițiile publice, actualizată;
- HG nr. 395/2016 pentru aprobarea Normelor Metodologice de aplicare a prevederilor referitoare la atribuirea Contractului de achiziție publică/acordului-cadru din Legea nr. 98/2016;
- Legea nr. 101/2016 privind remediile și căile de atac în materie de atribuire a contractelor de achiziție publică;
- Regulamentul (UE) 679 din 27 aprilie 2016 - GDPR - privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestora;
- Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE;
- Regulamentul (UE) NR. 910 din 23 iulie 2014 - eIDAS 2 - privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă europeană; prevederile specifice subsecvente ale standardului ETSI EN 319 521 în ce privește subsetul de cerințe privind livrare electronică înregistrată (ERD)
- Regulamentul (UE) 2024/1183 din 11 aprilie 2024 al Parlamentului European și al Consiliului de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală;
- Standardul ETSI EN 319 521 V1.1.1 din februarie 2019 - Standardul privind Semnăturile și infrastructurile electronice (ESI) - Politică și cerințe de securitate pentru furnizorii de servicii de livrare electronică înregistrată (ERD);
- Legea nr. 214 din 5 iulie 2024 - privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acestea;
- Ordonanța de Urgență nr. 155 din 30 decembrie 2024 - privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil;
- Legea nr. 58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României;
- Directiva (UE) 2022/2555 din 14 decembrie 2022 - NIS 2 - a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148;
- Legea nr. 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate și Normele de referință aprobate în 26 octombrie 2023;
- Ordonanța de urgență a Guvernului nr. 112/2018 privind accesibilitatea site-urilor web și a aplicațiilor mobile ale organismelor din sectorul public și a Normelor de monitorizare a conformității site-urilor web și a aplicațiilor mobile cu cerințele privind accesibilitatea, aprobate prin Decizia Președintelui ADR nr. 815/2022;
- Legea nr. 16 din 2 aprilie 1996 (*republicată* în 22 aprilie 2014) a arhivelor naționale;

- Legea nr. 201 din 25 iunie 2024 - pentru completarea Legii Arhivelor Naționale nr. 16/1996, precum și pentru modificarea și completarea Legii nr. 135/2007 privind arhivarea documentelor în formă electronică;
- Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei;

Ofertantul devenit Contractant are obligația de a respecta în executarea Contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii.

În acest sens, Ofertantul va prezenta o declarație din care să rezulte faptul că la elaborarea ofertei a ținut cont de obligațiile relevante din domeniile mediului, social și al relațiilor de muncă. Instituțiile competente de la care operatorii economici pot obține informațiile detaliate privind obligațiile relevante din domeniile mediului, social și al relațiilor de muncă sunt Ministerul Mediului și Ministerul Muncii, Familiei, Protecției Sociale și Persoanelor Vârstnice și de la Inspectoratele Teritoriale de Muncă, respectiv și de pe site-urile:

- http://www.anpm.ro/web/guest/legislatie
- http://www.inspectiamuncii.ro/legislatie

14 MANAGEMENTUL / GESTIONAREA CONTRACTULUI ȘI ACTIVITĂȚI DE RAPORTARE

Monitorizarea contractului se va realiza de către echipa de proiect prin întocmirea rapoartelor de progres/intermediare pe fiecare din fazele contractului. Atât Prestatorul, cât și Achizitorul vor urmări finalizarea și conformitatea cu scopul a livrabilelor contractului, plățile fiind efectuate pe livrabile după recepționarea acestora, conform mențiunilor privind decontarea.

14.1 Gestionarea relației dintre Contractant și Autoritatea Contractantă

Autoritatea Contractantă consideră că factorii critici ai realizării rezultatelor așteptate ale Contractului în termen, sunt: buna comunicare între echipele Autorității Contractante și Ofertantul devenit Prestator, implementarea în termen a livrabilelor contractului și disponibilitatea soluției propuse pe durata prestației.

14.2 Organizarea activităților pe durata contractului.

Autoritatea Contractantă va organiza prima întâlnire de lucru, cea de demarare a activităților contractului, cu scopul de a obține asigurarea că Autoritatea Contractantă și Ofertantul devenit Prestator au aceeași perspectivă asupra activităților și rezultatelor din Contract, întâlnire la care vor participa cel puțin reprezentanții de contract desemnați ai Autorității Contractante și ai Contractantului.

În cadrul acestei întâlniri se vor agrea și valida, de comun acord aspectele procedurale ce vor fi urmate de părți privind cadrul organizatoric stabilit pentru realizarea activităților Contractului, managementul și monitorizarea execuției acestuia, care să prezinte cu claritate, trasabil și măsurabil:

- calendarul Rapoartelor de execuție / monitorizare calitativă / cantitativă ale Contractului;
- responsabili / responsabilități / date contact ale Prestatorului și Autorității Contractante privind realizarea Contractului;
- măsuri precizând sesizarea / tratarea potențialelor incidente, modalitatea concretă de intervenție pentru asigurarea atingerii rezultatelor așteptate în termen;
- alte aspecte cu influență asupra execuției contractului.

Se va întocmi de către părți minuta întâlnirii având anexate datele privind responsabilii, datele de contact ale acestora și responsabilitățile, care se va distribui responsabililor / părților spre cunoștință și îndeplinire.

14.3 Modalitatea de comunicare

Pentru eficiență, comunicarea se va face prin e-mail, telefon sau în întâlniri de lucru sau de acceptare a rezultatelor parțiale, desfășurate alternativ și în mediu virtual, în conformitate cu Planul de lucru propus de Ofertant; pentru trasabilitate, oricare parte va putea formaliza într-un mesaj scris concluziile unei convorbiri telefonice.

14.4 Tratarea incidentelor

Partea interesată, sesizată din oficiu, va notifica responsabililor celeilalte părți orice incident, justificând caracterul, prioritatea și prognoza în perspectiva proprie asupra rezultatelor, prin mijloace potrivite situației (telefon/ e-mail/adresă). În contextul în care răspunsul primit nu este concludent, partea interesată va convoca / organiza întâlnirea de lucru în regim de urgență și în termen de 3 zile lucrătoare, iar cealaltă parte are obligația să-i dea curs.

În cadrul întâlnirii se vor expune de către părți faptele care au condus la incident, și, obligatoriu se vor agrea și consemna în minuta de ședință cel puțin concluzia asupra incidentului, după caz măsurile agreate de remediere / responsabili / responsabilități / modalitate de remediere.

14.5 Rapoartele/documentele solicitate de la Contractant

Pe durata execuției Contractului Ofertantul devenit Prestator va prevedea și întocmi rapoarte de progres/intermediare la încheierea fiecărei etape asociate livrabilelor, sau, la solicitarea întemeiată a Autorității Contractante și le va transmite prin e-mail managerului de proiect al Autorității Contractante. Fiecare raport va conține la final concluzii din care să reiasă nemijlocit încadrarea în termenele Planului de lucrări, după caz incidente.

La finalizarea Contractului Prestatorul va prevedea și întocmi raportul de finalizare a lucrărilor rezumând etapele finalizate versus termenele asumate și-l va transmite prin e-mail managerului de proiect al Autorității Contractante. Raportul va conține la final, după caz, o secțiune de concluzii și recomandări.

Toate rapoartele vor fi semnate cu semnătură electronică calificată.

14.6 Acceptarea rezultatelor parțiale și finale în cadrul Contractului

Odată ce Contractantul a finalizat un livrabil ofertat (furnizare și/sau prestare de servicii, configurare, instruire și punere în funcțiune), Achizitorul (prin comisia de recepție) are obligația de a-l inspecta, în termen de 5 zile lucrătoare, pentru a verifica conformitatea cu specificațiile tehnice stabilite în Caietul de sarcini și de a întocmi Procesul-verbal de recepție, după cum urmează:

1. Verificarea conformității:
    - se verifică dacă bunurile livrate sau serviciile prestate corespund specificațiilor tehnice din contract, din caietul de sarcini sau din alte documente relevante.
    - se verifică cantitatea și calitatea bunurilor/serviciilor.
    - se examinează documentația tehnică însoțitoare (certificate de calitate, garanții, instrucțiuni de utilizare etc.).
2. Testarea și punerea în funcțiune:
    - în cazul bunurilor care necesită instalare și punere în funcțiune, se efectuează testele necesare pentru a se verifica funcționarea corectă.
    - se instruiește personalul beneficiarului cu privire la utilizarea și întreținerea bunurilor/serviciilor.
3. Recepția provizorie (dacă este cazul):
    - Se întocmește un proces-verbal de recepție provizorie care consemnează rezultatele verificărilor și testelor efectuate.
    - Se identifică eventualele neconformități sau deficiențe și se stabilește un termen pentru remedierea acestora.
4. Remedierea deficiențelor:
    - Prestatorul are obligația de a remedia deficiențele constatate în termenul stabilit.
5. Recepția definitivă:
    - După remedierea deficiențelor, se efectuează o nouă verificare și se întocmește un proces-verbal de recepție definitivă.
    - Recepția definitivă atestă faptul că bunurile/serviciile sunt conforme și pot fi utilizate în scopul pentru care au fost achiziționate.

Parcurgerea tuturor etapelor antemenționate se poate consemna într-un singur Proces-verbal de recepție cu condiția înscrierii pe document a tuturor informațiilor relevante.

Documentele justificative pe baza cărora se vor deconta livrabilele de către Prestator sunt:

1. Procesul-verbal de recepție (care atestă recepția definitivă a livrabilului)
2. Raportul de activitate (aferent livrabilului)
3. Factura (transmisă prin SPV)

Rapoartele periodice și alte livrabile asimilate prevăzute în planul de lucrări trebuie realizate și predate Achizitorului la termenele prevăzute în acesta. După caz, odată cu recepționarea serviciilor, prestatorul va preda Achizitorului livrabilele subsecvente prevăzute în cerințele Caietului de sarcini. În situația în care Prestatorul nu prestează serviciile contractate în cadrul termenului de livrare stabilit, acesta se află în întârziere de drept, nefiind necesară punerea sa în întârziere printr-o altă notificare.

În cazul în care pe parcursul îndeplinirii contractului se constată că anumite elemente ale propunerii tehnice sunt inferioare sau nu corespund cerințelor prevăzute în Caietul de sarcini, prevalează prevederile Caietului de sarcini conform art. 147 alin. (2) din H.G. nr. 395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică/acordului-cadru din Legea nr. 98/2016.

14.7 Finalizarea serviciilor în cadrul Contractului

La finalizarea serviciilor, realizarea cantitativă / calitativă a rezultatelor va fi constatată și consemnată de către reprezentanții Achizitorului și Prestatorului în Procesul-verbal de recepție finală.

Autoritatea Contractantă va considera serviciile din cadrul Contractului finalizate în momentul în care:

1. toate cerințele cuprinse în Caietul de Sarcini au fost îndeplinite, respectiv s-a realizat recepția finală a serviciilor;

2. rezultatele au fost aprobate de Autoritatea Contractantă, pe baza cerințelor incluse în Contract

Contractul va fi considerat finalizat când rezultatele au fost aprobate de Autoritatea Contractantă pe baza cerințelor incluse în Contract (incluzând obligațiile de întocmire a rapoartelor de monitorizare/progres de către Prestator).

14.8 Monitorizarea realizării activităților și a rezultatelor pe perioada derulării Contractului

Monitorizarea contractului se va realiza de către echipa de proiect prin întocmirea rapoartelor de progres pe fiecare din fazele contractului.

14.9 Evaluarea performanței Contractantului

Categorie indicator	Indicator de performanță	Referința în contract / Caiet de Sarcini - TdR	Nivelul de performanță așteptat (conform contract / Caiet de Sarcini - TdR)	Ce se măsoară	Modalitatea de evaluare (vezi Tabelul „Modalitatea de evaluare a Indicatorilor de performanță")	Scop
Financiar	VPC - % de variație între prețul contractului și prețul estimat de Contractant (diferența dintre prețul contractului comparat cu oferta) FORMULA DE CALCUL: VPC (% DE VARIAȚIE) = (PREȚ FINAL CONTRACT / PREȚ INIȚIAL ESTIMAT*100) - 100	Valoarea estimată (caiet de sarcini) - Evaluarea ofertelor. Oferta de fundamentare a bugetului.	Variația costurilor estimate să fie mai mică de 10%	Calitatea și acuratețe a estimării costurilor	Foarte satisfăcător - 5 pct Satisfăcător - 4 pct Acceptabil - 3 pct Nesatisfăcător - 2 pct Foarte nesatisfăcător - 1 pct	Evaluarea corectitudinii și exactității estimării costurilor.
Calitatea livrabilelor	NCL - Nivelul de calitate al livrabilelor (/ conformitate cu cerințele)	Monitorizare - Caiet de Sarcini Rapoartele de monitorizare ale contractului	Implementare a conformă a cerințelor funcționale - eficiență în executarea contractului.	Nivelul de calitate al livrabilelor	Foarte satisfăcător - 5 pct Satisfăcător - 4 pct Acceptabil - 3 pct Nesatisfăcător - 2 pct Foarte nesatisfăcător - 1 pct	Evaluarea nivelului de implementare a cerințelor funcționale.

Modalitatea de evaluare a indicatorilor de performanță:

Indicator de performanță	Modalitatea de evaluare
VPC - % de variație între prețul contractului și prețul estimat de Contractant (diferența dintre prețul contractului comparat cu oferta) FORMULA DE CALCUL: VPC (% DE VARIAȚIE) = (PREȚ FINAL CONTRACT / PREȚ INIȚIAL ESTIMAT*100) - 100	Se acordă puncte în funcție intervalul variației costurilor, independent de faptul că aceasta este pozitivă sau negativă: Foarte satisfăcător - 5 pct: VPC în intervalul 0%, <=10% Satisfăcător - 4 pct: VPC în intervalul >10%, <=15% Acceptabil - 3 pct: VPC în intervalul >15%, <=25% Nesatisfăcător - 2 pct: VPC în intervalul >25%, <=50% Foarte nesatisfăcător - 1 pct: VPC depășește 50%

NCL - Nivelul de calitate al livrabilelor (/ conformitate cu cerințele)	Urmare a parcurgerii etapei de testare / recepție a livrabilelor, se acordă puncte evaluând felul în care acestea asigură conformitatea cu cerințele funcționale ale Caietului de Sarcini: Foarte satisfăcător - 5 pct: dacă toate componentele sistemului informatic, la momentul livrării, au fost conforme cerințelor și nu au fost necesare ajustări ale acestuia. Satisfăcător - 4 pct: dacă toate componentele sistemului informatic, la momentul livrării, au fost conforme cerințelor, dar au fost necesare ajustări nemateriale minore ale acestuia. Acceptabil - 3 pct: dacă toate componentele sistemului informatic recepționate au fost conforme cerințelor după ce s-au realizat corecții / modificări ale acestuia în termenele asumate prin contract, urmare a disfuncționalităților evidențiate de testele efectuate. Nesatisfăcător - 2 pct: dacă toate componentele sistemului informatic recepționate au fost conforme cerințelor doar după ce s-au realizat corecții / modificări ale acestuia cu depășirea termenelor asumate prin contract, urmare a disfuncționalităților evidențiate de testele efectuate. Foarte nesatisfăcător - 1 pct: A fost necesară rezilierea contractului din cauza disfuncționalităților semnificative ale sistemului informatic.

14.10 Asigurarea și controlul calității pe durata contractului

Se vor prezenta de către Prestator în cadrul Propunerii Tehnice elementele avute în vedere pentru prestarea serviciilor pe toată durata contractului, urmărind să asigure pentru beneficiar un nivel calitativ adecvat al prestației:
1. descrierea modului de asigurare și control al calității aplicabile proceselor pe care le derulează în activitatea din proiect.
2. descrierea modului în care va realiza monitorizarea evoluției contractului și descrierea criteriilor de calitate urmărite pe perioada desfășurării contractului, inclusiv tipul și frecvența rapoartelor de monitorizare a evoluției contractului.
3. următoarele proceduri de lucru: 1. Procedura de analiză și design, 2. Procedura de dezvoltare aplicații software, 3. Procedura de testare a livrabilelor software, 4. Procedura de control a produsului neconform, 5. Planul de instruire, 6. Procedura privind asistența tehnică, mentenanță și suport, 7. Procedura de agreare a schimbărilor, 8. Procedura de acceptanță.
Notă: Titulatura procedurilor solicitate este orientativă - ofertantul poate prezenta procedurile sub altă titulatură/structură, cu condiția ca acestea să releve cadrul activităților solicitate.
Cadrul procedural astfel prezentat va fi selectat și aprobat spre aplicare în contract sau lăsat la latitudinea prestatorului, în funcție de acordul părților exprimat în cadrul ședinței de organizare inițială a proiectului.
Neprezentarea în oferta tehnică a acestor documente va duce la descalificarea ofertei ca fiind neconformă.

15 PLATA SERVICIILOR

Plata serviciilor prestate se va efectua în termen de 30 de zile de la data înregistrării facturii la sediul Autorității Contractante.
Factura va putea fi emisă pentru unul sau mai multe livrabile/rezultate finale, cu condiția ca acestea să fi fost recepționate (acceptate) anterior de către Autoritatea Contractantă, pe baza unui proces-verbal de recepție.
Factura va fi însoțită de raportul de activitate aferent livrabilelor/rezultatelor finale măsurabile cuprinse în factură.

16 METODOLOGIA DE EVALUARE A OFERTELOR PREZENTATE

16.1 Criteriul de atribuire

Criteriu adoptat de Autoritatea Contractantă este cel mai bun raport calitate-preț, aplicat pentru evaluarea ofertelor considerate admisibile și conforme din punct de vedere tehnic, în pondere de 60% alocată Propunerii Tehnice pe criteriul „calitate”, respectiv 40% alocată Propunerii Financiare pe criteriul „preț”.

16.2 Algoritm de calcul

Va fi declarată câștigătoare oferta care obține cel mai mare număr total de puncte P, calculat ca sumă a punctajelor obținute pe factori de evaluare pe baza formulei
P = P1 + P2,
în care factorii de evaluare sunt:

Indicator punctaj	Criteriu	Factori de evaluare	Punctaj maxim acordat

P1	Preț	Prețul ofertei - prețul cel mai scăzut	40
P2	Calitate	Propunerea Tehnică - demonstrarea unui nivel calitativ superior prin propunerea planului de implementare și dovedirea experienței similare.	60
P = P1 + P2			100

P1 - Prețul ofertei

Pentru acest factor de evaluare, datorită ponderii de 40 % a criteriului „preț", s-au alocat 40 puncte din 100 total puncte.

Algoritm de calcul factor P1

Pentru factorul de evaluare „P1 - Prețul ofertei", punctajul se va acorda astfel:

a) Pentru cel mai scăzut dintre prețuri se acordă punctajul maxim alocat;

b) Pentru celelalte prețuri ofertate punctajul P(n) se calculează proporțional, astfel: **P(n) = (Preț minim ofertat / Preț n) x punctaj maxim alocat**.

P2 - Propunerea tehnică

Pentru factorul de evaluare P2, datorită ponderii de 60 % a criteriului „calitate", s-au alocat 60 puncte din 100 total puncte.

Oferta tehnică va fi evaluată în conformitate cu cerințele Caietului de sarcini. Punctele se vor acorda pentru specificațiile care îndeplinesc cel puțin cerințele minime conform factorilor de evaluare specificați.

Pentru sub factorii de evaluare punctajul se va aloca astfel:

2.1 Un total maxim de **30 puncte** se acordă sub factorului „**P2.1 Demonstrarea unei abordări/viziuni adecvate de implementare a contractului, precum și o planificare adecvată a resurselor umane și a activităților**" prin cei 6 sub factori de calitate ai Planului de lucru, respectiv câte un maxim de 5 puncte pentru fiecare:

- P2.1.1 Abordarea propusă pentru implementarea contractului.
- P2.1.2 Resursele (umane și materiale) și realizările corespunzătoare fiecărei activități.
- P2.1.3 Atribuțiile membrilor echipei în implementarea activităților contractului și, dacă este cazul, contribuția fiecărui membru al grupului de operatori economici, precum și distribuirea și interacțiunea sarcinilor și responsabilităților dintre ei.
- P2.1.4 Încadrarea în timp, succesiunea și durata activităților propuse și corelarea cu efortul prevăzut pentru experți.
- P2.1.5 Identificarea și încadrarea în timp a punctelor de reper semnificative în execuția contractului, inclusiv descrierea modului în care acestea vor fi reflectate în raportări, în special cele prevăzute în caietul de sarcini.
- P2.1.6 Abordarea propusă pentru managementul schimbării în organizație.

și

2.2 Un total maxim de **30 de puncte** se acordă sub factorului „**P2.2 - Experiența similară a experților**" prin cei 3 sub factori privind experiența similară a experților, respectiv câte un maxim de 10 puncte pentru fiecare:

- P2.2.1 Expert e-guvernare (1)
- P2.2.2 Expert e-guvernare (2)
- P2.2.3 Expert e-guvernare (3)

Oferta tehnică va fi evaluată în conformitate cu cerințele Caietului de sarcini. Punctele se vor acorda pentru specificațiile care îndeplinesc cel puțin cerințele minime conform factorilor de evaluare specificați.

Algoritm de calcul factor P2

Pentru factorul de evaluare „P2 Propunere Tehnică", punctajul se va acorda astfel:

1. Pentru fiecare sub factor de evaluare se acordă puncte.
2. Fiecare factor va fi apreciat în funcție de calificativul „foarte bine / bine / acceptabil". Comisia de evaluare va acorda calificativul luând în considerare liniile directoare specificate iar punctajul aferent fiecărui factor de evaluare va fi obținut prin acordarea notei corespunzătoare calificativului obținut de oferta respectivă la evaluarea acelui factor.
3. Fiecăruia din cei 6 sub factori (P2.1.1 - P2.1.6) ai sub factorului „P2.1 Demonstrarea unei abordări/viziuni adecvate de implementare a contractului, precum și o planificare adecvată a resurselor umane și a activităților" care vor fi utilizați de comisia de evaluare ca puncte de reper în aprecierea acestuia li se acordă calificative, iar fiecărui calificativ îi corespunde un punctaj: pentru calificativul „foarte bine" se acordă 5 puncte, pentru calificativul „bine" se acordă 3 puncte, pentru calificativul „acceptabil" se acordă 1 punct.
4. Punctajul sub factorului P2.1 se calculează prin însumarea punctajelor tehnice obținute în urma aplicării fiecărui sub factor de evaluare: **P2.1 = P2.1.1 + P2.1.2 + P2.1.3 + P2.1.4 + P2.1.5 + P2.1.6**
5. Fiecăruia din cei 3 sub factori (P2.2.1 - P2.2.3) ai sub factorului „P2.2. Experiența similară a experților", li se acordă calificativele pentru experiența expertului ce face obiectul factorului de evaluare, măsurată prin numărul de contracte de o complexitate comparabilă sau superioară la care a participat realizând activități similare cu cele ce urmează a le implementa în cadrul viitorului contract, după cum urmează: între 2 și 3 proiecte - se acordă calificativul „acceptabil" - 4 pct; între 4 și 5 proiecte - se acordă

calificativul „bine” - 7 pct; 6 sau peste 6 proiecte - se acordă calificativul „foarte bine” - 10 pct; pentru îndeplinirea cerinței minime din caietul de sarcini, (un proiect) oferta este admisibilă, dar nu se punctează.

6. Punctajul sub factorului P2.2 se calculează prin însumarea punctajelor tehnice obținute în urma aplicării fiecărui sub factor de evaluare: **P2.2 = P2.2.1 + P2.2.2 + P2.2.3**
7. Punctajul tehnic total al ofertei tehnice $P2_{ofertă}$ se calculează prin însumarea punctajelor tehnice obținute în urma aplicării fiecărui factor de evaluare: **$P2_{ofertă}$ = P2.1 + P2.2**

În situația în care egalitatea se menține, Autoritatea Contractantă are dreptul să solicite noi propuneri financiare, și oferta câștigătoare va fi desemnată cea cu propunerea financiară cea mai mică.

P2.1 Demonstrarea unei abordări/viziuni adecvate de implementare a contractului, precum și o planificare adecvată a resurselor umane și a activităților (punctaj maxim 30)		
Linii directoare: se va analiza informația furnizată în propunerea tehnică	Calificativ	Punctaj
Sub factori (2.1.1 - 2.1.6)		
P2.1.1 Abordarea propusă pentru implementarea contractului		
Abordarea propusă se bazează în mare măsură pe o serie de metodologii, metode și/sau instrumente testate, recunoscute și care demonstrează o foarte bună înțelegere a contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini, în corelație cu aspectele-cheie, precum și cu riscurile și ipotezele identificate.	foarte bine	5
Abordarea propusă se bazează parțial pe metodologii, metode și/sau instrumente testate, recunoscute și care demonstrează înțelegerea contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini, în corelație cu aspectele-cheie, precum și cu riscurile și ipotezele identificate.	bine	3
Abordarea propusă nu are la bază metodologii, metode și/sau instrumente testate, recunoscute și arată o înțelegere limitată a contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini.	acceptabil	1
P2.1.2. Resursele (umane și materiale) și realizările corespunzătoare fiecărei activități		
Resursele identificate și realizările indicate sunt corelate deplin/în mare măsură cu complexitatea fiecărei activități propuse.	foarte bine	5
Resursele identificate și realizările indicate sunt parțial corelate cu complexitatea fiecărei activități propuse.	bine	3
Resursele identificate și realizările indicate sunt corelate într-un mod limitat cu complexitatea activităților propuse.	acceptabil	1
P2.1.3. Atribuțiile membrilor echipei în implementarea activităților contractului și, dacă este cazul, contribuția fiecărui membru al grupului de operatori economici, precum și distribuirea și interacțiunea sarcinilor și responsabilităților dintre ei		
Sunt indicate responsabilitățile în execuția contractului și interacțiunea între membrii echipei, inclusiv cele referitoare la managementul contractului, activitățile de suport și, dacă este cazul, distribuirea și interacțiunea sarcinilor și responsabilităților între operatorii din cadrul grupului.	foarte bine	5
Sunt indicate parțial responsabilitățile în execuția contractului și interacțiunea între membrii echipei, inclusiv cele referitoare la managementul contractului, activitățile de suport și distribuirea și interacțiunea sarcinilor și responsabilităților între operatorii economici din cadrul grupului (dacă este cazul).	bine	3
Sunt indicate în mod limitat responsabilitățile în execuția contractului sau interacțiunea între membrii echipei, inclusiv cele referitoare la managementul contractului și activitățile de suport sau distribuirea și interacțiunea sarcinilor și responsabilităților între operatorii economici din cadrul grupului (dacă este cazul).	acceptabil	1
P2.1.4. Încadrarea în timp, succesiunea și durata activităților propuse și corelarea cu efortul prevăzut pentru experți		

Durata activităților corespunde deplin complexității acestora, iar succesiunea dintre acestea, inclusiv perioada de desfășurare, este stabilită în funcție de logica relației dintre acestea. Durata prevăzută pentru fiecare operațiune principală necesară este corelată cu activitățile prevăzute a fi realizate în lunile respective și resursele identificate pentru desfășurarea acestora. Numărul de zile de muncă distribuit pe categoriile de experți este corelat cu activitățile prevăzute a fi realizate în lunile respective și resursele identificate pentru desfășurarea acestora	foarte bine	5
Durata activităților corespunde parțial complexității acestora, iar succesiunea dintre acestea, inclusiv perioada de desfășurare este corelată doar parțial cu logica relației dintre acestea. Durata prevăzută pentru fiecare operațiune principală necesară este corelată parțial cu activitățile prevăzute a fi realizate în lunile respective și resursele estimate pentru desfășurarea acestora. Numărul de zile de muncă distribuit pe categoriile de experți este corelat parțial cu activitățile prevăzute a fi realizate în lunile respective și resursele estimate pentru desfășurarea acestora.	bine	3
Durata activităților este în mică măsură potrivită complexității acestora sau succesiunea dintre acestea, inclusiv perioada de desfășurare, este stabilită într-un mod foarte puțin adecvat în raport cu logica relației dintre acestea sau durata prevăzută pentru fiecare operațiune principală necesară este corelată în mică măsură cu activitățile prevăzute a fi realizate în lunile respective și resursele estimate pentru desfășurarea acestora. Numărul de zile de muncă distribuit pe categoriile de experți este corelat în mică măsură cu activitățile prevăzute a fi realizate în lunile respective și resursele estimate pentru desfășurarea acestora.	acceptabil	1
P2.1.5. Identificarea și încadrarea în timp a punctelor de reper semnificative în execuția contractului, inclusiv descrierea modului în care acestea vor fi reflectate în raportări, în special cele prevăzute în caietul de sarcini		
Punctele de reper identificate sunt semnificative pentru execuția contractului, sunt încadrate corect în timp și corelate corespunzător cu raportările, în special cele prevăzute în caietul de sarcini.	foarte bine	5
Punctele de reper identificate sunt în mică măsură semnificative pentru execuția contractului, dar sunt încadrate corect în timp și corelate corespunzător cu raportările, în special cele prevăzute în caietul de sarcini.	bine	3
Punctele de reper sunt identificate, dar nu sunt semnificative sau nu sunt încadrate corect în timp sau nu sunt corelate corespunzător cu raportările, în special cele prevăzute în caietul de sarcini.	acceptabil	1
P2.1.6. Abordarea propusă pentru managementul schimbării în organizație		
Abordarea propusă demonstrează o foarte bună înțelegere a contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini, în corelație cu aspectele-cheie, precum și cu riscurile și ipotezele identificate, integrând schimbarea organizațională cu cea informatică.	foarte bine	5
Abordarea propusă demonstrează parțial înțelegerea contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini, în corelație cu aspectele-cheie, precum și cu riscurile și ipotezele identificate, fără integrarea schimbării organizaționale cu cea informatică.	bine	3
Abordarea propusă arată o înțelegere limitată a contextului, respectiv a particularității sarcinilor stabilite în caietul de sarcini	acceptabil	1
Prin metodologii, metode și/sau instrumente testate referite în secțiunea P2.1.1. se înțelege că metodologiile, metodele și/sau instrumentele au fost utilizate în alte proiecte. Prin metodologii, metode și/sau instrumente recunoscute referite în secțiunea P2.1.1. se înțelege că metodologiile, metodele și/sau instrumentele sunt descrise în literatura de specialitate. Resursele referite în secțiunea P2.1.2. sunt umane și materiale. Se va lua în considerare și personalul suport.		
Oferta tehnică va fi evaluată în conformitate cu cerințele caietului de sarcini. Punctele se vor acorda pentru specificațiile care depășesc cerințele minime conform factorilor de evaluare specificați anterior.		

P2.2. Experiența similară a experților. (punctaj maxim 30)		
Linii directoare: se va analiza informația furnizată privind experiența experților	Calificativ	Punctaj
P2.2.1 Expert e-guvernare (1)		

Expertul face dovada participării în șase sau mai multe proiecte/contracte, în care a îndeplinit efectiv activități de analiză, proiectare sau reinginerie a fluxurilor de lucru digitale (administrative ori de business) sau a serviciilor digitale / facilitarea realizării interoperabilității electronice.	foarte bine	10
Expertul face dovada participării în patru sau cinci proiecte/contracte, în care a îndeplinit efectiv activități de analiză, proiectare sau reinginerie a fluxurilor de lucru digitale (administrative ori de business) sau a serviciilor digitale / facilitarea realizării interoperabilității electronice.	bine	7
Expertul face dovada participării în două sau trei proiecte/contracte, în care a îndeplinit efectiv activități de analiză, proiectare sau reinginerie a fluxurilor de lucru digitale (administrative ori de business) sau a serviciilor digitale / facilitarea realizării interoperabilității electronice.	acceptabil	4
P2.2.2 Expert e-guvernare (2)		
Expertul face dovada participării în șase sau mai multe proiecte/contracte, în care a îndeplinit efectiv activități de analiză, proiectare sau reinginerie a fluxurilor de lucru digitale (administrative ori de business) sau a serviciilor digitale / facilitarea realizării interoperabilității electronice.	foarte bine	10
Expertul face dovada participării în patru sau cinci proiecte/contracte, în care a îndeplinit efectiv activități de analiză, proiectare sau reinginerie a fluxurilor de lucru digitale (administrative ori de business) sau a serviciilor digitale / facilitarea realizării interoperabilității electronice.	bine	7
Expertul face dovada participării în două sau trei proiecte/contracte, în care a îndeplinit efectiv activități de analiză, proiectare sau reinginerie a fluxurilor de lucru digitale (administrative ori de business) sau a serviciilor digitale / facilitarea realizării interoperabilității electronice.	acceptabil	4
P2.2.3 Expert e-guvernare (3)		
Expertul face dovada participării în șase sau mai multe proiecte/contracte, în care a îndeplinit efectiv activități de analiză, proiectare sau reinginerie a fluxurilor de lucru digitale (administrative ori de business) sau a serviciilor digitale / facilitarea realizării interoperabilității electronice.	foarte bine	10
Expertul face dovada participării în patru sau cinci proiecte/contracte, în care a îndeplinit efectiv activități de analiză, proiectare sau reinginerie a fluxurilor de lucru digitale (administrative ori de business) sau a serviciilor digitale / facilitarea realizării interoperabilității electronice.	bine	7
Expertul face dovada participării în două sau trei proiecte/contracte, în care a îndeplinit efectiv activități de analiză, proiectare sau reinginerie a fluxurilor de lucru digitale (administrative ori de business) sau a serviciilor digitale / facilitarea realizării interoperabilității electronice.	acceptabil	4
Pentru probarea participării într-un proiect/contract, se solicită documente justificative care probează participarea persoanei propuse, cum ar fi certificate de predare-primire / recomandări / procese-verbale de recepție / certificate constatatoare / copii ale unor părți relevante ale contractelor pe care le-au îndeplinit / oricare alte documente doveditoare, care trebuie să îndeplinească cumulativ următoarele condiții: *1. Să precizeze obiectivul contractului din care să rezulte că acesta îndeplinește caracteristicile unui proiect similar.* *2. Din documente să reiasă clar:* *2.1. numele și prenumele persoanei propuse;* *2.2. perioada în care persoana propusă a desfășurat activități în cadrul proiectului similar;* *2.3. rolul (poziția) ocupată de persoana nominalizată și activitățile îndeplinite de persoana nominalizată în cadrul proiectului similar;* *Contractele prezentate ca experiență similară trebuie să fi inclus servicii de dezvoltare, implementare sau extindere a unor sisteme informatice integrate sau soluții software de nivel enterprise, având o complexitate comparabilă sau superioară cu cea a contractului ce urmează a fi atribuit.*		

17 PROTECȚIA DATELOR CU CARACTER PERSONAL

În executarea contractului prestatorul se angajează să depună toate diligențele pentru păstrarea confidențialității datelor cu caracter personal în acord cu prevederile legale în vigoare.

18 NEDISCRIMINARE ȘI EGALITATE DE ȘANSE/GEN

În executarea contractului de servicii, prestatorul va ține cont de obligațiile referitoare la respectarea principiului egalității de șanse/gen și de tratament egal, în cadrul relațiilor de muncă de orice fel. Prestatorul garantează nediscriminarea în procesul de gestionare a resurselor umane pe criterii de rasă, naționalitate, etnie, limbă, religie, categorie socială, convingeri, sex, orientare sexuală, vârstă, handicap, boală cronică necontagioasă, infectare HIV, apartenență la o categorie defavorizată, precum și orice alt criteriu cu potențial de discriminare.

Anexe

1. Contract de prestări servicii
2. Formular de propunere tehnică
3. Formulare