# Proiect Tehnic

## Direcția de Asistență Socială Drobeta-Turnu Severin 2024

Denumire Proiect:

**Digitalizarea proceselor de asistență socială la nivelul Municipiului Drobeta-Turnu Severin**

APLIX TECHNOLOGIES

11 IUNIE 2024

**Furnizor: APLIX TEHNOLOGIES**
**Beneficiar: Direcția de Asistență Socială Drobeta-Turnu Severin**
**Întocmit de:** Dorel Constantin Ilași

**Cuprins:**

# 1. INFORMAȚII GENERALE

## 1.1. Date despre obiectivul de investiție

Prezentul **Proiect Tehnic** este întocmit în contextul lansării Ghidului solicitantului „Digitalizare în beneficiul cetățenilor" ca parte din **Programul Regional Sud-Vest Oltenia 2021-2027** și a adoptării la nivelul Municipiului Drobeta-Turnu Severin a studiului de fezabilitate ce fundamentează implementarea la nivel local a proiectului **„Digitalizarea proceselor de asistență socială la nivelul Municipiului Drobeta-Turnu Severin"**, proiect destinat să continue eforturile pentru digitalizarea serviciilor publice la nivel local.

| | |
|---|---|
| **Denumirea Proiectului TIC** | „Digitalizarea proceselor de asistență socială la nivelul Municipiului Drobeta-Turnu Severin" |
| **Scopul proiectului:** | (1) Adoptarea de noi tehnologii în vederea îmbunătățirii semnificative a calității serviciilor publice pe care le are în competență,<br>(2) Standardizarea modului de lucru la nivelul tuturor instituțiilor subordonate și a partenerilor instituționali cu care colaborează în mod regulat,<br>(3) Creșterea gradului de interconectivitate și interoperabilitate cu toate entitățile publice și private care dețin atribuții în buna desfășurare a serviciilor publice la nivel local și<br>(4) Crearea de funcționalități noi în legătură cu serviciile publice electronice puse la dispoziția cetățenilor, mediului de afaceri și altor autorități sau instituții publice. |
| **Locația Proiectului:** | Sediile Direcției de Asistență Socială și ale instituțiilor subordonate |
| **Ordonator principal de credite**: | Municipiul Drobeta-Turnu Severin |
| **Investitor**: | Agenția pentru Dezvoltare Regională Sud-Vest Oltenia în calitate de Autoritate de Management (AM). |
| **Beneficiarul investiției:** | Direcția de Asistență Socială Drobeta-Turnu Severin<br>Instituțiile subordonate (Creșa Drobeta) |
| **Elaboratorul proiectului tehnic:** | Aplix Technologies |

## 1.2. Date privind obiectivele proiectului TIC

| | |
|---|---|
| **Obiectivul general** | Digitalizare în beneficiul cetățenilor și al firmelor - 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. |
| **Obiectivele specifice** | Valorificarea avantajelor digitalizării, în beneficiul cetățenilor, al companiilor, al organizațiilor de cercetare și al autorităților publice:<br>▪ Acces la tehnologie de ultimă generație; |

| | |
|---|---|
| | ▪ Interconectivitate și interoperabilitate la nivel local;<br>▪ Standardizarea procedurilor și a instrumentelor;<br>▪ Servicii publice cu grad de sofisticare digitală 5. |
| **Entitățile implicate:** | - Direcția de Asistență Socială Drobeta-Turnu Severin<br>- Creșa Drobeta |
| **Beneficiile proiectului TIC** | - **Beneficii pentru cetățeni:**<br>• Administrația publică accesibilă - toate instituțiile vor fi interconectate în cloud;<br>• Cetățeanul va putea solicita și primi documente de oriunde, oricând;<br>• Economie de timp – fără cozi, fără nicio deplasare fizică la instituțiile publice;<br>• Trasabilitate – cetățeanul va putea avea un istoric al interacțiunilor sale cu administrația;<br>• Siguranță – infrastructura cloud va implementa cele mai avansate sisteme de securitate cibernetică.<br>- **Beneficii pentru instituții:**<br>• Standardizarea modului de lucru;<br>• Asigurarea accesului la instrumente de lucru inovative;<br>• Asigurarea conformității legale în generarea actelor administrative în format electronic și respectarea condițiilor de valabilitate ale actului administrativ;<br>• Va asigura interconectivitatea și interoperabilitatea sistemelor publice;<br>• Va asigura scalabilitatea serviciilor publice și va permite un management eficient al costurilor de scalare;<br>• Va reduce birocrația, prin eliminarea proceselor administrative redundante sau perimate;<br>• Va asigura o mai bună colaborare și o partajare rapidă a informațiilor între toate instituțiile din Municipiul Mehedinți și din regiunea Sud-Vest Oltenia;<br>• Va eficientiza costurile – instituțiile publice vizate nu vor mai fi nevoite să asigure mentenanță pentru echipamentele hardware și software;<br>• Creșterea eficienței aparatului administrativ va determina scăderea costurilor aferente unor sisteme informatice disparate și astfel va duce la creșterea încrederii antreprenorilor în performanța statului și va genera creștere economică;<br>• Protejarea integrată a datelor, aplicațiilor și rețelelor;<br>• Gestionarea în mod securizat a accesului la servicii și resurse;<br>• Diminuarea riscului de infectare cu malware, prin utilizarea de mecanisme de protecție;<br>• Prevenirea atacurilor prin identificarea breșelor de securitate înainte de a fi exploatate sau combaterea acestora din fazele incipiente;<br>• Asigurarea managementului vulnerabilităților și aplicarea de patch-uri în vederea remedierii acestora; |

| | |
|---|---|
| | • Protejarea împotriva atacurilor care au ca scop limitarea serviciilor;<br>• Automatizarea proceselor, notificărilor și a reacțiilor;<br>• Minimizarea timpului de reacție în cazul atacurilor cibernetice;<br>• Reducerea plajei de atacuri cibernetice care pot fi derulate împotriva rețelelor și sistemelor informatice ale acestora de către actori statali sau cu motivație financiară; |
| **Locația unde se va implementa**: | Infrastructura va fi una de tip **cloud SaaS** ce va fi găzduită în unul dintre centrele de date ce întrunesc condițiile de conformitate și acreditare prevăzute de lege. Serviciile vor fi consumate local de către toate instituțiile beneficiare. |

### 1.3. Date privind obiectivele proiectului TIC

| | |
|---|---|
| **Descrierea scenariului tehnico economic conform SF** | Sub aspect tehnic soluția informatică va avea la bază o **Platformă de Distribuție Electronică Înregistrată** (*ERDP – Electronic Registered Delivery Platform*) care va include **6 componente critice**: **(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.<br>• **Managementul identităților electronice și autentificarea** - Managementul identităților electronice va adresa următoarele aspecte cheie:<br>o Stabilirea identității electronice a persoanele fizice și persoanele juridice (inclusiv alte instituții) la nivelul sistemului;<br>o Stabilirea identităților electronice ale structurilor interne ale instituției și a angajaților din aceste structuri (*ex. virtualizarea instituției, crearea identității electronice a angajaților, etc.*);<br>o Stabilirea seturilor de validări necesare asigurării unui control eficient al acurateței datelor:<br>o Identificarea și autentificarea în sistem;<br>o Procesul de administrare a drepturilor de acces specifice fiecărui tip de utilizator;<br>o Procedurile de actualizare și auditare a accesului la datele cu caracter personal *(ex. versionarea tuturor modificărilor de date*);<br>o Integrările necesare pentru a asigurare unor identități acurate |

| | |
|---|---|
| | pentru fiecare entitate în parte (STS, ROeID, *ANAF, RECOM, și alți furnizori de servicii de încredere, etc.*);<br>o Nomenclatoarele de obiecte necesare managementului identităților (*ex. nomenclator stradal, nomenclatorul unităților administrativ teritoriale, nomenclatorul instituțiilor publice, nomenclatorul tipurilor de persoane juridice, etc.*);<br>o Parametrizarea motoarelor de căutare (*ex. structuri de filtre, sortări, vizualizări, etc.*);<br>o Parametrizarea de rapoarte specifice mentenanței identităților;<br>o Aspectele de securitate specifice managementului identităților (*ex. stabilirea gradului de robustețe a parolelor de acces, asigurarea unicității identității la nivel de sistem, autentificare multifactor, semnătura electronică calificată și sigiliul electronic calificat etc.*).<br>***Notă:** Managementul identităților se va face centralizat în conformitate cu prevederile regulamentului ~~eIDAS~~eIDAS2 și ale standardului ETSI EN 319 521 V1.1.1 din februarie 2019.*<br>• **Înregistrarea operațiunilor administrative și managementul documentelor** - înregistrarea operațiunilor administrative va adresa următoarele aspecte specifice activității administrative:<br>o Stabilirea structurilor de date ce definesc operațiunile și actele administrative la nivelul sistemului;<br>o Modalitatea de înregistrare a operațiunilor administrative și a actelor administrative și de evitarea a dublei înregistrări;<br>o Modalitatea de generare a registrelor la nivelul instituției și mentenanța multianuală a acestora;<br>o Modalitatea de acordare a numerelor de înregistrare și de asigurare a unității acestora la nivel de sistem;<br>o Definirea și operaționalizarea procedurilor de registratură fizică și registratură online;<br>o Modalitatea de repartizarea a lucrărilor;<br>o Stabilirea și gestionarea drepturilor de acces la registrele de înregistrări;<br>o Sincronizarea registrelor cu arhiva electronică;<br>o Parametrizarea motoarelor de căutare (*ex. structuri de filtre, sortări, vizualizări, etc*); |

| | |
|---|---|
| | o Parametrizarea de rapoarte specifice gestiunii registrelor electronice și stabilirea drepturilor de acces la rapoarte;<br>o Aspectele de securitate specifice înregistrării operațiunilor și actelor administrative (*ex. asigurarea unicității numărului de înregistrare, asigurarea unicității operațiunii și actelor administrative, stabilirea drepturilor de acces la înregistrările din registre, etc.*).<br>***Notă:** Înregistrarea operațiunilor și actelor administrative se va face în conformitate cu prevederile standardului ISO 15489-1 din 2016 privind managementul înregistrărilor în sistemele de Records Management. Sistemul va implementa un mecanism de **jurnalizare completă și imuabilă** a tuturor operațiunilor de creare, modificare, consultare, distribuire și ștergere (logică) a înregistrărilor și documentelor. Aceste jurnale vor fi esențiale pentru a ~~permite auditul de conformitate cu cerințele CPG și pentru a~~ asigura integritatea și trasabilitatea informațiilor gestionate.*<br>• **Interconectarea și interoperabilitatea inter și intra-instituțională** (include fluxurile electronice automatizate de lucru) – va adresa următoarele aspecte ce țin de asigurarea schimbului de date, informații și documente în relația cu cetățenii și mediul de afaceri, în relația cu alte instituții și între structurile interne ale beneficiarilor:<br>o Operaționalizarea canalelor de comunicații inter și intra-instituționale menite să asigure transportul datelor;<br>o Operaționalizarea canalelor de comunicare cu cetățenii și mediul de afaceri;<br>o Asigurarea procedurilor de încărcare, transport, livrare și vizualizare a conținutului, a datelor și documentelor;<br>o Procedurile de parametrizare a fluxurilor de comunicare;<br>o Stabilirea structurilor de date și algoritmilor de validare ce fac obiectul transferului;<br>o Automatizarea capabilităților de expediere a conținutului;<br>o Parametrizarea livrărilor în funcție de competențele destinatarului;<br>o Asigurarea capabilităților de conversie a fișierelor în format PDF;<br>o Sincronizarea cu componenta de management al identităților, cu cea de înregistrare, precum și cu cea de arhivare și îndosariere electronică; |

| | |
|---|---|
| | o Configurarea tuturor formularelor electronice ce tranzitează fluxurile electronice de lucru și asigurarea exportului de date în formate standardizate către destinatari (*ex. formulare pentru cetățeni, formulare pentru activitatea internă a instituției, formulare destinate comunicării inter-instituționale, etc.*) ;<br>o Operaționalizarea interconectivității cu entitățile care dețin identitate electronică la nivelul platformei și cu cele care nu dețin o identitate electronică în sistem;<br>o Asigurarea mijloacelor colaborative de lucru (*ex. audio-video conferințe, partajarea de ecrane, chat, documente colaborative, transfer de fișiere, etc.*)<br>o Asigurarea și mentenanța **API-urilor RESTful** de interconectare cu furnizorii de servicii de semnare electronică calificată, cu furnizorii de servicii de sigilare electronică calificată, cu STS, ROeID, ANAF, RECOM, cu Platforma Națională de Interoperabilitate (PNI), cu alte sisteme informatice terțe autorizate să opereze în ~~CPG~~cloudul privat guvernamental (CPG) / cloudul regional (CR) și cu alți furnizori.<br>***Notă:** Interconectarea și interoperabilitate se va face în conformitate cu prevederile standardului ETSI EN 319 521 V1.1.1 / 2019 și ale legii 242 din 2022 privind schimbul de date între sisteme informatice. Schimburile de date realizate prin aceste API-uri vor respecta cu strictețe modelele de date comune și standardele semantice definite în Cadrul Național de Interoperabilitate (CNI) și detaliate în Normele de Referință pentru Realizarea Interoperabilității (NRRI), asigurând alinierea cu standardele europene de interoperabilitate semantică (de exemplu, cele promovate de SEMIC.EU, cum ar fi DCAT-AP). Soluția trebuie să fie capabilă să se integreze cu servicii partajate care ar putea fi disponibile în CPG/CR utilizând API-urile oficiale ale instituțiilor acolo unde PNI acționează ca broker de servicii.*<br>• **Arhivarea și îndosarierea electronică** – arhivarea electronică a documentelor va adresa problematica specifică referitoare le următoarele aspecte:<br>o Asigurarea procedurilor de creare și parametrizare multianuală a nomenclatorului arhivistic (grupele de documente);<br>o Gestionarea structurilor de metadate pentru documentele arhivate; |

| | |
|---|---|
| | ○ Asigurarea procedurilor de creare și parametrizare multianuală a structurii de îndosariere a actelor (dosarele de acte);<br>○ Acordarea drepturilor de acces la grupele și dosarele de documente;<br>○ Automatizarea arhivării electronice a documentelor;<br>○ Întreținerea listelor de documente;<br>○ Asigurarea procedurilor de acces la arhiva electronică istorică;<br>○ Asigurarea mecanismelor de mutare a documentelor între grupele de arhivă;<br>○ Asigurarea motoarelor de căutare în grupele arhivistice;<br>○ Implementarea mecanismelor de sortare a documentelor în vederea distrugerii;<br>○ Implementarea măsurilor de auditare a accesului la documente;<br>○ Parametrizarea de rapoarte specifice arhivării electronice și stabilirea drepturilor de acces la rapoarte.<br>***Notă:** Arhivarea electronică se va face în conformitate cu prevederile legale referitoare la arhivarea documentelor electronice, la administratorii de arhive electronice și cerințele ce trebuie îndeplinite de centrele de date care au ca obiect de activitate arhivarea electronică.*<br>• **Semnarea și sigilarea electronică calificată în cloud** – va adresa nevoile specifice ce țin de gestionarea fluxurilor de avizare și aprobare după cum urmează:<br>○ Sincronizarea semnăturii electronice calificate cu platforma pentru a operaționaliza fluxurile de avizare / aprobare configurate în activitatea curentă;<br>○ Apelarea serviciilor API pentru semnare și sigilare electronică calificată;<br>○ Crearea și managementul dinamic al fluxurilor de semnare consecutive sau concomitente (inclusiv anularea și reconfigurarea acestora);<br>○ Stabilirea, configurarea și managementul motivelor de semnare;<br>○ Crearea și întreținerea listelor de semnatari și a |

| | |
|---|---|
| | competențelor lor de semnare;<br>o Asigurarea serviciilor de validare a semnăturilor electronice calificate aplicate documentelor;<br>o Poziționarea semnăturilor pe document în funcție de context;<br>o Integrarea semnăturii olografe în semnătura electronică calificată;<br>o Autentificarea securizată în serviciul de semnare și semnarea documentelor fără ca acestea să părăsească sistemul;<br>o Integrarea cu componenta de management a identităților, cu cea de management al înregistrărilor, cu cea de interconectivitate și interoperabilitate multi-instituțională și cu arhiva electronică;<br>o Asigurarea serviciilor de semnare multi-vendor (*ex. sistemul să suporte semnarea electronică în flux cu semnături electronice de la mai mulți furnizori*);<br>o Asigurarea procedurilor de semnare cross-platform (*ex. o sesiune se semnare să poată parcurge mai multe platforme informatice*).<br>***Notă:** Managementul identităților se va face centralizat în conformitate cu prevederile regulamentului ~~eIDAS~~eIDAS2 și ale standardului ETSI EN 319 521 V1.1.1 / 2019.*<br>• **Securitatea și auditul platformei** – componenta de securitate va adresa nevoile specifice:<br>o Implementarea politicilor și procedurilor de securitate ce privesc comunicația între utilizatori;<br>o Implementarea instrumentelor de autentificare și autorizare pe baza rolurilor deținute de fiecare utilizator la nivel de sistem;<br>o Protejarea împotriva accesului neautorizat în sistem;<br>o Administrarea drepturilor de acces și parametrizarea algoritmilor de autorizare automată la conținutul din platformă al utilizatorilor;<br>o Implementarea de mecanisme de asigurare a integrității datelor și a restituirii acestora în situația unor incidente operaționale sau de securitate;<br>o Implementarea procedurilor de creare, gestionare și criptare a credențialelor de acces la sistem; |

| | |
|---|---|
| | o Capturarea motivelor de acces la date;<br>o Crearea și întreținerea dinamică a sistemului de log-uri;<br>o Stabilirea instrumentelor de monitorizare a platformei. |

## 2. CERINȚE GENERALE PRIVIND SOLUȚIA TEHNICĂ

### 2.1. Principii și opțiuni tehnologice în implementarea proiectului TIC

Implementarea unui proiect informatic este un proces complex, care necesită o planificare atentă și luarea în considerare a mai multor principii și opțiuni tehnologice. Iată o prezentare generală a acestora:

**Principii cheie în implementarea proiectului informatic:**

1. **Alinierea la obiectivele instituției:** Tehnologia trebuie să fie un instrument în slujba activității, nu un scop în sine. Proiectul informatic trebuie să fie conceput și implementat în așa fel încât să contribuie la atingerea obiectivelor strategice ale instituției.
2. **Planificare riguroasă:** O planificare detaliată este esențială pentru succesul proiectului. Aceasta include definirea clară a scopului, obiectivelor, bugetului, termenelor limită și resurselor necesare.
3. **Gestionarea riscurilor:** Orice proiect implică riscuri care trebuie identificate și evaluate; ulterior trebuie elaborate planuri de atenuare pentru a minimiza impactul lor potențial.
4. **Comunicare eficientă:** O comunicare deschisă și transparentă între toate părțile implicate (echipa de proiect, management, utilizatori finali) este esențială pentru a asigura succesul proiectului.
5. **Controlul calității:** Calitatea trebuie să fie o preocupare constantă pe tot parcursul proiectului. Trebuie implementate proceduri de asigurare a calității pentru a verifica dacă produsul final îndeplinește cerințele și așteptările.

**Opțiuni tehnologice în implementarea proiectului informatic:**

Alegerea tehnologiilor potrivite este crucială pentru succesul unui proiect informatic. Există o gamă largă de opțiuni disponibile, iar decizia trebuie luată în funcție de nevoile specifice ale proiectului și de resursele disponibile.

1. **Platforme de dezvoltare:** Alegerea platformei de dezvoltare (ex: Java, .NET, Python) depinde de tipul de aplicație care trebuie dezvoltată și de competențele echipei de dezvoltare.
2. **Baze de date:** Există mai multe tipuri de baze de date (relaționale, ne relaționale, NoSQL), fiecare cu propriile avantaje și dezavantaje. Alegerea depinde de volumul și tipul de date care trebuie stocate și de cerințele de performanță.
3. **Infrastructură hardware și software:** Decizia privind infrastructura hardware și software (servere, sisteme de operare, software de virtualizare) depinde de cerințele de performanță și scalabilitate ale aplicației.

4. **Tehnologii emergente:** Tehnologiile emergente, cum ar fi inteligența artificială, blockchain și internetul lucrurilor, pot oferi oportunități semnificative pentru inovație și creștere. Cu toate acestea, adoptarea lor trebuie făcută cu atenție, deoarece acestea pot implica și riscuri semnificative.

Implementarea cu succes a proiectului informatic necesită o abordare echilibrată, care să țină cont atât de principiile generale, cât și de opțiunile tehnologice specifice. O planificare atentă, o comunicare eficientă și o alegere informată a tehnologiilor pot contribui semnificativ la succesul proiectului.

Soluția tehnică ce va face obiectul achiziției va fi o aplicație de tip **Software as a Service (SaaS)**. Din perspectiva abordării arhitecturale, se va acorda prioritate soluțiilor ~~care sunt „cloud ready" (proiectate pentru a putea fi migrate și operate eficient în cloud) sau, preferabil,~~ **„cloud-native"** (proiectate și construite specific pentru a valorifica arhitecturile și serviciile cloud). Această soluție trebuie să fie capabilă să opereze în mod optim și securizat în cadrul **Cloudului Privat Guvernamental (CPG)/Cloudul Regional (CR)** și să utilizeze, acolo unde este cazul și aduce beneficii de eficiență și scalabilitate, serviciile de platformă (PaaS) și infrastructură (IaaS) ~~oferite de CPG/CR~~.

Alegerea tehnologiilor specifice de dezvoltare (cum ar fi limbaje de programare, framework-uri, baze de date) de către furnizorul soluției SaaS trebuie să fie fundamentată pe capacitatea acestora de a asigura conformitatea deplină cu cerințele de performanță, securitate, disponibilitate și interoperabilitate ~~ale CPG~~, așa cum sunt acestea definite în legislația specifică (Ordonanța de Urgență a Guvernului nr. 89/2022, Hotărârea Guvernului nr. 112/2023, Hotărârea Guvernului nr. 70/2023) și în normele tehnice subsecvente emise de autoritățile competente (ADR, MCID).

***Sub aspect strategic și pentru a nu limita sub nicio formă opțiunile potențialilor ofertanți, recomandăm ca modalitate corectă și în spiritul tratamentului egal față de agenții economici interesați să depună ofertă, să fie prezentate prin documentația de atribuire strict cerințele funcționale și de conformitate ce trebuie îndeplinite de soluțiile ce vor fi propuse, lăsând opțiunile tehnologice și de infrastructură exclusiv la latitudinea ofertanților.***

## 2.2. Cerințe tehnice generale privind infrastructura IT&C

***Sub aspect strategic și având în vedere abordarea propusă, respectiv una de tip SaaS (software ca serviciu) și având în vedere că aceasta va stoca date personale, recomandăm prezentate prin documentația de atribuire obligația agenților economici interesați să depună ofertă de a dovedi respectare cerințelor de conformitate specifice platformelor de distribuție electronică înregistrată, protecției datelor cu caracter personal, a securității cibernetice și arhivării electronice.***

***Ofertantul soluției SaaS va trebui să demonstreze, prin documentație tehnică și, eventual, certificări, că soluția sa operează pe o infrastructură (fie infrastructură proprie/contractată localizată în centre de date acreditate de ADR, fie direct pe infrastructura IaaS/PaaS a CPG/CR) care este pe deplin conformă cu cerințele de reziliență, securitate fizică și logică, și stocare a datelor pe teritoriul Uniunii Europene/României, așa cum sunt acestea stipulate în cadrul normativ ~~al CPG~~ și în cerințele specifice ale prezentului Proiect Tehnic (vezi și Secțiunea 4.9 Cerințe cloud, pagina 50). În cazul utilizării unor centre de date proprii de către ofertantul SaaS, acestea trebuie să dețină acreditările relevante emise de Autoritatea pentru Digitalizarea României (ADR), conform OUG 89/2022, Art. 16.***

## 2.3. Implementarea principiului Do No Significant Harm (DNSH)

Principiul „Do No Significant Harm" (DNSH) este un concept cheie în implementarea proiectelor finanțate din fonduri europene, inclusiv în domeniul IT care se referă la evitarea oricărui impact negativ semnificativ asupra mediului și a obiectivelor climatice. Aspectele care au fost luate în considerare în implementarea proiectului pentru a respecta principiul DNSH sunt:

**1. Eficiența energetică a infrastructurii IT:**

- **Hardware eficient energetic:** Alegerea serverelor, stocării și echipamentelor de rețea cu un consum redus de energie și certificări de eficiență energetică (Energy Star, etc.).
- **Virtualizare și cloud computing:** Utilizarea acestor tehnologii pentru a reduce numărul de servere fizice necesare și a optimiza utilizarea resurselor.
- **Răcire eficientă:** Implementarea de sisteme de răcire eficiente energetic în centrele de date.
- **Oprirea echipamentelor neutilizate:** Implementarea de politici pentru oprirea automată a echipamentelor IT atunci când nu sunt utilizate.

**2. Gestionarea deșeurilor electronice:**

- **Politici de reciclare:** Implementarea de politici clare pentru colectarea, reciclarea și eliminarea responsabilă a echipamentelor IT uzate.
- **Extinderea duratei de viață a echipamentelor:** Repararea și reutilizarea echipamentelor IT ori de câte ori este posibil, în loc de a le înlocui.
- **Achiziționarea de echipamente durabile:** Alegerea echipamentelor IT cu o durată de viață mai lungă și cu componente ușor de înlocuit.

**3. Impactul software-ului:**

- **Dezvoltarea de software eficient:** Scrierea de cod optimizat care să consume mai puține resurse de calcul și să reducă sarcina asupra hardware-ului.
- **Promovarea utilizării eficiente a software-ului:** Educarea utilizatorilor cu privire la modul în care pot utiliza software-ul în mod eficient pentru a reduce consumul de energie.

**4. Considerații privind lanțul de aprovizionare:**

- **Alegerea furnizorilor responsabili:** Colaborarea cu furnizori de hardware și software care au politici solide de mediu și sociale.
- **Evaluarea impactului transportului:** Luarea în considerare a impactului transportului echipamentelor IT și a modului în care acesta poate fi redus.

**5. Monitorizare și raportare:**

- **Măsurarea consumului de energie:** Implementarea de sisteme de monitorizare pentru a urmări consumul de energie al infrastructurii IT și a identifica oportunități de îmbunătățire.

- **Raportarea impactului asupra mediului:** Elaborarea de rapoarte periodice privind impactul asupra mediului al proiectului IT și măsurile luate pentru a-l reduce.

Prin implementarea acestor aspecte, proiectul IT contribuie la obiectivele de sustenabilitate și respecta principiul DNSH, chiar dacă impactul lor direct asupra mediului este mai puțin evident decât în alte sectoare.

### 2.4. Funcționalități specifice tehnologiilor avansate

Proiectul are în vedere implementarea de tehnologii avansate precum:

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

### 2.5. Principiile care stau la baza asigurării securității cibernetice

Securitatea cibernetică a proiectului se bazează pe câteva principii fundamentale care ghidează eforturile de protejare a sistemelor, rețelelor și datelor împotriva amenințărilor cibernetice:

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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.
7. **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.

8. **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.
9. **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.
10. **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 (confidențialitate, integritate, disponibilitate, autentificare, autorizare, non-repudiere, apărare în profunzime, cel mai mic privilegiu, actualizare constantă, educarea utilizatorilor) vor fi implementate în cadrul soluției SaaS printr-un **model de responsabilitate partajată (shared responsibility model)**, specific mediilor cloud:

- **Furnizorul soluției SaaS** 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).
- **Administratorii cloudului** 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.
- **Direcția de Asistență Socială Drobeta-Turnu Severin (Beneficiar)** este responsabilă 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).

Formatat: Bordură: : (Fără bordură)

## 2.6. Descrierea tehnică a proiectului TIC

Având în vedere caracterul evolutiv al soluției informatice fapt ce va face ca necesarul de procesare și stocare în fiecare an de exploatare să fie constant crescător beneficiarul înțelege să plaseze responsabilitatea scalabilității soluției în responsabilitatea exclusivă a furnizorului. Tot în responsabilitatea furnizorului este asigurarea soluției de backup în caz de dezastre, soluție care trebuie să îndeplinească aceleași caracteristici ca și soluția de bază. Furnizorul trebuie să asigure continuitatea furnizării serviciilor și o disponibilitate a serviciilor de minim 99,9% pe durata programului de lucru în decursul unui an.

În responsabilitatea beneficiarului rămâne asigurarea infrastructurii de comunicații (a rețelei) la sediul fiecăreia dintre instituțiile ce sunt vizate în proiect, precum și a echipamentelor necesare exploatării în condiții de securitate a sistemului (dispozitive fixe și mobile). Astfel, beneficiarul va asigura la fiecare sediul accesul la minim 2 rețele de comunicații în bandă largă indiferent de tipul acestora (fixe, mobile

sau una fixă și una mobilă). Soluția informatică va putea fi accesată prin conexiune de tip HTTPS de oriunde asigurându-se astfel criptarea traficului utilizatorilor. În funcție de resursele financiare disponibile beneficiarul poate opta și pentru alte soluții de securitate (IDS, IPS, SWG, VPN, etc.).

Securitatea va fi tratată la nivel de aplicație prin asigurarea unor politici ce privesc autentificarea, autorizarea, criptarea, jurnalizarea activităților și testarea.

## 3. CERINȚE FUNCȚIONALE DETALIATE ALE SOLUȚIEI TEHNICE

Proiectul TIC ce se dorește a fi implementat în activitatea curentă a Direcției de Asistență Socială Drobeta-Turnu Severin și a instituțiilor subordonate urmărește (1) asigurarea accesului cetățenilor și mediului de afaceri la toate serviciile publice oferite de instituțiile publice din județ și (2) interconectarea și interoperabilitatea între Direcția de Asistență Socială și toate instituțiile din municipiu, județ, regiune în vederea digitalizării complete a fluxurilor de comunicare interne și interinstituționale.

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 și central 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 Municipiul Drobeta-Turnu Severin
- Scăderea poverii administrative determinată de modul de lucru tradițional pe hârtie.

Proiectul TIC trebuie să fie de tip web-based, accesibil și funcțional la cele mai înalte standarde de calitate de utilizare atât pe dispozitivele de tip desktop, cât și pe orice tip de dispozitiv mobil (front office și back office), pe minim următoarele soluții de navigare pe internet: Google Chrome, Microsoft Edge, Mozilla Firefox, Safari.

Accesul la soluția informatică se va face prin URL securizat cu certificat site-SSL, pus la dispoziție de prestator. Nu vor fi acceptate soluțiile care pot fi accesate prin URL-uri formate pe bază de adrese IP.

Comunicațiile „browser to server” și „server to server” trebuie să fie criptate prin protocoale criptografice (HTTPS) menite să asigure securitatea comunicațiilor pe internet (SSL/TLS).

Având în vedere că soluția tehnică propusă va fi utilizată atât pentru operațiunile interne ale instituției cât și pentru a furniza servicii electronice beneficiarilor (cetățeni / persoane juridice), în temeiul prevederilor Directivei (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune și a legii nr. 58 / 2023 privind securitatea și apărarea cibernetică a României recomandăm ca asigurarea securității acesteia să fie asumată ca o obligație justificată rezonabil, asumată în sarcina agenților economici interesați alături de costurile generate independent de cadrul ofertei, cu caracter periodic regulat.

**Proiectul TIC** se dorește a fi o **platformă de distribuție electronică înregistrată** care respectă cerințele

tehnice și procedurale stipulate de următoarele standarde și acte normative naționale și europene:

**(1)** Standardul ETSI EN 319 521 V1.1.1 / 2019 - Standardul privind Semnăturile și infrastructurile electronice (ESI) - Politică și cerințe de securitate pentru furnizorii de servicii de livrare electronică înregistrată (ERDS);

**(2)** Standardul ISO 15489-1 / 2016 Ediția a 2 a privind managementul înregistrărilor (*records management*);

**(3)** Regulamentul (UE) nr. 910 / 2014 (~~eIDAS~~eIDAS2) ( actualizat in aprilie 2024 și reintrat în vigoare în 20 mai 2024) privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă europeană;

**(4)** Regulamentul (UE) 679 / 2016 - GDPR (intrat in vigoare în 25 mai 2018) privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestora;

**(5)** Directiva (UE) 2555 din 2022 (NIS2) privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune;

**(6)** Legea nr. 58 / 2023 privind securitatea și apărarea cibernetică a României;

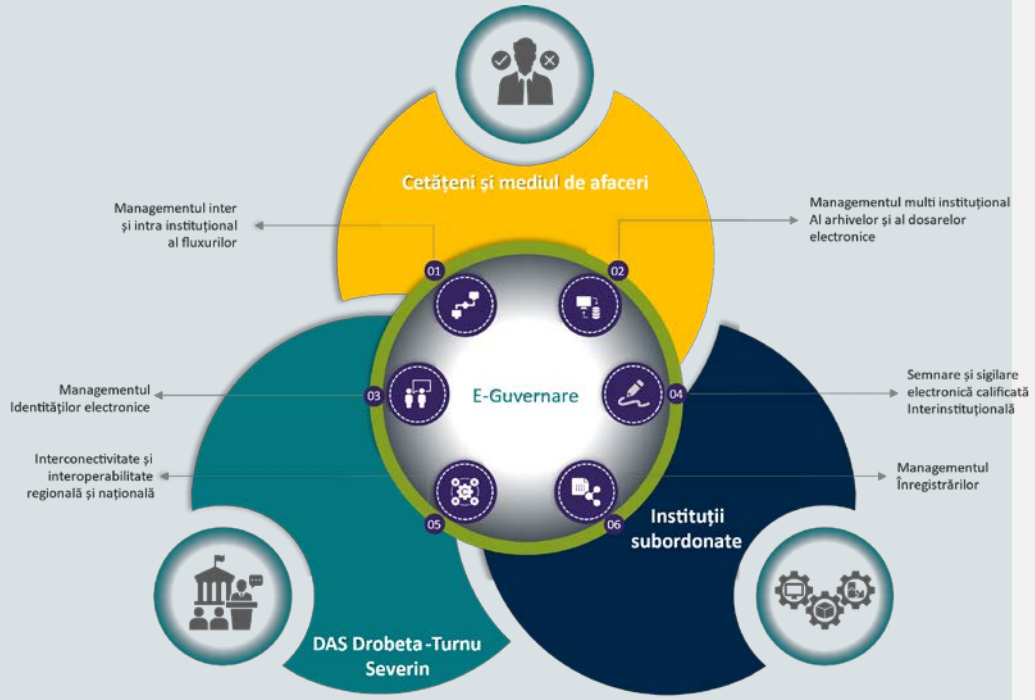
**(7)** Legea nr. 242/2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate și Normele de referință (aprobate în 26 octombrie 2023);

**(8)** Legea nr. 135 din 15 mai 2007 privind arhivarea documentelor în formă electronică + Normele de aplicare;

**(9)** 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.

Proiectul TIC va implementa conceptul de administrație digitală la nivel regional operaționalizând canalele de comunicații intra-/interinstituționale dedicate transferului de date și documente intern și între instituții, instrumente digitale de lucru care vor permite standardizarea tuturor proceselor interne și expunerea către cetățeni și mediul de afaceri a tuturor serviciilor publice și de asistență socială prestate de beneficiar. Identitatea electronică a cetățenilor și persoanelor juridice va fi gestionată centralizat, interconectat și interoperabil, oferind tuturor utilizatorilor, odată ce identitatea a fost stabilită, acces la toate instituțiile.

Proiectul TIC urmărește să eficientizeze activitatea funcționarilor publici și să îmbunătățească accesul cetățenilor la servicii online, asigurând fluidizarea fluxurilor de informații și a documentelor specifice între cetățeni, instituție, intra-/interinstituțional precum și creșterea gradului de trasabilitate la un nivel înalt de transparență decizională. Soluția va include un mediu de lucru colaborativ care va permite și va facilita cetățeanului accesul la serviciile publice aflate în responsabilitatea instituției asigurând prin elementele arhitecturale conexe) atât canale de comunicare cu alte entități publice sau private, cât și funcționalități adecvate lucrului în mediul digital.




Arhitectura soluției IT va fi centralizată, cu baze de date pe server, care va asigura consistența și unicitatea datelor, prevenind duplicările de orice fel. Orice modificare a aplicațiilor web ale platformei referitoare la securitate, formulare introducere date, meniuri, interfață grafică, raportare, se va face de către personal de specialitate, nu va genera downtime, rezultatul modificărilor fiind salvat pe disc (nu în memorie) și vor avea impact instantaneu în interfețele de lucru utilizator.

Proiectul TIC va asigura de asemenea, fluidizarea traficului de informații în rețeaua instituțiilor beneficiare în scopul îmbunătățirii serviciilor oferite către populație și agenții economici. Soluția va asigura suportul necesar tuturor componentelor sistemului la un nivel înalt de performanță și fiabilitate, furnizând în același timp baza pentru dezvoltări ulterioare din punct de vedere software și hardware - scalabilitate.

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**: **(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.


Interfețe grafice ale soluției informatice vor fi conforme cu bunele practici în materie de web-design fiind

personalizate în funcție de tipul de utilizator astfel încât să permită o interacțiune eficientă și un nivel de confort superior tuturor tipurilor de utilizatori.

### 3.1. Cerințe generale specifice platformelor de distribuție electronică înregistrată

Soluție 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 specifice platformelor de distribuție electronică pentru a asigura securitatea, integritatea și legalitatea serviciilor oferite derivă în principal din Regulamentul ~~eIDAS~~eIDAS2 (UE) nr. 910/2014 și din standardele tehnice ETSI asociate.

#### 3.1.1. Cerințe privind Integritatea și confidențialitatea conținutului utilizatorului

- Soluția informatică trebuie să asigure disponibilitatea, integritatea și confidențialitatea conținutului utilizatorului pe toată perioada cât acesta este în platformă (de la momentul încărcării conținutului până la momentul livrării acestuia către destinatar).
- Soluția trebuie să asigure confidențialitatea identității utilizatorului față de orice persoană care nu este îndreptățită să aibă acces la aceste informații (direct sau indirect).
- Integritatea conținutului utilizatorului și a metadatelor asociate acestuia trebuie să fi protejate atât pe durata stocării acestora, cât și pe durata transmiterii lor între expeditor și destinatar. Atunci când se impun modificări ale conținutului utilizatorului acestea trebuie aduse la cunoștința utilizatorului în mod transparent platforma stocând toate dovezile cu privire la forma inițială a conținutului.
- La nevoie conținutul utilizatorului trebuie să poată fi protejat astfel încât să înlăture posibilitatea ca datele să fie schimbate într-o manieră nedetectabilă, fie printr-o semnătură electronică calificată sau sigiliu electronic calificat, fie printr-un mecanism alternativ făcut disponibil de un furnizor de servicii de încredere calificat integrat în platformă.

  În acest caz platforma va deține capabilitățile tehnice necesare pentru a verifica (1) validitatea semnăturii electronice / sigiliului electronic / mecanismului alternativ și (2) caracterul „calificat” al instrumentului.

#### 3.1.2. Cerințe privind identificarea și autentificarea utilizatorilor

- **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. Procesul de stabilire a identității electronice a utilizatorilor (cetățeni, persoane juridice, funcționari) va fi pe deplin compatibil cu și 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~~eIDAS2, vor fi aliniate cu implementarea specifică din ROeID și cu cerințele de acces la diferitele tipuri de servicii

publice. **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~~ (de exemplu, aplicații de autentificare, token-uri hardware/software, notificări push, conform politicilor ADR/STS).

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~~eIDAS2).
- 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;
- Temenii și Condițiile de utilizare ai soluției informatice;
- Politica de confidențialitate.

### 3.1.3. 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, iar aceste jurnale de audit vor fi stocate în conformitate cu politicile de retenție și securitate ale CPG, așa cum sunt 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.

### 3.1.4. Alte cerințe specifice

Având în vedere că infrastructura de bază va fi găzduită într-un centru de date autorizat și certificat conform standardelor și bunelor practici în domeniu trebuie avute în vedere următoarele seturi de cerințe:

- **Securitatea fizică** (prevederile standardelor existente în domeniu trebuie respectate, ex. ISO 27002**)**
  - Accesul fizic la echipamentele care deservesc soluția informatică trebuie controlat cu strictețe.
  - Trebuie implementate măsuri care să minimizeze sau să înlăture pierderea, deteriorarea sau compromiterea activelor.
  - Trebuie implementate măsuri care să înlăture posibilitatea capacităților de procesare a informației sau a informației în sine.
  - Locația unde sunt amplasate echipamentele trebuie securizată într-un perimetru clar definit și protejată împotriva intruziunilor.
- **Managementul activelor**
  - Identificarea, inventarierea și clasificarea tuturor activelor folosite pentru operaționalizarea sistemului.
  - Implementare de măsuri de management al vulnerabilităților.
  - Măsuri de evaluare și minimizare a riscurilor.
  - Implementarea de instrumente de monitorizare și răspuns la incidentele de securitate.
  - Monitorizarea ciclului de viață al echipamentelor.
  - Asigurarea conformității și auditului.
- **Securitatea comunicațiilor**
  - Se va avea în vedere segmentarea sistemelor în mai multe zone în funcție de evaluarea riscurilor cu privire la relațiile funcționale, logice sau fizice între sisteme și servicii.
  - Pentru sistemele colocate în aceeași locație se are în vedere asigurarea aceluiași nivel de securitate și control.
  - Accesul și comunicațiile vor fi restricționate doar la strictul necesar pe fiecare zonă.
  - Politicile de administrare și securizare vor fi dedicate în funcție de senzitivitatea informației.
  - Platforma trebuie să folosească certificate de autentificare TLS sau echivalent.
- **Securitatea aplicațiilor / interfețelor**

- Soluția trebuie protejată împotriva virușilor și a altor tipuri de softuri neautorizate.
- Corecțiile de securitate vor aplicate într-un timp rezonabil după ce sunt disponibile.
- Corecțiile de securitate nu vor fi aplicate dacă introduc vulnerabilități sau instabilități suplimentare care depășesc beneficiile aplicării acestora.
- Motivele pentru care nu se aplică nicio corecție de securitate sunt documentate.

o **Răspunsul la incidente de securitate**

- Politica de monitorizarea a sistemelor trebuie să țină cont de senzitivitatea informației colectate și analizate.
- Trebuie implementate măsuri de detectare a indicatorilor unor potențiale incidente de securitate și de raportare a acestora ca și alarme (*ex. oprirea funcțiilor de colectare de log-uri*).
- Trebuie implementate măsuri pentru realizarea intervenției la timp și în mod coordonat în scopul limitării impactului breșelor de securitate prin alocarea de personal specializat.
- Trebuie implementate proceduri de notificare a organelor competente să intervină în situația identificării unui incident de securitate, iar persoanele fizice afectate trebuie de asemenea informate.

o **Activități de recuperare în caz de dezastru**

- La nivelul furnizorului trebuie să existe un plan de continuitate al afacerii care trebuie activat și respectat ori de câte ori este cazul.

## 3.2. Cerințe specifice componentelor platformei

### 3.2.1. Managementul identităților electronice și autentificarea

*Managementul identităților se va face centralizat în conformitate cu prevederile regulamentului ~~eIDAS~~eIDAS2 și ale standardului ETSI EN 319 521 V1.1.1 / 2019. Soluția SaaS va asigura o integrare bidirecțională și securizată cu **sistemul național ROeID** pentru validarea, crearea (acolo unde este cazul și permis de fluxurile ROeID) și utilizarea identităților electronice ale cetățenilor și funcționarilor. Se vor utiliza **API-urile oficiale** puse la dispoziție de ROeID (prin intermediul ADR și/sau STS) pentru acest scop, respectând protocoalele de comunicație și standardele de securitate impuse. Toate atributele de identitate stocate și procesate de soluția SaaS vor fi gestionate în strictă conformitate cu prevederile Regulamentului GDPR și ale Regulamentului ~~eIDAS~~eIDAS2. 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 98/2020~~CPG~~.*

Platforma trebuie să includă un proces riguros și auditabil al 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.

Identitățile electronice rezidente în soluția informatică vor putea fi create prin prezența fizica la

ghișeele instituției a solicitantului sau direct în mediul online prin mijloace de identificare la distanță și trebuie să fie unice și interdependente.

Identitățile persoanelor fizice și juridice se vor putea crea de toți funcționarii, în timp ce identitățile funcționarilor vor fi create doar de administratorii de sistem.

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 pentru editarea simultană a înregistrărilor.

Mecanismele de auditare vor cuprinde minim următoarele elemente:

- Colectarea corectă și completă a atributelor identității – toate validările de inputuri trebuie să fie corecte, preexistente și să respecte standardele în industrie.
- Capturarea și salvarea acordului de procesare a datelor cu caracter personal.
- Cererea de înregistrare semnată olograf înregistrată în Registratura electronică a instituției (pentru cazurile de identificare la ghișeu) .
- 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.
- Nivelul de încredere acordat identității (scăzut, substanțial, ridicat).
- Semnătura electronică calificată a funcționarului.
- Sigiliul electronic al instituției.

Identitatea electronică va fi în prealabil verificată/validată și ulterior inițiată de funcționarul public care a realizat identificarea (fie la ghișeu, fie prin mediul online) activarea efectivă a identității urmând a se face de către titularul de drept al acesteia.

Identitățile electronice (personale sau profesionale) 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).

Toate atributele verificate și validate care au stat la baza unei identități electronice realizată fizic la ghișeu (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.

Identitățile, inclusiv cele personale, vor putea avea asociate unul sau mai multe roluri la nivelul soluției informatice guvernate de modele de guvernanță digitală specifice. Pentru a evita orice dubiu prin model de guvernanță digitală se înțelege un ansamblu de reguli/proceduri care definesc identitatea/rolul. Aceste seturi de reguli/proceduri trebuie să vizeze cel puțin:

- Persoanele responsabile cu configurarea identității/rolului respectiv;
- Operațiunile specifice pe care identitatea/rolul le poate face;
- Consecințele juridice generate.

Fiecare identitate (personală sau profesională) va dispune de un set distinct de credențiale care

va identifica în mod unic o singură identitate.

Rolurile asociate unei identități fie ea personală sau profesională vor putea fi accesate și utilizate în baza credențialelor identității respective.

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

Identitățile electronice profesionale (cele de persoană juridica și funcționari) nu pot exista în cadrul soluției informatice în lipsa identității electronice personale care va fi de tip „Master".

Dezactivarea/Ștergerea identității Master (cea personală) va genera și dezactivarea/ștergerea tuturor celorlalte identități profesionale.

O persoană poate deține o singură identitate electronică personală și un număr nelimitat de identități electronice profesionale.

Atributele ce privesc identitatea electronică a persoanelor fizice sunt:

- Datele din actele de identitate ( CNP + toate actele de identitate);
- Adresă de email;
- Număr de telefon;
- Semnătura electronică calificată;
- Credențiale (utilizator și parolă) – pentru identitățile electronice efective.

Managementul spațiului virtual al persoanelor juridice se va realiza în mod colaborativ de către administratorul persoanei juridice/împuternicitul acestuia și funcționari, fiecăruia dintre aceștia revenindu-le următoarele responsabilități:

- **Responsabilități ale funcționarului:**
  - Verificarea corectitudinii și integrității datelor despre persoana juridică.
  - Verificarea corectitudinii și integrității datelor despre reprezentantul legal al persoanei juridice.
  - Activarea identității profesionale a reprezentantului legal al persoanei juridice.
  - Activarea identității persoanei juridice.

  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 la nivelul soluției informatice.

- **Responsabilități ale reprezentantului legal** al persoanei juridice/împuternicitului acestuia:
  - Inițierea/Activarea/Ștergerea/Dezactivarea/ Suspendarea identităților profesionale ale altor angajați.
  - Stabilirea serviciilor publice la care aceștia au acces.
  - Menținerea datelor despre persoana juridică la un nivel de acuratețe care să reflecte starea curentă a lucrurilor.

Fiecare identitate efectivă (personală sau profesională) va dispune de un set unic de credențiale. Credențialele vor constitui o dovadă irefutabilă de identificare și în baza lor se va

acorda accesul utilizatorului la sistem.

Atributele vizate de autoritatea contractantă în ceea ce privește identitatea electronică a persoanelor juridice sunt:

- Datele persoanei juridice – CUI.
- Extras constatator ONRC sau alte doveditoare tipului de persoană juridica (certificate, autorizații, licențe de funcționare, personalizat în funcție de tipul de persoană juridică și cadrul legal în care aceasta operează).
- Datele reprezentantului persoanei juridice sau ale împuternicitului acestuia.
- Credențiale (utilizator și parolă) – pentru identitățile electronice efective.

Rolurile asociate unei identități fie ea personală sau profesională vor putea fi accesate și utilizate în baza credențialelor identității la care sunt asociate, utilizatorul putând naviga între ele fără autentificări suplimentare.

Identitatea personală va permite utilizatorului deținerea controlului asupra existenței identităților profesionale.

O persoană poate deține o singură identitate electronică personală și un număr nelimitat de identități electronice profesionale.

Atributele vizate de autoritatea contractantă în ceea ce privește identitatea profesională a reprezentanților persoanelor juridice sunt:

- Denumirea organizației reprezentante;
- Denumirea departamentului;
- Informația despre funcția deținută;
- Adresa de email profesională;
- Număr de telefon;
- Persoana care a inițiat identitatea;
- Valabilitatea identității profesionale.

Atributele vizate de autoritatea contractantă în ceea ce privește rolurile asociate fiecărei identități în parte:

- Titulatura rolului;
- Identitatea căreia îi este asociat;
- Persoana care a generat rolul;
- Valabilitatea rolului.

Fiecare identitate electronică (personală/ profesională) va fi confirmată de titular pe un canal extern (email, sms, etc.) soluției informatice 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.

- **IDENTITATEA EFECTIVĂ**

Identitatea electronică indiferent de tipul ei (personală sau profesională) pentru a fi efectivă trebuie să îndeplinească în mod cumulativ 4 condiții:

- Să fie identificată printr-un identificator unic.

- Să dețină setul complet de atribute specifice tipului său de identitate.
- Să fie în mod conștient asumată de titularul acesteia.
- Să fie exercitată activ în spațiul virtual.

- **IDENTITATEA NEEFECTIVĂ**

Toate identitățile care includ în mod obligatoriu CNP sau CUI/CIF, dar care nu îndeplinesc în mod cumulativ condițiile identității electronice efective vor fi considerate neefective.

Până la momentul confirmării sale de către titular identitatea electronică va fi neefectivă.

Identitățile neefective vor putea deveni efective doar după ce vor fi complete, asumate explicit și exercitată la nivelul soluției informatice.

- **INDICIILE PRELIMINARE DE IDENTITATE**

Datele cu privire la un solicitant (ex. adresa de email, număr de telefon, etc.) care nu au asociat un CNP/CI/CIF și care sunt stocate la nivelul soluției informatice vor fi considerate indicii preliminare în stabilirea unei viitoare identități.

Indiciile preliminare de identitate vor fi asumate de funcționarul care le-a introdus în sistem și supuse auditării.

Soluția informatică trebuie să dețină capabilitatea de a captura, salva și operaționaliza parțial indiciile preliminare de identitate. Acestea vor genera consecințe juridice limitate în funcție de contextul în care sunt folosite.

Indiferent dacă identitatea electronică este efectivă, neefectivă sau doar sub forma unor indicii preliminare de identitate, soluția informatică trebuie să fie capabilă să implementeze modele de guvernanță digitală contextuală pentru acestea.

Identitățile (inclusiv documentația suport) vor putea fi exportate la nevoie către alte sisteme pe care instituția le va implementa asigurând astfel deplina independență a beneficiarului în relația cu furnizorul.

Managementul identităților trebuie realizat la nivelul platformei astfel încât să poată asigura o deplină conformitate cu prevederile regulamentelor europene GDPR și ~~eIDAS~~eIDAS2.

Din perspectiva GDPR soluția va descrie în detaliu:

- Modalitatea de anonimizare a datelor în interfețele de lucru curente (expuse riscului de a fi vizualizate de alte persoane).
- Modalitatea de asigurare a nivelului maxim de acuratețe a datelor personale.
- Modalitatea de capturare și stocare a acordului de procesare a datelor cu caracter personal.
- Modalitatea de capturare a motivului de acces la datele personale ale utilizatorului (din interfața de lucru sau din fișiere).

Din perspectiva ~~eIDAS~~eIDAS2 soluția trebuie să detalieze:

- Modalitatea de asigurare a nivelurilor de încredere scăzut, substanțial și ridicat, precum și modelul de guvernanță digital ce definește fiecare nivel de încredere.

- Procesul de tranziție de la un nivel la altul.
- Modalitatea de identificare online a utilizatorilor și capturarea și salvarea în cloud a identificării video a utilizatorului, precum și integrarea identificării în procesul de „audit trail" al soluției electronice.
- Calitatea sistemului de furnizor de servicii de încredere în vederea creării, verificării și validării semnăturilor electronice, a sigiliilor electronice sau a mărcilor temporale electronice, a serviciilor de distribuție electronică înregistrată și a certificatelor aferente serviciilor respective.

Soluția informatică trebuie să dețină capabilitatea de a stoca și operaționaliza prin modele de guvernanță digitală specifice identități electronice în următoarele stări logice:

- **Pentru persoanele fizice și juridice** în minim următoarele stări:
  - Perioada de inactivitate;
  - Perioada între momentul inițializării și momentul activării identității electronice;
  - Perioada de activitate;
  - Perioada de suspendare – ex. fraudă, detașare, indisponibilitate temporară, etc.;
  - Perioada ulterioară dezactivării.
- **Pentru funcționari:**
  - Perioada de inactivitate;
  - Perioada între momentul inițializării și momentul confirmării identității electronice;
  - Perioada de activitate;
  - Perioada în concediu;
  - Perioada de suspendare;
  - Perioada ulterioară dezactivării.

Informațiile privind identitatea electronică a utilizatorului vor fi făcute disponibile și accesibile fiecărui utilizator în parte într-o secțiune de tip „Contul meu" (denumirea este exemplificativă).

Din perspectiva utilizatorului persoană fizică interfața grafică trebuie să afișeze minim:

- Datele personale ale titularului identității electronice personale;
- Actele de identitate ale titularului actualizate;
- Date privind funcționarul care a creat identitatea electronică;
- Semnătura olografă a utilizatorului;
- Semnătura electronică calificată a titularului identității însoțită de toate detaliile acesteia (furnizor, perioada de valabilitate etc.);
- Modificarea parolei de acces la sistem.

Din perspectiva utilizatorului persoană juridică interfața grafică trebuie să afișeze minim:

- Datele personale ale titularului identității electronice profesionale;
- Datele specifice identității profesionale;
- Semnătura olografă a utilizatorului;
- Semnătura electronică calificată a titularului identității;
- Modificarea parolei de acces la sistem.

Din perspectiva utilizatorului funcționar interfața grafică trebuie să afișeze minim:

- Datele personale ale titularului identității electronice profesionale;
- Datele specifice identității profesionale;
- Semnătura olografă a utilizatorului;
- Semnătura electronică calificată a titularului identității;
- Modificarea parolei de acces la sistem.

Atributele identității electronice care nu sunt considerate ca având grad mare de sensibilitate (precum actele și datele personale), respectiv cele care în viața de zi cu zi sunt la îndemâna utilizatorului a fi modificate (email, număr de telefon, poza de profil, semnătura olografă) vor putea fi editate/actualizate 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.

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 IT 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.

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.

### 3.2.2. Înregistrarea operațiunilor administrative

***Notă:** Înregistrarea operațiunilor și actelor administrative se va face în conformitate cu prevederile standardului ISO 15489-1 din 2016 privind managementul înregistrărilor în sistemele de Records Management.*

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 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 asigură că dovezile autorizate ale activității sunt create, capturate, gestionate și făcute accesibile celor care au nevoie de ele, atâta timp cât este necesar.

Dintre beneficiile respectării prevederilor standardului trebuie menționate:

a. Asigură transparența și responsabilitate operațiunilor administrative;
b. Luarea deciziilor în cunoștință de cauză;
c. Managementul riscurilor de afaceri;
d. Continuitate în caz de dezastru;
e. Protecția drepturilor și obligațiilor organizațiilor și persoanelor;
f. Protecție și sprijin în litigiu;
g. Respectarea legislației și reglementărilor;
h. Reducerea costurilor printr-o eficiență sporită a afacerii;
i. Activități de cercetare și dezvoltare bazate pe dovezi;
j. Protecția memoriei instituționale, personale și colective.

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

- Recepția și repartizarea actelor intrate în instituție;
- Expedierea actelor către entități externe instituției circulația actelor de uz intern.

Registratura va fi structurată ținându-se cont de instrumentarul relațional clasic administrativ, respectiv **[LUCRARE – ACT – DOSAR].** 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.).
- ACTUL 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.
- DOSARUL va include întotdeauna mai multe lucrări asociate în jurul unui subiect comun.

Având în vedere nevoile specifice administrației publice beneficiarul dorește 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 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 pre configurate sau configurabile.

| **Cerințe de ordin conceptual 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 cel puțin următoarele caracteristici:<br>• Are un autor (cu o identitate efectivă/ neefectivă / indicii preliminare de identitate).<br>• Are un conținut care reflectă ceva ce a fost spus, făcut sau agreat.<br>• Este semnat și asumat în nume personal sau al altei persoane.<br>• A făcut obiectul unui proces de avizare/aprobare conform unui cadrul procedural intern.<br>• A făcut sau nu a făcut obiectul unui proces de înregistrare (are număr de înregistrare).<br>• 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:<br>• 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 următoarele condiții:<br>• Prezintă indicii clare ale autorului documentului.<br>• Poartă identitatea vizuală a instituției emitente.<br>• A parcurs un proces de semnare, avizare și aprobare agreat formal la nivelul instituției emitente.<br>• A fost înregistrat cu număr de înregistrare unic în evidențele instituției emitente. |
| **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:<br>• Să asigure încărcarea de fișiere în sistem individual sau prin batchuri, atât prin butoane de upload, cât și prin operațiuni tip „drag and drop” și „copy-paste”.<br>• Încărcarea trebuie să se poată face din arhiva electronică la care are acces și din calculator.<br>• Să asigure ștergerea fișierelor electronice din sistem cu excepția celor care au fost arhivate electronic a căror ștergere nu este permisă.<br>• 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).<br>• Să aibă integrată o procedură electronică de conformare cu originalul prin semnarea electronică calificată de către funcționar.<br>• Conformarea cu originalul prin semnare electronică calificată trebuie să poată fi făcută atât individual cât și multiplu<br>• 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.
- Semnarea electronică calificată trebuie să poată fi făcută atât individual cât și în batchuri.
- 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 dispună de calitatea de furnizor de servicii de încredere conform regulamentului ~~eIDAS~~eIDAS2 pentru validarea semnăturilor electronice calificate și a sigiliilor electronice calificate dintr-un document /act 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 a 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 drepturile de acces la grupe atât pentru scriere cât și pentru citire. Configurarea se va putea face individual sau ca grup predefinit de utilizatori din sistem.
- 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 următoarele 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.

| **Cerințe conceptuale privind lucrările electronice** |
|---|
| Soluția informatică trebuie să trateze „Lucrările” ca structuri logice caracterizate de minim următoarele atribute:<br>• Tipul lucrării;<br>• Numărul de înregistrare al lucrării (pentru cele înregistrate);<br>• Denumirea lucrării;<br>• Data și ora creării;<br>• Data și ora înregistrării;<br>• Data și ora primirii;<br>• Data finalizării;<br>• Modalitatea de finalizare;<br>• Cronologia lucrării - succesiunea de acțiuni și evenimente consemnate în conținutul lucrării marcate temporal;<br>• Datele despre participanții la lucrare, rolurile pe care aceștia îl au în lucrare și starea acestora;<br>• Conținutul lucrării – poate include mesaje, idei, sugestii, argumente, puncte de vedere, etc.;<br>• Documentele/Actele lucrării;<br>• Informații despre eventuale conexări;<br>• Guvernanța lucrării – setul particular de reguli și acțiuni care guvernează lucrarea în funcție de tipul ei;<br>• Starea lucrării (ex. de stări – fără a fi obligatorii sau limitate la acestea – neînregistrată, în lucru, finalizată, etc.);<br>• Orice alt eveniment sau obiect consemnat la nivelul lucrării și care poate contribui la crearea contextului de creare și derulare al lucrării (ex. rapoarte de citire, notificări, anunțuri, „counter” de mesaje, durată etc.). |
| **Cerințe specifice privind lucrările electronice** |
| Soluția informatică trebuie să asigure minim următoarele capabilități ce privesc lucrările electronice ce vor fi gestionate la nivelul instituției:<br>**1.** Să dispună de o secțiune de evidență a lucrărilor la care participă funcționarul.<br>**2.** Să permită vizualizarea tuturor lucrărilor la care utilizatorul participă în format listă/ tabel.<br>**3.** Să permită filtrarea/sortarea/căutarea lucrărilor în funcție de atributele menționate la secțiunea „Cerințe conceptuale despre lucrări”.<br>**4.** Să permită utilizatorului crearea/editarea/ semnarea/configurarea și expedierea lucrărilor pe fluxurile de lucru în funcție de tipul lor.<br>**5.** Să permită semnarea multiplă de lucrări (cu toate fișierele atașate) și expedierea automatizată a acestora pe fluxurile prestabilite – ex. pachete de lucrări.<br>**6.** Expedierea trebuie să se facă ca tranzacție și să aibă implementate proceduri de fallback în cazul în care apar erori în procesul de prelucrare și expediere.<br>**7.** Să permită expedierea automată a lucrărilor electronice către destinatari în batchuri (zeci, sute, mii, zeci de mii, sute de mii de lucrări deodată) – expedierea trebuie să tranziteze operațiunea de sigilare electronică calificată și să permită destinatarilor să revină cu răspuns către instituție.<br>**8.** Expedierea trebuie să se poată face atât în interiorul sistemului, cât și în afara lui.<br>**9.** Soluția informatică trebuie să furnizeze rapoarte de progres de expediere și, în cazul în care în procesul de expediere au apărut erori, acestea să fie capturate pentru a permite funcționarilor analizarea lor. |

10. Să dispună de o secțiune de „ciorne” destinată salvării lucrărilor care sunt în curs de editare și din diverse motive nu au putut fi definitivate și expediate. Utilizatorului i se va permite reluarea editării de unde a rămas.
11. Să dispună de o secțiune pentru arhivarea lucrărilor finalizate.
12. Să permită vizualizare istoricului detaliat al fiecărei lucrări la care a participat.
13. Să dispună de un „counter” de lucrări care să se actualizeze funcție de filtrele aplicate în lista de lucrări.
14. Să aibă definită la nivel de sistem o Procedura de Predare-Primire a lucrărilor.
15. Secțiunea de evidență a lucrărilor să fie integrată cu Registratura electronică a instituției, arhiva electronică a instituției, componenta de semnare și sigilare electronică calificată.
16. Să permită încărcarea de fișiere din calculator și din arhivele electronice aflate la dispoziția utilizatorului.
17. Să integreze nomenclatorul arhivistic electronic pentru a permite utilizatorului să salveze fișierele pe grupe și dosare electronice.
18. Să dispună în procesul de editare al unei lucrări de toate capabilitățile sistemului prezentate la actele electronice.
19. Să dispună de editoare de fișiere/mesaje text online ce includ elementele de formatare text standardizate la nivelul platformelor web.
20. Să fie integrate 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.).
21. 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.
22. Să implementeze în activitatea funcționarilor conceptul de „account manager” – titular unic pentru rezolvarea lucrării.
23. 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.
24. Să implementeze capabilități de automatizare a executării cursului lucrărilor – odată configurată lucrarea executarea operațiunilor să se succeadă fără o intervenție explicită a utilizatorului.

**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 reunesc 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 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 procedură de configurare a guvernanței digitale a dosarului de lucrare electronică

| |
|---|
| care trebuie să cuprindă informații despre minim următoarele aspecte:<br>o Crearea și ștergerea dosarului;<br>o Editarea atributelor dosarului;<br>o Adăugarea și ștergerea de lucrări electronice în dosar;<br>o Stabilirea drepturilor de acces la dosarul de lucrare electronică. |
| Soluția informatică propusă trebuie să asigure minim următoarele capabilități ce privesc dosarele electronice ce vor fi gestionate la nivelul instituției:<br>• 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.<br>• Să permită o arhitectură de tip „arbore” cu dosare și sub dosare în care relațiile de subordonare între dosare la nivelul soluției să poată fi modificate. |
| **Registru de lucrări și registre de acte** |
| **1.** Soluția informatică trebuie să permită crearea și configurarea registrelor instituției.<br>**2.** Soluția informatică trebuie să permită de asemenea posibilitatea ca mai multe structuri din instituție cu competențe similare să utilizeze același registru.<br>**3.** Registratura instituției va permite o evidență centralizată la nivelul Registrului Unic astfel încât toate lucrările realizate în activitatea curentă să se regăsească într-o singură interfață.<br>**4.** Registratura instituției va include un singur registru de lucrări la nivel de instituție, denumit Registrul Unic, și un număr nelimitat Registre de acte destinate fiecărei structuri din organigrama instituției (serviciu, birou, compartiment etc.).<br>**5.** Registrul Unic va asigura numere unice de înregistrare a lucrărilor, în timp ce Registrele de acte vor asigura numere de înregistrare unice actelor.<br>**6.** Registrul Unic va include atât lucrările de intrare și de ieșire, cât și lucrările interne.<br>**7.** Registrele trebuie să fie integrate cu arhiva electronică curentă.<br>**8.** 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. |
| **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).<br>Din acest motiv modalitatea de acordare a numerelor trebuie să fie riguros controlată și să reflecte întocmai realitatea.<br>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.<br>• Numerele de înregistrare date lucrărilor se vor acorda automat de sistem respectând ordinea cronologică a creării lucrărilor.<br>• Acordarea numerelor de înregistrare se va face incremental.<br>• Pentru lucrările de intrare numerele de înregistrare se vor acorda la momentul luării lor în evidență, deci la momentul intrării.<br>• 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.<br>• Acordarea numerelor de înregistrare trebuie să fie securizată, auditabilă.<br>• Soluția informatică trebuie să poată aloca numere lucrărilor atât în format individual, cât și în serii mari de lucrări denumite „batchuri” (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 să 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 ca în cazuri agreate la nivel instituțional ca lucrările (inclusiv actele pe care acestea le includ) să fie marcate ca fiind clasate.
- Soluția informatică nu va permite ștergerea numerelor de înregistrare.

**Cerințe privind registratura fizică digitalizată**

Registratura fizică digitalizată trebuie:

1. Să permită recepționarea solicitărilor de la alte entități fie ele persoane fizice sau juridice cu colectarea tuturor metadatelor relevante pentru lucrarea respectivă.
2. Să permită preluarea în format email/mesagerie electronică sau pe formulare tipizate a solicitărilor. Toate formularele tipizate existente și utilizate în cadrul instituției vor fi disponibile pentru preluarea solicitărilor de către funcționarii din registratură.
3. 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 email).
4. Să permită repartizarea lucrărilor pe fluxurile de resoluționare și ulterior către persoanele responsabile cu soluționarea acestora, capturând integral tot fluxul instituțional parcurs de lucrare.
5. 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.
6. 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
7. Să permită căutarea lucrărilor și vizualizarea conținutului acestora în Registrul Unic la solicitarea beneficiarului (persoană fizică, juridică sau funcționar), accesarea lor cu respectarea condițiilor impuse de GDPR, tipărirea și transmiterea actelor din lucrare cetățeanului prezentat la ghișeu.
8. Să vizualizeze toate solicitările pe care le-a repartizat, să le filtreze după cel puțin următoarele criterii:
   - Nume solicitant;
   - Număr de lucrare;
   - Nume destinatar;
   - Subiect;
   - Conținut;
   - CNP / CUI;
   - Data recepționării;
   - Data înregistrării.

| |
|---|
| 9. Căutarea va putea fi făcută prin filtre simple sau filtre conjugate astfel încât timpul de căutare să fie limitat la maxim.<br>10. Să arhiveze lucrările repartizate după ce acestea au fost finalizate.<br>11. Arhivarea lucrărilor trebuie să poată fi individuală (lucrare cu lucrare) sau în „batch" (mai multe lucrări arhivate printr-o singură operațiune). |
| **Cerințe privind registratura online automatizată** |
| Registratura online automatizată trebuie:<br>1. Să permită 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.<br>2. Repartizarea automatizată a lucrărilor recepționate prin mediul online trebuie să fie configurabilă în funcție de cel puțin următoarele criterii:<br>o Gradul de încărcare al funcționarului;<br>o Criteriul ierarhic (repartizarea automată către șeful de structură);<br>o Competența teritorială a funcționarului;<br>o Competența materială a funcționarului.<br>3. Să vizualizeze istoricul de solicitări al solicitantului în vederea evitării dublării solicitărilor.<br>4. Să vizualizeze toate solicitările care i-au fost repartizate pentru procesare, să le filtreze după cel puțin următoarele criterii:<br>o Nume solicitant;<br>o Număr de lucrare;<br>o Subiect;<br>o Conținut;<br>o CNP/CUI;<br>o Data recepționării;<br>o Data înregistrării;<br>o Starea lucrării.<br>5. Să repartizeze lucrarea fie către un alt funcționar din cadrul instituției, fie către o altă instituție atunci când este cazul.<br>6. Să organizeze consultări cu alți funcționari pentru a întocmi răspuns la cererile venite de la cetățeni.<br>7. 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 urmează să ia naștere în instituție (ex. se conexează la lucrarea existentă o nouă lucrare care urmează să ia naștere).<br>8. Să comunice online cu solicitanții în vederea solicitării de detalii suplimentare cu privire la solicitarea trimisă.<br>9. Să finalizeze/soluționeze solicitările primite prin una din modalitățile de finalizare disponibile în sistem.<br>10. Să arhiveze lucrările finalizate. |

### 3.2.3. Interconectarea și interoperabilitatea inter și intra-instituțională

***Notă:** Interconectarea și interoperabilitate se va face în conformitate cu prevederile standardului ETSI EN 319 521 V1.1.1 / 2019 și ale legii 242 din 2022 privind schimbul de date între sisteme informatice.*

Interconectivitatea și interoperabilitate vor fi operaționalizate prin intermediul **serviciului de**

**distribuție electronică înregistrată** care va permite:

- **Operaționalizarea canalelor de comunicare inter și intra-instituționale** menite să asigure transportul datelor între Direcția de Asistență Socială Drobeta-Turnu Severin și instituțiile subordonate – soluția informatică trebuie să permită încărcarea, transmiterea bidirecțională și livrarea către destinatar de conținut personalizat *(ex. fișiere și date structurate*) atât între structurilor interne ale instituției, cât și intre instituțiile vizate prin proiect.
- **Operaționalizarea canalelor de comunicare între funcționari și cetățeni / reprezentanții mediului de afaceri** – soluția informatică trebuie să includă o platforma multi-instituțională de interacțiune și comunicarea 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 toate serviciile publice de asistență socială oferite de beneficiar. Platforma de interacțiune cu cetățenii se dorește să asigure un punct centralizat de acces al cetățenilor la serviciile publice de asistență socială puse la dispoziție de Municipiul 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.
  - **Pentru PERSOANE FIZICE ȘI JURIDICE -** Soluția trebuie să adreseze următoarele cerințe funcționale specifice tuturor soluțiilor de comunicare, respectiv:
    - Să dispună de structura clasică de comunicări specifică tuturor clienților de email:
      - Primite;
      - Trimise;
      - Ciorne;
      - Șterse;
      - Arhivate.
    - Să permită schimbul de mesaje între utilizator și instituție.
    - Să permită construirea unui mesaj cu elementele clasice ale mesajelor de tip email, respectiv:
      - Destinatar;
      - Subiect;
      - Conținut mesaj;
      - Atașamente.
    - Să aibă integrate capabilități de conversie automată și manuală în PDF a atașamentelor.
    - Să dispună de capabilități integrate de semnare electronică calificată a fișierelor atașate.
  - **Pentru FUNCȚIONARI** - Soluția trebuie să adreseze următoarele cerințe funcționale specifice tuturor soluțiilor de comunicare, respectiv:
    - Să dispună de structura clasică de comunicări specifică tuturor clienților de email:

- Primite;
- Trimise;
- Ciorne;
- Arhivate.

- Să permită schimbul de mesaje bidirecțional între funcționari și toate tipurile de utilizatori.
- Să permită construirea unui mesaj cu elementele clasice ale mesajelor de tip email, respectiv:
  - Destinatar;
  - Subiect;
  - Conținut mesaj;
  - Atașamente.
- Să fie integrată cu registratura online automatizată pentru a permite transformarea unui mesaj/email în lucrare când aceasta întrunește condițiile cerute de instituție. Se dorește astfel evitarea transferului manual între soluții diferite de email a conținutului solicitărilor.
- Să aibă integrate capabilități de conversie automată și manuală în PDF a atașamentelor.
- Să permită conversia fișierelor în format PDF.
- Să dispună de capabilități de semnare electronică calificată a fișierelor atașate.

Soluția trebuie să integreze instrumente de lucru colaborativ:

- Schimbul bidirecțional de mesaje;
- Atașare de fișiere;
- Comunicarea individuală sau în grup;
- Audio conferință;
- Video conferință;
- Partajare de ecrane;
- Documente colaborative;
- Asigurarea procedurilor de încărcare, transport, livrare și vizualizare a conținutului, a datelor și documentelor.

Soluția trebuie să integreze comunicarea prin intermediul formularelor inteligente puse la dispoziția utilizatorilor. Formularele trebuie:

- Să fie grupate pe tipuri de utilizatori.
- Să asigure colectarea datelor în format structurat și validat la nivel de input.
- Să furnizeze contextual documentele justificative specifice aferente fiecărui tip de formular.
- Să dispună de o zonă de administrare care să 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.*).

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.

- **Procedurile de parametrizare a fluxurilor de comunicare** - soluția trebuie să permită configurarea de fluxuri predefinite cu respectarea următoarelor cerințe funcționale:
  - Respectarea competenței materiale și teritoriale 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.
  - Fluxurile predefinite să fie disponibile tuturor categoriilor de utilizatori (persoane fizice, juridice, funcționari – atât pe canalul offline (la ghișeu, cât și pe canalul online).

Soluția informatică propusă trebuie să dispună de capabilități de modelare de fluxuri cu respectarea următoarelor cerințe funcționale:

- Posibilitatea de modelare trebuie să fie disponibilă tuturor funcționarilor.
- Odată modelat fluxul acesta se va executa automat fără intervenția funcționarului.
- Să fie implementat un mecanism de „rollback” care să poată fi apelat motivat de oricare dintre participanții la flux.
- Modelarea fluxului să includă minim 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;
- 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;
- Stabilirea structurilor de date ce fac obiectul fluxului și a algoritmilor de validare ale acestora.

o **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.

o **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 email;
- Notificări în contul personal;
- Notificări de tip push (push notification) în aplicația mobilă.

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

**Notificări în contul personal și push notifications** - Soluția informatică trebuie să poată trimite notificări de tip „push" prin trimitere instantanee sau prin „coadă" cu respectarea următoarelor cerințe funcționale:

- Notificările să poată fi trimise targhetat minim către:
  - Un utilizator individual persoana fizică, juridică sau funcționar;
  - Către toți reprezentanții unei persoane juridice;
  - Către administratorii persoanelor juridice;
  - Către toți funcționarii;
  - Către toți funcționarii dintr-o anumită instituție;
  - Către toți reprezentanții persoanelor juridice.

- Să permită parametrizarea mesajului de trimis (număr de caractere).
- Să furnizeze informații de progres cu privire la trimiterea în batchuri mari de notificări.
- Să dispună de mecanisme de fallback implementate pentru gestionarea situațiilor când apar erori în procesul de trimitere.

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

o Asigurarea și mentenanța API-urilor de interconectare cu furnizorii de servicii de semnare electronică calificată, cu furnizorii de servicii de sigilare electronică calificată, cu STS, RoEID, ANAF, RECOM, cu alți furnizori.

*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.*

*Documentația tehnică a serviciilor API pentru realizarea interconectivității va fi prezentată de fiecare ofertant în cadrul procedurii de ofertare și verificată și testată de către expertul tehnic cooptat. Structurile de date menționate în documentație trebuie să fie complete și să respecte cerințele referitoare la lucrări și acte.*

### 3.2.4. Arhivarea electronică și îndosarierea electronică

***Notă:** Arhivarea electronică se va face în conformitate cu prevederile legale referitoare la arhivarea documentelor electronice, la administratorii de arhive electronice și cerințele ce trebuie îndeplinite de centrele de date care au ca obiect de activitate arhivarea electronică. Soluția SaaS va include funcționalități de arhivare electronică a documentelor în conformitate cu Legea nr. 135/2007 și normele de aplicare. 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", serviciu care operează în cadrul CPG/CR (cloudul privat public guvernamental/cloudul regional) sau este interconectat în mod sigur cu acesta. Furnizorul soluției SaaS va trebui să demonstreze 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.*

Arhivarea electronica vizează asigurarea următoarelor funcționalități:

o Asigurarea procedurilor de creare și parametrizare multianuală a nomenclatorului arhivistic (grupele de documente);

o Gestionarea structurilor de metadate pentru documentele arhivate;

o 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 trebuie să pună la dispoziția fiecărui tip de utilizator (persoană fizică, persoană juridică sau funcționar):

- Arhiva electronică de documente/acte – destinată să permită utilizatorului accesul rapid, direct din cloud, la toate documentele sale (atât documente personale, cât și acte emise instituție).
- Arhivă electronică de lucrări – destinată arhivării solicitărilor trimise către instituție și care au fost deja finalizate.

| **Cerințe specifice privind arhiva electronică de documente/acte a persoanelor fizice și juridice** |
|---|
| Soluția informatică propusă trebuie să dispună de următoarele capabilități tehnice:<br>**1.** Să fie integrată cu componenta de management a identităților electronice și să permită accesul la documente în funcție de nivelul de încredere (scăzut/substanțial sau ridicat).<br>**2.** Să fie integrată cu componenta de formulare electronice și cu soluția de email a sistemului astfel încât utilizatorul să poată încărca individual sau în batchuri documente direct din arhiva sa electronică.<br>**3.** Să permită utilizatorilor autorizați vizualizarea, descărcarea și tipărirea documentelor/actelor.<br>**4.** Să permită vizualizarea tuturor metadatelor stocate la nivelul sistemului pentru fiecare document/act în parte.<br>**5.** Să dispună de capabilități de filtrare, sortare și căutare în funcție de metadate relevante (ex. denumire fișier, număr de înregistrare, data, etc.).<br>**6.** Să permită utilizatorului ștergerea documentelor / actelor din arhiva personală.<br>**7.** Să nu permită utilizatorului ștergerea actelor transmise lui de către instituții.<br>**8.** Să permită utilizatorului să vizualizeze lucrarea din care a făcut parte actul emis și transmis lui de către instituție.<br>**9.** 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.<br>**10.** Să dispună de o politică de management a documentelor încărcate în sistem cel puțin din perspectiva:<br>o Formate de fișiere acceptate;<br>o Parametrii denumirilor fișierelor;<br>o Mărimea fișierelor;<br>o Scanarea documentelor.<br>Accesul la fișiere (la persoanele juridice care poată avea mai mulți reprezentanți soluția trebuie să stabilească drepturile de acces ale fiecăruia la fișiere). |

| Cerințe specifice privind arhiva electronică de lucrări a persoanelor fizice și juridice |
|---|
| Soluția informatică propusă trebuie să dispună de următoarele capabilități tehnice:<br>**1.** Să permită utilizatorilor autorizați vizualizarea lucrărilor și a documentelor asociate.<br>**2.** Să permită vizualizarea tuturor metadatelor stocate la nivelul sistemului pentru fiecare lucrare.<br>**3.** Să dispună de capabilități de filtrare, sortare și căutare în funcție de metadate relevante (ex. denumire, conținut, număr de înregistrare, dată, etc.).<br>**4.** Să nu permită utilizatorului ștergerea lucrărilor transmise lui de către instituții. |
| **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:<br>**1.** Furnizorul de cloud să fie certificat de ministerul/autoritățile de resort pentru servicii de arhivare electronică.<br>**2.** Să permită crearea nomenclatorului arhivistic electronic (conform prevederilor legale) și managementul arhivei electronice instituționale.<br>**3.** Să fie integrată în toate mijloacele de comunicare relevante (ce produc consecințe juridice) la nivelul soluției informatice propuse.<br>**4.** Să fie integrată cu componenta de management a identităților pentru a colecta actele de identitate ale utilizatorului direct din procedura de onboarding.<br>**5.** Să dispună de mecanisme auditabile (log-uri) explicite cu privire la orice modificare, acces sau operațiune ce are impact în arhiva electronică.<br>**6.** Să fie sincronizată cu registrele instituției pentru a asigura o bună trasabilitate și transparență în gestiunea actelor.<br>**7.** Să salveze toate metadatele relevante ale actelor în structura PDF a acestora.<br>**8.** 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 aceste obligații.<br>**9.** La cererea beneficiarului și fără costuri pentru acesta să îi pună la dispoziție un mecanism exact de extragere a metadatelor din fișierele exportate. |
| **Cerințe specifice privind arhiva de lucrări electronice a instituției** |
| Soluția informatică propusă trebuie să dispună de următoarele capabilități tehnice:<br>**1.** Să permită funcționarilor autorizați vizualizarea lucrărilor și a documentelor asociate.<br>**2.** Să permită vizualizarea tuturor metadatelor stocate la nivelul sistemului pentru fiecare lucrare.<br>**3.** Să dispună de capabilități de filtrare, sortare și căutare în funcție de metadate relevante (ex. denumire, conținut, număr de înregistrare, dată, etc.).<br>**4.** Să nu permită utilizatorului ștergerea lucrărilor transmise lui de către instituții. |

**3.2.5. Semnarea și sigilarea electronică calificată în cloud**

Soluția SaaS va integra servicii de semnare electronică calificată și sigilare electronică calificată, pe deplin conforme cu Regulamentul ~~eIDAS~~eIDAS2.~~1~~ Se va acorda prioritate utilizării certificatelor calificate pentru semnătură electronică și sigiliu electronic stocate în cloud, emise de prestatori de servicii de încredere calificați, și care sunt agreate pentru utilizare în infrastructura CPG/CR. ~~Soluția informatică ofertată va putea utiliza fără niciun fel de restricționare certificate calificate emise în conformitate cu prevederile regulamentului eIDAS de orice furnizor autorizat de pe teritoriul Europei~~.

Documentele încărcate în sistem vor putea fi semnate electronic cu orice tip de instrument criptografic acreditat (semnătură electronică cu certificat calificat stocat pe token sau semnătură electronică cu certificat calificat stocat în cloud la unul dintre furnizorii autorizați 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 trebuie să demonstreze integrarea cu cel puțin doi furnizori de servicii de încredere calificate recunoscuți la nivel european și, adițional, cu mecanismele de semnare/sigilare electronică ce ar putea fi oferite centralizat de către stat prin intermediul STS sau alte entități abilitate în contextul CPG/CR.~~Soluția informatică trebuie să dispună de integrare cu minim 2 furnizorii de servicii de încredere autorizați în acest sens la nivel european, și cu STS.~~

| **Semnarea electronică calificată** |
|---|
| Din perspectiva semnării electronice calificate beneficiarul urmărește realizarea următoarelor cerințe funcționale:<br>**1.** Să permită sincronizarea/desincronizarea certificatului calificat de semnare electronică cu sistemul.<br>**2.** Să permită integrarea semnăturii olografe în semnătura electronică calificată.<br>**3.** Să dispună de Integrarea semnăturii electronice calificate pe toate fluxurile de comunicare implementate la nivelul sistemului.<br>**4.** Să permită semnarea simplă (1 document) și semnarea în batchuri (mai multe documente) tuturor utilizatorilor din sistem.<br>**5.** Să permită un management contextual al motivelor de semnare.<br>**6.** Să permită semnarea în interiorul sau independent de existența unui flux de semnare.<br>**7.** Să permită verificarea și validarea semnăturilor electronice calificate aplicate pe documente/ acte, respectiv:<br>o Validarea tipului de semnătură;<br>o Verificarea lanțului de încredere al certificatului;<br>o Data și ora semnării;<br>o Identitatea celui care a semnat;<br>o Dacă documentul a fost sau nu modificat după semnare;<br>o Date privind valabilitatea certificatului calificat;<br>o Emitentul certificatului;<br>o Motivul de semnare.<br>**8.** 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.<br>**9.** Să permită operațiuni precum anularea semnării, revizuirea semnării, reluarea semnării.<br>**10.** Să permită vizualizarea listingului de solicitări de semnare și gestionarea cererilor/invitațiilor de semnare.<br>**11.** Să permită pre vizualizarea documentelor ce urmează a fi semnate fără să fie nevoie de descărcarea lor.<br>**12.** Să permită semnarea electronică calificată simultană a mai multor documente și semnarea de tip „queue” (coadă).<br>**13.** Să permită crearea și managementul dinamic al fluxurilor de semnare consecutive sau concomitente (inclusiv anularea și reconfigurarea acestora).<br>**14.** Să permită crearea și întreținerea listelor de semnatari și a competențelor lor de semnare.<br>**15.** Să permită proceduri de semnare cross-platforme. |
| **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~~eIDAS2 de orice furnizor |

| |
|---|
| autorizat 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 furnizorii de servicii de încredere autorizați în acest sens la nivel european și cu STS. |
| Din perspectiva sigilării electronice calificate autoritatea contractantă urmărește realizarea următoarelor cerințe funcționale:<br>**1.** Să permită sigilarea electronică calificată atât în regim de aplicare automată, cât și în regim de aplicare manuală.<br>**2.** Să permită sigilarea electronică calificată simultană a mai multor documente și sigilarea de tip „queue" (coadă).<br>**3.** 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.<br>**4.** Să fie integrat cu mecanismul de acordare a numerelor de înregistrare tuturor actelor originale sau luate în evidență în sistem.<br>**5.** Să dispună de mecanisme de tip „fallback" pentru cazurile în care documentele lansate spre sigilare electronică calificată prezintă erori structurale și nu pot fi sigilate necesitând intervenția unui operator în acest sens. |

### 3.2.6. Securitatea și Auditul platformei

Sistemul SaaS va genera și stoca jurnale de audit (log-uri) detaliate pentru toate acțiunile 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.

Aceste jurnale vor fi:

- Complete: Să înregistreze cine, ce, când, de unde și rezultatul acțiunii.
- Imuabile: Protejate împotriva modificărilor neautorizate sau ștergerii.
- Securizate: Stocate într-un mediu sigur, cu acces controlat.
- Disponibile: Pentru administratorii desemnați și pentru echipele de audit extern, conform prevederilor HG 70/2023 și HG 112/2023.
- Corelate: Să permită corelarea evenimentelor pentru investigarea incidentelor. Soluția va include mecanisme de detectare a anomaliilor în comportamentul utilizatorilor sau al sistemului și de alertare în timp real a personalului responsabil în cazul unor potențiale incidente de securitate.

Pentru asigurarea îndeplinirii cerințelor de securitate legate de constrângerile privind lucrul cu date cu caracter personal, vor fi respectate următoarele reguli

a. **Înregistrarea și accesul utilizatorilor** - sistemul va avea capabilitatea de a determina univoc dacă utilizatorul este cel care pretinde că este. Procesul de înregistrare cuprinde informații relevante privind utilizatorul: nume utilizator, parola și/sau certificatul și drepturile pe care le deține în sistem. Sunt prevăzute reguli parametrizate privind politica de securitate, precum complexitatea parolei, perioada de valabilitate a actelor care dovedesc identitatea, număr de încercări eșuate, informații privind datele în care sistemul a fost accesat.

b. **Autentificare / identificare** - utilizatorii care accesează informațiile și funcționalitățile sistemului sunt autentificați înainte de a li se permite accesul.

c. **Autorizare bazată pe roluri** - sistemul va restricționa drepturile de acces ale utilizatorului la funcționalitățile sistemului pe baza rolului desemnat acestuia. Fiecare utilizator are asociat

unul sau mai multe roluri. Fiecare rol are asociat un set de drepturi. Drepturile reprezintă prerogativele acordate unui utilizator de a efectua anumite activități în cadrul unui sistem informatic. Sistemul poate limita sau permite accesul unui utilizator la anumite date și funcționalități pe baza apartenenței la un rol.

d. **Control acces (autorizare)** - sistemul va include mecanisme de prevenire a utilizării neautorizate sau de manieră neautorizată a resurselor. Fiecărui utilizator autorizat i se asociază o autorizare. Controlul accesului constă în restricționarea capacității unui subiect de a folosi un sistem sau un obiect în acel sistem, precum și jurnalizarea activităților efectuate.

e. **Auditare** - activitățile derulate în sistem vor fi înregistrate, fiind posibilă auditarea ulterioară. Sistemul trebuie să aibă capacitatea de a înregistra toate tranzacțiile și incidentele din sistem, fiind posibilă analiza acestor înregistrări în scopul identificării modului de funcționare al sistemului și activităților derulate de utilizatori.

f. **Integritatea datelor** - datele stocate și procesate în sistem se doresc a fi corecte și complete. Sistemul trebuie să asigurare protecția, exactitatea și completitudinea datelor și a soluțiilor furnizate pentru stocarea și gestionarea acestora, dar și asigurarea împotriva manipulării frauduloase a datelor/informațiilor. Protecția împotriva dezastrelor va fi realizată prin crearea copiilor de rezervă incrementale și depline. Soluția trebuie să fie găzduită într-un data center ce are toate certificările / acreditările necesare pentru o astfel de soluție.

g. **Administrare (configurare)** - sistemul va permite aplicarea politicilor de securitate încorporate în arhitectura și funcționalitățile lui. Definirea utilizatorilor și grupurilor sau rolurilor, precum și atribuirea de drepturi se realizează de către utilizatori cu drepturi de administrator. Sistemul permite delegarea administrării drepturilor complet sau limitat la anumite operații (de exemplu, adăugare utilizator, schimbare parola) către alți utilizatori dintr-o organizație.

h. **Securitatea împotriva accesului neautorizat** - sistemul trebuie să fie protejat împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care acesta le stochează. Sistemul include următoarele facilități: controlul accesului utilizatorilor la sistemele de aplicații și fișierele de date; ierarhizarea în clase a utilizatorilor finali; facilități de administrare parole; permiterea accesului direct la bazele de date numai administratorilor de baze de date autorizați; asigurarea securității tuturor interfețelor sistemului informatic, prevenind accesul utilizatorilor neautorizați la sistem; raportarea pe baze periodice a detaliilor privitoare la accesul în sistem al utilizatorilor.

i. **Disponibilitate** - sistemul va asigura un proces de redundanță pentru a asigura utilizatorii de eventualele defecțiuni care pot surveni în timpul funcționării precum și asigurarea datelor, componentelor funcționale și serviciilor asociate către utilizatorii autorizați la momentul solicitării.

Pentru gestiunea riscurilor de securitate va fi implementată o politică generală de securitate. Politica de securitate va include prevederi referitoare la organizarea auditurilor periodice de securitate pentru a verifica politica și conformitatea cu regulile de securitate, precum și a stabili domeniile care necesită îmbunătățiri.

Pentru asigurarea securității sistemului se vor avea în vedere a fi implementate cel puțin următoarele măsuri:

1. **Separarea drepturilor de acces la date** - Asigurarea controlului centralizat al tuturor aspectelor legate de securitate (autentificare, autorizare, auditare), bazate pe separarea clară a dreptului de acces la date, conform rolurilor de securitate în sistem.
2. **Permisiunile utilizatorilor și semnătura electronică calificată** - Semnătura electronică calificată și permisiunile utilizatorilor sunt modalități de securitate care asigură autorizarea, confidențialitatea, autenticitatea și non-repudierea. Aceste servicii se bazează pe infrastructura de semnătură electronică calificată a soluției furnizată împreună cu furnizorii autorizați de servicii de încredere.
3. **Managementul utilizatorilor și a grupurilor de utilizatori** - Utilizatorii soluției informatice vor fi autorizați să lucreze doar asupra documentelor, actelor sau a altor elemente informaționale pentru care au permisiunile necesare. Un grup este caracterizat de un nume și de un set de permisiuni (desemnând rolurile acelui grup), care definesc accesul la funcționalitățile sistemului. Fiecare grup trebuie să conțină o listă de utilizatori, care preiau permisiunile de la grupul din care fac parte. La autentificare, sistemul verifică datele de acces ale utilizatorilor și le dă acces la informația disponibilă.
4. **Cererea de motivare a accesului** este realizată în cadrul unui sistem de control al accesului în care este stabilit: cine, cui, în conformitate cu care împuterniciri, care documente, pentru care acțiuni sau care tip de acces poate fi permis și în care condiții, și care presupune determinarea pentru toți utilizatorii a resurselor informaționale și program la care au acces pentru operații concrete de accesare (citire, scriere, modificare, ștergere, execuție) folosind resursele tehnice și program de accesare.
5. **Infrastructura de semnare și sigilare electronică calificată** - Soluția informatică va opera o aplicație de semnare electronică ce va permite utilizatorilor să semneze documente cu putere juridică. Semnătura electronică calificată, sigiliul electronic calificat și controlul accesului constituie măsurile de control de securitate, care asigură integritatea, confidențialitatea, disponibilitatea, autenticitatea și non-repudierea.
6. **Înregistrările de audit** - O necesitate importantă legată de securitate este necesitatea păstrării înregistrărilor de audit pentru analiza integrității sistemului și pentru monitorizarea activității utilizatorilor. Soluția informatică trebuie să se bazeze pe un mecanism de înregistrări de audit ce urmează practicile mondiale curente. Pentru garantarea securității la nivelul infrastructurii tehnico-logice este implementat auditul activ al securității informaționale.
7. **Disponibilitatea sistemului** - Utilizatorii soluției informatice depind într-o măsură considerabilă de disponibilitatea sistemului pentru a-și putea îndeplini sarcinile. Acest lucru ridică cerințe semnificative față de infrastructura sistemului informațional pentru ca aceasta să fie rezistentă la erori de hardware și software.
8. **Criptarea informației** - La transmiterea informației confidențiale, metoda de protecție a informației transmise prin toate tipurile de canale de comunicație, contra interceptării,

alterării sau a falsificării informației, este criptarea informației. Se recomandă mijloace de securizare criptografică a datelor cu rezistență garantată pentru nivelul necesar de confidențialitate și sistemul de chei electronice, ce asigură autentificarea mesajelor și schimb sigur de informație.

## 4. CERINȚE NON-FUNCȚIONALE ALE PROIECTULUI TIC

### 4.1. Backup și înaltă disponibilitate

- Soluția trebuie să asigure o protecție eficientă a datelor de diverse tipuri împotriva erorilor, prin stocarea copiilor de salvare;
- Soluția de backup trebuie să asigure copii de siguranță pentru mai multe versiuni ale aceleiași entități logice, astfel încât să ofere posibilitatea restaurărilor selective;
- Soluția trebuie să permită setarea perioadelor de păstrare a datelor salvate, în funcție de timpul la care a fost realizat backup-ul;
- Se solicită prezentarea în cadrul propunerii tehnice a modalității de realizare a back-up-ului precum și descrierea modului de realizare al acesteia (incluzând menționarea produselor utilizate, dacă este cazul);
- Soluția trebuie să asigure continuitatea serviciilor oferite utilizatorilor;
- Sistemul trebuie să permită funcționarea în regim de înaltă disponibilitate, cel puțin pentru componentele critice: sistemul de baza de date, serverul de aplicație;
- Se va asigura înalta disponibilitate a sistemului, utilizând mediul virtualizat sau mediul fizic, prezentând descrierea detaliată a modalității și a metodelor folosite pentru îndeplinirea cerinței în cadrul propunerii tehnice.

Soluția SaaS va fi găzduită într-o infrastructură care asigură înaltă disponibilitate (High Availability - HA) și mecanisme robuste de recuperare în caz de dezastru (Disaster Recovery - DR), în conformitate cu standardele și politicile Cloudului Privat Guvernamental/Cloudului Regional. Aceasta poate implica utilizarea unor centre de date multiple, cu redundanță geografică~~, așa cum sunt prevăzute pentru CPG~~. Furnizorul soluției SaaS va prezenta în oferta tehnică un Plan de Continuitate a Afacerii și Recuperare în Caz de Dezastru (BCP/DRP) detaliat, care trebuie să fie aliniat cu cerințele de reziliență ~~ale CPG,~~ așa cum sunt ele definite în OUG 89/2022, Art. 14.
Se vor defini și agrea contractual următorii indicatori critici:

- RPO (Recovery Point Objective): Timpul maxim acceptabil de pierdere a datelor în cazul unui incident major.
- RTO (Recovery Time Objective): Timpul maxim acceptabil pentru restabilirea serviciului după un incident major.

Acești indicatori (RPO și RTO) vor fi stabiliți în funcție de criticitatea serviciilor de asistență socială furnizate și vor fi incluși în Acordul de Nivel de Serviciu (SLA).

### 4.2. Performanța soluției propuse

- Sistemul trebuie să fie disponibil pentru utilizare zilnică~~, 24 ore/zi, 7 zile din 7.~~ Î iar în aceasta perioadă se va asigura suportul tehnic și se vor trata toate întreruperile ca incidente de o importanță ridicată (incident blocant) și prioritate maximă.
- Timpul maxim de întrerupere a sistemului în intervalul 22:00 - 06:00 a doua zi, trebuie să fie de maxim 10 ore pe an.
- Toate operațiunile de salvare a datelor (back-up) trebuie să se desfășoare în intervalul 00:00 și 05:00. Tot în acest interval se vor realiza și toate activitățile de întreținere și actualizare a sistemelor software.

Acordul de Nivel de Serviciu (SLA) încheiat cu furnizorul soluției SaaS va defini indicatori de performanță (KPIs) clari, măsurabili și relevanți pentru operațiunile specifice ale Direcției de Asistență Socială. Aceștia vor include, fără a se limita la: timpii de răspuns pentru tranzacțiile cheie (de exemplu, înregistrarea unei cereri, căutarea într-o bază de date, generarea unui raport), numărul de utilizatori concurenți suportați fără degradarea performanței, și capacitatea de procesare a unui volum specific de date într-un interval de timp dat.

SLA-ul va include penalități clare și aplicabile pentru nerespectarea indicatorilor de performanță agreați. Acești indicatori trebuie să fie monitorizabili în mod continuu, ideal prin instrumente și tablouri de bord accesibile atât beneficiarului, cât și, eventual, prin mecanisme de monitorizare centralizată ~~oferite de CPG~~.

Disponibilitatea serviciului (uptime) va fi de minim 99,9% calculată lunar, pe durata programului de lucru al instituției (Luni-Vineri, 08:00-16:00), excluzând ferestrele de mentenanță programată și anunțată în prealabil. Pentru serviciile publice online destinate cetățenilor, se va urmări o disponibilitate cât mai apropiată de 24/7. Nivelul de disponibilitate trebuie să fie conform cu cerințele ~~CPG~~ pentru servicii publice considerate critice (a se vedea și prevederile HG 70/2023 referitoare la SLA ~~în CPG~~).

### 4.3. Securitatea soluției propuse

- Sistemul trebuie să ofere, odată ce un utilizator s-a conectat, accesul protejat la datele personale/private. Astfel fiecare utilizator trebuie să poată accesa doar datele și funcționalitățile pentru care are drepturi.
- Sistemul trebuie să ofere securitate la nivelul cererilor venite de la utilizator. Serviciile din cadrul sistemului trebuie să aibă mecanisme proprii de securitate. Sistemul trebuie să fie protejat la executarea de comenzi rău intenționate către baza de date, realizându-se validarea parametrilor trimiși către aceasta.
- Mesajele și datele transportate în cadrul sistemului trebuie să fie securizate.

Furnizorul va permite și va facilita realizarea unor audituri de securitate periodice și teste de penetrare la intervale regulate de cel mult 12 luni ~~din partea beneficiarului sau a unor entități terțe desemnate de ADR și/sau SRI, în contextul operării în CPG~~.

Soluția SaaS va implementa în mod obligatoriu:

- Criptarea datelor în tranzit: Utilizând protocoale robuste și actuale (de exemplu, TLS 1.2 sau superior) pentru toate comunicațiile externe și interne.
- Criptarea datelor în repaus (at rest): Utilizând algoritmi de criptare puternici (de exemplu, AES-256 sau echivalent) pentru toate datele sensibile stocate în bazele de date și în sistemele de fișiere.
- Managementul robust al identității și accesului (IAM): Implementarea unor mecanisme stricte de control al privilegiilor (principiul celui mai mic privilegiu), separarea rolurilor, și auditarea detaliată a tuturor operațiunilor de acces și modificare a drepturilor.
- Protecție împotriva amenințărilor comune: Inclusiv, dar fără a se limita la, protecție împotriva injecțiilor SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), și alte vulnerabilități din topul OWASP.

### 4.4. Administrarea utilizatorilor

- Sistemul trebuie să permită administrarea utilizatorilor, a rolurilor acestora și a grupurilor de utilizatori.
- Accesul la funcționalitățile de administrare a utilizatorilor cetățeni trebuie să fie permis tuturor funcționarilor și reglementat conform procedurilor și politicilor agreate de către beneficiar.
- Accesul la funcționalitățile de administrare a utilizatorilor funcționari trebuie să fie permis doar administratorilor de platforma și reglementat conform procedurilor și politicilor agreate de către beneficiar privind drepturile acordate.
- Administrarea informațiilor despre utilizatori și datele de autentificare ale acestora va fi realizată unitar pentru toate componentele sistemului, utilizând funcționalitățile puse la dispoziție prin interfața sistemului.
- Administratorii sistemului trebuie să poată adăuga noi utilizatori, să inactiveze/activeze utilizatori (un utilizator inactiv rămâne în sistem dar nu se mai poate conecta) sau blocheze accesul unui utilizator în sistem pentru o perioadă determinată.
- Administratorii sistemului trebuie să poată adăuga noi roluri sau modifica rolurile existente, asocia drepturi de acces la roluri, să poată crea sau modifica grupuri de utilizatori.

### 4.5. Administrarea rolurilor

- Sistemul trebuie să ofere posibilitatea cumulării mai multor roluri de către un utilizator. Fiecare rol trebuie să aibă asociate un set de drepturi predefinite. Sistemul trebuie să permită accesul securizat al utilizatorilor la funcționalități pe baza rolurilor asociate.
- Drepturile de acces ale utilizatorilor trebuie să se poată configura din interfața sistemului.

### 4.6. Profilul utilizatorilor

Fiecare utilizator trebuie să aibă acces la profilul propriu în care să poată modifica datele personale, preferințele de notificare și parola de acces în sistem.

### 4.7. Flexibilitatea și funcționalitatea sistemului

Arhitectura sistemului va trebui să fie deschisă și bazată pe standarde larg acceptate în industrie. 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 sa 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 recunoscute și acceptate – XML/JSON/HTTP/HTTPS/SSL
- utilizarea unei arhitecturi modulare, minim „cloud ready”, și având propria soluție de virtualizare, bazată pe containerizare și micro servicii, care permite modificarea anumitor componente fără impact major în restul soluției;

- interfața ergonomica și ușor de utilizat. Interfața trebuie să fie coerentă din punct de vedere al elementelor de design al interfeței.

### 4.8. Proprietatea datelor

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

### 4.9. Cerințe cloud

Infrastructura cloud pe care va opera soluția SaaS ~~(fie infrastructura proprie a furnizorului SaaS, fie infrastructura IaaS/PaaS direct din CPG/CR)~~ trebuie să respecte următoarele condiții cumulative:

1. **Localizarea geografică**: Să opereze și să stocheze toate datele (inclusiv backup-urile) în centre de date localizate pe teritoriul Uniunii Europene, cu prioritate pe teritoriul României, conform politicilor naționale și cerințelor GDPR.
2. **Acreditare ADR**: Centrele de date utilizate ~~(dacă sunt diferite de cele operate direct de STS/ADR pentru CPG)~~ trebuie să fie acreditate de Autoritatea pentru Digitalizarea României (ADR) conform normelor în vigoare (stabilite în baza OUG 89/2022, Art. 16, și detaliate în HG 112/2023). Deținătorul infrastructurii cloud va prezenta dovada acestei acreditări (de exemplu, ca „administrator de arhivă electronică" și/sau „centru de date" autorizat ADR, în funcție de serviciile specifice oferite și de relevanța pentru datele gestionate de DAS Drobeta). ~~În cazul în care soluția SaaS rulează direct pe infrastructura CPG (Cloud Intern sau Cloud Dedicat), se va considera că această cerință este îndeplinită prin natura infrastructurii CPG.~~
3. **Criptarea datelor și a comunicațiilor**: Stocarea datelor în infrastructura cloud se va face pe volume criptate, iar toate comunicațiile, atât între componentele arhitecturale ale soluției SaaS, cât și între acestea și sistemele de stocare sau alte servicii ~~CPG,~~ se vor realiza utilizând protocoale criptate.
4. **Managementul cheilor de criptare**: Responsabilitatea pentru gestionarea securizată și documentată a cheilor de criptare (generare, stocare, rotație, revocare) va fi clar definită și trebuie să respecte bunele practici ~~și politicile CPG~~.
5. **Notificarea incidentelor GDPR**: După caz, ~~P~~personal responsabil pentru notificarea, incidentelor de încălcare a securității datelor cu caracter personal în termen de 72 de ore de la luarea la cunoștință (către autoritățile de reglementare, client, după caz a persoanelor vizate).

Formatat: Font: Nu Aldin

~~Infrastructura cloud în care este instalată soluția informatică ofertată trebuie să îndeplinească minim condițiile:~~
~~Să opereze și stocheze date într-un centru de rețea înlăuntrul Uniunii Europene, respectiv înlăuntrul jurisdicției Regulamentelor UE nr. 679/2016 cu privire la protecția datelor cu caracter personal (GDPR) și nr. 910/2014 privind serviciile de încredere și identitatea electronică (eIDAS).~~
~~Acreditat ADR „administrator de arhivă electronică";~~
~~Autorizat ADR „centru de date".~~
~~Stocarea datelor în infrastructura cloud se va face pe volume criptate iar comunicarea atât între componentele arhitecturale ale soluției cât și între acestea și cele de stocare se va face de asemenea~~

~~criptat. Responsabilitatea gestionării cheilor de criptare în condiții de securitate adecvate scopului (inclusiv înlocuirea acestora la intervale regulate), cade în sarcina prestatorului.~~

### 4.10. Suport tehnic

Pe toată durata prestării serviciilor prestatorul va asigura suport tehnic. În acest timp asistența va fi disponibilă în zilele lucrătoare în programul 8-17, printr-un sistem de înregistrare a problemelor prin web /mail. Prestatorul va asigura un punct de contact disponibil, dedicat personalului autorizat al Autorității Contractante unde se poate semnala orice problemă/defecțiune sau se solicită suport tehnic.

Prestatorul va răspunde în timp util la orice incident semnalat de autoritatea contractantă, în funcție de nivelul incidentului. Fiecare incident 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 funcționării produsului. Problema împiedică desfășurarea activității Autorității Contractante;
- Mare – impact semnificativ asupra funcționării 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 "urgent" intervenția va fi asigurată 24 x 7, 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 ora | o zi |
| Mare | 2 ore | 2 zile |
| Mediu | 4 ore | 2 zile lucrătoare |
| Minor | 4 ore | 3 zile lucrătoare |

### 4.11. Managementul calității

Se va solicita pe o perioadă de 10 zile în cadrul procedurii de atribuire, un mediu de testare al soluției informatice ofertate pentru a permite verificarea unui sub set de bază al funcționalităților solicitate, respectiv care trebuie să implementeze funcționalitățile solicitate prin Caietul de sarcini privind managementul identității electronice, managementul înregistrărilor, interconectivitatea și interoperabilitatea, semnarea și sigilare electronică.

Mediul de testare trebuie să dispună operațional de toate interconectările necesare între componentele solicitate, în scopul testării cu succes a acestora de către comisia de evaluare. Mediul de testare pus la dispoziție în cadrul procedurii de atribuire va trebui să demonstreze nu doar funcționalitățile de bază ale soluției SaaS, ci și capacitatea acesteia de integrare cu un mediu de testare sau simulare al Platformei Naționale de Interoperabilitate (PNI) și al sistemului ROeID, în măsura în care un astfel de mediu este disponibil și pus la dispoziție de către ADR și/sau STS pe durata evaluării.

În plus, se va evalua și conformitatea preliminară a soluției SaaS cu cerințele generale de listare în marketplace-ul de aplicații al Cloudului Privat Guvernamental, așa cum sunt acestea schițate în HG 70/2023, Art. 34 și următoarele.~~11~~ Chiar dacă achiziția prezentă este specifică pentru DAS Drobeta-Turnu Severin, o soluție care îndeplinește criteriile de listare în marketplace-ul CPG demonstrează un grad mai mare de maturitate, standardizare și potențial de reutilizare la nivelul administrației publice, aspecte care pot fi considerate avantajoase.

Principiul de testare va fi „așa cum e", în consecință nu sunt permise modificări sau dezvoltări de funcționalități pe parcursul perioadei de atribuire.

Se va menționa în Propunerea Tehnică:

- URL-ul de acces al mediului de testare
- Credenţiale de acces pentru: 1 Administrator de sistem; 3 conturi din fiecare tip de utilizator: persoane fizice, juridice și funcționari.

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

- Informații privind faptul că soluția propusă îndeplinește cerințele funcționale solicitate;
- URL-ul la care funcționalitatea poate fi accesată / detalii relevante de navigare pentru a ajunge la funcționalitatea implementată.

### 4.12. Planul de instruire a personalului

Activitatea de instruire ce va fi derulată odată cu momentul în care soluția IT este funcțională și poate fi utilizată de către personalul instituției.

Astfel, va fi furnizat pentru un număr de utilizatori-formatori, membrii ai grupului țintă, număr ce va fi stabilit la momentul aprobării proiectului, un program de instruire pe baza unei metodologii ce va cuprinde cel puțin următoarele condiții:

1. Obiectivul programului va viza îmbunătățirea nivelului de cunoștințe și abilități digitale ale cursanților în vederea folosirii corecte și eficiente la locul de muncă a soluției informatice implementate în cadrul proiectului;
2. Durata activității de instruire va include 2 componente:
   - una de învățare teoretică – câte o sesiune de 6 ore / zi, pe grupe de cursanți; acestea vor include și două module complementare, dedicate temelor orizontale, respectiv dezvoltare durabilă și egalitate de șanse.
   - una de învățare practică – câte două sesiuni de 4 ore /zi, pe grupe de cursanți.
3. Cursanții vor fi supuși unui proces de evaluare/examinare prin care va fi demonstrată dobândirea unor cunoștințe și abilități noi la finalizarea activității de formare/instruire. Procesul de evaluare a cunoștințelor dobândite se va derula la finalul cursului în urma absolvirii procesului de evaluare, cursanții vor primi un certificat de participare emis de entitatea ce furnizează programul de instruire, potrivit rezultatelor obținute de fiecare dintre aceștia.

Cursanții vor forma grupe de curs, potrivit metodologiei și calendarului de lucru propus de furnizor în conformitate cu cerințele, programul sesiunilor de instruire fiind agreat de comun acord astfel încât să permită participarea membrilor grupului țintă, probată prin liste de prezență.

În acest fel, toți membrii grupului țintă și personalul operațional vor deține, la finalul perioadei de implementare a proiectului, informațiile și cunoștințele necesare utilizării serviciilor și funcționalităților proprii soluției informatice implementate prin proiect și abilități crescute în vederea folosirii optime a acestora atât din perspectiva front office - în relație directă cu cetățenii, cât și din perspectivă back office.

## 4.13. Entitatea responsabilă cu implementarea proiectului

- **Denumire instituție:** Direcția de Asistență Socială Drobeta-Turnu Severin
- **Adresa:** Strada Română, nr.1, Municipiul Drobeta-Turnu Severin, Județul Mehedinți
- **CIF:** 15405118

## 4.14. Recomandări privind creșterea capacității manageriale și instituționale

Sub aspectul capacității manageriale se recomandă asigurarea unui nivel ridicat de perseverență în atingerea obiectivelor stabilite manifestat la nivelul tuturor șefilor de structuri din cadrul instituțiilor vizate de procesul de transformare digitală.

Asigurarea unei capacități manageriale solide este esențială pentru exercitarea atribuțiilor funcționale cu eficiență. Se vor avea în vedere:

- **Dezvoltarea competențelor digitale:**
  - **Identificarea nevoilor de formare**: Se vor evalua în mod regulat competențele digitale ale șefilor de structuri existenți și se vor identifica direcțiile în care aceștia ar putea avea nevoie de dezvoltare suplimentară.
  - **Programe de training personalizate:** În funcție de nevoile de dezvoltare se vor organiza programe de training adaptate nevoilor specifice ale șefilor de structuri cu privire la luarea deciziilor, managementul performanței și managementul schimbării.
  - **Mentoring și coaching**: Se vor implementa programe de mentorat și coaching pentru a oferi sprijin individualizat șefilor de structuri pentru a-i ajuta să-și dezvolte abilitățile de a performa în modele de guvernanță digitală instituțională.
  - **Învățare continuă**: Șefii de structuri vor fi încurajați să participe la conferințe, seminarii și cursuri online pentru a se menține la curent cu cele mai bune practici și tendințe în materie de transformare digitală instituțională.
- **Atragerea și reținerea angajaților cu veleități în domeniul administrației digitale:**
  - **Proces de recrutare eficient**: Dezvoltarea unui proces de recrutare riguros, care să identifice candidații cu cele mai potrivite competențe digitale și experiență pentru rolurile disponibile.
  - **Oportunități de dezvoltare în carieră**: Crearea unui mediu în care angajații să aibă oportunități de dezvoltare profesională continuă.

- **Crearea unei culturi la nivel de instituție care să susțină performanța managerială:**
    - **Leadership puternic**: Se vor face demersuri ca liderii organizației să promoveze o cultură instituțională bazată pe tehnologie.
    - **Comunicare deschisă și transparentă:** La nivelul instituției se va încuraja comunicarea deschisă între șefii de structuri și angajați, precum și între diferitele niveluri ale organizației.
    - **Recunoașterea și recompensarea performanței:** Se vor implementa capabilități digitale de evaluare a performanței.
    - **Feedback regulat:** Se va oferi feedback constructiv șefilor de structuri în mod regulat pentru a-i ajuta să-și îmbunătățească performanța.
- **Utilizarea tehnologiei pentru a sprijini managementul:**
    - **Platforme de învățare online:** Se vor utiliza platforme de e-learning pentru a oferi training și dezvoltare profesională tuturor angajaților.
    - **Instrumente de colaborare:** Se vor implementa instrumente online de lucru colaborativ pentru a facilita comunicarea și schimbul de informații între angajați.

### 4.15. Implementarea proiectului TIC

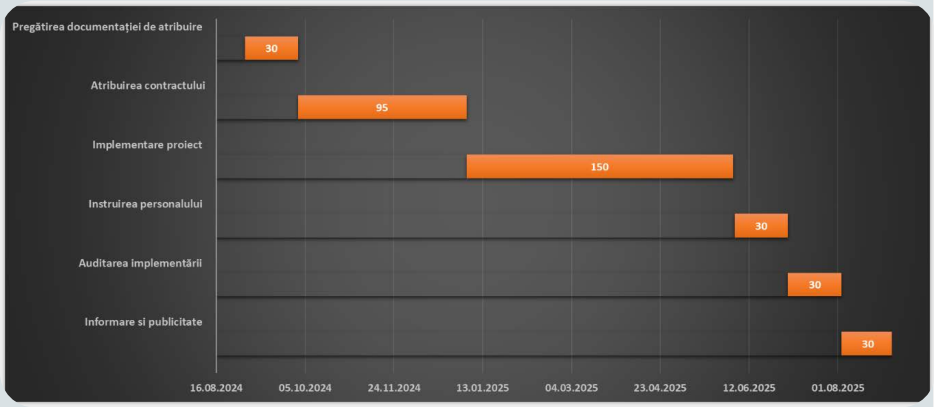
Implementarea proiectului va fi una etapizată, va include toate etapele prevăzute în legislația de specialitate și va respecta întocmai prevederile Ghidului solicitantului.

- **Durata proiectului**

  Proiectul va fi implementat pe o **perioadă de 12 luni** începând **de la momentul semnării contractului de finanțare**, activitățile incluzând pregătirea documentației de atribuire, evaluarea ofertelor, atribuirea și semnarea contractului cu furnizorul selectat și monitorizarea implementării efective.

- **Graficul de implementare**

  Graficul estimativ de implementare al proiectului reflectă etapizarea și activitățile stabilite în cadrul proiectului și respectă intervalul menționat în Ghidul solicitantului. Intervalele evidențiate pot fi ajustate de echipa de proiect în funcție de modul efectiv de derulare a proiectului și de factorii ce vor apărea pe parcursul implementării.




*Figură 1: Graficul estimativ al proiectului*

**Contract:** 4198/15.04.2024

**Beneficiar:** Direcția de Asistență Socială Drobeta-Turnu Severin

**Data:** 11.06.2024
**Întocmit de:** Dorel Constantin Ilași - Director Tehnic

**Furnizor:** APLIX TEHNOLOGIES
**Reprezentant legal:** Alexandra Maria Nedelea - administrator