PROIECT TEHNIC

Digitalizarea administrației publice locale în Comuna Bătrâni

Beneficiar: UAT Comuna Bătrâni
Elaborator proiect tehnic: Civic Soft SRL

Cuprins

1. OBIECTIVELE PROIECTULUI

1.1. Date despre obiectivul de investiție

Prezentul **Proiect Tehnic** este întocmit în contextul lansării apelului de finanțare PRSM/473/PRSM_P1/OP1/ RSO1.2/PRSM_A38 parte din **Programul Regional Sud-Muntenia 2021-2027**, **Prioritatea 1** – O regiune mai competitivă prin inovare, digitalizare și întreprinderi dinamice, **Obiectivul specific RSO 1.2** – Valorificarea avantajelor digitalizării, în beneficiul cetățenilor, al companiilor, al organizațiilor de cercetare și al autorităților publice, **Operațiunea B** – Valorificarea avantajelor digitalizării, în beneficiul cetățenilor, al organizațiilor de cercetare și al autorităților publice, prin investiții în dezvoltarea infrastructurii serviciilor și echipamentelor IT relevante și necesare

UAT Comuna Bătrâni, județul Prahova, ca organ al administrației publice locale, este instituție eligibilă conform prevederilor Ghidului Solicitantului în cadrul prezentului apel de finanțare. Identificând oportunitatea, UAT Comuna Bătrâni a procedat la realizarea demersurilor necesare pentru realizarea unui proiect de transformare digitală și dezvoltare a serviciilor publice digitale pe care instituția le furnizează către cetățeni și mediul de afaceri. Prezentul proiect tehnic a fost realizat pe baza programului de finanțare, a prevederilor ghidului solicitantului și în corelare cu studiul de fezabilitate.

1.2. Date privind obiectivele proiectului TIC

Solicitant/beneficiar	**Comuna Bătrâni - Județul Prahova**
Denumirea proiectului	**„Digitalizarea administrației publice locale în Comuna Bătrâni”**
Denumirea Soluției Informatice	Sistem informatic de gestiune integrată a datelor și documentelor în cadrul comunei Bătrâni
Relevanța față de Obiectivul de politică 1	Proiectul contribuie la realizarea obiectivului de politică 1, respectiv **digitalizarea administrației și a serviciilor publice în cadrul UAT Comuna Bătrâni**
Obiectivele specifice proiectului TIC	1. Modernizarea infrastructurii hardware a instituției 2. Implementarea tehnologiei cloud 3. Digitalizarea serviciilor publice 4. Asigurarea securității cibernetice 5. Creșterea capacității administrative prin dezvoltarea competențelor digitale 6. Asigurarea interconectivității și interoperabilității 7. Asigurarea egalității de șanse
Elaboratorul proiectului tehnic	Civic Soft SRL
Scopul proiectului	Digitalizarea activității UAT Comuna Bătrâni din perspectiva front-office și back-office prin furnizarea serviciilor publice la grad 5 de sofisticare digitală
Activități în implementare vizate în componenta IT	1. Achiziția echipamentelor hardware și software TIC care sprijină digitalizarea, inclusiv servicii de instalare, configurare și punere în funcțiune 2. Achiziția de licențe pentru soluții de tip cloud computing ce vizează: o Aplicații front office - platforme de interacțiune cu cetățenii o Aplicații back office care:

	i. digitalizează procesele administrative ce stau la baza serviciilor publice destinate cetățenilor și mediului de afaceri ii. facilitează gestiunea integrată și accesarea datelor și documentelor emise de mai multe instituții/servicii locale sau servicii/departamente/compartimente din cadrul aceleiași instituții 3. Dezvoltarea la grad 5 de sofisticare a serviciilor publice digitale 4. Implementarea de tehnologii de inteligență artificială care să sprijine incluziunea și egalitatea de șanse **5.** Creșterea capacității administrative în domeniul digitalizării prin pregătirea personalului ce va utiliza soluția de digitalizare precum și pregătirea personalului ce va asigura administrarea soluției
Serviciile publice dezvoltate prin proiect (număr minim)	1. Cerere de restituire 2. Cerere de compensare 3. Cerere istoric rol 4. Cerere de scutire 5. Cerere transfer auto 6. Declarație fiscală pentru stabilirea taxei pentru servicii de reclamă și publicitate 7. Declarație pentru stabilirea valorii reale a lucrărilor executate în baza autorizației de construcție 8. Cerere de activare cont Ghișeul.ro 9. Declarație de impunere pentru stabilirea taxei pentru utilizarea locurilor publice 10. Declarație de încetare a taxei de ocupare a domeniului public 11. Cerere pentru îndreptarea erorilor de plată 12. Declarație de impunere pentru stabilirea taxei de salubrizare 13. Acordarea ajutorului de urgență 14. Acordarea Venitului Minim de Incluziune 15. Acordarea indemnizației de creștere a copilului 16. Acordare alocație de stat 17. Acordare stimulent de inserție 18. Acordare servicii sociale - urgență 19. Acordarea ajutorului de urgență 20. Cerere acordare îngrijire la domiciliu 21. Cerere instituționalizare 22. Cerere indemnizație persoană cu dizabilități 23. Cerere referat pentru scutire de la plata tarifului de utilizare a rețelelor de drumuri naționale 24. Cerere acordare tichete sociale pentru grădiniță 25. Cerere acordare trusou nou-născut 26. Cerere aprobare/încetare indemnizație persoană cu dizabilități 27. Solicitare efectuare anchetă socială 28. Audiențe online
Beneficiile proiectului TIC	➢ Beneficii pentru cetățeni: o Administrația publică accesibilă - toate instituțiile vor fi interconectate în cloud; o Cetățeanul va putea solicita și primi documente de oriunde, oricând; o Economie de timp – fără cozi, fără nicio deplasare fizică la instituțiile publice; o Trasabilitate – cetățeanul va putea avea un istoric al interacțiunilor sale cu administrația;

	○ Siguranță – infrastructura cloud va implementa cele mai avansate sisteme de securitate cibernetică. ➢ Beneficii pentru instituție: ○ Standardizarea modului de lucru; ○ Asigurarea accesului la instrumente de lucru inovative; ○ Asigurarea conformității legale în generarea actelor administrative în format electronic și respectarea condițiilor de valabilitate ale actului administrativ; ○ Va asigura interconectivitate și interoperabilitate sistemelor publice; ○ Va asigura scalabilitate serviciilor publice și va permite un management eficient al costurilor de scalare; ○ Va reduce birocrația, prin eliminarea proceselor administrative redundante sau perimate; ○ Va asigura o mai bună colaborare și o partajare rapidă a informațiilor între toate instituțiile implicate în exercitarea competențelor partajate; ○ Va eficientiza costurile – instituțiile publice vizate nu vor mai fi nevoite să asigure mentenanță pentru echipamentele hardware și software; ○ 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; ○ Protejarea integrată a datelor, aplicațiilor și rețelelor; ○ Gestionarea în mod securizat a accesului la servicii și resurse; ○ Diminuarea riscului de infectare cu malware, prin utilizarea de mecanisme de protecție; ○ Prevenirea atacurilor prin identificarea breșelor de securitate înainte de a fi exploatate sau combaterea acestora din fazele incipiente; ○ Asigurarea managementului vulnerabilităților și aplicarea de patch-uri în vederea remedierii acestora; ○ Protejarea împotriva atacurilor care au ca scop limitarea serviciilor (distributed denial-of- service - ddos); ○ Automatizarea proceselor, notificărilor și a reacțiilor; ○ Minimizarea timpului de reacție în cazul atacurilor cibernetice; ○ 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 de implementare	• Proiectul va fi implementat **la nivel local** în toate structurile UAT Comuna Bătrâni. • Infrastructura va fi cloud și va fi găzduită într-un centru de date ce întrunește condițiile de conformitate, securitate și acreditare prevăzute de lege.
Grup țintă	- Autorități și instituții publice locale și centrale; - Mediul de afaceri; - Societatea civilă, adică consumatori finali ai noilor produse și servicii
Ținta stabilită prin proiect	**RCR11 = 1.292 persoane * 12,3% = 159 persoane** **Notă explicativă: 1.292 persoane (16-74 ani, conform Recensământului Populației și Locuințelor runda 2021 realizat de INS) * 12,3% (ponderea populației interesate să interacționeze cu autoritățile publice conform datelor statistice INS) = 159 persoane*

1.3. Descrierea scenariului tehnico-economic conform Studiului de Fezabilitate

Sub aspect tehnic serviciile publice vor fi dezvoltate pe o Platformă cloud, web-based, de tip Saas, care, pentru atingerea obiectivelor proiectului va include **6 componente critice**:

(1) Managementul identităților electronice și autentificarea (alături de capabilitățile de interconectare cu platforma națională RoeID)
(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
(6) Securitatea și auditul platformei

Aplicația, prin intermediul framework-ului de integrare, va fi capabilă să ”consume” în mod nativ identitățile electronice rezidente în platforma de management al identităților asigurând stocarea, vizualizarea, sortarea și filtrarea istoricului de comunicare al fiecărei identități. Soluția va stoca metadate specifice comunicărilor inter și intra-instituționale precum și stări specifice proceselor din administrația publică.

Soluția va include o componentă de semnare și sigilare electronică calificată ce va presupune atât opțiunea primară, cât una de back-up și care va permite semnarea și sigilarea electronică calificată a documentelor, individuală sau în pachete, direct în fluxul de lucru fără a fi nevoie de descărcarea fișierelor. Fluxurile vor putea fi definite atât inter cât și intra instituțional.

Aplicația va fi integra atât capabilități de comunicare prin formulare electronice de tip smart asigurând conversia automată a conținutului acestora în format PDF cât și **instrumente de inteligență artificială contextuală precum speech to text, text tu speech, traduceri din/în mai multe limbi** având în vedere caracterul incluziv al programului de finanțare.

Aplicația va asigura conformitatea cu prevederile actelor normative europene eIDAS, GDPR și Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului Europei din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, precum și cu standardele europene ETSI EN 319 401 V2.3.1 privind Cerințe generale ale politicii pentru furnizorii de servicii de încredere valabil la momentul derulării procedurii de atribuire, respectiv ETSI EN 319 521 V1.1.1 (2019-02) privind Politica și cerințele de securitate pentru furnizorii de servicii de livrare electronică înregistrată.

Soluția trebuie să integreze în mod unitar și armonios componente de:

- Interfața grafică
- Autentificare
- Registratură fizică digitalizată și registratura online automatizată
- Arhiva electronică automatizată și arhivă fizică retro digitalizată
- Managementul fluxurilor de lucru cu documente / acte
- Semnare electronica calificată în browser - Guvernanță digitală a drepturilor de semnare la nivelul întregii instituții
- Sigilare electronică calificată în cloud, integrare cu furnizorii autorizați de servicii de încredere
- Comunicare electronică și Chat integrat în sistem
- Notificări (de sistem si de tip push în aplicația mobilă)
- Formulare electronice atât pentru uzul utilizatorilor externi (cetățeni, mediul de afaceri, colaboratori, furnizori, etc), cât și pentru uzul intern al angajaților.

- Comunicare externă - Interconectivitatea cu un număr nelimitat de instituții ale administrației publice centrale si locale, deconcentrate sau de orice alt tip câtă vreme există o formă de constituire legală și un canal de comunicare asumat oficial de către aceasta

- **Managementul identităților electronice și autentificarea –** managementul identităților electronice va adresa următoarele aspecte cheie:
  - Stabilirea identității electronice a persoanelor fizice și persoanelor juridice (inclusiv alte instituții) la nivelul sistemului;
  - Stabilirea identităților electronice ale structurilor interne ale instituției și ale angajaților din aceste structuri (ex. configurarea soluției informatice prin virtualizarea instituției, crearea identităților electronice ale angajaților, etc.);
  - Stabilirea setului de validări necesare asigurării unui control eficient al acurateței datelor;
  - Identificarea și autentificarea în sistemul informatic;
  - Procesul de administrare a drepturilor de acces specifice fiecărui tip de utilizator;
  - Procedurile de actualizare și auditare a accesului la datele cu caracter personal;
  - Integrările necesare pentru asigurarea unor identități precise pentru fiecare entitate în parte (interconectare cu ANAF, RECOM, servicii de încredere);
  - Nomenclatoarele de obiecte necesare managementului identităților (ex. Nomenclator stradal, nomenclatorul unităților administrativ-teritoriale, nomenclatorul instituțiilor publice, nomenclatorul tipurilor de persoane juridice, etc.);
  - Parametrizarea motoarelor de căutare (ex. structuri de filtre, sortări, vizualizări, etc.);
  - Parametrizarea de rapoarte specifice mentenanței identităților;
  - Aspectele de securitate specifice managementului identităților (ex. stabilirea gradului de dificultate al parolelor de acces, asigurarea unicității identității la nivel de sistem, autentificarea multifactor, semnătura electronică calificată și sigiliul electronic calificat etc.)

  ***Notă:** Managementul identităților se va face centralizat în conformitate cu prevederile regulamentului eIDAS și ale standardului ETSI EN 319 521 V1.1.1 din februarie 2019*

- **Înregistrarea operațiunilor administrative și managementul documentelor** – Înregistrarea operațiunilor administrative va adresa următoarele aspecte specifice activității instituțiilor publice:
  - Stabilirea structurilor de date ce definesc operațiunile și actele administrative la nivelul sistemului;
  - Modalitatea de înregistrare a operațiunilor administrative și a actelor administrative și de evitarea a dublei înregistrări;
  - Modalitatea de generare a registrelor la nivelul instituției și mentenanța multianuală a acestora;
  - Modalitatea de acordare a numerelor de înregistrare și de asigurare a unității acestora la nivel de sistem;
  - Definirea și operaționalizarea procedurilor de registratură fizică și registratură online;
  - Modalitatea de repartizarea a lucrărilor;
  - Stabilirea și gestionarea drepturilor de acces la registrele de înregistrări;
  - Sincronizarea registrelor cu arhiva electronică;

- Parametrizarea motoarelor de căutare (*ex. structuri de filtre, sortări, vizualizări, etc.*);
- Parametrizarea de rapoarte specifice gestiunii registrelor electronice și stabilirea drepturilor de acces la rapoarte;
- 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.*).

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

- **Arhivarea și îndosarierea electronică –** arhivarea electronică a documentelor va adresa problematica specifică referitoare la următoarele aspecte:
  - Asigurarea procedurilor de creare și parametrizare multianuală a nomenclatorului arhivistic (grupele de documente);
  - Gestionarea structurilor de metadate pentru documentele arhivate;
  - Asigurarea procedurilor de creare și parametrizare multianuală a structurii de îndosariere a actelor (dosarele de acte);
  - Acordarea drepturilor de acces la grupele și dosarele de documente;
  - 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.

***Notă:** Arhivarea electronică se va face în conformitate cu prevederile legale referitoare la arhivarea documentelor electronice*

- **Semnarea și sigilarea electronică calificată în cloud –** va adresa nevoile specifice ce țin de gestionarea fluxurilor de avizare și aprobare după cum urmează:
  - Sincronizarea semnăturii electronice calificate cu platforma pentru a operaționaliza fluxurile de avizare / aprobare configurate în activitatea curentă;
  - Apelarea serviciilor API pentru semnare și sigilare electronică calificată;
  - Crearea și managementul dinamic al fluxurilor de semnare consecutive sau concomitente (inclusiv anularea și reconfigurarea acestora);
  - Stabilirea, configurarea și managementul motivelor de semnare;
  - Crearea și întreținerea listelor de semnatari și a competențelor lor de semnare;
  - Asigurarea serviciilor de validare a semnăturilor electronice calificate aplicate documentelor;

- Poziționarea semnăturilor pe document în funcție de context;
- Integrarea semnăturii olografe în semnătura electronică calificată;
- Autentificarea securizată în serviciul de semnare și semnarea documentelor fără ca acestea să părăsească sistemul;
- Integrarea cu componenta de management a identităților, cu cea de management al înregistrărilor, cu cea de interconectivitate și interoperabilitate multiinstituțională și cu arhiva electronică;
- Asigurarea serviciilor de semnare multi-vendor (*ex. sistemul să suporte semnarea electronică în flux cu semnături electronice de la mai mulți furnizori*);
- Asigurarea procedurilor de semnare cross-platforme (*ex. o sesiune de semnare să poată parcurge mai multe platforme informatice*).

- **Securitatea și auditul platformei –** componenta de securitate va adresa nevoile specifice:
  - Implementarea politicilor si procedurilor de securitate ce privesc comunicația între utilizatori;
  - Implementarea instrumentelor de autentificare și autorizare pe baza rolurilor deținute de fiecare utilizator la nivel de sistem;
  - Protejarea împotriva accesului neautorizat în sistem;
  - Administrarea drepturilor de acces și parametrizarea algoritmilor de autorizare automată la conținutul din platformă al utilizatorilor;
  - Implementarea de mecanisme de asigurare a integrității datelor și a restituirii acestora în situația unor incidente operaționale sau de securitate;
  - Implementarea procedurilor de creare, gestionare și criptare a credențialelor de acces la sistem;
  - Capturarea motivelor de acces la date;
  - Crearea și întreținerea dinamică a sistemului de loguri
  - Stabilirea instrumentelor de monitorizare a platformei

2. CERINȚE PRIVIND SOLUȚIA TEHNICĂ

2.1. Cerințe generale. 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. Redăm 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 conceput și implementat în așa fel încât să contribuie la atingerea obiectivelor strategice ale instituției.
2. **Planificarea 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 rezultatul 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, nerelaționare, NoSQL), fiecare cu propriile avantaje și dezavantaje. Alegerea depinde de volumul și de tipul de date care trebuie stocate și de cerințele de performanță.

3. **Infrastructura 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 IOT, 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.

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 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 să fie 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.

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 respectă 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;
- Instrumente de inteligență artificială

Pentru a asigura o accesibilitate sporită serviciilor ce vor fi dezvoltate și pentru asigurarea respectării principiului egalității de șanse autoritatea contractantă are în vedere integrarea contextuală a instrumentelor de inteligență artificială (IA) precum face recognition, speech to text, text to speech, navigare cu comandă vocală, traduceri automatizate din mai multe limbi de circulație internațională. In

acest sens, modalitatea de implementare a acestor tehnologii inovative va trebui să fie documentată și dovedită în procedura de atribuire. Tehnologiile trebuie să suporte limba română la un nivel calitativ ridicat.

2.5. Prevederi de securitate

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.

2.6. Aspecte privind incluziunea, nediscriminarea și egalitatea

- Cerințe funcționale privind **designul universal:**

1. **Utilizare echitabilă**
   - **Eliminarea barierelor**: Serviciile digitale vor fi implementate într-un mod care va elimina barierele de acces pentru persoanele cu dizabilități cum ar fi barierele de navigare, de percepție a informațiilor sau de interacțiune.

- **Opțiuni alternative**: Se vor oferi opțiuni alternative de accesare a informațiilor și de utilizare a serviciilor cum ar fi versiuni text ale conținutului audio-video, formulare online care pot fi completate și vocal sau posibilitatea de a mări/micșora textul
- **Evitarea discriminării**: Designul în care vor fi expuse serviciile publice digitale va evita orice formă de discriminare, directă sau indirectă, pe bază de dizabilitate, sex, vârstă, origine etnică sau orice alt criteriu.

2. **Flexibilitate în utilizare**
   - **Adaptabilitate**: Serviciile digitale trebuie să fie adaptabile și să se modeleze conform situației particulare a fiecărui solicitant
   - **Accesibilitate**: Soluția de furnizare a serviciilor publice trebuie să poată fi accesată de pe orice tip de dispozitiv precum computere, tablete, telefoane mobile și să se adapteze la orice tip de ecran.
   - **Opțiuni de interacțiune**: Se conferă diverse opțiuni de interacțiune cu platforma cum ar fi utilizarea mouse-ului, a tastaturii, a comenzilor vocale ori a tehnologiilor assistive.
3. **Utilizare simplă și intuitivă**
   - **Claritate și simplitate**: Informațiile vor fi prezentate într-un limbaj clar, concis și ușor de înțeles, evitând jargonul sau termenii tehnici.
   - **Structură logică**: Soluția ce va fi implementată va dispune în mod obligatoriu de o structură logică și ușor de navigat cu meniuri intuitive și o organizare clară a informațiilor.
   - **Ghidare și asistență**: Utilizatorilor li se va oferi ghidare și asistență prin tutoriale, instrucțiuni video, chat și posibilitate de video call.
4. **Informațiile să fie perceptibile**
   - **Contrast și lizibilitate**: Soluția va asigura un contrast adecvat între text și fundal, iar textul va fi lizibil și ușor de perceput indiferent de condițiile de iluminare sau de abilitățile vizuale ale utilizatorului.
   - **Modalități multiple de prezentare**: Informațiile vor fi prezentate în mai multe modalități precum text, video, audio etc.
5. **Toleranță la eroare**
   - **Prevenirea erorilor**: Designul o să prevină erorile prin validarea datelor introduse de utilizatori oferind mesaje de eroare corespunzătoare
   - **Corectarea erorilor**: Se va oferi posibilitatea de a corecta erorile ușor și rapid fără a pierde date introduse anterior.
   - **Mesaje de eroare clare**: Mesajele de eroare vor fi clare, concise și informative indicând clar natura erorii și modul de remediere.
6. **Efort fizic scăzut**
   - **Comenzi vocale**: Se va oferi posibilitatea de navigare prin voce ori de transpunere a vocii în text
   - **Design ergonomic**: Interfața ce se dorește a fi implementată prin proiect trebuie să fie concepută ergonomic pentru a minimiza oboseala și disconfortul utilizatorilor
7. **Dimensiuni și spațiu pentru acces și utilizare**:
   - **Mărirea textului**: Utilizatorii vor putea mări textul sau alte elemente de pe ecran fără a afecta lizibilitatea sau funcționalitatea.
   - **Spațiere adecvată**: Se va asigura o spațiere adecvată între elementele de pe ecran pentru a facilita navigarea și a evita aglomerarea vizuală
   - **Compatibilitate cu tehnologiile assistive**: Platforma ce se dorește a fi implementată prin proiect va fi în mod obligatoriu compatibilă cu diversele tehnologii assistive cum ar fi cititoarele de ecran, lupă de ecran etc.

- Cerințe funcționale privind **adaptarea rezonabilă:**

1. **Pentru persoanele cu dizabilități de vedere**

a. **Compatibilitate cu cititoarele de ecran** astfel încât persoanele cu dizabilități de vedere să poată naviga și accesa informațiile cu ușurință
b. **Contrast de culoare adecvat**: Platforma trebuie să asigure un contrast suficient de mare între text și fundal ori să permită modificarea acestuia pentru a facilita citirea pentru persoanele cu deficiențe de vedere
c. **Opțiuni de mărire a textului**: Platforma trebuie să permită utilizatorilor să mărească dimensiunea textului, fără a afecta formatarea sau lizibilitate
d. **Navigabilitatea prin tastatură**: Platforma trebuie să permită navigarea în întregime folosind doar tastatura, fără a fi nevoie de mouse

2. **Pentru persoanele cu dizabilități de auz**
   a. **Subtitrări pentru conținut video**: Materialele video trebuie să fie însoțite de subtitrări pentru a fi accesibile persoanelor cu deficiențe de auz
   b. **Transcrieri text**: Pe lângă subtitrări este util să se ofere și transcrieri text are materialelor audio/video.
3. **Pentru persoanele cu dizabilități cognitive**
   a. **Limbaj simplu și clar:** Informațiile trebuie prezentate într-un limbaj simplu, clar și concis, ușor de înțeles
   b. **Structură clară și organizată:** Platforma trebuie să aibă o structură clară și organizată, cu meniuri și navigare intuitive
   c. **Opțiuni de personalizare**: Platforma poate oferi opțiuni de mărire/micșorare a fontului sau schimbare a acestuia pentru a fi mai ușor de citit
4. **Pentru persoanele cu dizabilități motorii:**
   a. **Compatibilitate cu tehnologiile asistive**: Platforma trebuie să fie compatibilă cu tehnologii asistive precum voice-to-text, text-to-speech, speech-to-navigation,
   b. **Timp suficient pentru completarea formularelor**: Se va acorda timp suficient pentru completarea formularelor online, pentru a permite persoanelor cu dizabilități motorii să le completeze fără dificultate.
5. **Alte adaptări rezonabile**:
   a. **Opțiuni de limbă**: Platforma trebuie să fie disponibilă în mai multe limbi, inclusiv în limbile minorităților naționale
   b. **Feedback și suport**: Se va oferi un mecanism ușor de utilizat de a oferi feedback și a solicita suport

3. DESCRIEREA TEHNICĂ A PROIECTULUI

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.

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

3.1. Cerințele funcționale ale sistemului

Dezvoltarea serviciilor publice digitale în cadrul UAT Comuna Bătrâni reprezintă un demers complex ce implică o serie de soluții tehnice pentru furnizare lor de către instituție la gradul 5 de sofisticare digitală. Astfel ele trebuie expuse prin intermediul unui sistem informatic care să **(1)** prezinte capabilități de interconectare și interoperabilitate pentru schimburile de date (ex. serviciile să poată fi accesate prin și

intermediul identității electronice create de platforma națională RoeID), **(2)** să fie accesibil de pe orice dispozitiv, **(3)** să poată gestiona atât depunerea solicitărilor pentru serviciile publice (front-office) cât și **(4)** gestiunea internă a procedurilor operaționale de furnizare a respectivului serviciu (back-office). În egală măsură, pentru furnizarea acelor servicii ce implică schimburi de date cu alte instituții, platforma trebuie să prezinte capabilitățile tehnice de comunicare bidirecțională cu alte entități, atât ale administrației publice centrale, ale administrației publice locale, cât și cu entități private.

Pentru transpunerea serviciilor comunei Bătrâni complet în mediul digital soluția trebuie să asigure:

- Deplina conformitate cu legislația națională și europeană în ceea ce privește activitățile administrației publice și gestionarea serviciilor publice aflate în responsabilitate;
- Standardizare și uniformizarea proceselor interne și a instrumentarului digital utilizat la nivelul tuturor instituției;
- Interconectarea și interoperabilitatea între instituții și sisteme;
- Asigurarea pentru cetățeni și mediul de afaceri a unui punct de acces centralizat la serviciile publice gestionate de instituție;
- Transpunerea completă a modului de lucru de la cel tradițional, pe hârtie, la digital;
- Realizarea e-guvernării depline la nivel instituțional;
- Implementarea măsurilor de securitate cibernetică;
- Asigurarea egalității de șanse, de gen, a incluziunii și nediscriminării

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 un sistem informatic de gestiune integrată a datelor și documentelor, sistem de tip Saas, 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) (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.

(10) Legea nr. 214 din 5 iulie 2024 privind utilizarea semnăturii electronice, a mărcii temporale și prestarea serviciilor de încredere bazate pe acesta

Proiectul TIC va implementa conceptul de administrație digitală la nivel local în cadrul comunei Bătrâni 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 prestate de solicitant. 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 structurile instituției și la toate serviciile publice dezvoltate prin proiect.

Proiectul TIC urmărește să eficientizeze activitatea angajaților 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 instituției 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.

3.2. Cerințe generale specifice platforma de gestiune integrată a datelor și documentelor

Soluția informatică va face posibilă transmiterea datelor între expeditor și destinatar prin mijloace electronice și va furniza dovezi referitoare la manipularea datelor transmise (inclusiv dovada trimiterii și

primirii datelor) și care protejează datele transmise împotriva riscului de pierdere, furt, daune sau orice modificări neautorizate. Datele generate în interiorul platformei care dovedesc că 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 (UE) nr. 910/2014 și din standardele tehnice ETSI asociate.

3.2.1. 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.

3.2.2. 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.

  Mijloace de stabilire a identității electronice pot fi:

  - Prin prezența fizică a individului (în cazul persoanelor fizice) sau a reprezentantului persoanei 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 de Regulamentul (UE) 910/2014 (eIDAS)
  - Cu ajutorul unui certificat calificat emis de un furnizor de servicii de încredere calificat în conformitate cu prevederile regulamentului
  - Alte metode de identificare recunoscute la nivel național care furnizează garanții similare prezenței fizice

  Procesul de stabilire a identității electronice a utilizatorului trebuie parcurs într-un mediu sigur și controlat, toate dovezile rezultate în urma acestuia (inclusiv consimțământul persoanei) trebuie capturate și stocate la nivelul platformei.

Toate evenimentele referitoare la identitatea inițială a utilizatorului și a autentificărilor ulterioare trebuie jurnalizate.

În cazuri speciale în care stabilirea identității electronice a utilizatorului nu poate fi construită respectând cerințele menționate anterior, deși identificarea fizică a avut loc (ex. persoana refuză crearea identității la nivelul sistemului informatic) se vor reține la nivelul sistemului indicii preliminare de identitate și dovezi clare ce stabilesc răspunderea operatorului care a procesat informația (ex. log-uri de sistem)

- **Autentificarea**

Platforma trebuie să îi permită autentificarea utilizatorului înainte ca acestuia să i se acorde acces la conținutul din platformă.

Mijloacele de autentificare pot fi:

- Mecanisme de autentificare multi-factor
- Semnătura 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 (cetățeni, persoane juridice, angajați)

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;

- Prin intermediul identității electronice existente la nivelul platformei naționale de identitate digitală RoeID prin intermediul interconectării și schimbului de date între platformele electronice
- Credenţiale de acces (utilizator și parolă), caz în care se va aplica unul din următoarele nivele suplimentare:
- Dispozitiv de autentificare hardware cu 2 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 platformei trebuie să includă funcționalități 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 orice circumstanță, pagina principală 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 peroane fizice și persoane juridice și să prezinte cumulativ, în mod transparent, potențialilor utilizatori:

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

3.2.3. Cerințe privind evenimentele din cadrul platformei și dovezile acestora

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

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

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

3.2.4. Alte cerințe specifice

Având în vedere că infrastructura de bază pentru dezvoltarea serviciilor digitale 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 aflate în aceeași locație (colocate) 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.
- **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 personalului specializat
- **Activități de recuperare în caz de dezastru**
  - La nivelul furnizorului trebuie să existe un plan de continuitate al afacerii care trebuie respectat ori de câte ori este cazul

3.3. Arhitectura funcțională a sistemului

Soluția trebuie să integreze în mod unitar și armonios componente de:

- Interfața grafică
- Autentificare
- Registratură fizică digitalizată și registratura online automatizată
- Arhiva electronică automatizată și arhivă fizică retro digitalizată
- Managementul fluxurilor de lucru cu documente / acte
- Semnare electronica calificată în browser - Guvernanță digitală a drepturilor de semnare la nivelul întregii instituții
- Sigilare electronică calificată în cloud, integrare cu furnizorii autorizați de servicii de încredere
- Comunicare electronică și Chat integrat în sistem
- Notificări (de sistem si de tip push în aplicația mobilă)
- Formulare electronice atât pentru uzul utilizatorilor externi (pacienți, colaboratori, furnizori, etc), cât și pentru uzul intern al angajaților.

- Comunicare externă - Interconectivitatea cu un număr nelimitat de instituții ale administrației publice centrale si locale, deconcentrate sau de orice alt tip câtă vreme există o formă de constituire legală și un canal de comunicare asumat oficial de către aceasta

3.3.1. Interfața Grafică

Interfața grafică a soluției ofertate trebuie să fie conformă cu bunele practici în materie de web-design („Web Content Accessibility Guidelines") și să respecte următoarele cerințe:

- **Intuitivă**
    - Elementele de design se regăsesc în pagină urmând o logică elementară și ușor de folosit (titluri, subtitluri, meniuri, opțiuni etc) – interfața destinată funcționarilor trebuie să urmeze logica administrativă, terminologia și instrumentele de lucru specifice mediului administrației publice
    - Denumirile butoanelor să fie relevante și să respecte modelele standardizate la nivelul industriei
    - Existența butonului „Ajutor" acolo unde este reală nevoie de explicații suplimentare.
- **Predictibilă**
    - Elementele grafice (butoane, iconițe, meniuri, câmpuri bifă („check box"), butoane tip radio etc.) să se comporte conform standardelor industriei – toate aceste ele-mente trebuie să se comporte conform cu standardele de experiență utilizator existente la nivel global
- **Minimalistă**
    - Fiecare fereastră a soluției trebuie cuprindă strictul necesar de elemente și să nu creeze un sentiment de povară din punct de vedere vizual pentru utilizator
- **Încărcare rapidă**
    - Autoritatea contractantă va testa viteza de încărcare a soluției ofertate cu instrumente de auditare independente și va extrage rapoarte de performanță detaliată a soluției
- **Să prezinte cu claritate opțiunile de lucru**
    - Opțiunile pe care utilizatorul le are (lista „drop-down", meniuri, sub meniuri) să fi clare, contextuale și să nu prezinte informație reziduală (de care utilizatorul nu are nevoie in contextul în care se află)
- **Să comunice ușor cu utilizatorul**
    - Soluția ofertată trebuie să dispună de un sistem de notificări în timp real care să însoțească operațiunile care sunt în curs de derulare sau doar ce au fost realizate, cum ar fi spre exemplu mesajul este in curs de trimitere, mesajul a fost trimis, documentele au fost semnate, documentele au fost arhivate, a apărut o eroare, etc
    - Comunicarea să se facă preponderent prin imagini și iconițe – textul trebuie evitat cât de mult posibil
- **Să folosească stiluri personalizate în funcție de acțiunile făcute de utilizator**
    - Butoanele de acțiune să aibă o formatare standardizată (forma, culoare, mă-rime, etc)
    - Elementele și simetria input-urilor de tip text să creeze un sentiment de ordine și claritate la navigarea prin pagină

- **Să fie atractivă**
    - Având în vedere paleta foarte largă de audiență urmărită nuanțele de culoare trebuie sa fie din cele generaliste utilizate de platformele de social media
- **Să fie personalizabilă**
    - Interfață trebuie să beneficieze de elemente de personalizare precum nume prenume, poza de profil, etc.
- **Să gestioneze erorile în mod prietenos**
    - Va fi verificată capabilitatea soluției ofertate de a permite utilizatorului posibilitatea de a reveni în pagina anterioară
    - Ieșirea accidentală din pagină trebuie prevenită prin mesaje de avertizare
- **Să folosească o terminologie specifică fiecărui tip de utilizator**
    - Terminologia pentru interfețele utilizatorilor persoane fizice și persoane juridice să fie una generalistă care să permită utilizatorului înțelegerea cu ușurință a sensului cuvintelor și descrierea funcționalităților – acolo unde este necesar se va verifica existența tul-tip-urilor explicative.
- **Să prezinte un număr optim de alegeri pe care utilizatorul le poate face**
    - Opțiunile de alegere („drop list”, meniuri, sub meniuri, etc) puse la dispoziția utilizatorului trebuie filtrate contextual în funcție tipul de identitate (persoană fizică sau juridica), instituție, identitate profesională, rol deținut la nivelul instituției, compartiment, astfel încât numărul de opțiuni să reflecte specificul activității și contextul particular în care utilizatorul se află.
- **Să ofere explicații contextuale cu privire la funcționalități**
    - Existența tooltip-urilor explicative și structura acestora
    - Butoane de ajutor contextual care să ajute utilizatorul să înțeleagă funcționalitatea folosită
- **Să dispună de validări relevante pentru formularele ce trebuie completate**
    - La nivelul tuturor interfețelor si formularelor web folosite pentru interacțiunea utilizatorului cu soluția informatică vor fi verificate existența validărilor de conținut menite asigura corecta și completa colectare a datelor.

Interfața grafică a soluției ofertate trebuie să fie una personalizată în funcție de tipul de utilizator care să permită o interacțiune eficientă și un nivel de confort superior tuturor tipurilor de utilizatori.

Interfața va fi disponibilă cel puțin în limba română.

Interfața va respecta cerințele privind designul universal și adaptarea rezonabilă pentru a permite oricui accesul facil la servicii publice digitale, respectând astfel incluziunea, egalitatea și principiile nediscriminării.

3.3.2. Autentificare

Soluția informatică trebuie să dispună de o singură pagină de înregistrare și autentificare pentru toate tipurile de utilizatori (angajați, cetățeni, persoane juridice, colaboratori, furnizori, etc.).

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.

Ofertantul va menționa care dintre următoarele metode de autentificare va fi folosită:

- Credenţiale de acces (utilizator și parolă)
- Semnătură electronică calificată

Dacă autentificarea în soluția informatică se face pe bază de credenţiale de acces ofertantul va menționa pe care dintre următoarele metode 2FA le folosește soluția:

- Token Hardware 2FA
- OTP via SMS sau email
- Token Software
- Push Notifications 2FA
- Alte forme de 2FA bazate pe infrastructura de autentificare a dispozitivului utilizat (ex. voice / face recognition, fingerprints, etc)

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

- Validarea identității
- Validarea parolei
- Confidențialitatea parolei
- Vizualizare parolă
- Recuperare nume de utilizator
- Recuperare parolă
- Validare 2FA
- Revalidare 2FA

Soluția 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 soluției trebuie să permită inițierea procesului de „onboarding" (înregistrarea utilizatorilor persoane fizice și persoane juridice) și să prezinte în mod transparent potențialilor utilizatori:

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

Soluția trebuie să pună la dispoziția potențialilor utilizatori un canal de suport permanent prin care aceștia să poată beneficia de suport în procesul de onboarding. Canalul de comunicare destinat suportului potențialilor utilizatori în perioada premergătoare înregistrării / autentificării trebuie să fie securizat și protejat împotriva atacurilor cibernetice.

3.3.3. Registratura Electronică

Registratura electronică va fi utilizată în scopul operaționalizării înregistrării și evidenței intrărilor și ieșirilor de corespondență de către personalul dedicat din cadrul instituției, atât pentru corespondența primită fizic, cât și pentru cea recepționată sau expediată prin mediul online.

Funcțiile registraturii

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

- recepția și repartizarea actelor intrate în instituție
- expedierea actelor către entități externe instituției
- circulația actelor de uz intern.

Instrumentarul administrativ

Registratura va fi structurată ținându-se cont de instrumentarul relațional clasic administrativ, respectiv **LUCRARE - ACT – DOSAR.**

Astfel:

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

Tipuri de registratură

Având în vedere nevoile specifice administrației publice autoritatea contractantă dorește instalarea unei soluții informatice care să adreseze într-o manieră standardizată și integrată următoarele componente specifice activității de registratură:

- Activitatea de registratură fizică digitalizată – respectiv intrările de solicitări și ieșirea de corespondență prin ghișeele instituției
- Activitatea de registratură online automatizată – intrările și ieșirile realizate direct prin mediul virtual

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

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

- Are un autor (cu o identitate efectivă / neefectivă / indicii preliminare de identitate)
- Are un conținut care reflectă ceva ce a fost spus, făcut sau agreat
- Este semnat și asumat în nume personal sau al altei persoane

- A făcut obiectul unui proces de avizare/aprobare conform unui cadrul procedural intern
- A făcut sau nu a făcut obiectul unui proces de înregistrare (are număr de înregistrare)
- Poate origina într-un sistem electronic sau reprezintă o copie semnată electronic calificat pentru conformitate cu originalul a unui document pe hârtie.

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

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

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

- Prezinta indicii clare ale autorului documentului
- Poartă identitatea vizuală a instituției emitente
- A parcurs un proces de semnare, avizare si aprobare agreat formal la nivelul instituției emitente
- A fost înregistrat cu număr de înregistrare unic în evidențele instituției emitente

Cerințe specifice privind actele electronice

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

- Să asigure încărcarea de fișiere în sistem individual sau prin serii/loturi, atât prin butoane de încărcare, cât și prin operațiuni tip „drag and drop” și „copy-paste” – încărcarea trebuie să se poată face din arhiva electronică la care are acces și din calculator
- Să asigure ștergerea fișierelor electronice din sistem, cu excepția celor care au fost arhivate electronic a căror ștergere nu este permisă.
- Să asigure conversia (automat și manual) în format PDF a fișierelor din surse externe sistemului încărcate în sistem și a celor redactate in sistem (minim următoarele formate de fișiere electronice jpg, jpeg, bmp, png, doc, docx, odf)
- Conversia în format PDF trebuie să poată fi făcută atât individual, cât și în loturi.
- Să aibă integrată o procedură electronică de conformare cu originalul prin semnarea electronică calificată de către funcționar.
- Conformarea cu originalul prin semnare electronică calificată trebuie să poată fi făcută atât individual, cât și în loturi.
- Să asigure versionarea documentelor electronice aflate în proces de a deveni acte (aflate pe fluxurile de avizare, aprobare, înregistrare)
- Să poată asigura colectarea cu ușurință a tuturor meta datelor 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 si 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.
- La semnarea electronică să permită inserarea de elemente vizuale în formate .jpg, .jpeg, .png, cum ar fi sigla, semnătură olografă, etc. Semnarea electronică calificată trebuie să poată fi făcută atât individual cât și în serii/loturi.
- Să permită utilizatorului amplasarea semnăturii electronice calificate astfel încât să nu se suprapună cu textul. Dacă documentul încărcat în sistem are factor de rotire amplasarea semnăturii electronice trebuie să țină cont de acest element.
- Să dispună de facilități de arhivare electronică, precum și facilități de stocare (stocare)
- Să aibă implementate politici de control al dimensiunii fișierelor
- Să dispună de capabilități de separare a paginilor unui document și salvarea ca documente diferite, de ordonare / reordonare a paginilor în cadrul aceluiași document, de concatenare a mai multor fișiere
- Să implementeze servicii de încredere în înțelesul Regulamentului UE nr. 910/2014, respectiv să asigure crearea, verificarea și validarea semnăturilor electronice, a sigiliilor electronice dintr-un document / 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 asigura capabilitatea de face referințe electronice actelor electronice către un număr nelimitat de dosare electronice.
- Actele electronice vor putea fi salvate pe grupe acte specifice activității fiecărui structuri din organigrama
- Să permită configurarea drepturilor de acces
- Să asigure capabilități de configurare a drepturile de acces la grupe atât pentru scriere cât și pentru citire cât pentru scriere. 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 in care a fost înregistrat este interzisă.
- În relația lor cu dosarele electronice, actele electronice vor putea face obiectul următoarelor operațiuni:
    - Salvarea în dosar
    - Ștergere din dosar
    - Mutare în alt dosar
    - Creare referință în alt dosar
    - Comparare fișiere
- Să permită gruparea actelor pe grupe care vor putea face obiectul următoarelor tipuri de operațiuni:
    - Crearea si 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:

- Tipul lucrării
- Numărul de înregistrare al lucrării (pentru cele înregistrate)
- Denumirea lucrării
- Data și ora creării
- Data și ora înregistrării
- Data și ora primirii
- Data finalizării
- Modalitatea de finalizare
- Cronologia lucrării - succesiunea de acțiuni și evenimente consemnate în conținutul lucrării marcate temporal
- Datele despre participanții la lucrare, rolurile pe care aceștia îl au în lucrare și starea acestora
- Conținutul lucrării – poate include mesaje, idei, sugestii, argumente, puncte de vedere, etc.
- Documentele/Actele lucrării
- Informații despre eventuale conexări
- Guvernanța lucrării – setul particular de reguli și acțiuni care guvernează lucrarea în funcție de tipul ei
- Starea lucrării (ex. de stări – fără a fi obligatorii sau limitate la acestea – ne-înregistrată, în lucru, finalizată, etc.)
- În funcție de experiența de utilizare creată la nivelul soluției ofertate (la latitudinea furnizorului), 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, contor de mesaje, durata, etc)

Cerințe specifice privind lucrările electronice

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

- Să dispună de o secțiune de evidență a lucrărilor la care participă angajatul
- Să permită vizualizarea tuturor lucrărilor la care utilizatorul participă în format listă / tabel
- Să permită filtrarea / sortarea / căutarea lucrărilor în funcție de atributele menționate la secțiunea „Cerințe conceptuale despre lucrări”
- Să permită utilizatorului crearea / editarea / semnarea / configurarea și expedierea lucrărilor pe fluxurile de lucru în funcție de tipul lor
- Să permită semnarea multiplă de lucrări (cu toate fișierele atașate) și expedierea automatizată a acestora pe fluxurile prestabilite – ex. pachete de lucrări
- Expedierea trebuie să se facă ca tranzacție și aibă implementate proceduri de „fallback” în cazul în care apar erori în procesul de prelucrare si expediere.

- Să permită expedierea automată a lucrărilor electronice către destinatari în serii mari (ex. zeci, sute, mii, zeci de mii, sute de mii de lucrări deodată acolo unde se impune) – expedierea trebuie să tranziteze operațiunea de sigilare electronică calificată și să permită destinatarilor să revină cu răspuns către instituție.
- Expedierea trebuie să se poată face atât în interiorul sistemului, cât și în afara lui.
- Soluția informatică trebuie să furnizeze rapoarte de progres de expediere și, în cazul în care în procesul de expediere au apărut erori, acestea sa fie capturate pentru a permite funcționarilor analizarea lor.
- Să 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.
- Să dispună de o secțiune pentru arhivarea lucrărilor finalizate
- Să permită vizualizare istoricului detaliat al fiecărei lucrări la care a participat
- Să dispună de un contor de lucrări care să se actualizeze funcție de filtrele aplicate în lista de lucrări
- Să aibă definită la nivel de sistem o Procedura de Predare-Primire a lucrărilor
- Secțiunea de evidență a lucrărilor să fie integrată cu Registratura electronică a instituției, Arhiva electronică a instituției, Componenta de semnare și sigilare electronică calificată
- Să permită încărcarea de fișiere din calculator și din arhivele electronice aflate la dispoziția utilizatorului
- Să integreze nomenclatorul arhivistic electronic pentru a permite utilizatorului sa salveze fișierele pe grupe și dosare electronice
- Să dispună în procesul de editare al unei lucrări de toate capabilitățile sistemului prezentate la actele electronice
- Să dispună de editoare de fișiere / mesaje text online ce includ elementele de formatare text standardizate la nivelul platformelor web
- 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 specifica la momentul redactării lucrării celorlalți participanți (activ, în concediu, suspendat, etc)
- Să dispună de nomenclator de procese cu guvernanță predefinită care să permită filtrarea în pagina utilizatorului doar a acelor tipuri de procese conforme cu competența sa materială sau teritorială
- Să implementeze în activitatea funcționarilor conceptul de „manager de cont” – titular unic pentru rezolvarea lucrării.
- Să permită configurarea lucrării prin operațiuni precum crearea conținutului lucrării, stabilirea rolurilor și responsabilităților fiecărui participant, modelarea / remodelarea fluxului de semnare al documentelor lucrării, etc

- 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 instituției menționăm că la nivelul acesteia 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 trebuie asigure minim următoarele capabilități ce privesc dosarele electronice ce vor fi gestionate la nivelul instituției:

- Să dispună de o procedura de configurare a guvernanței digitale a dosarului de lucrare electronică care trebuie sa cuprindă informații despre minim următoarele aspecte:
    - Crearea și Ștergerea dosarului
    - Editarea atributelor dosarului
    - Adăugarea și ștergerea de lucrări electronice în dosar
    - Stabilirea drepturilor de acces la dosarul de lucrare electronică

Cerințe specifice privind dosarele de acte electronice

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

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

Registru de lucrări și registre de acte

Soluția informatică trebuie să permită crearea și configurarea registrelor instituției.

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

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.

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 (inspecție tehnică regională, servicii etc.).

Registrul Unic va asigura numere unice de înregistrare lucrărilor, în timp ce Registrele de acte vor asigura numere de înregistrare unice actelor.

Registrul Unic va include atât lucrările de intrare și de ieșire, cât și lucrările interne.

Registrele trebuie să fie integrate cu Arhiva Electronica Curentă

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. Operațiunea este numită în termeni uzuali „automatizarea închiderii de an”.

Înregistrarea lucrărilor și actelor - termeni și condiții

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

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

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

- Numerele de înregistrare date lucrărilor se vor acorda automat de sistem respectând ordinea cronologică a creării lucrărilor.
- Acordarea numerelor de înregistrare se va face incremental
- Pentru lucrările de intrare numerele de înregistrare se vor acorda la momentul luării lor în evidență, deci la momentul intrării.
- Pentru lucrările interne și cele de ieșire numerele de înregistrare se vor acorda în momentul în care lucrarea a parcurs fluxul de avizare și aprobare, respectiv a fost semnată electronic calificat de toți semnatarii și sigilată electronic calificat cu sigiliul electronic al instituției
- Acordarea numerelor de înregistrare trebuie fie securizata, auditabilă
- 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 meta datele 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 meta date.
- Soluția informatică trebuie să permită funcționarului ca, la nevoie, acesta sa poată stabili amplasarea în cadrul documentului a numărului de înregistrare – locul unde va fi vizibil pe document fiind important pentru a evita suprapunerea numărului de înregistrare peste conținutul actului.
- Soluția trebuie să permită tipărirea la nevoie a numărului de înregistrare pentru lucrările primite și luate în evidență la ghișeu.
- Soluția informatică nu va permite ștergerea numerelor de înregistrare.

Cerințe privind registratura fizică digitalizată

Registratura fizică digitalizată trebuie:

- să permită recepționarea solicitărilor de la alte entități fie ele persoane fizice sau juridice cu colectarea tuturor meta datelor relevante pentru lucrarea respectivă.
- 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.

- 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)
- Să permită repartizarea lucrărilor pe fluxurile de resoluționare și ulterior către persoanele responsabile cu soluționarea acestora, capturând integral tot fluxul instituțional parcurs de lucrare
- Să dispună de o secțiune de Ciorne destinată salvării lucrărilor care sunt în curs de editare și din diverse motive nu au putut fi expediate
- Să permită comunicarea actelor de ieșire atunci când titularul solicitării / împuternicitul acestuia se prezintă la ghișeu. În cazul comunicării către împuterniciți sistemul trebuie să condiționeze comunicarea de încărcarea în sistem a împuternicirii
- Să permită căutarea lucrărilor și vizualizarea conținutului acestora în Registrul Unic la solicitarea beneficiarului (persoana fizica, juridică sau funcționar), accesarea lor cu respectarea condițiilor impuse de GDPR, tipărirea și transmiterea actelor din lucrare cetățeanului prezentat la ghișeu.
- 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
- Căutarea va putea fi făcută prin filtre simple sau filtre conjugate astfel încât timpul de căutare să fie limitat la maxim.
- Să arhiveze lucrările repartizate după ce acestea au fost finalizate. Arhivarea lucrărilor trebuie să poată fi individuală (lucrare cu lucrare) sau în serii/loturi (mai multe lucrări arhivate printr-o singură operațiune).

Cerințe privind registratura online automatizată

Registratura online automatizată trebuie:

- să permită recepționarea automatizată online a solicitărilor de la alte entități fie ele persoane fizice sau juridice cu colectarea tuturor meta datelor relevante pentru lucrarea respectivă.
- Repartizarea automatizată a lucrărilor recepționate prin mediul online trebuie să fie configurabilă în funcție de cel puțin următoarele criterii:

- gradul de încărcare al angajatului
- criteriul ierarhic (repartizarea automată către șeful de structură)
- competența teritorială a angajatului (către anumite inspecții teritoriale)
- competența materială a angajatului

- Să vizualizeze istoricul de solicitări al solicitantului în vederea evitării dublării solicitărilor
- Să vizualizeze toate solicitările care i-au fost repartizate pentru procesare, să le filtreze după cel puțin următoarele criterii:
  - Nume solicitant
  - Număr de lucrare
  - Subiect
  - Conținut
  - CNP / CUI
  - Data recepționării
  - Data înregistrării
  - Starea lucrării
- Să repartizeze solicitarea fie către un alt angajat din cadrul instituției, fie către o altă instituție atunci când este cazul.
- Să organizeze consultări cu alți angajați pentru a întocmi răspuns la cererile venite de la cetățeni
- 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)
- Să comunice online cu solicitanții în vederea solicitării de detalii suplimentare cu privire la solicitarea trimisă
- Să finalizeze / soluționeze solicitările primite prin una din modalitățile de finalizare disponibile în sistem. Finalizarea trebuie să poată fi individuală (lucrare cu lucrare) sau în serii/loturi (mai multe lucrări finalizate printr-o singură operațiune).
- Să arhiveze lucrările finalizate. Arhivarea lucrărilor trebuie să poată fi individuală (lucrare cu lucrare) sau în serii/loturi (mai multe lucrări arhivate printr-o singură operațiune).

3.3.4. Arhiva Electronică

Cerințe de ordin conceptual privind arhiva electronică

Soluția informatică trebuie să pună la dispoziția fiecărui tip de utilizator (persoana fizica, persoana juridica sau funcționar):

- o 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)
- o arhivă electronică de lucrări – destinată arhivării solicitărilor trimise către instituție și care au fost deja finalizate.

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

Soluția informatică trebuie să dispună de următoarele capabilități tehnice:

- Să fie integrată cu componenta de management a identităților electronice și permită accesul la documente în funcție de nivelul de încredere (scăzut / substanțial sau ridicat)
- Să fie integrată cu componenta de formulare electronice și cu soluția de comunicare electronică a sistemului astfel încât utilizatorul sa poată încărca individual sau în loturi documente direct din arhiva sa electronică
- Să permită utilizatorilor autorizați vizualizarea, descărcarea și tipărirea documentelor / actelor
- Să permită vizualizarea tuturor meta datelor stocate la nivelul sistemului pentru fiecare document / act în parte
- Să dispună de capabilități de filtrare, sortare și căutare în funcție de meta date relevante (ex. denumire fișier, număr de înregistrare, data, etc)
- Să permită utilizatorului ștergerea documentelor / actelor din arhiva personală
- Să nu permită utilizatorului ștergerea actelor transmise lui de către instituții
- Să permită utilizatorului să vizualizeze lucrarea din care a făcut parte actul emis si transmis lui de către instituție
- Să dispună de mecanisme de colectare nativă și implicită (fără ca utilizatorul să facă un efort suplimentar în acest sens) a meta datelor prin inputuri controlate, validate și parametrizate în vederea asigurării unui nivel superior de acuratețe a acestor informații

Să dispună de o politică de management a documentelor încărcate în sistem cel puțin din perspectiva:

- Formate de fișiere acceptate
- Parametrii denumirilor fișierelor
- Mărimea fișierelor
- Scanarea documentelor

Accesul la fișiere (la persoanele juridice care poată avea mai mulți reprezentanți soluția trebuie stabilească drepturile de acces ale fiecăruia la fișiere).

Cerințe specifice privind arhiva electronică de lucrări a persoanelor fizice și juridice

Soluția informatică trebuie să dispună de următoarele capabilități tehnice:

- Să permită utilizatorilor autorizați vizualizarea lucrărilor și a documentelor asociate
- Să permită vizualizarea tuturor meta datelor stocate la nivelul sistemului pentru fiecare lucrare
- Să dispună de capabilități de filtrare, sortare și căutare în funcție de meta date relevante (ex. denumire, conținut, număr de înregistrare, data, etc)
- 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:

- Să permită crearea nomenclatorului arhivistic electronic (conform prevederilor legale) și managementul arhivei electronice instituționale
- Să fie integrată în toate mijloacele de comunicare relevante (ce produc consecințe juridice) la nivelul soluției informatice

- Să fie integrată cu componenta de management a identităților pentru a colecta actele de identitate ale utilizatorului direct din procedura de înrolare („onboarding”)
- Să dispună de mecanisme auditabile (log-uri) explicite cu privire la orice modificare, acces sau operațiune ce are impact în arhiva electronică.
- Să fie sincronizată cu registrele instituției pentru a asigura o bună trasabilitate și transparență în gestiunea actelor
- Să salveze toate meta datele relevante ale actelor în structura PDF a acestora
- Să poată exporta la cererea beneficiarului, în format structurat și fără costuri pentru beneficiar toate actele existente în sistem și datele colectate ca obligație legală a instituției. Datele care există în sistem în vederea personalizării experienței de utilizare nu fac subiectul aceste obligații.

Soluția informatică trebuie dispună de capabilități de:

- Configurare de fluxuri predefinite
- Modelare contextuală de fluxuri

Cerințe specifice privind arhiva de lucrări electronice a instituției

Soluția informatică trebuie să dispună de următoarele capabilități tehnice:

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

3.3.5. Managementul Fluxurilor De Lucru Cu Documente / Acte

Configurarea de fluxuri predefinite

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

- Competența materială și teritorială a angajaților
- Structura organizatorică a instituției (structura de compartimente și relațiile ierarhice dintre acestea)
- Gradul de încărcare al angajaților
- Procedurile interne ale instituției
- Modelarea fluxurilor de lucru trebuie să fie facilă și să nu necesită un nivel ridicat de expertiză IT
- Trecerea la un flux de lucru ajustat nu trebuie să influențeze structurile de date create de versiunile anterioare ale fluxului.
- Modelarea fluxului să includă 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
- Parcursul instituțional pe care îl poate avea
- Eventuale condiționări specifice determinate de guvernanța instituțională (ex. competență teritorială)
- Condiționări cu privire la semnarea electronică a documentelor
- Termenii și condițiile înregistrării, procesării, finalizării și arhivării electronice a lucrărilor astfel generate

- Fluxurile predefinite să fie disponibile tuturor categoriilor de utilizatori (persoane fizice, juridice, funcționari – atât pe canalul offline la ghișeu, cât și pe canalul online).

Modelarea contextuală a fluxurilor electronice

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

- Posibilitatea de modelare trebuie sa fie disponibilă tuturor angajaților
- Odată modelat fluxul acesta se va executa automat fără intervenția angajatului
- Să fie implementat un mecanism de „rollback" care să poată 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

3.3.6. Semnarea Si Sigilarea Electronica Calificată

Semnarea electronică calificată

Soluția informatică 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 informatică trebuie să dispună de integrare cu minim 2 furnizorii de servicii de încredere autorizați în acest sens la nivel european.

Din perspectiva semnării electronice calificate autoritatea contractantă urmărește realizarea următoarelor cerințe funcționale:

- Să permită sincronizarea / desincronizarea certificatului calificat de semnare electronică cu sistemul
- Să permită, opțional, integrarea semnăturii olografe în semnătura electronică calificată
- Să dispună de integrarea semnăturii electronice calificate pe toate fluxurile de comunicare implementatele nivelul sistemului
- Să permită semnarea simplă (1 document) și semnarea în serii (mai multe documente) tuturor utilizatorilor sistemului
- Să permită un management contextual al motivelor de semnare
- Să permită semnarea in interiorul sau independent de existența unui flux de sem-nare
- Să permită verificarea și validarea semnăturilor electronice calificate aplicate pe documente / acte, respectiv:
    - Validarea tipului de semnătură
    - Verificarea lanțului de încredere al certificatului
    - Data și ora semnării
    - Identitatea celui care a semnat
    - Dacă documentul a fost sa u nu modificat după semnare
    - Date privind valabilitatea certificatului calificat
    - Emitentul certificatului
    - Motivul de semnare
- Să permită poziționarea semnăturii electronice calificate vizibile pe document la libera alegere a utilizatorului – daca documentul suport va avea factor de rotație inserat aplicarea va ține cont de acesta.
- Să permită operațiuni precum anularea semnării, revizuirea semnării, reluarea semnării,
- Să permită vizualizarea listingului de solicitări de semnare și gestionarea cererilor / invitațiilor de semnare
- Să permită semnarea multiplă (mai multe Lucrări deodată) cu posibilitatea de selectare a lucrărilor care vor face obiectul semnării
- Să permită pre vizualizarea documentelor ce urmează a fi semnate fără să fie ne-voie de descărcarea lor
- Să permită semnarea electronică calificată simultana a mai multor documente și semnarea de tip „queue” (coadă)

Sigilarea electronică calificată

Soluția informatică va putea utiliza fără niciun fel de restricționare sigilii electronice calificate găzduite în cloud emise în conformitate cu prevederile regulamentului eIDAS de orice furnizor autorizat de pe teritoriul Europei.

Accesul soluției informatice 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.

Din perspectiva sigilării electronice calificate autoritatea contractantă urmărește realizarea următoarelor cerințe funcționale:

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

3.3.7. Comunicare Electronică Și Chat Integrat În Sistem

Soluția informatică trebuie să dispună de capabilități de:

- Comunicare electronică integrată în sistem
- Comunicare electronică în afara sistemului
- Chat integrat în sistem

Cerințe specifice soluției de comunicare electronică integrată în sistem

Soluția de comunicare electronică integrată în sistem trebuie fie disponibilă tuturor utilizatorilor persoane fizice, persoane juridice și angajați.

PERSOANE FIZICE ȘI JURIDICE

Soluția de comunicare trebuie să adreseze următoarele cerințe funcționale specifice tuturor soluțiilor de tip „email client", respectiv:

- Să dispună de structura clasica de comunicări specifica 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 permită conversia fișierelor în format PDF să se poată face individual sau în serii/loturi
- Să dispună de capabilități de semnare electronică calificată a fișierelor atașate

ANGAJAȚI

Soluția de comunicare trebuie să adreseze următoarele cerințe funcționale specifice tuturor soluțiilor de tip „email client", respectiv:

- Să dispună de structura clasica de comunicări specifica tuturor clienților de email
  - Primite
  - Trimise
  - Ciorne
  - Arhivate
- Să permită schimbul de mesaje bidirecțional între angajați și toate tipurile de utilizatori
- Să permită schimbul bidirecțional de mesaje via email cu persoanele fizice si reprezentanții persoanelor juridice indiferent dacă acestea dețin sau nu identitate electronică la nivelul sistemului, dacă sunt sau nu sunt utilizator în sistem.
- 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 se poată face individual sau în serii/loturi
- Să dispună de capabilități de semnare electronică calificată a fișierelor atașate

Cerințe specifice soluției de chat integrat în sistem

Soluția de chat integrată în sistem trebuie fie disponibilă tuturor utilizatorilor persoane fizice, persoane juridice și angajați.

PERSOANE FIZICE ȘI PERSOANE JURIDICE

Soluția de chat integrată cu soluția informatică trebuie îndeplinească următoarele cerințe funcționale:

- Să dispună de funcționalitățile specifice soluțiilor de chat, respectiv:
  - Schimbul bidirecțional de mesaje
  - Atașare de fișiere
  - Comunicarea individuală sau in grup
  - Audio conferință

- Video Conferință
- Partajare de ecrane

ANGAJAȚI

- Să dispună de funcționalitățile specifice soluțiilor de chat, respectiv:
  - Schimbul bidirecțional de mesaje
  - Atașare de fișiere
  - Comunicarea individuală sau in grup
  - Audio conferință
  - Video Conferință
  - Partajare de ecrane

Angajații vor putea să activeze / dezactiveze la libera lor inițiativă funcționalitatea chat a persoanelor fizice și juridice.

3.3.8. Notificări (De Sistem Și De Tip „Push”1 În Aplicația Mobilă)

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

- Notificări pe email
- Notificări în contul personal
- Notificări de tip „push” în aplicația mobilă

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

Notificări pe email

Soluția informatică 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 notificări de tip „push” în aplicația mobilă

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

- Notificările să poată fi trimise către utilizatori / grupuri de utilizatori minim către:
  - Un utilizator individual persoana fizică, juridica sau funcționar
  - Către toți reprezentanții unei persoane juridice
  - Către Administratorii persoanelor juridice
  - Către toți angajații
  - Către toți angajații dintr-o anumită structură
  - Către reprezentanții persoanelor juridice
  - Către utilizatorii asociați unei adrese poștale
- Să permită parametrizarea mesajului de trimis (număr de caractere)
- Să furnizeze informații de progres cu privire la trimiterea de notificări în serii/loturi mari
- Să dispună de mecanisme de „fallback” implementate pentru gestionarea situațiilor când apar erori în procesul de trimitere.

[1] notificare transmisă la momentul unui eveniment de sistem către dispozitivul mobil.

3.3.9. Formulare Electronice

Soluția trebuie să implementeze:

- **Un constructor de formulare care să permită dezvoltarea, personalizarea și parametrizarea in cadrul proiectului a oricărui tip de formular necesar aferent serviciului public digital**
- comunicare pe bază de formulare inteligente pentru uzul utilizatorilor externi (cetățeni) și pentru uzul intern al angajaților.

Formularele implementate 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 sa permită instituției să configureze fiecare formular în parte.
- Să dispună de posibilitatea de a fi salvate in 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.

Cerințele funcționale menționate la secțiunea documente / acte electronice se vor aplica întocmai și în cazul formularelor.

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 meta datele colectate și relevante în fiecare context.

Se vor implementa formulare și procese front-office/back-office pentru toate serviciile publice ale instituției.

3.3.10. Comunicare Internă / Externă

Soluția informatică trebuie să furnizeze capabilități de comunicare electronică bidirecțională atât cu entitățile înregistrate în sistem, cât și cu cele din afara sistemului (via email).

3.4. Managementul utilizatorilor și accesul la sistem

Soluția informatică trebuie să includă un proces riguros și auditabil al managementului identităților electronice (cetățeni, persoane juridice, angajați, colaboratori, furnizori, etc.). Pentru a evita orice neclaritate, prin termenul auditabil se înțelege capabilitatea soluției informatice de a crea și stoca în mod agregat înregistrări exacte pentru fiecare pas descris in 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 a solicitantului la oricare dintre sediile instituției sau direct prin mediul online. Identitățile utilizatorilor trebuie să fie unice și interdependente.

Pentru autentificarea în platforma electronică utilizatorii vor putea utiliza de asemenea și identitatea electronică creată în platforma națională RoeID. Sistemul informatic instalat în UAT Comuna Bătrâni va

dispune de interconectare cu platforma națională RoeID prin utilizarea API-urilor astfel încât utilizatorii, dacă dețin deja o identitate electronică certificată de sistemul național, să nu mai fie nevoiți să parcurgă un nou proces de identificare și validare.

Identitățile electronice ale utilizatorilor non-angajați se vor putea crea de către angajații instituției în funcție de drepturile asociate de către administratorul de sistem, în timp ce identitățile electronice ale angajaților vor fi create doar de administratorii de sistem.

Operațiunile de creare / modificare a identităților electronice se vor face în regim de tranzacție și vor dispune de proceduri de „fallback" pentru cazurile 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 electronice – toate validările de inputuri trebuie să fie corecte, preexistente și să respecte standardele in industrie
- Capturarea și salvarea acordului de procesare a datelor cu caracter personal
- Pentru identitățile realizate la ghișeu cererea de înregistrare va fi semnata olograf și înregistrată în Registratura electronică a instituției
- 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 publice

Identitatea electronică va fi în prealabil verificată/validată și ulterior inițiată de angajatul care a realizat identificarea, 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 (indiferent ca este personală sau profesională, persoană fizică sau juridică) vor fi asumate personal de angajatul care a realizat validarea atributelor prin semnarea electronica 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 credenţiale 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 angajat) nu vor putea 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 va putea deține o singură identitate electronică personală și un număr nelimitat de identități electronice profesionale.

Ofertantul va descrie în detaliu:

- modul în care gestionează atributele identităților electronice (personale și profesionale) raportat la cerințele funcționale menționate
- cum asigură relația de interdependență dintre identitatea personală și cea profesională
- cum asigură asocierea de roluri la fiecare tip de identitate
- cum asigură modele de guvernanță particularizată pe fiecare rol în parte
- cum gestionează procesul de actualizare a atributelor identității fără a afecta corectitudinea și consistența versiunilor anterioare ale atributelor în contextul activității instituției publice (istoricul de lucrări al utilizatorului).

Soluția informatică trebuie să poată gestiona minim următoarele atribute în ceea ce privește identitatea electronică a persoanelor fizice:

- Datele din actele de identitate (CNP + toate actele de identitate)
- Adresa de email
- Număr de telefon
- Semnătura electronică calificată (în cazurile în care utilizatorul deține)
- Credenţiale (utilizator și parolă) – pentru identitățile electronice efective

Managementul identității electronice a persoanelor juridice se va realiza în mod colaborativ de către administratorul persoanei juridice / împuternicitul acestuia și angajații UAT Comuna Bătrâni, fiecăruia dintre aceștia revenindu-le următoarele responsabilități:

- Responsabilități ale angajatului:
    - Verificarea corectitudinii și integrității datelor despre persoana juridica
    - 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 juridica la un nivel de acuratețe care să reflecte starea curenta a lucrurilor.

Fiecare identitate efectivă (personală sau profesională) va dispune de un set unic de credenţiale. Credențialele vor constitui o dovadă irefutabilă de identificare și în baza lor se va acorda accesul utilizatorului la sistem.

Soluția informatică trebuie să poată gestiona minim următoarele atribute în ceea ce privește identitatea electronică a persoanelor juridice:

- 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
- Credenţiale (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.

Soluția informatică trebuie să poată gestiona minim următoarele atribute în ceea ce privește identitatea electronică a reprezentanților persoanelor juridice:

- 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 sau al furnizorului.

Raportat la gradul de operaționalizare al identităților acestea pot fi:

- Efective
- Neefective
- Indicii preliminare de identitate certificate de angajați

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 de identitate** în stabilirea unei viitoare identități. Indiciile preliminare de identitate vor fi asumate de angajatul care le-a introdus in sistem și supuse auditării.

Soluția informatică trebuie să dețină capabilitatea de a captura, salva și operaționaliza 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 guvernantă digitală contextuală pentru acestea.

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

Din perspectiva GDPR ofertantul 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 ofertantul trebuie să detalieze:

- Modalitatea de asigurare a nivelurilor de încredere scăzut, substanțial si 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 si juridice în minim următoarele stări:
  - Perioada de inactivitate
  - Perioada între momentul inițializării și momentul activării identității electronice
  - Perioada de activitate

    - Perioada de suspendare – ex. suspiciuni de fraudă, detașare, indisponibilitate temporară, etc.
    - Perioada ulterioară dezactivării
- Pentru angajați:
    - 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 si accesibile fiecărui utilizator in 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
- Poza de profil
- Actele de identitate ale titularului actualizate
- Semnătura olografă a utilizatorului (dacă este înregistrată de utilizator)
- Semnătura electronică calificată a titularului identității (dacă există) 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
- Poza de profil
- Semnătura olografă a utilizatorului (dacă este înregistrată de utilizator)
- Semnătura electronică calificată a titularului identității
- Modificarea parolei de acces la sistem

Din perspectiva utilizatorului angajat interfața grafică trebuie să afișeze minim:

- Datele personale ale titularului identității electronice profesionale
- Datele specifice identității profesionale
- Poza de profil
- Semnătura olografă a utilizatorului (dacă este înregistrată de utilizator)
- 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, 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 angajaților.

Pentru restul informațiilor se va cere validarea de către angajat și acolo unde există posibilitatea semnarea lor electronică calificată de către titularul identității electronice.

Informațiile despre toți utilizatorii persoane fizice, persoane juridice sau angajați vor fi făcute disponibile și accesibile tuturor angajaților în baza principiului „nevoii de a cunoaște".

Informațiile vor putea fi accesate doar individual și condiționat de existența unui motiv temeinic. Motivul accesului va fi capturat în sistem pentru a asigura conformitatea cu prevederile GDPR.

Pentru a evita orice dubiu, soluția ofertată nu va permite niciunui tip de utilizator angajat vizualizarea tuturor identităților personale din sistem sub forma de listă și fără un motiv exprimat și capturat la momentul accesului.

Angajații 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

3.5. Interconectarea și interoperabilitatea inter și intra-instituțională

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 și în relația cu alte instituții și între structurile interne ale beneficiarului:

- Operaționalizarea canalelor de comunicații inter și intra-instituționale menite să asigure transportul datelor;
- Operaționalizarea canalelor de comunicare cu cetățenii și mediul de afaceri;
- Asigurarea procedurilor de încărcare, transport, livrare și vizualizare a conținutului, a datelor și documentelor;
- Procedurile de parametrizare a fluxurilor de comunicare;
- Stabilirea structurilor de date și algoritmilor de validare ce fac obiectul transferului;
- Automatizarea capabilităților de expediere a conținutului;
- Parametrizarea livrărilor în funcție de competențele destinatarului;
- Asigurarea capabilităților de conversie a fișierelor în format PDF;
- Sincronizarea cu componenta de management al identităților, cu cea de înregistrare, precum și cu cea de arhivare și îndosariere electronică;
- 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.);
- Operaționalizarea interconectivității cu entitățile care dețin identitate electronică la nivelul platformei și cu cele care nu dețin o identitate electronică în sistem;
- Operaționalizarea interconectivității cu cei care dețin o identitate electronică la nivelul platformei naționale ROeID
- Asigurarea mijloacelor colaborative de lucru (ex. audio-video conferințe, partajarea de ecrane, chat, documente colaborative, transfer de fișiere, etc.);
- Asigurarea și mentenanța API-urilor de interconectare cu furnizorii de servicii de semnare electronică calificată, cu furnizorii de servicii de sigilare electronică calificată, cu ANAF, cu RECOM, cu alți furnizori.
- Asigurarea API-urilor cu furnizorii de servicii de încredere (ex. Serviciul de Telecomunicații Speciale)
    - Să asigure conexiunile securizate cu furnizorii de servicii de încredere în vederea garantării

stabilității serviciilor de semnare și sigilare electronică calificată

- Asigurarea componentei de interconectare pe bază de link
    - Să faciliteze operaționalizarea spațiilor virtuale de interconectare a entităților din sistem și să garanteze utilizarea acestora cu respectarea principiilor de standardizare și uniformitate
- Asigurarea API-urilor cu aplicații interne
    - Să asigure transferul bidirecțional de date, informații și fișiere în format electronic între aplicațiile prezente și viitoare ce vor alcătui sistemul informatic integrat.
- Asigurarea registrelor de validări de interoperabilitate
    - Să gestioneze seturile de validări specifice fiecărui atribut de sistem și să garanteze utilizarea acestora cu respectarea principiilor de standardizare și uniformizare
- Asigurarea API-urilor cu aplicații externe
    - Să permită transferul bidirecțional de date, informații și fișiere în format electronic între aplicațiile interne ale sistemului informatic și aplicații externe acestuia utilizate de alte entități
    - Să verifice compatibilitatea atributelor identităților electronice ale tuturor tipurilor de utilizatori conform principiilor interoperabilității sistemelor.
- Asigurarea API-urilor ce facilitează instrumentele de inteligență artificială (speech to text, text to speech, automated translations , speech to neavigation, etc.)
    - Să asigure consumarea serviciilor de inteligență artificială (AI) în regim de stabilitate și continuitate prin intermediul API-urilor puse la dispoziție de aceste platforme

***Notă:** Interconectarea și interoperabilitatea 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 interoperabilitatea vor fi operaționalizate prin intermediul **platformei de distribuție electronică înregistrată** care va permite:

- **Operaționalizarea canalelor de comunicare inter și intra-instituționale** menite să asigure transportul datelor între comuna Bătrâni și alte instituții publice în mod bidirecțional
- **Operaționalizarea canalelor de comunicare între angajați și cetățeni / reprezentanții mediului de afaceri** – pentru **furnizarea** la cel mai înalt nivel tehnologic a **serviciilor publice digitale** aflate în competența comunei Bătrâni soluția instalată la nivelul beneficiarului pe baza căreia vor fi dezvoltate serviciile digitale trebuie să prevadă capabilități de interacțiune cu cetățenii (persoane fizice, persoane juridice) prin mecanisme de comunicare bidirecțională între angajați și aceștia. Prin această platformă cetățenii vor dobândi acces de oriunde, de pe orice dispozitiv fix sau mobil și în orice moment la toate serviciile publice dezvoltate prin proiect. Această componentă a sistemului informatic urmărește să asigure un punct de acces centralizat la serviciile publice oferite de instituție. Soluția trebuie să fie disponibilă tuturor utilizatorilor persoane fizice, persoane juridice și angajați și să fie configurată în funcție de specificul de utilizare al fiecărui tip de utilizator. (cerințele funcționale sunt detaliate în secțiunea „Cerințe specifice soluției de comunicare electronică integrată în sistem” din cadrul capitolului ”Arhitectura funcțională a sistemului)

Raportat la soluțiile de interoperabilitate prin care soluțiile 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.

3.6. Securitatea și auditul platformei

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 pentru un astfel de sistem informatic.

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 a parolei;
- 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.

3.7. Confidențialitatea datelor

Din perspectiva protecției și confidențialității datelor, beneficiarul se va asigura respectarea prevederilor Regulamentului (UE) 679 / 2016 (GDPR) (intrat în vigoare în 25 mai 2018) privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestora la nivelul tuturor entităților unde se implementează.

Prin proiect se vor implementa măsuri tehnice în vederea respectării celor 7 principii de bază ale GDPR, respectiv:

- Legalitate, corectitudine și transparență;
- Limitarea scopului prelucrării;
- Minimizarea datelor supuse prelucrării;
- Acuratețea în colectarea și întreținerea datelor;
- Limitarea perioadei de stocare a datelor;
- Integritatea și confidențialitatea datelor;
- Responsabilitate procesatorilor.

Din perspectiva GDPR ofertantul 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 proprietății datelor, datele rezultate din exploatarea soluției informatice de către utilizatori (angajați ai UAT Comuna Bătrâni) sunt proprietatea exclusivă a instituției, iar datele introduce de către utilizatori externi (persoane fizice, persoane juridice) sunt proprietatea exclusivă a acestora

3.8. Cerințe non-funcționale ale proiectului TIC

3.8.1. 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, reprezentând descrierea detaliată a modalității și a metodelor folosite pentru îndeplinirea cerinței în cadrul propunerii tehnice.

3.8.2. Performanța soluției propuse a fi instalate

- Sistemul trebuie să fie disponibil pentru utilizare zilnică, 24 ore/zi, 7 zile din 7. 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.

3.8.3. 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.

3.8.4. 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/HTTP/HTTPS/SSL
- utilizarea unei arhitecturi modulare 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.

3.8.5. 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 oră	O zi
Mare	2 ore	2 zile
Mediu	4 ore	2 zile lucrătoare
Minor	4 ore	3 zile lucrătoare

3.8.6. 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.

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. RESURSE

4.1. Personal și instruire

Activitatea de instruire ce va fi derulată odată cu momentul în care soluția IT este funcțională, serviciile publice sunt dezvoltate și sunt puse în funcțiune și platforma poate fi utilizată de către personalul instituției.

Astfel, va fi furnizat pentru un număr de utilizatori-formatori, membrii ai grupului țintă, 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.

4.2. Resurse materiale

Pentru buna desfășurare a proiectului din partea beneficiarului se va forma câte un grup de persoane reprezentativ pentru toate structurile care vor performa testarea serviciilor dezvoltate pe perioada proiectului. Aceste persoane vor dispune de:

- **Resurse hardware:**
  - **Calculatoare**: desktop-uri, laptop-uri, servere, tablete.
  - **Dispozitive periferice**: imprimante, scanere, camere web, mouse, tastatură.
  - **Rețele**: routere, switch-uri, cabluri, acces la internet.
  - **Echipamente de stocare a datelor**: hard disk-uri, SSD-uri, unități optice, cloud storage.
- **Resurse software:**
  - **Sisteme de operare:** Windows, macOS, Android, iOS.
  - **Aplicații software:** programe de procesare text, foi de calcul, baze de date.
  - **Semnături electronice calificate**
  - **Sigiliu electronic calificat**
- **Cunoștințe și informații:**
  - **Documentație tehnică:** manuale de utilizare, ghiduri de instalare, tutoriale video.
  - **Licențe** – dreptul de utilizare al utilizatorilor
  - **Standarde și protocoale:** reguli și convenții pentru asigurarea interoperabilității.
  - **Experiența și expertiza:** cunoștințe acumulate de specialiști în domeniu.

5. MENTENANȚĂ ȘI SUSTENABILITATE

5.1. 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 comunei Bătrâni.

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.

5.2. Sustenabilitate și scalabilitate

În cadrul proiectului sustenabilitatea și scalabilitatea soluției sunt esențiale pentru a asigura un viitor responsabil și eficient. Prin implementarea soluției de tip SaaS cloud based beneficiarul urmărește minimizarea impactului negativ asupra mediului prin reducerea consumului de energie, gestionarea deșeurilor electronice și promovarea unor practici responsabile în întregul ciclu de viață al produselor și serviciilor IT. Aceasta implică utilizarea de hardware și software eficiente energetic, optimizarea infrastructurii IT, virtualizarea serverelor și implementarea unor politici de achiziții responsabile

Pentru a asigura perspectiva scalabilității soluției avute în vedere furnizorii trebuie să aibă în vedere capacitatea soluțiilor ofertate de a se adapta la creșterea volumului de date, traficului și numărului de utilizatori fără a afecta performanța sau a necesita investiții suplimentare. Soluțiile propuse trebuie să răspundă rapid la creșteri neanticipate ale traficului și să își extindă operațiunile fără a întâmpina dificultăți.

Îmbinarea sustenabilității cu scalabilitatea este crucială pentru a asigura durabilitatea proiectului astfel că ofertanții trebuie să ia în considerare în propunerile tehnice pe care le vor face atât impactul asupra mediului, cât și capacitatea de adaptare la creșterea consumului de conținut din partea utilizatorilor.

Soluția instalată pentru dezvoltarea serviciilor publice prin proiect va viza, pe lângă conformitatea cu normele de identitate electronica, protecția datelor cu caracter personal și securitatea cibernetică, și conformitatea în materie de dezvoltare durabilă, respectiv egalitatea de șanse, de gen și nediscriminarea, accesibilitatea, protecția mediului, inclusiv integrarea principiului DNSH.

Astfel pentru implementarea și sustenabilitatea proiectului se va urmării respectarea următoarelor principii:

1. **Eficiența resurselor**

- **Optimizarea codului**: Scrierea de cod eficient care consumă mai puține resurse de calcul (CPU, memorie, energie).
- **Minimizarea amprentei de carbon**: Reducerea impactului asupra mediului prin optimizarea infrastructurii și a proceselor de dezvoltare.
- **Utilizarea de hardware eficient energetic**: Alegerea de servere și echipamente cu consum redus de energie.

*** Modalitatea de adresare**

- Prin implementarea proiectului **se va urmări selectarea de furnizori de servicii de cloud care au certificări relevante în ceea ce privește protecția mediului**
- Se va acorda o atenție sporită modalității de scriere a codului astfel încât acesta să fie cât mai eficient din punct de vedere energetic – acest lucru se va realiza prin respectarea bunelor practici și a standardelor și framework-urilor de programare existente.

2. Durabilitatea pe termen lung:

- **Mentenanța facilă**: Utilizarea de software ușor de întreținut și actualizat, pentru a prelungi durata de viață a aplicației.
- **Scalabilitate**: soluțiile informatice vizate prin proiect trebuie să poată gestiona creșterea numărului de utilizatori și a volumului de date fără a afecta performanța sau a necesita resurse suplimentare semnificative.
- **Modularitate**: Construirea de software modular, care permite înlocuirea sau actualizarea componentelor individuale fără a afecta întregul sistem.

*** Modalitatea de adresare**

- Prin implementarea proiectului se va urmări ca experiența de utilizare să fie cât mai facilă iar actualizările să nu creeze disconfort sau disfuncționalități în utilizare
- Vor fi avute în vedere soluții care asigură scalabilitate în raport cu evoluția numărului de utilizatori
- Soluțiile vor permite înlocuirea fără a fi afectat sistemul per ansamblu

3. Incluziune și accesibilitate:

- **Accesibilitate**: Proiectarea de software accesibil tuturor utilizatorilor, inclusiv persoanelor cu dizabilități.
- **Diversitate și incluziune:** Promovarea diversității și incluziunii în procesul de dezvoltare a software-ului.
- **Echitabilitate**: Asigurarea că software-ul este accesibil și util pentru toate grupurile sociale.

*** Modalitatea de adresare**

- Soluțiile informatice vor asigura persoanelor cu dizabilități un nivel de utilizare ridicat prin încorporare inteligenței artificiale contextual pentru a compensa nevoi precum: imposibilitatea de a scrie la tastatura (speech to text), imposibilitatea de înțelege scrisul (text to speech), imposibilitatea navigării prin sistem cu mijloacele uzuale precum mouse, pad, etc (web navigation through voice command), sau necunoașterea unor limbi străine (automated translations), etc.

- Se vor avea in vedere de asemenea implementarea de soluții dedicate pentru persoanele cu probleme de vedere (Standard WCAG)

4. **Impact social pozitiv:**

   - **Dezvoltarea de software care abordează probleme sociale:** Crearea de aplicații care contribuie la rezolvarea problemelor sociale, cum ar fi sărăcia, inegalitatea sau schimbările climatice.
   - **Responsabilitate socială**: Luarea în considerare a impactului social al software-ului dezvoltat.
   - **Etică în dezvoltarea software**: Respectarea principiilor etice în toate etapele procesului de dezvoltare.

*** Modalitatea de adresare**

- Prin proiect vor fi vizate soluții care **vor conduce la scăderea consumului de hârtie, reducerea nevoii de a transporta corespondența, limitarea consumului de consumabile pentru scannere si imprimante prin digitalizarea completă a relației cu cetățenii, mediul de afaceri și alte instituții.**

5. **Colaborare și comunitate:**

   - **Software open-source**: Promovarea și utilizarea de software open-source.
   - **Comunități de dezvoltare**: Participarea activă în comunitățile de dezvoltare software.

*** Modalitatea de adresare**

- Prin proiect vor fi vizate instalarea și punerea în funcțiune de soluții ce utilizează instrumente open source astfel încât soluțiile să fie cât mai accesibile pentru dezvoltarea și utilizarea serviciilor publice digitale. Utilizarea soluțiilor bazate pe open source va face posibilă punerea la dispoziția utilizatorilor cu titlu gratuit a unor componente de instruire digitală pentru persoanele defavorizate care nu au acces la instrumente digitale complexe.

Elaborator studiu:

Civic Soft SRL

Prin administrator,

Guguci Ciprian