

CAIET DE SARCINI

pentru achiziția serviciilor pentru Dezvoltarea și implementarea sistemului digital
ePatrimoniu

Cuprins

1. Informații generale	5
1.1 Introducere	5
1.2 Autoritatea contractantă	7
1.3 Contextul realizării achiziției	8
1.4. Descrierea situației actuale	9
1.5. Beneficiile anticipate	10
2. Informații referitoare la contract	11
2.1 Obiectul contractului	11
2.2 Durata contractului și locul desfășurării activităților	12
2.3 Scopul contractului și rezultate așteptate	13
2.4 Sursa de finanțare	14
3. Grupuri țintă și utilizatori	14
3.1 Categorii de utilizatori	14
3.2 Roluri și drepturi de acces în sistemul digital	17
3.2.1 Niveluri de acces în sistemul digital ePatrimoniu	18
4. Cerințe generale privind soluția tehnică	21
4.1 Principii generale de proiectare și funcționare	21
4.2 Caracteristici esențiale	23
5. Descrierea arhitecturii sistemului	24
5.1 Arhitectura logică	24
5.2 Arhitectura fizică	32
6. Cerințele componentelor software ale sistemului digital ePatrimoniu	36
6.1 Componenta e-Guvernare (componentă aplicativă)	36
6.1.1 Scopul implementării	36
6.1.2 Cerințe și funcționalități generale	40
6.1.3 Cerințe funcționale pentru etapele fluxurilor	44
6.1.4 Cerințe funcționale privind arhivarea electronică	46
6.2 Componenta Management Patrimoniu Cultural (MPC) (componentă aplicativă)	47
6.2.1 Cerințe generale	47
6.2.2. Cerințe privind implementarea ontologiilor	48
6.2.3 Cerințe privind modelarea datelor la nivel logic	52
6.2.4 Cerințe privind gestionarea tezaurelor terminologice și vocabularelor controlate	56
6.2.5 Cerințe privind interfața de creare și editare a resurselor	58
6.2.6. Cerințe privind importul și exportul datelor în bloc	61
6.2.7. Cerințe privind interfața de căutare	64
6.2.8 Cerințe privind instrumentul de afișare și filtrare dinamică a datelor	68
6.2.9 Cerințe privind vizualizarea imaginilor, materialelor audio-video și a	

obiectelor 3D	68
6.2.10 Cerințe privind submodulul GIS și gestionarea datelor geospațiale	72
6.2.11 Cerințe privind funcționalitățile de prezentare și valorificare atractivă a resurselor culturale digitale	76
6.2.12 Cerințe privind analiza datelor / dovezilor referitoare la patrimoniul cultural (existente în baza de date) și generarea de statistici și rapoarte în funcție de diverse criterii	78
6.2.13 Generare automată a descrierilor pentru resurse	79
6.2.14 Cerințe privind integrarea componentei e-Guvernare cu componenta MPC	79
6.3 Componenta Gestiunea identității și accesul utilizatorilor (IAM) (componentă suport)	82
6.4 Componenta Middleware unificat de integrare (componentă suport)	85
6.5 Componenta Backup și restaurare (componentă suport)	86
6.6 Componenta Managementul incidentelor (ticketing) (componentă suport)	89
6.7. Componenta Monitorizare a performanței și disponibilității (componentă suport)	90
6.8. Componenta Managementul evenimentelor de securitate (SIEM)	90
6.9 Componenta de protecție servicii web (componentă suport)	93
7. Cerințe funcționale și nefuncționale transversale ale Sistemului digital ePatrimoniul	99
7.1 Niveluri de prezentare ale Sistemului digital ePatrimoniul	99
7.1.1 Interfața publică	100
7.1.2 Dashboard-ul intern	104
7.2 Realizare de interogare și analiză rapoarte pe baza datelor din sistem	117
7.3 Interoperabilitate și integrare cu alte sisteme	121
7.3.1 Cerințe de implementare a API-urilor dezvoltate	121
7.3.2 Autentificare și autorizare	121
7.3.3 Operații CRUD pe resurse	121
7.3.4 Design și standarde de implementare	122
7.3.5 Cerințe privind integrarea cu alte servicii publice	122
7.3.6 Cerințe privind interconectarea cu Biblioteca digitală Europeană (Europeana.eu)	124
7.3.7 Alte cerințe privind interoperabilitatea	125
7.4 Inteligență artificială	125
7.4.1 Funcționalități de sprijin pentru e-guvernare și procese administrative	126
7.4.2 Cerințe generale de conformitate și interoperabilitate	131
7.4.3 Considerente de implementare	132
7.4.4 Indicatori de Performanță AI	133
7.5 Securitate și confidențialitate	133
7.5.1 Controale de securitate	134
7.5.2 Confidențialitatea și protecția datelor cu caracter personal	140
7.6 Accesibilitate și UI/UX	145

7.6.1 Accesibilitate	146
7.6.2 UI/UX	147
8 Implementare, mentenanță, garanție și suport tehnic	149
8.0 Faza de pre-analiză	153
8.1 Faza de analiză	158
8.2 Faza de proiectare	160
8.3 Faza de dezvoltare, migrare și testare	161
8.3.1. Dezvoltare	162
8.3.2. Migrarea datelor	164
8.3.3. Testare	164
8.4. Faza de punere în producție	168
8.5 Instruire pentru utilizatori și administratori	170
8.6 Faza de stabilizare operațională a sistemului	173
8.7. Mentenanță corectivă și evolutivă	174
8.7.1 Mentenanța corectivă	174
8.7.2 Mentenanța evolutivă	176
8.8. Garanție și suport tehnic	176
9. Managementul contractului	177
9.1 Documente	177
9.2 Gantt orientativ pentru faze și etape majore	189
9.3 Gestionarea riscurilor și relația Prestator – Autoritate Contractantă	198
9.4 Conformitate legală, drepturi asupra codului sursă și licențiere	198
10. Recepția și plata serviciilor	202
10.1 Recepția	202
10.2 Plata	203
11. Resurse umane și expertiza necesară pentru realizarea activităților contractului și obținerea rezultatelor	204
11.1 Experți cheie solicitați pe categorie de expertiză	204
11.2 Profilul experților cheie	207
11.3 Alte condiții referitoare la calificarea experților	218
11.4 Alți experți non-cheie	220

1. Informații generale

1.1 Introducere

Prezentul caiet de sarcini a fost întocmit în conformitate cu prevederile Legii nr. 98/2016 privind achizițiile publice, cu modificările și completările ulterioare, și ale Hotărârii de Guvern nr. 395/2016 pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică/acordului-cadru din Legea nr. 98/2016 privind achizițiile publice, cu modificările și completările ulterioare.

Caietul de sarcini face parte integrantă din documentația de atribuire și conține specificațiile tehnice, respectiv ansamblul cerințelor obligatoriu de îndeplinit, pe baza cărora se elaborează propunerea tehnică de către ofertant.

Caietul de Sarcini conține indicații privind regulile de bază care trebuie respectate, astfel încât potențialii ofertanți să elaboreze propunerea tehnică corespunzător cu necesitățile autorității contractante.

Pentru scopul prezentului caiet de sarcini, ca parte integrantă a documentației de atribuire, orice activitate, componentă, cerință, funcționalitate sau responsabilitate descrisă într-un anumit capitol din caietul de sarcini și nespecificată în mod explicit în alt capitol trebuie interpretată ca fiind menționată în toate capitolele. Ofertantul are obligația de a interpreta coerent cerințele și de a include în oferta sa toate activitățile necesare pentru îndeplinirea în integralitate a obiectului contractului, chiar dacă unele cerințe nu sunt repetate în mod expres în toate secțiunile documentației.

În conformitate cu regulile de elaborare a documentației de atribuire prevăzute la art. 156 din Legea nr. 98/2016, specificațiile tehnice din prezentul caiet de sarcini care precizează un anumit producător, o anumită origine sau un anumit procedeu care caracterizează serviciile prestate și care se referă la mărci, brevete, tipuri, la o origine sau la o producție specifică se consideră a fi însoțite de cuvintele „sau echivalent”, indiferent dacă aceste cuvinte sunt prevăzute expres sau nu în prezentul document.

Ofertanții au obligația de a răspunde integral și explicit tuturor cerințelor prevăzute în prezentul caiet de sarcini, acestea fiind considerate cerințe minime. Ofertele vor fi redactate într-o formă care nu limitează, condiționează sau restrânge aria de acoperire sau complexitatea serviciilor solicitate.

Se admit doar oferte integrale, care respectă toate cerințele minime obligatorii atât din punct de vedere cantitativ, cât și calitativ. Ofertele care nu îndeplinesc toate cerințele minime solicitate prin caietul de sarcini vor fi declarate neconforme. Nu sunt acceptate oferte parțiale. Nu se acceptă depunerea de oferte alternative. Ofertele care nu vor fi considerate relevante raportat la obiectul contractului și care nu pot îndeplini necesitățile și cerințele din caietul de sarcini vor fi declarate neadecvate. Orice ofertă care se abate de la cerințele minime va fi considerată admisibilă numai în condițiile în care demonstrează, în mod clar și justificat, că soluția propusă asigură un nivel calitativ superior celui solicitat, fără a afecta caracterul complet și funcțional al livrabilelor și serviciilor.

Prevederile prezentului Caiet de sarcini se completează cu informațiile și cerințele din Studiul de fezabilitate și Proiectul tehnic atașate.

Ofertantul este pe deplin responsabil pentru interpretarea corectă și completă a tuturor cerințelor tehnice, funcționale și administrative, și trebuie să asigure prin propunerea tehnică îndeplinirea integrală a obiectului contractului.

Oferta tehnică aferentă acestei proceduri de atribuire va fi obligatoriu redactată integral în limba română, nerespectarea acestei cerințe ducând la declararea acesteia ca fiind neconformă.

În cazul în care la ofertă sunt atașate documente tehnice privind produsele oferite (cataloage, certificate, acorduri tehnice, altele similare), într-o limbă străină alta decât limba engleză, acestea vor fi obligatoriu însoțite de traducerea autorizată a acestora în limba română.

Ofertantul declarat câștigător se obligă să prezinte toate documentele/informațiile solicitate de către persoanele autorizate și/sau organismele de control/audit existente la nivel european și național.

Astfel, ofertantul declarat câștigător se obligă să asigure accesul neîngrădit al autorităților naționale cu atribuții de verificare, control și audit, al serviciilor Comisiei Europene, al Curții Europene de Conturi, al reprezentanților Direcției Naționale Anticorupție, al reprezentanților Parchetului European – EPPO, al reprezentanților serviciului specializat al Comisiei Europene - Oficiul European pentru Lupta Antifraudă - OLAF, precum și al reprezentanților Departamentului pentru Lupta Antifraudă - DLAF, în limitele competențelor ce le revin, în cazul în care aceștia efectuează investigații/verificări/controale/auditori la fața locului și solicită declarații, evidențe, documente justificative, informații și date statistice referitoare la investiție.

Ofertantul declarat câștigător are obligația de a transmite, înaintea semnării contractului de achiziție publică, datele și informațiile cu privire la beneficiarul real al fondurilor alocate din PoCIDIF, conform prevederilor Directivei (UE) 2015/849 a Parlamentului European și a Consiliului din 20 mai 2015 privind prevenirea utilizării sistemului financiar în scopul spălării banilor sau finanțării terorismului, de modificare a Regulamentului (UE) nr. 648/2012 al Parlamentului European și al Consiliului și de abrogare a Directivei 2005/60/CE a Parlamentului European și a Consiliului și a Directivei 2006/70/CE a Comisiei. Astfel, înaintea semnării contractului de achiziție, reprezentantul legal al ofertantului va completa o declarație pe propria răspundere privind beneficiarul real, conform modelului din secțiunea „Formulare” a documentației de atribuire, sub sancțiunea prevederilor art. 326 din Codul Penal privind falsul în declarații.

De asemenea, în conformitate cu prevederile articolelor 56 și 57 din Legea nr. 129/2019 pentru prevenirea și combaterea spălării banilor și finanțării terorismului, precum și pentru modificarea și completarea unor acte normative, cu modificările și completările ulterioare, precum și în conformitate cu prevederile articolelor 34⁴ și 34⁵ din Ordonanța Guvernului nr. 26/2000 cu privire la asociații și fundații, cu

modificările și completările ulterioare, ofertantului declarat câștigător îi revine obligația actualizării informațiilor de fiecare dată când are loc o modificare a acestora, sub rezerva aplicării sancțiunilor contravenționale și a dizolvării societății, asociației sau fundației, după caz.

Prestatorii au obligația de a informa, în paralel, atât autoritatea contractantă, cât și ONRC/ Ministerul Justiției ori de câte ori intervine o modificare la declarația privind beneficiarul real al persoanei juridice, pe durata de valabilitate a contractului.

Cerința se va aplica în mod corespunzător și în cazul subcontractorilor și/sau terților susținători.

1.2 Autoritatea contractantă

Autoritatea contractantă este Ministerul Culturii (denumit în continuare „MC”), prin Unitatea de Management a Proiectului (denumită în continuare „UMP”), în calitate de lider de parteneriat și beneficiar al finanțării nerambursabile acordate de către AM PoCIDIF pentru implementarea proiectului intitulat "ePatrimoniu" (cod SMIS 320807), denumit în continuare „proiect”.

MC este organ de specialitate al administrației publice centrale, cu personalitate juridică, în subordinea Guvernului, care elaborează și asigură aplicarea strategiei și politicilor în domeniul culturii.

MC este autoritatea care asigură protejarea patrimoniului cultural, inclusiv a patrimoniului imaterial, prin crearea cadrului legislativ specific și prin programe de evaluare, protecție, clasare, restaurare, conservare și punere în valoare (inclusiv digitalizare și accesibilizare). Acesta acționează în baza cadrului legal stabilit prin Hotărârea Guvernului nr. 90/2010 privind organizarea și funcționarea Ministerului Culturii, cu modificările și completările următoare, precum și a altor acte normative relevante, cum ar fi: Legea nr. 422/2001 privind protejarea monumentelor istorice, Legea nr. 182/2000 privind protejarea patrimoniului cultural național mobil etc.

Aceste responsabilități sunt exercitate fie direct, fie prin instituții subordonate, precum Institutul Național al Patrimoniului (denumit în continuare „INP”) sau serviciile publice deconcentrate (direcțiile județene de cultură sau a municipiului București – denumite în continuare „DJC”). Un rol important îl joacă comisiile de specialitate, organisme științifice de specialitate în domeniul protejării patrimoniului cultural, fără personalitate juridică, care funcționează pe lângă Ministerul Culturii/serviciile deconcentrate (Comisia Națională a Monumentelor Istorice, Comisia Națională de Arheologie, Comisia Națională a Muzeelor și Colecțiilor, Comisia Națională pentru Salvagardarea Patrimoniului Cultural Imaterial, precum și alte comisii de specialitate din domeniul culturii).

UMP este organismul fără personalitate juridică constituit la nivelul MC, separat din punct de vedere tehnic și organizatoric de alte structuri ale ministerului, responsabil de gestionarea finanțărilor rambursabile și nerambursabile ale MC.

În cadrul acestei proceduri, MC-UMP îndeplinește rolul de autoritate contractantă („AC”), respectiv Beneficiar în cadrul contractului.

1.3 Contextul realizării achiziției

Ministerul Culturii a semnat contractul de finanțare pentru implementarea proiectului cod SMIS 320807, intitulat *ePatrimoniu*, o inițiativă strategică menită să transforme modul în care patrimoniul cultural este administrat și valorificat în România. Proiectul este cofinanțat de Uniunea Europeană prin POCIDIF, P2. *Digitalizare în administrația publică centrală și mediul de afaceri*, RSO1.2: *Valorificarea avantajelor digitalizării, în beneficiul cetățenilor, al companiilor, al organizațiilor de cercetare și al autorităților publice*, Acțiunea 2.2 *E-guvernarea și digitalizarea în beneficiul cetățenilor*, Măsura 2.2.3 *Digitalizarea în cultură*. Proiectul este implementat în parteneriat cu Serviciul de Telecomunicații Speciale. Perioada de implementare a proiectului se încheie în Decembrie 2029.

Scopul proiectului este realizarea unui sistem digital – platformă națională comună pentru furnizarea de servicii publice digitale în domeniul patrimoniului cultural, care oferă servicii semnificativ îmbunătățite de e-guvernare legate de patrimoniul cultural atât cetățenilor, cât și entităților private (companii și organizații neguvernamentale) care interacționează cu Ministerul Culturii fie direct, fie prin intermediul instituțiilor subordonate acestuia, pentru obținerea de informații și documente.

Sistem digital național *ePatrimoniu* va centraliza informațiile despre patrimoniul cultural mobil, imobil și imaterial și va permite furnizarea de servicii publice electronice pentru cetățeni, instituții și specialiști din domeniu. Acest sistem digital va înlocui procedurile administrative pe hârtie cu soluții electronice moderne, facilitând furnizarea online de servicii precum: eliberarea avizelor de intervenție asupra monumentelor istorice, autorizarea cercetărilor arheologice, emiterea certificatelor de acreditare pentru experți etc. Prin implementarea unei soluții tehnice integrate pentru realizare a sistemului digital *ePatrimoniu* se urmărește creșterea eficienței administrative, reducerea birocrăției, transparența decizională și protejarea activă a patrimoniului cultural național.

La finalul perioadei de implementare, va exista un singur sistem digital funcțional, care va reuni toate informațiile existente în diverse platformele digitale dedicate patrimoniului mobil și imobil, cu posibilitatea de a accesa servicii de e-guvernare și fluxuri digitale pentru specialiștii și deținătorii de patrimoniu. Se preconizează un număr de 65.000 de utilizatori de noi servicii și aplicații digitale publice.

Pentru realizarea cu succes și încadrarea în termenul de realizare a proiectului, este necesară achiziționarea serviciilor de „dezvoltare a sistemului digital *ePatrimoniu*”.

1.4. Descrierea situației actuale

La nivelul Ministerului Culturii a fost dezvoltată aplicația pilot SIPCI (<https://patrimoniu-cultural.ro/>) pentru colectarea și centralizarea dovezilor referitoare la patrimoniul cultural imobil.

Sistemul digital ePatrimoniu va include o secțiune privind managementul bunurilor culturale imobile, care implică preluarea, extinderea și optimizarea funcționalităților aplicației pilot SIPCI și a informațiilor existente, astfel încât acestea să devină un suport activ pentru actul administrativ digitalizat prin servicii de tip e-guvernare. Componenta managementul patrimoniului cultural va fi dezvoltată astfel încât să permită, printre altele, înregistrarea de monumente istorice digitizate prin tehnologie 3D de tip high quality records.

Totodată, la nivelul Ministerului Culturii a fost dezvoltată platforma informatică on-line Biblioteca Digitală a României – Culturalia (<https://culturalia.ro>), care constituie o bază de date unificată a bunurilor culturale mobile și a registrelor digitale cu elemente de patrimoniu existente în România. Aceasta reunește într-un sistem integrat peste 750.000 de resursele digitale variate din domeniul patrimoniului cultural mobil.

Sistemul digital ePatrimoniu va realiza preluarea, extinderea și optimizarea funcționalităților Bibliotecii Digitale a României (<https://culturalia.ro>) prin dezvoltarea unei Componente managementul patrimoniului cultural și prin importul bunurilor digitalizate existente în Culturalia, a imaginilor, informațiilor și metadatelor despre acestea, astfel încât să devină un suport activ pentru actul administrativ digitalizat prin servicii de tip e-guvernare.

De asemenea, Componenta managementul patrimoniului cultural va permite legarea și agregarea informațiilor și a metadatelor relaționate privind localizarea și dreptul de proprietate / administrare asupra bunurilor culturale mobile cu informațiile și metadatele bunurilor culturale imobile (patrimoniu construit), astfel încât imaginea de ansamblu asupra localizării geografice și / sau a elementelor de identificare la un moment de timp să poată fi făcută cu ușurință și exactitate. Această legătură între informații va permite dezvoltarea de funcționalități de prezentare moderne prin realizarea de expuneri dinamice, precum galerii sau tururi virtuale, realitate augmentată etc.

De asemenea, funcționalitățile optimizate ale sistemul digital ePatrimoniu va eficientiza modul de stocare a informațiilor și metadatelor aferente modelului de ontologie adaptat și a cerințelor tehnologice și funcționale actuale și va permite introducerea și/sau importul, catalogarea și documentarea de noi bunuri culturale mobile, precum și exportul acestora în Biblioteca Digitală Europeană (Europeana) prin API-uri / protocolul OAI-PMH (Open Archives Initiative Protocol for Metadata Harvesting).

1.5. Beneficiile anticipate

Beneficiile realizării sistemului digital ePatrimoniu constau în servicii semnificativ îmbunătățite de e-guvernare legate de patrimoniul cultural, adresate atât cetățenilor, cât și entităților private (companii și organizații neguvernamentale) care interacționează cu Ministerul Culturii fie direct, fie prin intermediul instituțiilor subordonate acestuia, pentru obținerea de informații și documente.

Totodată se va crea o bază de date dedicată patrimoniului cultural, care va fi populată cu date corelate pentru a contextualiza situația despre monumente istorice – adresă actualizată, numărul de cadastru pentru conectare la registrul de cadastru, geolocalizarea, proprietarul, informații despre arhitectură, istorie și istoric de restaurare a clădirii etc., precum și informații despre alte tipuri de bunuri mobile și de patrimoniu imaterial.

În același timp, sistemul digital va contribui la trecerea de la procesele pe hârtie la serviciile electronice, urmând a fi furnizate fluxuri digitale și servicii e-guvernare de tipul eliberării avizelor de intervenție, autorizațiilor de cercetare arheologică, certificatelor de acreditare experți etc.

La finalul contractului, va exista un sistem digital funcțional, care va reuni toate informațiile existente în platformele digitale dedicate patrimoniului imobil, mobil și imaterial și posibilitatea de a accesa servicii de e-guvernare și fluxuri digitale de specialiști și deținătorii de patrimoniu.

Principalele beneficii identificate sunt:

- Digitalizarea patrimoniului cultural – transformarea digitală a bunurilor culturale mobile, imobile și imateriale într-un sistem național unic, cu funcții de arhivare, catalogare partajată și acces online extins;
- Acces public rapid, transparent și centralizat – o interfață unică pentru cetățeni, specialiști, autorități și instituții, care oferă acces la informații digitale relevante din domeniul patrimoniului cultural;
- Unificarea și interoperabilitatea bazelor de date – integrarea platformelor existente într-un sistem digital unic, interconectat cu registre naționale și europene (ex: Europeana), dar și cu baze de date administrative (financiare, cadastrale, teritoriale etc.);
- Simplificarea și digitalizarea proceselor administrative – furnizarea online a avizelor, autorizațiilor, certificatelor și altor servicii de e-guvernare pentru patrimoniu, cu trasabilitate și eficientizarea fluxurilor;
- Crearea unui ghișeu unic digital pentru patrimoniu – un sistem digital unificat care concentrează toate tipurile de servicii și informații despre patrimoniu imobil, mobil, arheologic și imaterial;
- Conservarea digitală pe termen lung – arhivarea durabilă a colecțiilor culturale în format digital;

- Promovarea patrimoniului cultural la nivel internațional – vizibilitate crescută prin alinierea la standardele internaționale de metadate și interconectarea cu platforme internaționale, precum Europeana;
- Accesibilitate și incluziune digitală – sistem digital multilingv (română și engleză), conform cu standardele de accesibilitate web, adaptat pentru persoane cu dizabilități;
- Sustenabilitate și dezvoltare continuă a sistemului – actualizări tehnologice periodice, arhitectură scalabilă și implicarea comunității în co-crearea de conținut și extinderea resurselor digitale;
- Conservarea și valorificarea patrimoniului imaterial – digitalizarea și promovarea tradițiilor, expresiilor orale, meșteșugurilor și altor elemente de patrimoniu viu;
- Sprijin pentru educație, cercetare și turism cultural – oferirea de resurse digitale pentru profesori, elevi, studenți, cercetători și turiști, în scop educativ, științific și de promovare turistică;
- Creșterea eficienței administrative – automatizarea fluxurilor de lucru, reducerea timpului de procesare și uniformizarea documentației la nivel național;
- Reducerea costurilor pentru utilizatori – acces online gratuit sau cu costuri reduse, eliminând nevoia deplasărilor și timpul pierdut pentru solicitări fizice;
- Promovarea identității culturale și a diversității etnice – reprezentarea echilibrată a patrimoniului tuturor comunităților, inclusiv minoritățile, în sistemul digital național;
- Crearea unei infrastructuri tehnologice moderne – implementarea de componente avansate precum GIS (pentru localizarea patrimoniului și evaluarea riscurilor seismice sau de inundații), inteligență artificială (AI) pentru analiză semantică, baze de date inteligente și interconectarea cu sisteme cartografice;
- Susținerea unei transformări economice inovatoare – prin conectivitate TIC regională, digitalizare extinsă și acces deschis la resurse, proiectul sprijină modernizarea administrației, realizarea unor analize de politici publice și decizii bazate pe date, fundamentarea și elaborarea de programe de investiții și evaluarea acestora, prioritizarea investițiilor și monitorizarea progreselor și dezvoltare economică bazată pe cunoaștere.

2. Informații referitoare la contract

2.1 Obiectul contractului

Obiectul contractului îl constituie **dezvoltarea și implementarea sistemului digital ePatrimoniu**, o platformă digitală națională comună destinată managementului

resurselor culturale și furnizării de servicii publice digitale în domeniul patrimoniului cultural.

Contractul include, dar fără a se limita la acestea:

- prestarea serviciilor de analiză, proiectare, dezvoltare software, testare, interconectare, configurare, operaționalizare
- livrarea tuturor componentelor funcționale, tehnice, administrative și software ale sistemului
- furnizarea tuturor licențelor software necesare instalării și funcționării sistemului digital
- realizarea interoperabilității cu alte sisteme și platforme relevante la nivel național, european, internațional
- popularea cu date preluate din bazele de date ale Autorității contractante și ale instituțiilor subordonate, indicate în prezentul Caiet de sarcini;
- integrarea sistemului în infrastructura existentă
- configurarea mediului de producție și punerea acestuia în exploatare
- instruirea utilizatorilor și transferul cunoștințelor către Autoritatea Contractantă
- mentenanța corectivă și evolutivă, suportul tehnic și garanția.

Rezultatul final al contractului trebuie să fie un sistem complet funcțional, integral testat, configurat, interconectat, operațional și integrat, cu date migrate, pregătit pentru utilizare imediată în mediul de producție, dezvoltat în conformitate cu toate cerințele tehnice, funcționale, administrative, de securitate, de interoperabilitate și de orice altă natură prevăzute în prezentul caiet de sarcini. Sistemul digital funcțional integrat final va fi în stare complet operațională, fără a necesita intervenții, dezvoltări, configurări, ajustări sau costuri suplimentare din partea autorității contractante sau a unor terți pentru punerea sa în exploatare, toate aceste activități fiind incluse în obligațiile Prestatorului și în prețul contractului.

2.2 Durata contractului și locul desfășurării activităților

Contractul intră în vigoare la data semnării de către ultima parte și se finalizează la data executării integrale a obligațiilor asumate de ambele Părți.

Durata contractului se compune din:

- perioada între data constituirii garanției de bună execuție și data recepției finale a sistemului digital ePatrimoniu
- perioada între data recepției finale a sistemului digital ePatrimoniu și data recepției finale a serviciilor de mentenanță.
- perioada între data recepției finale a serviciilor de mentenanță și data finalizării perioadei de garanție.

Data recepției finale a **sistemului** este data la care sistemul digital funcțional integrat final este operațional în mediul de producție, recepționat calitativ și fără obiecțiuni de către AC printr-un **proces-verbal de recepție calitativă finală a sistemului digital ePatrimoniu**. Sistemul digital varianta finală integrată trebuie să fie pus în producție conform metodologiei de implementare descrisă în secțiunile 8.4 și 9.2. Data recepției finale a sistemului nu poate fi mai târziu de 30 Noiembrie 2029.

Data recepției finale a **serviciilor de mentenanță** este data la care se finalizează perioada de asigurare a mentenanței corective și evolutive, recepționată calitativ și fără obiecțiuni de către AC printr-un **proces-verbal de recepție calitativă finală a serviciilor de mentenanță**.

Data recepției finale a **serviciilor** este data la care se finalizează perioada de garanție recepționată calitativ și fără obiecțiuni de către AC printr-un **proces-verbal de recepție finală**.

Activitățile contractului se vor desfășura la sediul Contractantului sau ale Autorității contractante. Locația de desfășurare a întâlnirilor de lucru și de monitorizare a progresului activităților, corespunzătoare fiecărei faze din contract se stabilește de Autoritatea Contractantă pentru fiecare întâlnire. În funcție de subiectele abordate, părțile pot agreea ca aceste întâlniri de lucru să se desfășoare și online.

2.3 Scopul contractului și rezultate așteptate

Scopul contractului este de a susține transformarea digitală și modernizarea gestionării patrimoniului cultural național prin dezvoltarea și implementarea unui sistem digital național comun, care să asigure acces facil, transparent și integrat la informațiile și serviciile publice digitale aferente patrimoniului cultural.

Prin acest sistem se urmărește creșterea eficienței administrative, promovarea identității culturale, facilitarea accesului democratizat la resurse culturale pentru cetățeni, instituții și cercetători, precum și conservarea durabilă și valorificarea patrimoniului cultural material și imaterial al României, în conformitate cu standardele internaționale și bunele practici în domeniu.

Principalele rezultate așteptate constau în:

- un sistem digital național unic pentru patrimoniul cultural, care integrează informații despre patrimoniul imobil, mobil, arheologic și imaterial, în format digital structurat și accesibil, populat cu date și informații importate din sursele existente (ex. culturalia, SIPCI, DocPat, eGISpat, RAN, Acera etc)
- un ghișeu digital unic pentru furnizarea de servicii de e-guvernare în domeniul patrimoniului cultural;
- servicii de e-guvernare aferente patrimoniului cultural, destinate specialiștilor și deținătorilor de patrimoniu, cu trasabilitate, standardizare procedurală și interoperabilitate cu alte sisteme și platforme digitale publice;

- infrastructură IT completă (hardware & software), creată pentru stocarea, accesarea și arhivarea în siguranță a datelor și obiectelor digitale asociate patrimoniului;
- sistem GIS integrat, pentru vizualizarea geospațială a patrimoniului imobil și identificarea riscurilor (seism, inundații etc) prin conexiuni specifice;
- tezaure terminologice și ontologii specializate, aliniate cu standardele internaționale, dezvoltate și integrate în sistemul digital pentru descrierea coerentă și interoperabilă a resurselor culturale;
- un Catalog Național Partajat dezvoltat, cu mecanisme de achiziție online de metadata și expunere prin portal web, aplicații mobile și API-uri;
- funcționalități AI pentru procesare inteligentă implementate;
- interfață multilingvă și accesibilă, inclusiv pentru persoane cu dizabilități;
- un instrument integrat de realizare resurse digitale pentru profesori, elevi, studenți, cercetători și turiști, în scop educativ, științific și de promovare turistică;
- obținerea recunoașterii de către europeana.eu ca platformă agregatoare pentru obiectele culturale digitale naționale, care să poată partaja obiecte direct cu aceasta (în funcție de capacitatea europeana.eu).
- funcționalități avansate de analiză și interogare a datelor pentru prioritizarea intervențiilor asupra patrimoniului;
- depozit digital sigur pentru stocarea pe termen lung a obiectelor digitale și copiilor de siguranță;
- funcționalități de dezvoltare profiluri publice ale direcțiilor județene de cultură.

2.4 Sursa de finanțare

Cheltuielile aferente prezentei achiziții sunt eligibile conform bugetului proiectului *ePatrimoniul*, finanțat prin POCIDIF.

3. Grupuri țintă și utilizatori

3.1 Categoriile de utilizatori

Implementarea cu succes a sistemului digital ePatrimoniul presupune implicarea și colaborarea unui număr variat de factori interesați, atât interni, cât și externi, care vor beneficia în mod direct sau indirect de funcționalitățile platformei și de digitalizarea proceselor administrative din domeniul patrimoniului cultural.

Principalii factori interesați în implementarea contractului sunt utilizatorii sistemului digital:

- administratori de sistem;

- angajați ai Ministerul Culturii - autoritatea publică centrală responsabilă de coordonarea, protecția, conservarea și valorificarea patrimoniului cultural național;
- angajați ai direcțiilor județene pentru cultură, respectiv a municipiului București - au un rol esențial în protejarea și valorificarea patrimoniului cultural național, acționând ca servicii publice deconcentrate ale Ministerului Culturii și implementează strategiile și politicile ministerului la nivel local, în conformitate cu prevederile legale;
- angajați ai Institutului Național al Patrimoniului - instituție publică de importanță națională, cu personalitate juridică, subordonată Ministerului Culturii, având rol esențial în protejarea, conservarea, restaurarea și valorificarea patrimoniului cultural național;
- membri ai comisiilor de specialitate ale Ministerului Culturii - organisme științifice de specialitate, fără personalitate juridică, cu rol consultativ și de avizare în domeniul protejării și valorificării patrimoniului cultural. În mod organizat, ele sunt structurate pe domenii specifice — arheologie, patrimoniu construit / imobil, patrimoniu mobil și patrimoniu imaterial — iar fiecare comisie are competențe dedicate în câte un domeniu. Astfel, comisiile examinează și avizează documentații de intervenție, clasificări, metodologii, dosare de candidatură pentru titluri de patrimoniu, propun politici sau priorități de protecție și gestionează contestațiile din domeniul patrimoniului.

Comisiile de specialitate ale Ministerul Culturii pe domenii:

Arheologie:

Comisia Națională de Arheologie (CNA)

Comisia Națională Limes (CNL)

Comisia Națională pentru Soluționarea Contestațiilor în Domeniul Arheologiei (CNSCDA)

Patrimoniu construit/imobil (monumente, ansambluri, situri):

Comisia Națională a Monumentelor Istorice (CNMI) cu secțiunile specialitate: a. Secțiunea de Evidență, b. Secțiunea Tehnică Arhitectură și Inginerie, c. Secțiunea de Urbanism și Zone Protejate, d. Secțiunea de Componente Artistice, e. Comisiile Zonale ale Monumentelor Istorice (CZMI)

Comisia pentru Soluționarea Contestațiilor în Domeniul Patrimoniului Cultural Imobil

Patrimoniu mobil:

Comisia Națională a Muzeelor și Colecțiilor (CNMC)

Patrimoniu imaterial / intangibil:

Comisia Națională pentru Salvagardarea Patrimoniului Cultural Imaterial (CNSPCI)

- experți / specialiști / verificatori atestați de MC;
- angajați ai autorităților administrației publice locale din cadrul unităților administrativ-teritoriale: comisiile de specialitate ale consiliului local, aparatul de specialitate al primarului sau al consiliului județean, precum și compartimentele funcționale sau instituțiile subordonate relevante, cu atribuții legale, respectiv competențe decizionale în domeniul urbanismului și al amenajării teritoriului la nivel local, precum și în domeniul protejării patrimoniului cultural.
- angajați ai instituțiilor culturale - muzee, biblioteci, ai unităților de cult și ai altor entități publice sau private care dețin bunuri aparținând patrimoniului cultural național și au obligații stricte reglementate prin legislația specifică, ce vizează protejarea, conservarea, inventarierea și valorificarea patrimoniului.
- angajați ai autorităților administrației centrale, ai companiilor și instituțiilor publice (Ministerul Dezvoltării Lucrărilor Publice și Administrației, Ministerul Energiei, Ministerul Investițiilor și Proiectelor Europene, Ministerul Mediului, Apelor și Pădurilor, Ministerul Transportului, Ministerul Afacerilor Interne, Ministerul Finanțelor, Agenția Națională de Cadastru și Publicitate Imobiliară, Institutul Național de Statistică, Administrația Fondului de Mediu, Inspectoratul de Stat în Construcții, Secretariatul General al Guvernului, Platforma Națională de Reducere a Riscului la Dezastre, etc.)
- persoanele fizice și juridice din România, în calitate de deținători, proprietari sau administratori de bunuri aparținând patrimoniului cultural național, care au obligații stricte stabilite prin legislația relevantă, ce vizează asigurarea protejării, conservării și valorificării patrimoniului.
- mediul privat: companii de proiectare, execuție, producători de materiale de construcții, case de licitație, notari publici etc.
- laboratoare de restaurare;
- cercetători, arheologi, detectoriști, meșteșugari;
- organizațiile neguvernamentale care activează în domeniul patrimoniului cultural;
- cetățeni.

NOTĂ: Lista de mai sus nu este exhaustivă. O listă detaliată a actorilor implicați va fi elaborată în faza de analiză și proiectare a soluției, urmând a fi actualizată, dacă este cazul, în faza de dezvoltare, migrare și testare.

3.2 Roluri și drepturi de acces în sistemul digital

Rolurile și drepturile de acces în cadrul sistemului digital ePatrimoniu vor fi definite în detaliu în fazele de analiză și proiectare (detaliat în secțiunile 8.1 și 8.2), precum și pe parcursul dezvoltării și după punerea în producție a sistemului digital, în funcție de atribuțiile fiecărei categorii de utilizatori și de nivelul de acces necesar pentru desfășurarea activităților specifice.

Rolurile și drepturile de acces în cadrul sistemului digital ePatrimoniu vor fi definite și gestionate pentru a asigura confidențialitatea, integritatea și disponibilitatea datelor, conformitatea cu legislația în vigoare și trasabilitatea acțiunilor utilizatorilor prin log-uri de audit.

Fiecare rol va avea permisiuni detaliate, configurabile, în funcție de nivelul de responsabilitate și acces. Se vor putea defini roluri personalizate pentru cazuri particulare și se va implementa un sistem de autentificare securizată [informații detaliate în subsecțiunea 7.3.2 din prezentul caiet de sarcini].

Accesul la anumite date va fi reglementat în conformitate cu legislația privind protecția datelor (GDPR) și cu nivelul de clasificare a informațiilor [informații detaliate în secțiunea 7.5 din prezentul caiet de sarcini].

Conturile de acces vor fi asociate exclusiv persoanelor fizice, fiecare utilizator având un cont individual, unic și identificabil (prin cod unic de identificare și/sau prin certificat digital). Suplimentar față de nivelul de utilizator persoană fizică, sistemul va cuprinde un nivel distinct de **entități organizaționale**, care reprezintă structuri juridice, precum: instituții publice, societăți comerciale, organizații neguvernamentale sau alte forme de organizare legal constituite. Entitățile organizaționale vor avea o serie de **attribute** asociate care vor fi definite în faza de analiză (exemple: entitate cu contribuții în MPC, solicitant de avize, etc)

Adăugarea unei entități organizaționale de către o persoană fizică

Persoana fizică care este reprezentantul legal al entității respective sau persoana fizică împuternicită expres de către reprezentantul legal al entității, autentificată în sistem, va putea **adăuga** o entitate organizațională.

Procesul de adăugare presupune introducerea datelor de identificare ale entității și, după caz, încărcarea documentelor justificative (ex. acte doveditoare privind calitatea de reprezentant legal sau împuternicire). Persoana fizică va deveni **administratorul entității organizaționale** și va putea acționa în sistemul digital în numele entității, fără a pierde caracterul personal al contului său de utilizator.

În funcție de tipul entității și tipul de operațiuni asociate în sistem, se vor implementa validări suplimentare necesare.

Administratorul unității organizaționale va putea fi schimbat cu o altă persoană fizică, printr-un proces de validare și înregistrare documentată.

Asocierea unei persoane fizice cu o entitate organizațională

Persoanele fizice autentificate în sistem vor putea solicita **asocierea** lor cu entități organizaționale. Cererea de asociere va fi aprobată sau respinsă de administratorul entității organizaționale, iar solicitantul va fi notificat cu privire la rezoluție.

3.2.1 Niveluri de acces în sistemul digital ePatrimoniu

Sistemul digital ePatrimoniu va cuprinde un model de control al accesului bazat pe roluri (RBAC – Role Based Access Control), extins cu reguli contextuale și permisiuni configurabile la nivel de utilizator, entitate organizațională, componentă și tip de resursă. Nivelurile de acces vor fi definite astfel încât să asigure un echilibru între securitate, trasabilitate, flexibilitate operațională și respectarea cadrului legal.

3.2.1.1 Acces public - Neautentificat

Acest nivel de acces este destinat publicului larg și nu necesită autentificare în sistem.

Utilizatorii cu acces public vor putea consulta, fără drept de modificare, informații publice despre patrimoniul cultural (registre publice, fișe publicabile, hărți, galerii, statistici agregate), accesa informații generale despre serviciile publice digitale disponibile, vizualiza anunțuri, calendare ale ședințelor comisiilor, decizii publice și alte informații de interes general.

Sistemul digital va cuprinde mecanisme care asigură filtrarea și protejarea datelor, astfel încât utilizatorii cu acces public să poată vizualiza doar informațiile autorizate și să fie prevenit accesul neautorizat la fluxuri de e-guvernare sau la date cu caracter restricționat sau personal.

3.2.1.2 Utilizator autentificat – persoană fizică

Acest nivel de acces este asociat tuturor utilizatorilor autentificați în sistem, persoane fizice, care dețin un cont individual, unic și identificabil. Acest nivel reprezintă baza pentru toate celelalte niveluri de acces din sistem.

În funcție de rolurile atribuite, un utilizator autentificat va putea:

- accesa dashboard-ul intern al platformei, iniția, completa și urmări solicitări în cadrul serviciilor de e-guvernare;
- încărca documente, semna electronic și primi documente emise de autorități;
- accesa funcționalități din componenta de Management Patrimoniu Cultural, în limita drepturilor acordate;
- acționa fie în nume propriu, fie în numele unei entități organizaționale asociate, dacă există o astfel de asociere validă.

Un utilizator persoană fizică poate acționa în nume propriu sau în numele și pe seama altei persoane, în calitate de împuternicit, în baza unei împuterniciri valabile, înregistrate și validate în sistem, în condițiile stabilite de cadrul legal aplicabil. Acțiunile efectuate în baza unui mandat vor fi marcate distinct și jurnalizate corespunzător.

3.2.1.3 Utilizator asociat unei entități organizaționale

Acest nivel de acces se aplică utilizatorilor persoane fizice care sunt asociați uneia sau mai multor entități organizaționale înregistrate în sistem.

Drepturile utilizatorului vor fi determinate cumulativ de:

- rolurile generale ale utilizatorului;
- rolurile și permisiunile acordate la nivelul fiecărei entități;
- tipul entității (instituție publică, operator economic, ONG etc.).

Utilizatorii asociați unei entități vor putea, în funcție de permisiuni:

- iniția și gestiona procese de e-guvernare în numele entității;
- completa, actualiza și administra date aferente patrimoniului gestionat de entitate;
- accesa istoricul acțiunilor și documentelor generate în numele entității.

3.2.1.4 Administrator de entitate organizațională

Administratorul de entitate este o persoană fizică ce are drepturi extinse de administrare asupra unei entități organizaționale asociate.

Administratorul de entitate va avea dreptul de a:

- gestiona datele de identificare și profilul entității;
- asocia și dezasocia utilizatori persoane fizice entității;
- defini și atribui roluri și permisiuni la nivel de entitate;
- controla accesul utilizatorilor la funcționalitățile și datele entității;
- revoca drepturi și suspenda accesul utilizatorilor, în condițiile stabilite de sistem.

Rolul de administrator de entitate este limitat strict la entitatea respectivă și nu conferă drepturi asupra altor entități sau asupra configurării generale a sistemului.

3.2.1.5 Utilizatori instituționali / funcționali

Acest nivel de acces este destinat utilizatorilor din cadrul autorităților și instituțiilor publice implicate în procesele administrative și de avizare (Ministerul Culturii, instituții subordonate, direcții județene, comisii de specialitate etc.).

În funcție de rolul funcțional atribuit, acești utilizatori vor putea:

- gestiona și soluționa solicitări în cadrul fluxurilor de e-guvernare;
- analiza documentații, formula observații, avize și decizii;
- participa la activitatea comisiilor de specialitate (inclusiv vot electronic);
- accesa și actualiza date din componenta de Management Patrimoniu Cultural, în limitele competențelor legale.

Permisiunile vor fi diferențiate în funcție de instituție, domeniu de competență și poziție funcțională.

3.2.1.6 Administrator de sistem

Administratorul de sistem reprezintă nivelul cel mai înalt de acces și este limitat la un număr restrâns de utilizatori autorizați.

Administratorii de sistem pot avea roluri diferențiate, în funcție de atribuții.

Administratorii de sistem vor avea dreptul de a:

- configura și administra utilizatorii, rolurile și permisiunile globale;
- gestiona structura de roluri, nomenclatoare și setări generale ale platformei;
- configura fluxuri, șabloane, servicii electronice și parametri tehnici;
- accesa funcționalități de audit, monitorizare și raportare;
- interveni pentru mentenanță, suport și securitate.

Accesul administratorilor de sistem va fi strict controlat, protejat prin mecanisme de autentificare consolidată, jurnalizat și supus mecanismelor de audit.

3.2.1.7 Principii generale privind nivelurile de acces

- Drepturile de acces vor fi acordate pe principiul **minimului necesar** (least privilege) și vor fi revizuite periodic sau ori de câte ori intervin modificări ale rolului sau statutului utilizatorului.
- Toate acțiunile utilizatorilor vor fi jurnalizate pentru asigurarea trasabilității. Jurnalurile de audit vor fi protejate împotriva modificării sau ștergerii neautorizate și vor fi păstrate conform politicilor de retenție stabilite.
- Nivelurile de acces vor putea fi extinse și ajustate în fazele de analiză și proiectare, fără modificarea arhitecturii de bază.
- Sistemul va permite definirea de roluri personalizate și combinații de permisiuni, în funcție de nevoile operaționale și de cadrul legal aplicabil.
- Exercițarea drepturilor în sistem poate avea loc fie în nume propriu, fie în numele unei entități organizaționale asociate. Drepturile și acțiunile disponibile la nivel de entitate sunt condiționate de rolurile atribuite utilizatorului în cadrul entității respective și de tipul entității.

4. Cerințe generale privind soluția tehnică

4.1 Principii generale de proiectare și funcționare

Sistemul digital ePatrimoniu trebuie proiectat, dezvoltat, instalat, interconectat, configurat, operaționalizat, testat și pus în funcțiune ca un sistem **complet integrat, scalabil, deschis, extensibil și flexibil**, cu atribute înalte de **securitate, disponibilitate și interoperabilitate**. Acesta va comunica cu alte sisteme

informaționale relevante prin interfețe conforme cu standardele deschise, detaliate în prezentul document.

Sistemul digital ePatrimoniu va fi proiectat și realizat ca un **sistem centralizat**, administrat la nivel național și va fi utilizat de către instituții publice, instituții culturale, persoane fizice și juridice, publicul larg.

Sistemul digital ePatrimoniu va interconecta toate categoriile de patrimoniu și resurse culturale (imobil, arheologic, mobil, imaterial) și va reprezenta un **ghişeu unic** de acces la informații și servicii legate de patrimoniu. Sistemul digital va permite și integrarea cu sisteme informatice din domenii conexe (administrație financiară, cadastru, urbanism etc.) și va facilita furnizarea de **servicii publice digitale** (e-guvernare).

Implementarea tuturor cerințelor tehnice și funcționale descrise în prezentul document se va realiza în baza analizei și proiectării de detaliu, pentru fiecare componentă în parte, cu reflectarea tuturor cerințelor legislative în vigoare la data respectivă și cu posibilitatea de adaptare la viitoarele modificări legislative.

Pentru reducerea riscurilor, maximizarea controlului calității și asigurarea adaptabilității în timp real, Prestatorul va adopta o **metodologie de dezvoltare incrementală și iterativă**, însoțită de livrări și puneri în producție parțiale (jaloane funcționale). Planificarea incrementală va avea la bază calendarul și metodologia descrise în secțiunile 8 și 9.2.

La sfârșitul fazei de **dezvoltare, migrare și testare** trebuie să fie acoperite toate cerințele și specificațiile solicitate în prezentul document, cele definite în **faza de analiză și proiectare**, precum și cele care vor fi identificate în timpul **fazei de punere în producție**.

Sistemul digital ePatrimoniu va cuprinde o **bază de date comună**, dedicată patrimoniului cultural, care va fi populată cu date corelate, în scopul contextualizării, de exemplu, a situației monumentelor istorice. Exemple de astfel de date includ: adresa actualizată, numărul de cadastru (pentru conectare la registrul de cadastru și carte funciară), geo-localizarea, proprietarul, informații despre arhitectură, istorie și istoricul de restaurare a clădirii etc., precum și informații despre alte tipuri de bunuri culturale (mobile și imateriale).

Acest sistem digital va include atât funcționalitățile existente în Biblioteca Digitală a României, cât și pe cele ale catalogului partajat al instituțiilor culturale, adică va permite atât alimentarea partajată/cooperativă a acestora, cât și facilitarea accesului public la acestea, pe lângă interoperabilitatea cu Biblioteca Digitală Europeană (europeana.eu).

Sistemul digital va respecta implementa **principiile FAIR** (Findable, Accessible, Interoperable, Reusable), acestea oferind un cadru pentru asigurarea că datele publice sunt ușor de găsit, accesibile, compatibile și reutilizabile atât pentru utilizatori umani, cât și pentru mașini, precum și regulile Linked Data sau Linked Open Data.

Software-ul aferent sistemului digital ePatrimoniu va fi livrat sub licență EUPL v.1.2 (European Union Public License) sau o licență echivalentă permisivă, cu asigurarea posibilității de reutilizare, modificare, extindere și redistribuire de către Autoritatea Contractantă, fără restricții suplimentare

Toate livrabilele software, inclusiv codul sursă, documentațiile, scripturile, componentele de configurare și instrumentele asociate dezvoltate sau personalizate în cadrul prezentului contract devin proprietatea exclusivă a Autorității Contractante, care dobândește toate drepturile patrimoniale de autor asupra acestora, nelimitate în timp și spațiu. Prestatorul nu va avea dreptul de a reproduce, reutiliza, modifica, cesa, publica sau distribui, în tot sau în parte, elemente ale soluției tehnice livrate, decât cu acordul expres, prealabil și scris al Autorității Contractante. Cerințele specifice se regăsesc în secțiunea 9.4.

Dezvoltarea sistemului digital ePatrimoniu se va face în contact continuu cu echipa Autorității Contractante, astfel încât specialiștii acesteia să-i poată monitoriza evoluția, să fie familiarizați cu arhitectura sistemului și codul-sursă și să se asigure, astfel, minimizarea dependenței față de dezvoltator.

Dezvoltarea sistemului se va face pe o platforma bazată pe standarde deschise și arhitectură SOA (Arhitectură Orientată pe Servicii).

Sistemul se va implementa în infrastructura de cloud computing existentă în centrul de date STS, infrastructură care virtualizează, prin instrumente OpenSource (OpenStack), infrastructura fizică de procesare, stocare și comunicare ce va fi achiziționată în cadrul proiectului, printr-o procedură de achiziție distinctă și care va asigura infrastructura de mașini virtuale/containere necesară, precum și soluția de *disaster recovery* într-un centru de date diferit de cel de producție. Suportul aferent platformei de cloud (OpenStack) nu face obiectul prezentului caiet de sarcini.

Infrastructura de mașini virtuale / containere, care va fi pusă la dispoziția viitorului Prestator în centrul de date STS, nu asigură licențiere comercială pentru sistemele de operare, serverele de aplicație sau soluțiile de baze de date. **Prin urmare, orice soluție informatică propusă trebuie să includă licențele necesare funcționării în mediul de cloud și să fie detaliate în propunerea tehnică.** Prestatorul asigură Autorității Contractante drept de utilizare neexclusiv, pe întreaga durată a contractului, inclusiv pe perioada de mentenanță evolutivă, corectivă și garanție, fără costuri pentru Autoritatea Contractantă.

4.2 Caracteristici esențiale

Soluția tehnică propusă pentru realizarea sistemului digital ePatrimoniu trebuie să asigure un ansamblu de caracteristici esențiale care să garanteze performanța, scalabilitatea, securitatea, interoperabilitatea și sustenabilitatea pe termen lung.

Sistemul digital va fi construit pe o **arhitectură modulară**, orientată pe servicii (SOA / microservicii), care să permită separarea clară a componentelor, extinderea facilă și

întreținerea eficientă. Acesta va fi proiectat în paradigma cloud-native, utilizând containere orchestrate (ex. Kubernetes), pentru a asigura disponibilitate ridicată (High Availability), reziliență și scalabilitate dinamică. Vor fi implementate mecanisme automate de load balancing și failover, iar infrastructura va include un mecanism de disaster recovery cu obiective minime RPO (Recovery Point Objective) ≤ 2 ore și RTO (Recovery Time Objective) ≤ 4 ore. [informații detaliate se regăsesc în secțiunea 5.1 din prezentul caiet de sarcini]

Sistemului digital ePatrimoniu va include funcționalități **Low-Code / No-Code**, care să permită configurarea și extinderea fluxurilor de lucru, șabloanelor, formularelor și rapoartelor. Funcționalitățile Low-Code / No-Code ale sistemului trebuie să utilizeze standardele BPMN 2.0 și, unde este cazul DMN, pentru definirea proceselor, fluxurilor și a regulilor decizionale și să fie capabile să importe și să exporte aceste definiții în formatele standard corespunzătoare. Aceasta va permite administratorilor sistemului crearea și modificarea fluxurilor electronice de lucru aferente serviciilor publice digitale, definirea de șabloane de documente, formulare și nomenclatoare, configurarea regulilor de validare, notificare și rutare, personalizarea interfețelor și a conținutului afișat utilizatorilor. [informații detaliate se regăsesc în subcapitolul 6.1 din prezentul caiet de sarcini]

Soluția tehnică propusă pentru sistemul digital ePatrimoniu va respecta standardele naționale și europene de interoperabilitate (EIF/NIF) și va utiliza **protocoale deschise** (REST/JSON, XML, CSV). Vor fi dezvoltate **API-uri publice și documentate**, care să asigure integrarea cu alte sisteme informatice relevante la nivel național și european [informații detaliate se regăsesc în subcapitolul 7.3 din prezentul caiet de sarcini].

Sistemul digital ePatrimoniu va fi proiectat conform principiilor **secure-by-design** și **privacy-by-design**, în conformitate cu cerințele GDPR și legislația specifică. Vor fi implementate mecanisme avansate de securitate: autentificare și autorizare bazate pe standarde (OAuth2, OpenID Connect, SAML), criptarea datelor în tranzit și în repaus (TLS 1.2+, AES-256), jurnalizare completă a acțiunilor utilizatorilor și auditare permanentă, protecție împotriva atacurilor cibernetice (WAF, DDoS, brute force, injection). Accesul la sistem se va realiza prin integrare cu platformele de identitate naționale și europene (ROeID, eIDAS). [informații detaliate se regăsesc în secțiunea 7.5 din prezentul caiet de sarcini]

Sistemul digital ePatrimoniu trebuie să asigure **funcționare continuă (24/7)**, cu o disponibilitate anuală de minimum **99,9%**, și timpi de răspuns corespunzători volumului estimat de utilizatori (minimum 65.000 utilizatori unici). Toate procesele critice vor beneficia de mecanisme automate de monitorizare, alertare și recuperare rapidă.

Sistemul digital trebuie să fie accesibil și funcțional în toate browserele moderne, inclusiv Google Chrome, Mozilla Firefox, Microsoft Edge, Safari și Opera, fără limitări de funcționalitate sau compatibilitate.

Interfața utilizator a sistemului digital ePatrimoniu va respecta standardele **WCAG 2.2 AA** privind accesibilitatea web, va fi **multilingvă (română și engleză)** și adaptată

pentru persoane cu dizabilități. Designul va fi unitar și intuitiv, asigurând o experiență coerentă între componentele sistemului de e-guvernare, management al patrimoniului și administrare. [informații detaliate se regăsesc în subsecțiunea 7.6.1 din prezentul caiet de sarcini]

Sistemul digital ePatrimoniu va implementa **principiile FAIR** (Findable, Accessible, Interoperable, Reusable) și regulile **Linked (Open) Data**, utilizând ontologii internaționale consacrate (CIDOC CRM, FRBRoo, EDM) și modele semantice naționale (CPoT).

În cadrul Sistemul digital ePatrimoniu vor fi asigurate mecanisme de publicare și export de **date deschise** în formate standard, pentru reutilizarea acestora de către terți.

Sistemul digital ePatrimoniu va integra funcționalități de **inteligență artificială (AI)** și **machine learning** cel puțin pentru: categorizarea automată a resurselor culturale și îmbogățirea metadatelor, analiză semantică, recomandări contextuale și detectarea anomaliilor, suport decizional pentru politici publice și managementul patrimoniului etc. [informații detaliate se regăsesc în secțiunea 7.4 din prezentul caiet de sarcini]

Soluția tehnică propusă sistemul digital **ePatrimoniu** va fi portabilă între medii și infrastructuri cloud, inclusiv în Cloud-ul Guvernamental, fără dependențe de tehnologii proprietare sau licențe restrictive. Se vor utiliza tehnologii deschise și interoperabile, compatibile cu infrastructura de virtualizare OpenStack a STS. [subcapitolul 5.2]

Toate componentele sistemului digital ePatrimoniu vor fi dezvoltate cu respectarea principiului „**Do No Significant Harm**” (**DNSH**), optimizând consumul energetic și resursele IT și vor fi proiectate pentru **evolutivitate** și **întreținere facilă** pe termen lung.

5. Descrierea arhitecturii sistemului

5.1 Arhitectura logică

Arhitectura logică a sistemului digital ePatrimoniu va fi organizată pe următoarele niveluri:

- *Nivelul de prezentare* – asigură interacțiunea utilizatorului cu sistemul, oferind un punct de acces cu o interfață grafică intuitivă către funcționalitățile oferite de cele două componente aplicative ale sistemului: de e-guvernare și management de patrimoniu;
- *Nivelul de aplicații* – include funcționalitățile principale ale sistemului pentru utilizatori din cadrul componentelor aplicative ale sistemului;
- *Nivelul de date* – cuprinde componentele responsabile cu stocarea, accesarea și gestionarea eficientă a tuturor datelor din cadrul sistemului;
- *Nivelul de suport* – integrează servicii esențiale pentru funcționarea, mentenanța și fiabilitatea sistemului precum: modulul de **administrare** (gestionarea utilizatorilor, configurații), **monitorizare** (urmărirea performanței,

detectarea problemelor, incidente securitate), **managementul incidentelor** (rezolvarea problemelor), **backup și recuperare** (salvarea datelor și a configurațiilor și restabilirea lor).

- *Nivelul de integrare* – se ocupă cu interconectarea componentelor sistemului și cu alte sisteme externe. Roluri: interfațare cu servicii externe (API-uri, microservicii, baze de date externe), transformarea datelor (ex: XML ↔ JSON), implementarea fluxurilor de integrare (ex: cu ERP-uri, CRM-uri).
- *Nivelul de securitate* – include politici de acces și protecție împotriva atacurilor, autentificare și autorizare, criptarea comunicațiilor și a datelor etc.

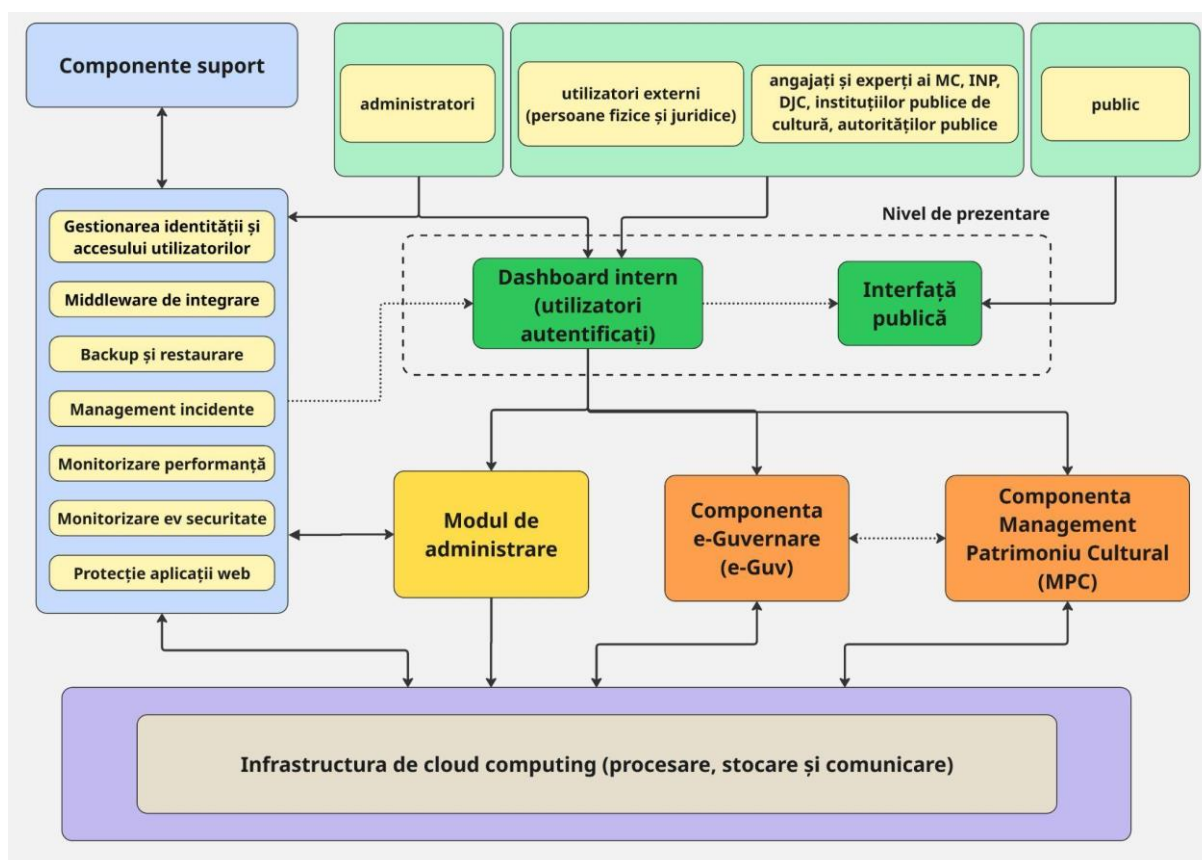


Figura 1 – Arhitectura logică a Sistemului Digital ePatrimoniu

Pe diagrama din Figura. 1, prezentată mai sus sunt reflectate următoarele componente:

- **Componente aplicative:**
 - **Componenta e-Guvernare (e-Guv)**, prin intermediul căreia vor fi implementate servicii de e-guvernare pentru serviciile publice oferite de Ministerul Culturii și instituțiile subordonate acestuia, cu atribuții și activități de avizare, autorizare, emitere acorduri, certificare etc. Cerințele detaliate care trebuie îndeplinite de această componentă sunt prezentate în secțiunea 6.1 din prezentul caiet de sarcini;

- o **Componenta Management Patrimoniu Cultural (MPC)**, prin intermediul căreia se va realiza managementul datelor în sprijinul conservării și gestionării eficiente a resurselor patrimoniului cultural. Cerințele detaliate care trebuie îndeplinite de această componentă sunt prezentate în secțiunea 6.2 din prezentul caiet de sarcini;
- **Componente suport:**
 - o **Componenta pentru gestionarea identității și accesului utilizatorilor**, prin intermediul căreia se asigură gestiunea identității utilizatorilor, permițând administrarea centralizată a rolurilor și permisiunilor utilizatorilor. Cerințele detaliate care trebuie îndeplinite de această componentă sunt prezentate în secțiunea 6.3 din prezentul caiet de sarcini
 - o **Componenta Middleware unificat de integrare**, prin intermediul căreia se asigură integrarea componentelor aplicative, cu cele suport și cu sisteme informatice externe. Cerințele detaliate care trebuie îndeplinite de această componentă sunt prezentate în secțiunea 6.4 din prezentul caiet de sarcini;
 - o **Componenta de backup și restaurare**, prin intermediul căreia se asigură realizarea copiilor de siguranță ale sistemului, precum și restaurarea acestora la nevoie. Cerințele detaliate care trebuie îndeplinite de această componentă sunt prezentate în secțiunea 6.5 din prezentul caiet de sarcini;
 - o **Componenta de management a incidentelor (ticketing)**, prin intermediul căreia se asigură managementul incidentelor (ticketing) semnalate de către utilizatorii Ministerului Culturii, DJC și INP către Prestator. Cerințele detaliate care trebuie îndeplinite de această componentă sunt prezentate în secțiunea 6.6 din prezentul caiet de sarcini;
 - o **Componenta de monitorizare a performanței și disponibilității**, prin intermediul căreia se asigură supravegherea continuă a performanței și disponibilității sistemului. Cerințele detaliate care trebuie îndeplinite de această componentă sunt prezentate în secțiunea 6.7 din prezentul caiet de sarcini;
 - o **Componenta de management a evenimentelor de securitate**, prin intermediul căreia se asigură colectarea, indexarea, analizarea și corelarea tuturor log-urilor (ex: server de aplicații, web, sisteme de operare, aplicații, etc), cu scopul de a detecta și alerta în cazul apariției amenințărilor de securitate. Cerințele detaliate care trebuie îndeplinite de

această componentă sunt prezentate în secțiunea 6.8 din prezentul caiet de sarcini;

- o **Componenta de protecție aplicații web**, prin intermediul căreia se asigură protecția la nivelul traficului HTTP și HTTPS către serviciile web-based, împotriva atacurilor cibernetice, precum și protecție la nivel Layer 7, împotriva tentativelor de tip Brute Force, URL Fuzzing, Denial of Service sau alte tipuri de atacuri care exploatează vulnerabilitățile aplicațiilor web. Cerințele detaliate care trebuie îndeplinite de această componentă sunt prezentate în secțiunea 6.9 din prezentul caiet de sarcini.

Componentele suport trebuie să fie platforme software mature, deja introduse în circuitul comercial (open-source sau COTS), personalizate conform cerințelor prezentului caiet de sarcini din secțiunile 6.3-6.9.

Componentele suport vor fi furnizate cu licențiere perpetuă și suport inclus pe perioada mentenanței și garanției și vor fi instalate în infrastructura sistemului digital ePatrimoniu.

Pe durata perioadei de mentenanței și garanției, Prestatorul are obligația de a realiza toate update-urile și upgrade-urile necesare pentru menținerea funcționalității și securității componentelor suport, fără costuri suplimentare pentru Autoritatea Contractantă.

Nivelul de prezentare va fi structurat în două medii distincte:

1. **Interfața publică** reprezintă nivelul public de acces al sistemului digital ePatrimoniu, accesibilă fără autentificare, destinată informării, transparenței și valorificării patrimoniului cultural național. Aceasta permite publicului larg accesul la informații despre bunuri culturale, registrele publice, activitatea instituțiilor de specialitate, precum și la resurse digitale (texte, imagini, materiale audio-video, date geospațiale), prin mecanisme de căutare și explorare intuitive. Interfața publică asigură prezentarea coerentă și atractivă a patrimoniului cultural, în conformitate cu standardele de accesibilitate și interoperabilitate. Cerințele detaliate care trebuie îndeplinite de această componentă sunt prezentate în subcapitolul 7.1.1

2. **Dashboard Intern:** destinat utilizatorilor autentificați și structurat în module și submodule, reprezintă interfața centrală de lucru a sistemului digital ePatrimoniu pentru utilizatorii autentificați (angajați ai Ministerului Culturii, INP, DJC, membri ai comisiilor de specialitate, experți, administratori, etc). Acesta asigură acces unificat, securizat și personalizat la funcționalitățile operaționale ale sistemului, facilitând desfășurarea activităților administrative, de avizare, management al patrimoniului și guvernare digitală. O secțiune importantă a dashboardului intern este **Modulul de administrare ePatrimoniu**, nucleul operațional pentru gestionarea, configurarea și controlul funcționalităților sistemului digital. Aceasta asigură mecanismele necesare pentru administrarea

utilizatorilor și rolurilor, gestionarea șabloanelor și a modelelor de documente, precum și monitorizarea acțiunilor printr-un submodul dedicat de audit, trasabilitate și raportare probleme. Cerințele detaliate care trebuie îndeplinite de această componentă sunt prezentate în subcapitolul 7.1.2;

Pentru creșterea performanței și a disponibilității sistemului digital, soluția tehnică propusă va include mecanisme de distribuție a conținutului la nivel Edge, de tip CDN (Content Delivery Network), prin care resursele statice vor fi replicate și livrate din puncte de prezență distribuite, contribuind la reducerea latenței, optimizarea traficului și protecția împotriva atacurilor distribuite de tip Denial of Service (DDoS). Acesta va asigura:

- caching distribuit la nivel global pentru conținut static (imagini, fișiere multimedia, documente, resurse GIS, tile-uri 2D/3D);
- optimizare automată a imaginilor (redimensionare dinamică, conversie în formate moderne precum WebP și AVIF);
- protecție DDoS la nivel Edge;
- posibilitatea invalidării programatice a cache-ului prin API (cache purge selectiv sau global);
- integrare cu restul sistemului digital.

Arhitectura sistemului digital ePatrimoniu va fi construită pe un model de înaltă disponibilitate, astfel încât defectarea unei componente/funcționalități să nu afecteze funcționalitatea întregului sistem digital. În acest sens, arhitectura sistemului va fi constituită din soluții redundante, cu asigurarea disponibilității și balansarea încărcării (cluster HA) pentru **componentele funcționale critice ale sistemului**, respectiv:

- Componenta e-Guvernare (e-Guv)
- Componenta de Management Patrimoniu Cultural PCM
- Modulul de administrare
- Componenta de protecție a aplicațiilor web.

Componenta de Management Patrimoniu Cultural va folosi o tehnologie cloud-native, astfel încât întreruperea funcționării oricărui server / nod nu va avea un impact asupra funcționării, astfel:

- Este necesară utilizarea de tehnologii software de tipul micro serviciilor. Containerul care furnizează microserviciul încapsulează propriul cod, datele de configurare, dependențele și datele utilizate pentru buna sa funcționare.
- Se vor implementa tehnologii și practici specifice arhitecturii cloud-native, bazate pe instanțe efemere, scalabile automat și orchestrate centralizat. Serviciile vor fi stateless și interschimbabile, astfel încât infrastructura să asigure elasticitate, reziliență și suport multi-tenancy. Fiecare serviciu va fi provizionat în mașini sau containere individuale, iar scalabilitatea va fi

asigurată prin dezvoltarea pe orizontală. Orice întrerupere a unui container/mașină virtuală nu va fi sesizată de utilizatorii finali.

- Funcționalitățile vor fi modularizate și compactate, astfel încât să fie capabile să încorporeze nativ avantajele oferite de platforma de virtualizare unde vor fi găzduite.
- Se vor utiliza serviciile disponibile în platforma de virtualizare, acolo unde este posibil. Dezvoltarea aplicațiilor, integrarea și instalarea automată în platforma de virtualizare se vor face de Prestator.
- Vor fi utilizate containere și, acolo unde nu se poate, mașini virtuale. În acest mod va fi asigurată portabilitatea și consistența între diverse medii virtuale. Prin încapsularea într-un singur pachet software a codului micro serviciului, inclusiv a tuturor bibliotecilor și modulelor necesare funcționării acestuia, se va asigura independența față de o platformă suport anume.
- Containerele vor fi agregate într-o platformă de orchestrare a containerelor, ce facilitează automatizarea și modalitatea de a crea configurații declarative, precum Kubernetes.

Componenta e-Guvernare va folosi o tehnologie cloud-native, astfel încât întreruperea funcționării oricărui server / nod nu va avea un impact asupra funcționării, astfel:

- Arhitectura va fi proiectată pentru a putea fi rulată în medii virtualizate și cloud, permițând distribuirea componentelor pe mai multe noduri și asigurând toleranță la erori.
- Funcționalitățile vor fi organizate modular, astfel încât componentele să poată fi actualizate, repornite sau relocate independent, fără afectarea funcționării generale a sistemului.
- Serviciile vor suporta rularea în regim redundant, cu mecanisme de echilibrare a încărcării (load balancing), pentru a asigura continuitatea serviciilor în cazul indisponibilității unui nod.
- Datele și configurațiile vor fi separate de logica sistemului digital, astfel încât repornirea sau înlocuirea unui nod să nu conducă la pierderi de date sau întreruperi sesizabile pentru utilizator.

Soluțiile tehnice propuse vor permite oprirea temporară a unui nod pentru mentenanță și suport, sistemul digital fiind în acest timp disponibil pentru activitățile normale.

Backup și restaurare. Vor fi efectuate copii ale bazelor de date ale sistemului digital ePatrimoniu, precum și ale fișierelor de configurare ale acestuia cel puțin în modul următor:

- copie completă o dată pe săptămână, înlocuind anterioara copie backup;
- backup incremental plecând de la ultima copie completă timp de o săptămână, zilnic.

Procesul de efectuare a unei copii de siguranță va fi automat.

Prestatorul va pune la dispoziția Autorității Contractante un mecanism de efectuare a copiilor de siguranță și restaurare, testată și documentată, astfel încât sistemul să revină la o situație anterioară în cazul unei ștergeri accidentale/intenționate de date sau în cazul compromiterii sistemului (ex. atac ransomware)

Utilizatorii cu rol de administrator de sistem, prin intermediul unei interfețe web, vor administra salvările de siguranță ale sistemului digital, va putea modifica perioada și frecvența acestora. (informații detaliate se regăsesc în secțiunea 6.5 din prezentul caiet de sarcini)

Disaster Recovery. Sistemul digital va avea o „Locație Principală”, dar și o „Locație Secundară” de recuperare în caz de dezastru („Disaster Recovery”) de tip „hot-site”, cu o putere de calcul mai mică, dar cu aceeași capacitate de stocare, astfel că datele vor fi stocate și în locația secundară pentru a minimiza riscul pierderilor de date.

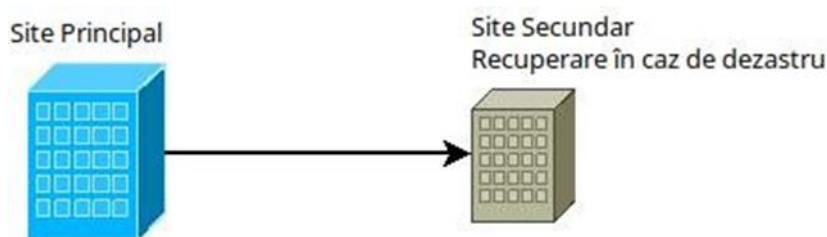


Figura 2 - Arhitectură recuperare în caz de dezastru

Sistemul va fi capabil să comute și să funcționeze din locația secundară cu un RTO (Recovery Time Objective) de maximum 4 ore și cu RPO (Recovery Point Objective) de maximum 2 ore.

Mediile de operare. Pentru asigurarea performanței și funcționării optime a sistemului digital, vor fi asigurate următoarele medii:

- a) **Mediul de producție** - asigură funcționarea în producție a sistemului;
- b) **Mediul de dezvoltare** – asigură mediul pe care vor fi dezvoltate noi funcționalități ale sistemului, atât înainte, cât și după punerea în producție;
- c) **Mediul de testare** – asigură mediul pe care vor fi testate noi funcționalități ale sistemului, atât înainte, cât și după punerea în producție;
- d) **Mediul de disaster-recovery** – va fi folosit pentru restabilirea funcționării sistemului în urma unui dezastru și va avea rolul de a minimiza impactul nefuncționării centrului de date de producție și de a asigura continuitatea operațiunilor.

Mediul de producție și mediul de testare vor fi găzduite în Centrul de date Principal, care va avea, din punct de vedere al numărului de noduri, respectiv al modalității de asigurare a disponibilității și scalabilității sistemului, aceeași arhitectură tehnică, diferențe existând doar la nivelul dimensionării acestor medii.

Mediul de disaster-recovery va fi găzduit în Centrul de date Secundar, dimensionat pentru a permite restaurarea rapidă a funcționării sistemului și pentru funcționarea acestuia pentru o perioadă scurtă de timp, până la repunerea în funcțiune a mediului de producție.

Dimensionarea resurselor computaționale și de stocare (vCPU, RAM, Storage) alocate celor 4 medii cade în sarcina exclusivă a Ofertantului, care are obligația de a estima și solicita resursele necesare în funcție de prevederile caietului de sarcini, stack-ul tehnologic propus, arhitectura aplicațiilor, necesarul pentru compilare/build, pipeline-uri CI/CD. **Ofertantul va justifica această dimensionare în Propunerea Tehnică.**

În dezvoltarea și implementarea sistemului digital ePatrimoniu vor fi preluate date din sisteme precum Culturalia.ro (Biblioteca digitală a României), Patrimoniu-cultural.ro (Sistemul Informatic pentru Patrimoniul Cultural Imobil), [Repertoriul Arheologic Național](http://Repertoriul-Arheologic-Național), DocPAT (Programul pentru evidența informatizată a patrimoniului cultural mobil), Acera.cimec.ro (Sistemul de Administrare a Cercetărilor Arheologice din România), Bunuri culturale mobile clasate în Patrimoniul Cultural Național, eGISpat (Sistem informațional geografic pentru protecția patrimoniului cultural național imobil) etc. și date despre registre administrative existente. Pentru detalii, se pot consulta informațiile din subsecțiunea 8.3.2 din prezentul caiet de sarcini.

Sistemul digital ePatrimoniu va transmite date către Biblioteca Digitală Europeană (Europeana.eu) prin utilizarea modelului de date EDM [Europeana Data Model], un standard conceput pentru a facilita colectarea, organizarea și partajarea datelor culturale în format digital la nivel european. Pentru detalii, a se consulta informațiile din subsecțiunea 7.3.6 din prezentul caiet de sarcini.

5.2 Arhitectura fizică

Arhitectura fizică a sistemului digital ePatrimoniu este prezentată în figura următoare:

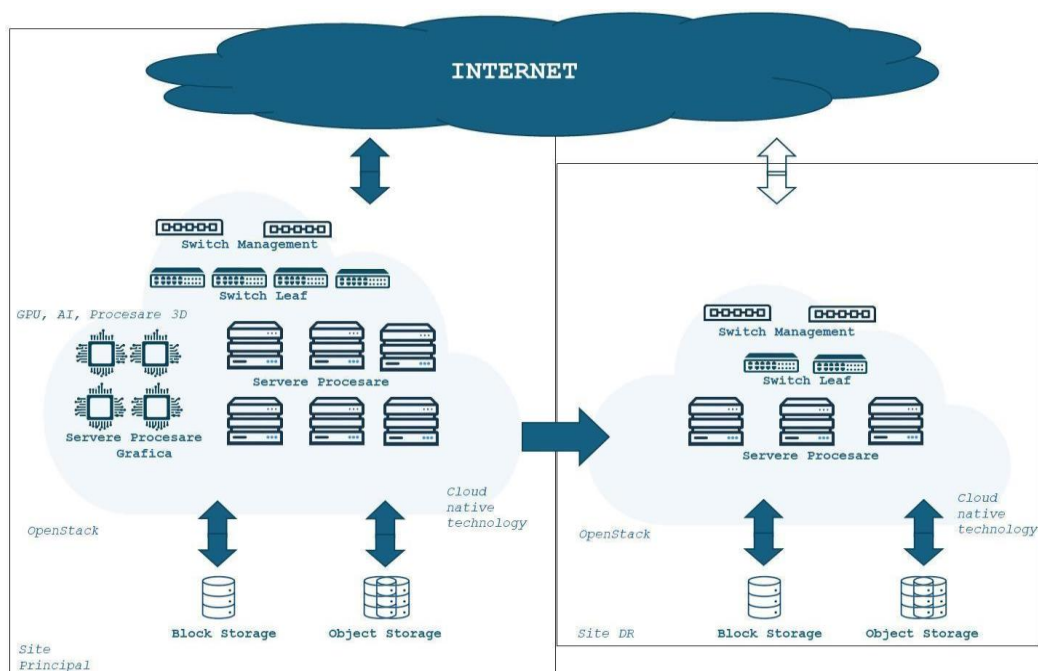


Figura 3 – Arhitectura fizică a Sistemului digital ePatrimoniu

Imaginea de mai sus prezintă o vedere de ansamblu a echipamentelor hardware ce vor asigura funcționalitatea sistemului digital ePatrimoniu. Locația de recuperare în caz de dezastru (dreapta) va avea capacitatea de stocare similară cu cea a site-ului principal (stânga), asigurând siguranța datelor. Puterea computațională este mai mică, scopul fiind, în cazul unui dezastru, de a menține serviciile operaționale în regim de avarie și fără pierderi de date, până când locația principală va putea fi din nou operațională.

Dimensionarea hardware a site-ului principal:

- 6 servere procesare echipate cu:
 - minim 2 procesoare de tip x86, având următoarele caracteristici: Frecvența: 2.2 GHz sau superior; Cache: 120 MB L3 cache sau superior; Număr de core-uri per procesor: minim 32 core-uri cu 64 fire de execuție;
 - Minim 1024 GB Registered ECC DDR5 memorie instalată
- 2 servere procesare grafică echipate cu:
 - minim 2 procesoare de tip x86, având următoarele caracteristici: Frecvența: 2.2 GHz sau superior; Cache: 120 MB L3 cache sau superior; Număr de core-uri per procesor: minim 32 core-uri cu 64 fire de execuție;
 - Minim 1024 GB Registered ECC DDR5 memorie instalată
 - Minim 1 modul de procesare grafică, care să îndeplinească următoarele performanțe și/sau funcționalități: FP64: 30 teraFLOPs, FP64 Tensor Core: 60 teraFLOPs, FP32: 60 teraFLOPs, TF32 Tensor Core: 835 teraFLOPs,

BFLOAT16 Tensor Core: 1,671 teraFLOPS, FP16 Tensor Core: 1,671 teraFLOPS, FP8 Tensor Core: 3,341 teraFLOPS, INT8 Tensor Core: 3,341 TOPS

- Vor fi incluse licențele necesare în vederea utilizării concurente, de către mai multe mașini virtuale/instanțe, a resurselor aferente acestor module de procesare.
- Echipament de stocare enterprise de tip obiect, cu următoarele caracteristici:
 - tip cluster multi-nod cu capabilități de procesare și de stocare, având posibilitatea de a replica datele la distanță, către sisteme similare multiple și să permită accesul de tip activ-activ la datele stocate în centrele de date;
 - include cel puțin 1 PiB capacitate de stocare utilă (fără deduplicare, compresie sau alte mecanisme de extindere virtuală a spațiului de stocare) rezultată după configurarea redundanței pentru stocarea datelor, configurație ce va asigura integritatea datelor în cazul defectării simultane a două disk-uri, respectiv a unui întreg nod.
 - Include cel puțin 4 noduri pentru asigurarea unui nivel ridicat de performanță și disponibilitate pentru procesele de salvare a datelor precum și pentru asigurarea unei politici avansate de protecție și redundanță la nivel de nod și de disc.
 - Fiecare nod trebuie să fie echipat cu minim 128GB RAM și 960GB SSD pentru accelerarea datelor.
- Echipament de stocare de tip block dual-controller din clasa Mid-range/Enterprise cu disponibilitate 99.999%, cu următoarele caracteristici:
 - două controlere hardware (fizice) prin care se pot scrie și citi datele în mod block (SAN), redundante, hot-swap
 - 8 porturi 25 Gbps SFP28 pentru acces de block (iSCSI) complet echipate pentru conectivitate
 - Cel puțin 256 GB pentru memorie cache de tip RAM
 - minim 80 TB spațiu de stocare brut de tip Flash
 - asigură cel puțin 130000 IOPS cu un profil de 50% rată de citire, 50% rată de scriere, 100% random, dimensiune IO de 8K.
 - Funcționalități inline de deduplicare și compresie activate pe toate seturile de date;
 - Timp de răspuns către servere < 1 ms;

Dimensionarea hardware a site-ului de recuperare în caz de dezastru:

- 3 servere procesare echipate cu:

- minim 2 procesoare de tip x86, având următoarele caracteristici: Frecvența: 2.2 GHz sau superior; Cache: 120 MB L3 cache sau superior; Număr de core-uri per procesor: minim 32 core-uri cu 64 fire de execuție;
- Minim 1024 GB Registered ECC DDR5 memorie instalată
- 2 servere procesare grafică echipate cu:
 - minim 2 procesoare de tip x86, având următoarele caracteristici: Frecvența: 2.2 GHz sau superior; Cache: 120 MB L3 cache sau superior; Număr de core-uri per procesor: minim 32 core-uri cu 64 fire de execuție;
 - Minim 1024 GB Registered ECC DDR5 memorie instalată
 - Minim 1 modul de procesare grafică, care să îndeplinească următoarele performanțe și/sau funcționalități: FP64: 30 teraFLOPs, FP64 Tensor Core: 60 teraFLOPs, FP32: 60 teraFLOPs, TF32 Tensor Core: 835 teraFLOPs, BFLOAT16 Tensor Core: 1,671 teraFLOPS, FP16 Tensor Core: 1,671 teraFLOPS, FP8 Tensor Core: 3,341 teraFLOPS, INT8 Tensor Core: 3,341 TOPS
 - Vor fi incluse licențele necesare în vederea utilizării concurente, de către mai multe mașini virtuale/instanțe, a resurselor aferente acestor module de procesare.
- Echipament de stocare enterprise de tip obiect, cu următoarele caracteristici:
 - tip cluster multi-nod cu capabilități de procesare și de stocare, având posibilitatea de a replica datele la distanță, către sisteme similare multiple și să permită accesul de tip activ-activ la datele stocate în centrele de date;
 - include cel puțin 1 PiB capacitate de stocare utilă (fără deduplicare, compresie sau alte mecanisme de extindere virtuală a spațiului de stocare) rezultată după configurarea redundanței pentru stocarea datelor, configurație ce va asigura integritatea datelor în cazul defectării simultane a două disk-uri, respectiv a unui întreg nod.
 - Include cel puțin 4 noduri pentru asigurarea unui nivel ridicat de performanță și disponibilitate pentru procesele de salvare a datelor precum și pentru asigurarea unei politici avansate de protecție și redundanță la nivel de nod și de disc.
 - Fiecare nod trebuie să fie echipat cu minim 128GB RAM și 960GB SSD pentru accelerarea datelor.
- Echipament de stocare de tip block dual-controller din clasa Mid-range/Enterprise cu disponibilitate 99.999%, cu următoarele caracteristici:
 - două controlere hardware (fizice) prin care se pot scrie și citi datele în mod block (SAN), redundante, hot-swap

- 8 porturi 25 Gbps SFP28 pentru acces de block (iSCSI) complet echipate pentru conectivitate
- Cel puțin 256 GB pentru memorie cache de tip RAM
- minim 80 TB spațiu de stocare brut de tip Flash
- asigură cel puțin 130000 IOPS cu un profil de 50% rată de citire, 50% rată de scriere, 100% random, dimensiune IO de 8K.
- Funcționalități inline de deduplicare și compresie activate pe toate seturile de date;
- Timp de răspuns către servere < 1 ms;

Echipamentele hardware ce vor asigura funcționalitatea sistemului digital ePatrimoniu vor fi achiziționate printr-o procedură de achiziție distinctă și vor fi integrate în infrastructura de cloud computing existentă în centrul de date STS. Această infrastructură utilizează virtualizarea prin instrumente OpenSource (OpenStack) și va asigura infrastructura de mașini virtuale/containerere necesară pentru Sistemul digital ePatrimoniu.

Pentru toate componentele sistemului informatic propus, Ofertanții vor include în **propunerea tehnică** sistemele de operare și sistemele de gestiune a bazelor de date necesare și compatibile cu produsele software oferite, fiind în responsabilitatea viitorului Prestator orice problemă de funcționare cauzată de eventuale incompatibilități.

Pentru toate componentele sistemului informatic care expun interfețe de comunicație, Ofertanții vor include în **propunerea tehnică** certificate digitale de tip SSL / TLS valide și compatibile cu soluția software oferită, emise de o autoritate de certificare recunoscută (trusted CA), ale cărei certificate sunt acceptate de principalele browsere și sisteme de operare, fiind în responsabilitatea viitorului Prestator orice problemă de funcționare sau securitate cauzată de configurarea necorespunzătoare sau de utilizarea unor certificate neconforme. Configurarea, instalarea și administrarea certificatelor SSL / TLS, inclusiv achiziția, implementarea mecanismelor de criptare a comunicațiilor (HTTPS), configurarea versiunilor de protocol securizate și reînnoirea acestora pe întreaga durată a contractului cad în sarcina Prestatorului. Soluția propusă va asigura acoperirea tuturor domeniilor și subdomeniilor utilizate (de tip single-domain, multi-domain sau wildcard, după caz).

Configurarea tuturor resurselor și stack-ului tehnologic, inclusiv crearea și dimensionarea mașinilor virtuale/containerelor, instalarea sistemelor de operare, a sistemelor de gestiune a bazelor de date, inclusiv, dar fără a se limita la, configurarea echipamentelor de stocare și a celorlalte echipamente ce țin de infrastructura proiectului, este în sarcina Prestatorului.

Ofertanții vor prezenta în **propunerea tehnică** propria dimensionare a infrastructurii virtuale necesare (număr de instanțe, vCPU, RAM, spațiu de stocare), adaptată

specificului soluției software oferite, cu condiția încadrării în resursele disponibile și îndeplinirii cerințelor din caietul de sarcini.

6. Cerințele componentelor software ale sistemului digital ePatrimoniu

6.1 Componenta e-Guvernare (componentă aplicativă)

6.1.1 Scopul implementării

Componenta de e-guvernare a sistemului digital ePatrimoniu are ca scop:

- digitalizarea integrală a serviciilor publice legate de patrimoniul cultural furnizate de Ministerul Culturii și de instituțiile subordonate acestuia, care implică activități de avizare, autorizare, acreditări, certificare sau alte acte administrative
- simplificarea și standardizarea **proceselor administrative** din domeniul patrimoniului cultural, reducerea birocrăției, creșterea transparenței și asigurarea accesului rapid al cetățenilor / entităților private la serviciile publice oferite
- optimizarea și coordonarea integrată a tuturor proceselor administrative ce au ca scop îndeplinirea de serviciilor publice digitale din domeniul patrimoniului cultural
- contribuie la transformarea digitală a administrației publice în domeniul patrimoniului cultural, în concordanță cu principiile guvernării digitale, interoperabilității și reutilizării datelor.

În scopul unei înțelegeri unitare,

- **procesul** (administrativ) se definește ca un ansamblu structurat de activități corelate, desfășurate de unul sau mai mulți actori, prin care intrările, reprezentate de informații, cereri sau documente furnizate de beneficiari, sunt prelucrate și transformate în rezultate concrete, precum avize, autorizații sau atestări, în vederea furnizării unui serviciu public sau îndeplinirii unei funcții instituționale. Procesul are un scop clar, implică roluri și responsabilități definite și este guvernat de reguli și proceduri specifice.
- un **flux** reprezintă succesiunea operațională de pași prin care se desfășoară un proces, de la inițiere (precum depunerea unei solicitări) până la finalizare (precum emiterea unei autorizații), incluzând deciziile și traseele alternative. Un proces poate include unul sau mai multe fluxuri, corespunzătoare diferitelor scenarii de desfășurare.
- un **proces integrat** reprezintă un proces distinct, corelat procedural cu un proces principal, al cărui rezultat constituie o condiție necesară pentru continuarea sau finalizarea acestuia. Procesul integrat are propriile activități, actori și reguli, însă rezultatul său este utilizat în cadrul procesului principal, fără de care acesta nu poate fi finalizat. De exemplu, procesul de avizare a

documentației reprezintă un proces integrat în cadrul procesului de emitere a unei autorizații, avizarea constituind o condiție obligatorie pentru emiterea acesteia.

Prin intermediul acestei componente, sistemul digital ePatrimoniu va integra toate fluxurile electronice aferente proceselor administrative dedicate patrimoniului cultural – minimum 53 de servicii publice digitale precum cele exemplificate mai jos:

Nr. crt.	Tip	Instituții	Denumire aviz / autorizație / acord / certificare
P1	Imobil-MI	MC / DJC	Ordin de clasare sau comunicare privind neclasarea în Lista Monumentelor Istorice
P2	Imobil-MI	MC / DJC	Ordin de declasare sau comunicare privind nedeclasarea din Lista Monumentelor Istorice
P3	Imobil-MI	MC / DJC	Ordin de schimbare de grupă valorică sau comunicare privind neschimbarea de grupă valorică în Lista Monumentelor Istorice
P4	Imobil-MI	DJC	Obligație de folosință a monumentului istoric
P5	Imobil-MI	MC / DJC	Aviz pentru intervenții asupra imobilelor monumente istorice grupa valorică A
P6	Imobil-MI	DJC	Aviz pentru intervenții asupra imobilelor monumente istorice grupa valorică B
P7	Imobil-MI	MC	Aviz pentru componente artistice la imobilele monumente istorice grupa valorică B
P8	Imobil-MI	DJC	Aviz pentru intervenții la clădiri din zone construite protejate
P9	Imobil-MI	DJC	Aviz pentru intervenții la clădiri din zone de protecție a monumentelor istorice categorie A
P10	Imobil-MI	DJC	Aviz pentru intervenții la clădiri din zone de protecție a monumentelor istorice categorie B
P11	Imobil-MI	MC	Comunicare privind exercitare / neexercitare drept preempțiune la vânzarea monumentelor istorice categorie A
P12	Imobil-MI	DJC	Comunicare privind exercitare / neexercitarea dreptului de preempțiune la vânzarea monumentelor istorice categorie B
P13	Imobil-MI	MC	Aviz expropriere monumente istorice
P14		DJ C	Aviz expropriere monumente istorice
P15	Imobil-MI	MC	Aviz concesiune și închiriere monumente istorice
P16		DJ C	Aviz concesiune și închiriere monumente istorice

Nr. crt.	Tip	Instituții	Denumire aviz / autorizație / acord / certificare
P17	Imobil-MI	MC	Aviz pentru darea în administrare / folosință gratuită / închirierea / concesiunea monumentelor istorice
P18		DJC	Aviz pentru darea în administrare / folosință gratuită / închirierea / concesiunea monumentelor istorice
P19	Imobil-MI	MC	Aviz pentru vânzarea monumentelor în care funcționează spații comerciale și de prestări servicii aflate în proprietatea privată a statului, în administrarea consiliilor județene sau a celor locale și a celor din patrimoniul regiilor autonome
P20		DJC	Aviz pentru vânzarea monumentelor în care funcționează spații comerciale și de prestări servicii aflate în proprietatea privată a statului, în administrarea consiliilor județene sau a celor locale și a celor din patrimoniul regiilor autonome
P21	Imobil-MI	MC	Aviz pentru vânzarea imobilelor din zona de protecție a monumentelor istorice în care funcționează spații comerciale și de prestări servicii aflate în proprietatea privată a statului, în administrarea consiliilor județene sau a celor locale și a celor din patrimoniul regiilor autonome
P22		DJC	Aviz pentru vânzarea imobilelor din zona de protecție a monumentelor istorice în care funcționează spații comerciale și de prestări servicii aflate în proprietatea privată a statului, în administrarea consiliilor județene sau a celor locale și a celor din patrimoniul regiilor autonome
P23	Imobil-MI	DJC	Aviz pentru introducerea monumentelor istorice în circuit public
P24	Imobil	MC	Aviz pentru documentații de amenajarea teritoriului (PUZ, PUG, PUD), urbanism, intervenții și comunicări privind neemiterea avizului
P25		DJC	Aviz pentru documentații de amenajarea teritoriului (PUZ, PUG, PUD), urbanism, intervenții și comunicări privind neemiterea avizului
P26	Imobil	MC	Aviz pentru planuri de management ale ariilor naturale protejate (pentru MMAP)
P27	Imobil - Arheologie	MC	Autorizație de cercetare arheologică

Nr. crt.	Tip	Instituții	Denumire aviz / autorizație / acord / certificare
P28	Imobil - Arheologie	MC / DJC	Certificat de descărcare de sarcină arheologică
P29	Imobil - Arheologie	MC	Aviz pentru intervențiile în zone cu patrimoniu arheologic reperat / descoperit întâmplător
P30		DJC	Aviz pentru intervențiile în zone cu patrimoniu arheologic reperat / descoperit întâmplător
P31	Imobil - Arheologie	DJC	Aviz specific pentru vânzare de teren agricol situat în extravilan în zone cu patrimoniu arheologic reperat Legea 17/2014
P32	Imobil - Arheologie	MC	Autorizație de utilizare a detectoarelor de metale în siturile arheologice
P33	Imobil - Arheologie	MC	Aviz prealabil obținerii autorizației de deținere a detectoarelor de metale
P34	Mobil	MC	Ordin de clasare bunuri culturale mobile
P35		DJC	Certificat de clasare bunuri culturale mobile
P36	Mobil	MC	Comunicare privind exercitare / neexercitare drept de preemțiune în cazul vânzării bunurilor culturale mobile clasate în tezaur
P37	Mobil	MC	Certificat de export definitiv / temporar pentru bunuri culturale mobile
P38		DJ C	Certificat de export definitiv / temporar pentru bunuri culturale mobile
P39	Mobil	MC	Autorizație agenți economici comercializare bunuri culturale mobile
P40	Mobil	MC	Autorizație laboratoare de restaurare
P41	Mobil	MC	Aviz prealabil înființare muzee
P42	Mobil	DJC	Nota de constatare privitoare la îndeplinirea condițiilor și criteriilor de înființare muzee/colecții
P43	Mobil	MC / DJC	Ordin acreditare / reacreditare muzee și colecții publice
P44	Mobil	MC	Aviz reorganizare muzee
P45	Imobil	MC	Avizul privind concepția artistică a monumentului de for public
P46	Imobil	DJC	Aviz cu privire la amplasarea plăcilor comemorative
P47	Experți - imobil	INP	Certificat de atestare în domeniul protejării monumentelor istorice în calitatea de specialist; expert; expert tehnic
P48	Experți - arheologie	MC	Certificat de atestare a personalului de specialitate din domeniul arheologiei

Nr. crt.	Tip	Instituții	Denumire aviz / autorizație / acord / certificare
P49	Experți - mobil	MC	Certificat de acreditare a conservatorilor și restauratorilor în domeniul conservării și restaurării patrimoniului cultural mobil
P50	Imaterial	MC	Acordarea Titlului de <i>Tezaur uman viu</i>
P51	General	MC / DJC	Solicitări diverse
P52	Mobil	MC	Ordin de declarare bunuri culturale mobile
P53	Mobil	MC	Schimbarea categoriei juridice a bunurilor culturale mobile

Procesele / Fluxurile sunt cu titlu exemplificativ. Acestea pot suferi modificări ca număr, tip, denumire etc. și vor fi discutate în perioada de analiză.

6.1.2 Cerințe și funcționalități generale

Componenta de e-Guvernare va furniza un mediu digital unitar pentru interacțiunea dintre Autoritatea Contractantă, instituțiile subordonate și beneficiarii serviciilor publice (persoane fizice și juridice). Sistemul digital va cuprinde depunerea, soluționarea și transmiterea electronică a cererilor și documentelor aferente proceselor de avizare, autorizare, certificare, acreditare etc. fără necesitatea prezenței fizice a solicitantului la sediile instituțiilor.

Sistemul digital va include:

- **o zonă publică** (accesibilă fără autentificare), conform capitolului 7.1.1, destinată informării generale despre serviciile oferite, registre publice, ședințele comisiilor de specialitate și alte informații relevante. În zona publică vor fi publicate informații actualizate despre procese administrative asociate diferitelor registre și evidențe.
- **o zonă privată**, accesibilă utilizatorilor autentificați, în care aceștia pot depune solicitări, urmări stadiul procesării și primi documentele emise.

Componenta va avea integrat un **configurator de fluxuri digitale** care se bazează pe un sistem low-code / no-code, care, prin interfețe grafice intuitive, va permite crearea, configurarea și modificarea rapidă a proceselor, fluxurilor, etapelor, formularelor și șabloanelor electronice, fără a fi necesare cunoștințe de programare.

Configuratorul va realiza modelarea proceselor de lucru în conformitate cu standardul deschis BPMN 2.0 (Business Process Model and Notation), precum și modelarea regulilor decizionale, acolo unde este cazul, în conformitate cu standardul DMN (Decision Model and Notation).

Componenta va realiza importul și exportul modelelor de proces și al regulilor asociate în formatele standard BPMN 2.0 XML și DMN XML, asigurând portabilitatea, interoperabilitatea și posibilitatea reutilizării acestora într-un alt sistem compatibil cu aceste standarde. Modelele de proces și regulile de business vor fi definite și

gestionate fără utilizarea unor extensii sau attribute proprietare care să împiedice reutilizarea, interoperabilitatea sau migrarea acestora către un alt sistem compatibil cu standardele BPMN 2.0 și DMN.

Configuratorul fluxurilor din sistemul digital ePatrimoniu va cuprinde, fără a se limita la, următoarele acțiuni asupra proceselor / fluxurilor de lucru:

- modelarea completă a fluxurilor administrative ce compun procesul de lucru, inclusiv definirea etapelor, tranzițiilor, punctelor de decizie, subproceselor, fluxurilor paralele, condițiilor de rutare și evenimentelor de tip mesaj, temporizator, eroare sau escaladare;
- configurarea task-urilor umane și automate, inclusiv atribuirea utilizatorilor sau grupurilor, generarea automată de documente și transmiterea de notificări;
- asocierea și configurarea formularelor și șabloanelor documentare la nivel de etapă, precum și gestionarea variabilelor de proces și a datelor aferente fiecărei instanțe;
- definirea regulilor de business utilizate pentru rutarea proceselor, configurarea termenelor procedurale, a mecanismelor de escaladare și a notificărilor automate;
- gestionarea versiunilor fluxurilor, publicarea acestora, menținerea instanțelor active pe versiuni anterioare și auditarea modificărilor efectuate asupra modelelor;
- testarea modelelor de proces înainte de publicare
- clonarea fluxurilor, respectiv crearea unui flux nou pe baza unui flux existent, cu preluarea automată a configurațiilor, etapelor, regulilor, condițiilor și parametrilor definiți în fluxul sursă. Fluxul rezultat va primi un identificator unic generat automat conform unei secvențe stabilite și va putea fi redenumit și modificat independent, fără a afecta fluxul original;
- comasarea fluxurilor, respectiv generarea unui flux nou prin combinarea a două fluxuri existente, incluzând integrarea logică a etapelor, regulilor și parametrilor acestora. Procesul de comasare va include mecanisme asistate pentru identificarea și rezolvarea eventualelor conflicte (de exemplu, ordine diferită a etapelor sau condiții incompatibile), precum și posibilitatea ajustării manuale a fluxului rezultat înainte de salvare. Fluxurile sursă vor rămâne nemodificate, iar operațiunea va fi auditabilă (utilizator, dată, fluxuri implicate);
- gestionarea versiunilor fluxurilor și a ciclului de viață al acestora, inclusiv publicarea, menținerea instanțelor active pe versiuni anterioare și auditarea modificărilor efectuate asupra modelelor;

Componenta va asigura gestionarea ciclului de viață al fiecărui flux de lucru, incluzând cel puțin următoarele stări:

- **Draft** – flux în curs de elaborare, editabil integral, neutilizabil în operațiuni;

- **Publicat** – flux activ și disponibil pentru utilizare; modificările majore vor conduce la generarea unei noi versiuni în starea Draft;
- **Anulat/Arhivat** – flux inactiv, păstrat în scop de trasabilitate, fără posibilitate de modificare.

Componenta va include salvarea intermediară a datelor introduse într-o etapă a fluxului de lucru, astfel încât utilizatorul să poată reveni ulterior pentru completarea sau modificarea informațiilor, până la momentul transmiterii sau finalizării etapei respective. După avansarea procesului în etapa următoare, editarea informațiilor din etapa anterioară nu va mai fi permisă, cu excepția cazurilor expres prevăzute prin configurarea fluxului.

Componenta va asigura păstrarea și gestionarea versiunilor fișierelor încărcate de utilizatori, inclusiv compararea, revenirea la versiuni anterioare și gestionarea metadatelor asociate, asigurând trasabilitate și coerență completă a documentațiilor. Componenta va permite și distribuirea automată a documentelor înregistrate către compartimentele responsabile, urmărirea fluxurilor de lucru și a stadiului fiecărui proces startat.

Formularele web care compun serviciile electronice vor avea la bază un editor de text WYSIWYG, astfel încât informația introdusă în câmpuri să poată fi formatată similar Microsoft Office Word (de exemplu: gestiunea paragrafelor și a stilurilor de text) astfel încât aspectul textului afișat în fereastra de editare trebuie să fie identic cu cel afișat în documentul generat prin intermediul sistemului, respectiv să fie identic cu cel afișat public. Totodată vor include, pentru unele câmpuri, controale de culegere a informației de tip text simplu, text multilinie, listă de selecție valori dintr-un nomenclator, bifă (checkbox) etc., precum și mecanisme de completare automată a câmpurilor conexe, în situațiile în care selectarea unei valori dintr-un nomenclator implică preluarea unor informații asociate aceleiași înregistrări din baza de date. Definirea și administrarea regulilor de preluare, corelare și mapare a datelor vor fi configurabile din interfața de administrare.

Formularele web vor realiza, pentru unele câmpuri, validări ale datelor introduse de utilizator, pentru verificarea respectării unor constrângeri referitoare la: localizarea spațială a utilizatorului, tipul informațiilor care trebuie completate, lungimea minimă sau maximă a textului, la limite ale valorilor numerice sau ale datelor calendaristice etc.

În cazul serviciilor electronice prin care se depune o solicitare, la finalizarea procesului aferent depunerii cererii, sistemul va genera un document electronic (.pdf) care cuprinde toate informațiile completate de către solicitant în formularele web aferente pașilor de proces deja urmați, pentru a permite solicitantului să verifice informațiile introduse înainte de transmiterea solicitării. Generarea documentelor electronice în baza informațiilor structurate completate de către solicitant în formularele web se va baza pe șabloane configurabile, în care vor fi incluse atât informații structurate culese

din formularele aferente serviciului electronic, cât și paragrafe formate de text predefinit.

Prestatorul va configura minimum 50 de șabloane electronice inițiale, adaptabile ulterior de către utilizatori autorizați.

În cadrul *fazei de dezvoltare, migrare și testare*, *Componenta de e-Guvernare* va include funcționalități dedicate integrării și preluării datelor din registrele și evidențele electronice deja existente, administrate de Ministerul Culturii, Institutul Național al Patrimoniului și alte instituții subordonate. Această integrare are rolul de a asigura continuitatea operațională, valorificarea istoricului proceselor anterioare și evitarea dublării eforturilor de introducere a datelor. În această categorie vor fi incluse, fără a se limita la acestea, *Registrul Arheologilor*, *Registrul experților și specialiștilor*, *Registrul operatorilor economici autorizați în domeniul restaurării și conservării bunurilor culturale* și alte baze de date relevante. Datele vor fi migrate cu păstrarea integrității informațiilor și prin realizarea de mapări între entitățile și câmpurile existente și ontologia sistemului, astfel încât registrele să poată fi actualizate și utilizate direct în procesele de e-Guvernare, fără a fi necesară o reintroducere manuală a informațiilor.

Fluxurile electronice vor fi corelate cu datele și resursele culturale gestionate în *Componenta MPC* care gestionează evidența bunurilor culturale imobile, mobile și imateriale. Integrarea dintre cele doua componente va permite schimbul de date și corelarea automată a proceselor administrative digitale cu informațiile despre bunurile culturale gestionate. Se va avea în vedere faptul că ontologia implementată în sistem va include clase și relații și pentru *Componenta de e-Guvernare* a platformei ePatrimoniu. Această integrare va permite corelarea automată între bunurile culturale și procesele administrative care le vizează, precum și păstrarea unui istoric complet, coerent și consultabil al tuturor activităților aferente unui bun cultural, derulate conform prevederilor din subsecțiunea 6.2.14 din prezentul caiet de sarcini.

Totodată, în *faza de analiză și proiectare* vor fi avute în vedere integrări și / sau interogări cu alte baze de date și sisteme informatice naționale, administrate de instituții publice, în vederea: simplificării proceselor administrative, validării automate a datelor furnizate de utilizatori și reducerii sarcinilor administrative și a solicitărilor suplimentare adresate acestora, conform prevederilor din secțiunea 7.3 din prezentul caiet de sarcini.

Asistentul virtual integrat în platformă va oferi sprijin contextual utilizatorilor, de exemplu în completarea formularelor și în furnizarea răspunsurilor personalizate utilizatorilor, utilizând modele de inteligență artificială configurabile. [pentru detalii se va consulta secțiunea 7.4 a prezentului caiet de sarcini].

6.1.3 Cerințe funcționale pentru etapele fluxurilor

6.1.3.1 Inițierea, depunerea și înregistrarea solicitărilor

Utilizatorii autentificați vor avea acces la serviciile electronice într-o manieră structurată, fiecare serviciu fiind prezentat cu o descriere clară, cu lista documentelor necesare și formularul aferent pentru depunerea electronică. Utilizatorul va putea regăsi ușor serviciul dorit și informațiile asociate despre obținerea acestuia. De exemplu: serviciul va putea fi accesat atât din interfața aferentă Bunului cultural din *Componenta de management patrimoniu*, cât și din meniul aferent din *Componenta de e-Guvernare*.

Fiecare utilizator va beneficia de un dosar digital propriu, care va centraliza documentele încărcate în platformă. Sistemul va permite reutilizarea documentelor existente din dosarul digital al utilizatorului în cadrul unor procese sau solicitări noi, fără a fi necesară reîncărcarea acestora.

Formularele web vor permite completarea ghidată și atașarea documentelor în format electronic, inclusiv fișiere de mari dimensiuni, iar sistemul va verifica automat respectarea constrângerilor de format și dimensiune ale fișierelor, dar și validarea semnăturilor electronice.

Serviciile electronice vor fi centrate pe activități și pe finalitatea acestora, constând într-o succesiune de pași, care includ, după caz:

- ecrane de informare;
- ecrane care conțin formulare web care trebuie completate și care permit încărcarea de fișiere (de mari dimensiuni) - documente/fotografii/documente scanate etc.;
- ecrane care permit efectuarea plății electronice a tarifelor percepute pentru serviciile solicitate;
- ecrane de vizualizare a unor documente generate automat de către sistemul digital, în baza informațiilor furnizate până la acel moment.

Succesiunea pașilor va fi configurabilă, iar sistemul va permite personalizarea conținutului și a regulilor de validare pentru fiecare tip de serviciu.

Pașii din proces vor putea avea asociate termene limită pentru realizarea acțiunii setate la configurare, iar depășirea termenului va declanșa o acțiune automată a sistemului (ex. notificare expediată către responsabilul acțiunii, închiderea sau suspendarea procesului etc.).

La finalizarea depunerii, sistemul va genera un dosar electronic unic, asociat solicitantului și serviciului selectat, care va însoți fluxul administrativ până la finalizare. Solicitantul va primi notificare automată în sistem și pe email cu numărul de înregistrare și va putea urmări online stadiul procesării.

Înregistrarea solicitărilor se va realiza automat în registrele electronice configurate în sistem. Pentru solicitările primite în format letric, înregistrarea se va face de către utilizatorii autorizați, prin scanarea și introducerea documentelor în fluxurile de avizare.

6.1.3.2 Direcționarea și circuitul intern de aprobare

Sistemul digital va asigura rutarea automată a solicitărilor către compartimentele/instituțiile competente (utilizatorii din cadrul acestora), conform regulilor de flux definite. Documentele depuse vor fi verificate și, dacă este cazul, se vor solicita clarificări și/sau completări. Documentele de răspuns vor fi elaborate, avizate și aprobate exclusiv în format electronic prin intermediul sistemului digital, semnate digital de actorii implicați și arhivate automat într-un depozit operațional. Fluxurile de aprobare vor fi atât paralele cât și secvențiale, în funcție de specificul procesului administrativ. Avizarea și aprobarea internă a documentelor de răspuns la solicitările de furnizare a serviciilor se realizează prin intermediul unui flux digital de transmitere a documentului de la o persoană la alta, cu notificarea automată pe email a utilizatorilor implicați în fiecare etapă a procesului. Toate etapele de procesare vor fi jurnalizate automat, cu evidențierea timpilor de răspuns și a responsabililor, în vederea asigurării trasabilității complete și a monitorizării performanței administrative.

6.1.3.3 Organizarea comisiilor de specialitate

Având în vedere rolul comisiilor de specialitate în cadrul proceselor de e-guvernare dedicate patrimoniului cultural, activitatea acestora va fi gestionată printr-un submodul dedicat, care va permite secretariatelor configurarea componenței comisiilor, programarea ședințelor, transmiterea documentațiilor, generarea ordinii de zi și a proceselor verbale și colectarea voturilor în format electronic. Alocarea dosarelor pe ședințe sau către membrii comisiilor se va putea realiza fie automat (prin select individual sau select multiplu), fie prin mecanisme randomizate. Documentele depuse vor fi verificate și, dacă este cazul, se vor solicita clarificări și/sau completări. Rezultatele deliberărilor și documentele aferente vor fi integrate automat în fluxurile de avizare.

Deciziile comisiilor vor fi integrate în fluxul digital de avizare, iar rezultatul acestora va determina continuarea procesului administrativ. În situația în care hotărârea este favorabilă, autoritatea competentă (Ministerul Culturii, Institutul Național al Patrimoniului sau direcțiile județene pentru cultură) va putea emite avizul/certificatul/autorizația/documentul corespunzător, cu referințiere directă la documentația analizată. În cazul în care hotărârea este nefavorabilă, solicitantul va fi notificat ulterior, cu posibilitatea de a depune o contestație, care va fi soluționată de comisia de contestații.

Sistemul digital va permite astfel urmărirea în timp a fiecărui dosar, indicând data ședinței, participanții, documentele analizate și rezultatul deliberărilor, consolidând transparența și eficiența procesului decizional. Atât solicitanții cât și membrii comisiilor vor putea fi notificați cu privire la participarea la ședințe.

6.1.3.4 Transmiterea documentelor de răspuns

Toate documentele de răspuns vor fi emise și transmise în format electronic, semnate digital conform OUG 38/2020. Sistemul va permite notificarea automată a solicitantului prin email și în contul propriu, cu posibilitatea descărcării documentelor emise. În

cazurile prevăzute de lege sau solicitate expres, sistemul va permite tipărirea și eliberarea documentelor în format letric.

6.1.4 Cerințe funcționale privind arhivarea electronică

Componenta e-Guvernare va include funcționalități avansate de arhivare electronică, care vor asigura păstrarea, organizarea și gestionarea documentelor în format electronic, pe baza unei structuri logice de dosare electronice asociate fluxurilor de lucru. Componenta va permite stocarea documentelor într-un depozit electronic centralizat, cu gestiune riguroasă a drepturilor de acces, controlul versiunilor, trasabilitatea completă a modificărilor, integrarea nomenclatorului arhivistic și aplicarea automată a termenelor de păstrare.

Fiecare document electronic va putea fi asociat mai multor dosare fără duplicarea fișierelor, asigurând o utilizare eficientă a spațiului de stocare. Prestatorul trebuie să asigure și structura de metadate arhivistice obligatorii (identificator unic, dată, autor, tip document, termen de păstrare, semnătură digitală, marcă temporală).

Semnarea documentelor se va realiza utilizând certificate digitale calificate, prin implementarea protocoalelor OpenID Connect și PKCE, conform standardelor PADES/CADES/XADES.

Componenta de e-Guvernare va putea fi configurată să solicite ca anumite documente atașate de către utilizatori să fie semnate electronic, caz în care se va verifica validitatea semnăturii electronice (prin integrarea cu serviciile OCSP - Online Certificate Status Protocol, în conformitate cu RFC 6960). Sistemul va semna utilizatorului dacă semnătura nu este validă și nu va permite parcurgerea pașilor următori ai serviciului electronic.

Componenta de e-Guvernare va avea și rol de sistem de arhivă electronică pentru datele asociate serviciilor publice digitale încorporate. Această componentă a Sistemului Digital trebuie proiectată și dezvoltată pentru a permite la punerea în producție avizarea de către Autoritatea pentru Digitalizarea României (ADR) ca sistem electronic de arhivare, conform legislației în vigoare. Prestatorul va implementa funcționalitățile necesare de integritate, autenticitate, confidențialitate, disponibilitate și audit ale Sistemului Digital pentru a fi pregătit de avizare în conformitate cu Ordinul ADR nr. 20.717/2024 privind acreditarea administratorilor de arhivă electronică și avizarea sistemelor de arhivare.

De asemenea Prestatorul va livra și documentația tehnică necesară pentru depunerea dosarului de avizare ADR, inclusiv specificațiile de securitate, descrierea fluxurilor arhivistice și manualul de administrare.

6.2 Componenta Management Patrimoniu Cultural (MPC) (componentă aplicativă)

Scopul acestei componente este de:

- realizare a managementul datelor necesare identificării, inventarierii, evidenței, conservării și gestionării eficiente a resurselor culturale, precum și pentru identificare riscuri, prioritizare investiții, inspecție și control
- creșterea accesibilității publicului larg la date digitalizate din patrimoniul cultural național, de înaltă calitate și bazat pe noile tehnologii (interfața de căutare)
- prezentare și valorificare atractivă a resurselor culturale digitale pentru a susține educația și cercetarea, precum și pentru a promova turismul cultural
- furnizare date pentru politici publice și decizii bazate pe date.

Prin resursă, în sensul prevederilor din acest document, se înțelege: **obiect fizic** (cum ar fi un obiect de patrimoniu cultural), **entitate temporală** (cum ar fi activitate sau eveniment), **actor** (cum ar fi o persoană sau o organizație) sau **obiect conceptual** (cum ar fi o imagine, un document sau alt purtător de informații).

Inventarierea monumentelor istorice reprezintă acțiunea de strângere a totalității informațiilor, imaginilor, planșelor, materialelor audio-video și 3D, documentelor, studiilor, cercetărilor și a documentațiilor cu privire la identificarea imobilelor susceptibile de a dobândi calitatea de monument istoric, a imobilelor clasate ca monumente istorice, a monumentelor istorice declasate, precum și a celor distruse sau dispărute. Inventarul monumentelor istorice reprezintă o bază de date actualizată permanent prin operațiunile necesare de corelare, în vederea asigurării unei informări permanente și exacte în legătură cu situația imobilelor monumente istorice.

6.2.1 Cerințe generale

Funcționalitățile Componentei MPC trebuie să cuprindă:

- utilizarea ontologiilor ca mijloc de a denumi și defini formal tipurile de date, proprietățile și relațiile dintre clase care descriu o resursă
- modelarea datelor la nivel logic prin implementarea teoriei grafurilor în realizarea schemelor de date pentru a proiecta și organiza structuri de date care să reprezinte eficient entitățile (instanțele), clasele, relațiile, dependențele și ierarhiile
- utilizarea de tezaure terminologice pentru gestionarea vocabulelor controlate necesare descrierii și indexării informațiilor într-un mod consistent și uniform
- crearea, vizualizarea, actualizarea și ștergerea resurselor cu păstrarea istoricului
- importul și parsarea de resurse și de scheme de date diferite sub formă de grafuri

- introducerea, căutarea și vizualizarea resurselor digitale, a imaginilor și materialelor audio-video și 3D
- un submodul GIS pentru gestionarea datelor geospațiale
- realizarea de instrumente de prezentare și valorificare atractivă a resurselor culturale digitale
- afișarea în interfața publică (pentru utilizatori neautentificați) a unor indicatori statistici agregați, precum: „cele mai vizualizate bunuri”, „resurse cu cele mai multe descărcări”, „cele mai accesate fișe de monumente” etc.
- furnizarea de date pentru fundamentarea de politici publice și decizii bazate pe date
- integrarea cu Componenta de e-Guvernare și cu alte sisteme externe.

Această Componentă poate fi dezvoltată de la zero sau poate fi dezvoltată pornind de la o platformă software de management al patrimoniului cultural matură și adecvată.

6.2.2. Cerințe privind implementarea ontologiilor

6.2.2.1 Definiție ontologie și beneficii

Ontologia reprezintă un cadru conceptual care definește și organizează informațiile despre elementele de patrimoniu cultural într-un mod structurat și interoperabil. Aceasta include stabilirea unui vocabular comun și a relațiilor dintre diferitele entități (de exemplu, opere de artă, monumente, artefacte, documente) și proprietățile acestora (creator, perioadă, stil, locație etc.), facilitând astfel colectarea, gestionarea, analiza, căutarea și partajarea eficientă a informațiilor către alte sisteme digitale.

Aceasta permite nu doar descrierea izolată a obiectelor culturale, ci și reprezentarea relațiilor dintre acestea, reflectând astfel rețeaua complexă de contexte istorice, culturale și sociale în care obiectele au generat sau generează semnificații. Ontologia sprijină astfel interpretarea și analiza avansată a datelor culturale, facilitând cercetarea și accesul la informații în domeniul patrimoniului cultural.

Ontologia aduce multiple beneficii în domeniul patrimoniului cultural, îmbunătățind gestionarea, accesul și înțelegerea colecțiilor de obiecte culturale cum ar fi:

- Standardizarea și consistența datelor: prin stabilirea unui vocabular comun și a unor relații clare între concepte, ontologia asigură standardizarea și consistența informațiilor despre obiectele de patrimoniu cultural. Aceasta facilitează comunicarea și schimbul de date între diferite instituții culturale, cum ar fi muzee, arhive și biblioteci.
- Interoperabilitatea: ontologia facilitează interoperabilitatea între diferite sisteme și platforme de gestionare a datelor, permițând integrarea și accesul la diverse resurse și colecții de patrimoniu cultural, indiferent de proveniența sau formatul

lor. Aceasta permite utilizatorilor să acceseze și să exploreze colecții vaste de date culturale din surse multiple printr-o singură interogare.

- Căutare îmbunătățită și descoperire: utilizarea ontologiei permite dezvoltarea de sisteme de căutare semantică, care pot interpreta nevoile utilizatorilor într-un mod mai precis și pot returna rezultate mai relevante, bazate pe contextul și semnificația cererilor de căutare, nu doar pe cuvinte-cheie.
- Reprezentarea complexă a cunoștințelor: ontologia permite modelarea relațiilor complexe între obiecte culturale, oferind o înțelegere mai profundă a contextului istoric, cultural sau artistic. Aceasta include relații temporale, spațiale, cauzale și conceptuale, care ajută la reconstruirea rețelelor de semnificații și influențe dintre obiecte.
- Facilitarea cercetării: Cercetătorii beneficiază de ontologie prin capacitatea de a efectua analize complexe și interdisciplinare, explorând conexiuni și tendințe ascunse în datele culturale. Acest lucru poate duce la descoperiri noi și la o mai bună înțelegere a istoriei și culturii.
- Conservarea și sustenabilitatea: ontologia contribuie la conservarea digitală a patrimoniului cultural prin organizarea meticuloasă și arhivarea datelor. Asigură că informațiile sunt păstrate într-un format structurat și accesibil pentru viitoarele generații, facilitând sustenabilitatea pe termen lung a resurselor culturale.

Din punct de vedere al Componentei MPC o ontologie reprezintă un model formalizat care clasifică entitățile în clase, definește relațiile permise dintre aceste clase și stabilește reguli semantice pentru validarea conexiunilor și structurii datelor, asigurând interoperabilitatea și coerența reprezentării cunoștințelor.

6.2.2.2 CIDOC-CRM, extensii, completări și ontologii complementare

Componenta MPC va utiliza ultima versiune oficială a ontologiei CIDOC-CRM ca referință, la momentul implementării contractului (standard ISO 21127:2014) care oferă un cadru semantic pentru modelarea relațiilor complexe dintre entitățile din patrimoniul cultural (<http://www.cidoc-crm.org/>).

Prestatorul va avea în vedere și implementarea unor modele compatibile, recunoscute în comunitatea științifică ale CIDOC-CRM (<https://cidoc-crm.org/collaborations>, <https://cidoc-crm.org/extensions/>), ca de exemplu: pentru arheologie (CRMarchaeo), documentarea și analiza structurilor arheologice existente (CRMba), cercetare științifică (CRMsci), digitizare (CRMdig), spațiu și timp (CRMgeo), studiul documentelor antice și epigrafie (CRMtex), informații și colecții bibliografice (LRMoo), precum și pentru gestionarea și partajarea informațiilor despre raționament, premise, concluzii și pașii de raționare (CRMinf) precum și European Data Model [EDM], adoptat de către Biblioteca Digitală Europeană (europeana.eu).

Pentru domenii specializate, precum numismatica sau patrimoniul imaterial, pot fi incluse și alte ontologii consacrate precum Nomisma (<https://nomisma.org/ontology>) și The Reactive Heritage Digital Twin Ontology (RHDTO) (<https://www.mdpi.com/1424-8220/24/12/3978>).

Prestatorul poate propune și implementarea altor ontologii, în funcție de specificul și cerințele contextuale, dar acestea sunt supuse acceptului Autorității Contractante.

Integrarea, dacă este cazul, va fi realizată **prin mapare semantică pe CIDOC CRM a conceptelor și definițiilor împrumutate din ontologiile alternative**. Prestatorul nu va introduce în Componenta MPC modele paralele care să creeze conflicte ontologice.

Având în vedere că ontologia nu este doar un set de metadata, Prestatorul o va implementa în Componenta MPC cu toate cadrele complexe de relații și reguli care modelează modul în care elementele ei interacționează și se raportează unele la altele.

Denumirea proprietăților, sub-proprietăților, claselor, sub-claselor, meta-datelor ce aparțin ontologiei vor avea și denumiri alternative cu scopul de a afișa într-un mod user friendly și pentru utilizatorul nespecializat anumite proprietăți. (Ex. „E64 End of Existence” va afișa Finalul perioadei).

În situația în care, pentru a se asigura acoperirea tuturor situațiilor contextuale aferente patrimoniului cultural din România, se introduc clase sau proprietăți suplimentare față de modelul de bază CIDOC CRM, în special pentru clase și/sau proprietăți care nu sunt aferente extensiilor CIDOC CRM, Prestatorul are obligația de a documenta **extensia ontologică** astfel încât noile concepte să fie integrate în arborele conceptual al CIDOC CRM, respectând structura și convențiile oficiale de documentare (cod, denumire, definiție, relații cu domeniu și codomeniu, proprietăți inverse, etc). Documentarea trebuie să includă atât diagrama ierarhică (arborele de moștenire a claselor și proprietăților), regulile de numire și namespace, precum și modul de utilizare și gestionare a extensiilor în cadrul sistemului.

La crearea Modelelor de Resurse și a Ramurilor, sistemul digital va impune ontologia pe întreg graful aplicând toate regulile corespunzătoare pentru clasele de noduri (Entități CRM) și arce (Proprietăți CRM).

În cadrul sistemului va fi permisă și crearea unui graf fără ontologie, care nu va defini astfel clase CRM specifice pentru noduri și arce.

În cazul în care un atribut specific unui Model de Resurse, cum ar fi „Sistem de încălzire” pentru clădiri, nu poate fi mapat direct la o clasă sau proprietate din ontologia CIDOC CRM, se va permite extinderea ontologiei prin utilizarea unui nod semantic pentru a crea o conexiune simbolică între entitatea principală (clădire) și attributele specifice. În acest caz:

- Nodul semantic „Caracteristici tehnice” acționează ca un nod intermediar care nu stochează date, ci grupează logic attributele specifice.

- Proprietatea "P67 refers to" din CIDOC CRM este utilizată pentru a lega acest nod semantic de entitatea principală, asigurând conformitatea cu ontologia.
- Nodul „Sistem de încălzire” este apoi adăugat sub nodul semantic, permițând stocarea datelor specifice.

6.2.2.3 Mecanisme de validare, asigurare a calității și continuității

Prestatorul va crea în cadrul Componentei MPC mecanisme automate de validare prin care se va asigura că atât calitatea cât și consistența datelor vor fi monitorizate și asigurate. Fiecare set de date va fi supus verificărilor de validare cel puțin la încărcarea inițială, la import sau migrare, la actualizarea ulterioară a datelor, precum și ori de câte ori intervin modificări ale regulilor de validare sau ale modelului de date. Verificările vor urmări respectarea regulilor minime obligatorii pentru fiecare tip de entitate și relație. De exemplu, se va testa dacă obiectele, evenimentele, locurile, persoanele și datele asociate respectă regulile minime obligatorii (de exemplu, un obiect trebuie să aibă un titlu și o localizare; un strat arheologic trebuie să fie tipizat și legat de sit; un loc trebuie să aibă o geometrie validă). În acest scop, prestatorul va implementa în sistem seturi de reguli formale care descriu modul corect de reprezentare a entităților și relațiilor, conform modelului național adoptat (CIDOC CRM și extensiile sale), ca de exemplu fișiere SHACL (Shapes Constraint Language).

Modelul de validare a datelor va fi integrat și în fluxurile de lucru și va produce rapoarte detaliate asupra erorilor și neconformităților.

Prestatorul se va asigura că Componenta MPC permite adăugarea ulterioară în ontologia implementată de attribute specifice care nu sunt acoperite de CIDOC-CRM și/sau nu sunt incluse în ontologia dezvoltată în cadrul prezentului contract, precum și noi vocabulare controlate sau tezaure terminologice dezvoltate de Autoritatea Contractantă. Extensibilitatea trebuie să fie documentată și să nu afecteze regulile existente.

6.2.2.4 Versionarea ontologiei

Pentru a asigura stabilitatea și continuitatea sistemului digital în raport cu evoluțiile versiunilor oficiale ale CIDOC CRM și extensiilor acestuia, precum și alte tipuri de situații în care ontologia poate suferi modificări, Prestatorul va implementa un mecanism de versionare a ontologiei, incluzând, dacă este cazul, și extensiile dezvoltate în cadrul contractului. Acest mecanism va permite urmărirea și gestionarea modificărilor apărute de la o versiune la alta (de exemplu, clase sau proprietăți marcate ca *deprecated*). Totodată, sistemul digital va cuprinde funcționalități de verificare că datele introduse în sistem rămân valide și interogabile indiferent de versiunea utilizată, prin furnizarea unor proceduri și scripturi de migrare care să permită adaptarea automată sau asistată a datelor la noile structuri.

Prestatorul are obligația de a furniza instrucțiuni privind mecanismul de versionare a ontologiei care să evidențieze modul de lucru, modalitatea de realizare a modificărilor și să conțină regulile de mapare către noile versiuni.

Datele modelate conform ontologiei implementate vor putea fi utilizate și exportate în formate RDF standard, conform cerințelor privind interoperabilitatea și exportul de date prevăzute în prezentul caiet de sarcini.

6.2.3 Cerințe privind modelarea datelor la nivel logic

Principalele concepte care vor fi utilizate sunt definite astfel:

- **Resurse:** vor reprezenta înregistrări individuale în baza de date, descrise prin attribute și relații. Exemplu: o clădire istorică precum „Biserica Stavropoleos” este o resursă care conține date despre nume, locație și descriere.
- **Modele de Resurse:** vor reprezenta structuri de nivel superior care vor defini categoriile de resurse, inclusiv grafurile asociate. Exemplu: Modelul „Clădiri” specifică attribute precum „Nume” și „Locație”, permițând crearea de instanțe precum „Biserica Stavropoleos”.
- **Ramuri:** vor reprezenta sub-structuri reutilizabile ale grafurilor, utilizate pentru transferul de noduri între modele. Exemplu: Ramura „Adresă” cu noduri „Stradă” și „Oraș” poate fi inclusă în modelele „Clădiri” și „Siturile Arheologice” pentru consistență.
- **Grafuri:** vor reprezenta structuri de bază compuse din noduri, arce și grupuri de noduri, care vor defini relațiile semantice. Exemplu: În graful „Clădiri”, un nod „Stil arhitectural” (tip termen de vocabular) este conectat prin arcul „P2 has type” la clasa E55 Type din CIDOC CRM.
- **Noduri:** vor reprezenta attribute individuale care colectează date, cu tipuri precum string, geojson-collection sau file-list. Exemplu: Nodul „Data construcției” (tip Date) stochează „1724” pentru „Biserica Stavropoleos”.
- **Grupuri de Noduri:** vor reprezenta colecții de noduri care colectează date corelate, utilizate pentru a crea secțiuni de formular. Exemplu: Grupul „Detalii tehnice” include nodurile „Sistem de încălzire” și „Tip ventilație”, stocând date în blocuri de date.
- **Blocuri de Date:** vor reprezenta unități de stocare a valorilor pentru un grup de noduri într-o instanță de resursă. Exemplu: Un bloc pentru „Detalii descriptive” conține {„Nume”: „Biserica Stavropoleos”, „Descriere”: „Biserică ortodoxă” }.
- **Secțiuni de Formular:** vor reprezenta componente UI care configurează interfața de introducere a datelor pentru grupuri de noduri. Exemplu: Secțiunea „Detalii descriptive” afișează widget-uri pentru „Nume” (câmp text) și „Descriere” (zonă text), salvând datele în blocuri de date.

- **Termeni de Vocabular:** vor reprezenta elemente controlate, organizate în scheme și colecții pentru clasificare. Exemplu: Termenul „ortodoxă” din colecția „Stiluri arhitecturale” clasifică „Biserica Stavropoleos”.
- **Instanțe de Resurse:** vor reprezenta înregistrări concrete ale unui Model de Resurse. Exemplu: „Biserica Stavropoleos” este o instanță a Modelului „Clădiri”, cu blocuri de date stocate în baza de date relațională și indexate în motorul de căutare și analiză distribuită.
- **Relații Personalizate:** vor fi definite în interfața de gestionare a termenilor de vocabular pentru a desemna conexiuni între instanțe. Exemplu: Relația „construită de” conectează „Biserica Stavropoleos” la „Ioanichie Stratonikeas”.

6.2.3.1 Configurarea structurii datelor - editorul de modele și grafuri

Componenta MPC va include un editor (panou de administrare) de modele și grafuri care va permite utilizatorilor autorizați să configureze structura de introducere a înregistrărilor, adică modul în care datele sunt organizate logic și prezentate în aplicație, fără a necesita modificări directe la nivelul codului sursă sau al tabelelor fizice ale bazei de date, incluzând:

- Crearea, modificarea, exportul, importul, duplicarea și validarea automată la salvare a Modelelor de Resurse și a Ramurilor
- Configurarea Ramurilor.
- Gestionarea secțiunilor de formulare (interfețelor de introducere a datelor)
- Gestionarea permisiunilor.

Astfel se va asigura personalizarea structurii logice a datelor prin modificarea metadatelor, fără a afecta structura fizică a bazei de date (tabele, coloane, relații).

În cadrul editorului se vor putea construi grafurile, seturi structurate de noduri și grupuri de noduri ce reprezintă nucleul unui Model de Resurse sau al unei Ramuri

Grafurile vor fi construite prin adăugarea de noduri (sau Ramuri existente) într-o structură relațională de tip rețea semantică și cu respectarea regulilor ontologice. Adăugarea unui nod nou va presupune și stabilirea tipului de date asociat.

6.2.3.2 Tipuri de date disponibile

În cadrul sistemului digital vor fi disponibile cel puțin următoarele tipuri de date, existând posibilitatea de extindere cu tipuri noi/custom de date:

- Semantic – utilizate pentru a crea conexiuni simbolice între alte noduri, în general pentru a respecta regulile ontologice
- String – utilizate pentru a stoca text, cum ar fi numele sau descrierea unei resurse cu formatare și hyperlink-uri
- Number: Stochează un număr.

- File-list: Stochează unul sau mai multe fișiere (imagini, documente etc.)
- Vocabulary term: utilizat pentru stocarea unui Termen de vocabular (un element de vocabular controlat utilizat pentru a defini și clasifica resursele). Utilizatorii vor putea alege un Termen de vocabular dintr-o listă derulantă.
- Vocabulary term-list: Stochează mai mulți Termeni de vocabular într-un singur nod.
- GeoJSON-collection: stochează informații despre locație. Se va utiliza pentru un nod care ar trebui afișat ca un strat suplimentar pe harta principală de căutare.
- Custom field values: Similar cu „Vocabulary term”, pentru a prezenta utilizatorului o listă derulantă sau un set de butoane radio. Spre deosebire de „Vocabulary term”, această listă derulantă nu va proveni din vocabularul controlat la nivelul soluției, ci dintr-o listă de valori pe care se definește local în configurația nodului și nu sunt partajate la nivel de sistem. Exemplu: un nod „Stare de conservare” cu valorile „Bună”, „Medie”, „Proastă”
- Custom field values-list: permite prezentarea utilizatorului a unei liste derulante sau a unui set de opțiuni (cum ar fi casete de selectare) din care pot fi alese mai multe valori simultan. Exemplu: un nod „Tipuri de utilizare” cu valorile „Rezidențial”, „Comercial”, „Educațional”, din care utilizatorul poate selecta mai multe opțiuni, cum ar fi „Rezidențial” și „Comercial” pentru o clădire cu utilizare mixtă.
- Date: Stochează o dată în calendar
- node-value: Stochează o referință la un alt nod din graf.
- boolean: pentru a stoca o valoare „da”/„nu” sau „adevărat”/„fals”.
- url: Stochează o adresă web;
- resource-instance: Încorporează o instanță de resursă separată în acest nod. De exemplu, s-ar putea adăuga un nod numit „Evaluat de” la o ramură de evaluare a condiției și utiliza acest tip de date. Acest lucru ar permite asocierea unui individ stocat în baza de date ca resursă de tip Actor cu o anumită evaluare a condiției.
- resource-instance-list: Stochează o listă de instanțe de resurse într-un singur nod.

Prestatorul va construi cel puțin 50 de Modele de Resurse în cadrul contractului.

6.2.3.3 Construirea secțiunilor de formulare

În cadrul editorului aferent Componentei MPC se vor putea construi secțiunile de formulare care vor fi expuse în interfața utilizatorului. Acestea vor fi construite pe baza documentelor specifice diferitelor fluxuri administrative în care sunt implicate

elementele de patrimoniu precum fișa analitică de inventariere a monumentului istoric, obligația privind folosința monumentului istoric etc.

Secțiunile de formulare vor fi construite într-o structură de tip arborescent, similar cu ceea ce vor vedea utilizatorii atunci când încep să creeze o resursă utilizând acest Model de Resurse. Se va pune accent pe experiența utilizatorului, pe ușurința de navigare, regăsire și completare a datelor, lipsa piedicilor și neclarităților în experiența utilizatorului.

Structura arborescentă va conține o listă de secțiuni de formulare din Modelul de Resurse, dintre care unele pot fi imbricate în altele. Pentru fiecare grup de noduri din arborele de graf se va configura o secțiune de formular corespunzător în arborele de secțiuni de formulare.

Secțiunile de formulare vor putea include unul sau mai multe widget-uri. Acestea vor corespunde nodurilor din graf care colectează date. Editorul va permite previzualizarea modului în care un utilizator care introduce date va vizualiza secțiunile de formular în interfață. Editorul va asigura definirea permisiunilor până la nivelul secțiunii de formular.

Definirea permisiunilor va fi posibilă prin selectarea unui utilizator sau a unui grup de utilizatori și apoi atribuirea uneia din următoarele permisiuni:

- **Ștergere:** Permite utilizatorilor să șteargă instanțe ale acestui grup de noduri.
- **Fără acces:** Interzice utilizatorilor să vizualizeze sau să editeze instanțe ale acestui grup de noduri. Se va utiliza acest nivel de permisiune pentru a ascunde date sensibile de utilizatorii neautentificați (publicul).
- **Citire:** Permite utilizatorilor să vizualizeze secțiunea de formular a acestui grup de noduri.
- **Creare/Actualizare:** Permite utilizatorilor să creeze sau să editeze instanțe ale acestui grup de noduri. Aceasta oferă utilizatorilor posibilitatea să editeze anumite informații despre o resursă, fiind în același timp restricționați de la editarea altor informații.

Prestatorul va construi cel puțin 50 de secțiuni de formulare în cadrul contractului.

6.2.3.4 Versionare

Componenta MPC va permite versionarea Modelelor de Resurse și Ramurilor printr-un flux de lucru bazat pe stările draft / publicat. Astfel, în cadrul sistemului digital fiecare graf (model de resurse și ramură), va exista în una din următoarele stări:

Versiune Curentă - reprezintă versiunea activă a grafului utilizată pentru instanțele de resurse. În starea publicată:

- Structura grafului este blocată.

- Se pot modifica în continuare elementele legate de interfața de utilizator (etichete ale secțiunilor de formular, etichete de widget-uri etc.).
- Permisunile de editare pot fi configurate.

Versiune Draft - reprezintă starea în care se pot efectua modificări nepublicate asupra structurii grafului, precum:

- Modificarea structurii grafului (adăugarea/eliminarea de grupuri de noduri, noduri etc.).
- Actualizarea configurațiilor secțiunilor de formular.
- Schimbarea setărilor widget-urilor.
- Dacă se creează o nouă versiune a grafului, instanțele de resurse care utilizează o versiune anterioară vor deveni disponibile doar pentru citire.

Versiune Publicată – reprezintă versiunea utilizată activ pentru toate operațiunile legate de resurse, cum ar fi introducerea datelor, interogarea și validarea.

6.2.4 Cerințe privind gestionarea tezaurelor terminologice și vocabularelor controlate

6.2.4.1 Gestionarea vocabulare și importul de tezaure terminologice (scheme de vocabulare)

Un **Vocabular Controlat** este o listă **finită și predefinită** de termeni autorizați, destinată să asigure **consistența datelor** și să elimine ambiguitatea (sinonimele, variațiile de ortografie). Din punct de vedere tehnic, funcționează ca un set de **valori permise** dintr-un domeniu de date (similar cu o enumerare sau o listă de valori fixe) care trebuie stocate și referite centralizat.

Un **Tezaur Terminologic** este o formă avansată de Vocabular Controlat care nu doar listează termenii autorizați, ci **modelează explicit relațiile semantice** dintre aceștia. Structura sa se bazează pe relații ierarhice (Termen Mai Larg/Mai Îngust), de echivalență (Termen Preferat/Sinonim) și asociative (Termeni Înruțiți), conform standardului **SKOS (Simple Knowledge Organization System)**. Din punct de vedere tehnic, acesta trebuie implementat ca un **graf de termeni** care permite interogarea semantică și navigarea ierarhică în interfața utilizatorului.

Componenta MPC va dispune de o interfață grafică prin care utilizatori autorizați vor avea posibilitatea de a gestiona termenii de vocabular (vocabulare controlate) utilizați în listele derulante și câmpurile din diversele secțiuni de formulare ale sistemului digital.

Gestionarea termenilor de vocabular (vocabulare controlate) se va realiza prin capabilitatea de a crea, actualiza, modifica, importa, exporta și șterge atât schemele de termeni de vocabular (care agregă unul sau mai mulți termeni de vocabular și relațiile semantice dintre aceștia), cât și colecțiile de termeni de vocabular (grupări tematice de termeni selectați dintr-una sau mai multe scheme), utilizate pentru a

popula liste derulante sau butoane radio în secțiunile de formular ale instanțelor de resurse.

Schemele de termeni de vocabular vor fi organizate ierarhic și se vor putea defini relații multiple (un termen putând aparține mai multor categorii superioare), adică o structură de tip graf orientat (DAG), conform practicilor SKOS (broader / narrower / related). De exemplu, un castel este un tip de fortificație, dar este și o clădire rezidențială.

Componenta MPC va cuprinde și funcționalități de:

- import de termeni de vocabular din tezaure terțe precum și posibilitatea importului unei scheme de termeni de vocabular prin încărcare unui fișier XML / JSON / CSV / RDF compliant SKOS.
- export de termeni de vocabular și ai unei scheme de termeni de vocabular sub formă de fișier XML / JSON / CSV / RDF compliant SKOS.
- vizualizarea schemelor de termeni de vocabular sub formă de grafuri și definirea de relații de tip one-to-many între termeni de vocabular care nu sunt legați printr-o relație de tip părinte-copil.

În cadrul Componentei MPC utilizatorii avansați vor putea defini relații personalizate între instanțele de resurse prin utilizarea termenilor de vocabular din vocabularele controlate. În acest sens, în interfața grafică de gestionare a termenilor de vocabular, se va asigura posibilitatea creării unui termen de vocabular personalizat (ex. „proiectat de”) și inversul său (ex. „a proiectat”) în cadrul unei scheme ce conține tipuri de relații resursă-la-resursă, urmat de adăugarea în colecția de tipuri de relații resursă-la-resursă, pentru a fi disponibile în liste derulante. În acest mod, în editor se va putea asocia relația personalizată și inversul său cu un nod de tipul resource-instance sau resource-instance-list, care ulterior se poate integra în Modelul de Resurse dorit (ex. „Clădiri”). După publicarea grafului, relațiile personalizate (ex. „Catedrala Sagrada Familia proiectata de Antonio Gaudi”) pot fi utilizate la crearea sau editarea instanțelor de resurse, asigurând trasabilitatea și interoperabilitatea conform standardelor SKOS și CIDOC CRM.

De asemenea, utilizatorii autorizați vor putea să asocieze conceptele din cadrul unui tezaur cu formularele de introducere a datelor, să actualizeze tezaurele terminologice într-o manieră compliantă cu SKOS (<http://www.w3.org/2004/02/skos/>), iar acolo unde este cazul, să extindă aceste tezaure cu modele OWL/RDF, pentru integrarea cu ontologia de referință.

Valorile proprietăților, sub-proprietăților, claselor, sub-claselor și/sau meta-datele vor fi îmbogățite cu termeni din vocabularele Getty dar și cu nomenclatoare, vocabulare controlate sau tezaure terminologice dezvoltate sau în curs de dezvoltare, furnizate de Autoritatea Contractantă, pentru a spori eficiența, consistența și interoperabilitatea informațiilor. Utilizarea acestora asigură că toate datele sunt introduse într-un mod consistent și standardizat. Aceasta previne variațiile și erorile care pot apărea din introducerea manuală sau liberă a informațiilor, cum ar fi diferențele de ortografie sau

utilizarea de sinonime. Termenii din vocabularele controlate și tezaurele terminologice vor fi cel puțin în română și engleză.

6.2.4.2 Versionare

Sistemul digital va cuprinde un mecanism de versionare a vocabulelor, care să permită urmărirea modificărilor (adăugări, redenumiri, înlocuiri, scoateri din uz) și menținerea compatibilității între versiunile succesive.

Va exista posibilitatea de marcare a termenilor ca „învechiți” (deprecated), păstrându-le identificatorul și istoricul de utilizare și se va oferi posibilitatea de a indica termenul recomandat ca înlocuitor. Termenii marcați ca deprecated vor fi semnalați vizual în interfața de administrare și vor fi excluși din utilizarea curentă, dar vor rămâne accesibili pentru compatibilitate și trasabilitate.

Va fi permisă și ștergerea unui termen de vocabular, dar înainte de această operație sistemul va verifica dacă termenul este utilizat în blocuri de date asociate secțiunilor de formular ale instanțelor de resurse. Dacă termenul este utilizat, se afișează un mesaj de avertizare care informează utilizatorul că toate instanțele termenului trebuie înlocuite cu un termen de vocabular alternativ din aceeași schemă, înainte de a permite ștergerea și va realiza înlocuirea automată (totală sau parțială) cu termenul selectat de utilizator. Dacă termenul nu este utilizat, ștergerea poate fi efectuată direct de către utilizator prin metode disponibile în interfața aplicației.

Prestatorul va importa cel puțin 50 tezaure terminologice (scheme de vocabulare) în cadrul contractului.

6.2.5 Cerințe privind interfața de creare și editare a resurselor

6.2.5.1 Interfața de creare și editare a resurselor

Componenta MPC va cuprinde de o interfață de utilizator intuitivă și configurabilă pentru crearea, editarea, vizualizarea și gestionarea resurselor conform modelelor definite în sistem.

În interfața de editare a resurselor culturale trebuie să existe o structură logică și intuitivă de secțiunile de formulare, care să faciliteze introducerea, găsirea și accesarea conținutului relevant de către utilizatori. Se va organiza conținutul în secțiuni și sub-secțiuni relevante pentru utilizatori, pe baza cercetărilor realizate de Prestator și a bunelor practici de proiectare a interfețelor digitale, astfel încât să fie asigurată o structură logică, coerentă și ușor de utilizat.. Se va efectua planificarea și executarea iterativă de teste de utilizabilitate, atât calitative cât și cantitative, pe parcursul întregului ciclu de dezvoltare a Componentei MPC, precum și revizuirea și îmbunătățirea continuă, pe toată perioada de derulare a contractului (chiar și după

recepționarea intermediară a componentei), a soluțiilor de design UI/UX pe baza rezultatelor testelor, pentru a răspunde cât mai bine nevoilor utilizatorilor.

Componenta MPC va permite încorporarea unor secțiuni de formular în altele (secțiuni părinte și secțiuni copil), fără ca utilizatorul să experimenteze o navigare ierarhică, ci un design ergonomic, intuitiv și ușor de utilizat. După salvarea datelor introduse, se va afișat un raport cu datele introduse ale resursei, prin utilizare întregului ecran și publicarea compactă a informațiilor pentru a nu fi necesară o scrolare obositoare.

Se va integra în sistemul digital unui editor de text, astfel încât informația introdusă în câmpuri să poată fi formatată similar Microsoft Office Word (de exemplu: gestiunea paragrafelor și a stilurilor de text). Astfel, se va folosi un editor de tip WYSIWYG („*what you see is what you get*”) care să permită formatarea directă a textului, astfel încât aspectul textului afișat în fereastra de editare să fie identic cu cel afișat în documentul generat prin intermediul sistemului, respectiv să fie identic cu cel afișat public.

6.2.5.2 Prevenirea duplicatelor

Componenta MPC va cuprinde mecanisme care să permită utilizatorilor interni, ca în momentul începerii catalogării, să caute și să identifice dacă resursa pe care vor să o descrie este deja catalogată în platformă, astfel evitând duplicarea efortului. În situația în care resursa există deja în sistem, utilizatorul va putea folosi datele deja existente, iar orice completări sau observații vor fi asociate, automat, cu identitatea utilizatorului care le va introduce în sistem.

6.2.5.3 Validare modificărilor

Toate datele introduse de un utilizator cu rol de Editor de resurse pentru crearea sau modificarea unei resurse vor fi provizorii, până când un Curator de resurse le va aproba transformându-le în resurse cu valoare autoritară. Va exista și posibilitatea de validare automată în funcție de tipul resurselor. Datele respinse vor fi stocate pentru un termen limitat de timp (se va stabili în perioada de analiză / implementare) într-o componentă de tip recycle-bin și vor putea fi șterse de către utilizatorii autorizați sau prin proces automat, cu confirmarea utilizatorilor autorizați, la expirarea perioadei limitate.

Curatorii de resurse vor fi notificați automat cu privire la datele provizorii și le vor putea accepta sau respinge, gestionând acest proces direct din interfața Componentei MPC.

În interfața de editare a unei resurse, utilizatorii autorizați vor putea vizualiza o diagramă de relații care ilustrează conexiunile dintre nodurile de tip resource-instance (ex. relații de tip „parte din”, „asociat cu”, „autor al”, „proveniență” etc.).

6.2.5.4 Ciclul de viață al resurselor gestionate

Componenta MPC va avea implementată o metodă de gestionare a ciclului de viață al instanțelor de resurse.

Astfel instanțele de resurse vor avea una din următoarele stări:

- Draft – pe perioada de editare și îmbogățire și validare a datelor specifice;
- Propus – variantă inițiată de către un utilizator, care necesită aprobare pentru activare din partea altui utilizator;
- Activă – disponibilă pentru accesul publicului;
- Retrasă – când a devenit nerelevantă.

În acest sens, se vor implementa reguli pentru tranziția între stări, precum și logica de validare și permisiunile asociate tranzițiilor între stări.

Soluția va permite configurarea de etape personalizate ale ciclului de viață pentru anumite instanțe sau tipuri de resurse, pentru a răspunde nevoilor specifice de curatoriere a datelor patrimoniului cultural. În cazurile justificate, pot fi prevăzute și extinderi funcționale punctuale, fără afectarea regulilor generale de validare, trasabilitate și permisiuni.

6.2.5.5 Permisuni în interfața de editare

În interfața de editare a unei resurse, utilizatorii autorizați vor putea:

- să șteargă instanțele de noduri asociate cu instanța de resursă (cu confirmare și validare). Datele instanțelor de noduri sunt datele care descriu o anumită instanță de resursă conform structurilor definite de „ramuri”. De exemplu, instanța „Catedrala Notre-Dame” cu structura modelului de resurse „Clădiri” cu ramura „Detalii tehnice” și noduri „Sistem de încălzire” și „Locație”. Dacă utilizatorul alege să șteargă instanța nodului „Locație” din ramura „Detalii tehnice”, nodul „Locație” este dezasociat din ramură pentru acea instanță de resurse.
- să șteargă instanța de resurse în întregime, cu respectarea drepturilor de acces și păstrarea unui jurnal al acțiunii.
- să vizualizeze istoricul modificărilor asupra unei resurse (cine, când, ce câmpuri au fost modificate).

Sistemul digital va asigura mecanisme de validare a datelor la salvare, gestionarea automată a versiunilor (draft / aprobat / respins) și trasabilitatea completă a modificărilor efectuate asupra resurselor.

6.2.5.6 Validarea fișierelor la încărcare

Sistemul digital va permite configurarea restricțiilor aplicabile fișierelor încărcate de utilizatori în interfața de editare, inclusiv cu privire la tipurile de fișiere acceptate, dimensiunea maximă și regulile de validare. La momentul încărcării, sistemul va valida tipul, integritatea și conformitatea fișierelor și va avertiza utilizatorul cu privire la neconformitățile identificate. Pentru fișierele atașate resurselor, validarea va urmări cel

puțin respectarea formatelor acceptate, a limitelor de dimensiune și a regulilor generale de securitate aplicabile fișierelor încărcate în sistem.

6.2.5.7 Multilingvism și transliterare

Sistemul va avea un mecanism care să permită utilizatorului să catalogheze un bun cultural să adauge metadate legate de transliterarea caracteristicilor acestuia în alte limbi. (de exemplu: Mihai vs. Michaly vs. Mihaiu; Alecsandri – Aleksandri – Alexandri; Brașov – Brassó/Brasso – Kronstadt – Kruhnen – Corona- Brassovia).

6.2.5.8 Trasabilitate, proveniență, versiuni și restaurare

Sistemul va avea un mecanism care să permită trasabilitatea introducerii metadatelor („provenance”), cu alte cuvinte un utilizator să poată vedea cine a produs metadatele, când și pe ce bază. În acest scop, completările sau actualizările vor fi introduse în baza de date cu posibilitatea identificării celui care le-a introdus, păstrându-se în sistem și versiunile anterioare. Această funcționalitate de identificare va fi disponibilă numai pentru utilizatorii cărora li s-a acordat acest rol / permisiune.

Sistemul va avea funcționalități de salvare a versiunilor anterioare ale informațiilor aparținând unei resurse culturale și se va putea reveni oricând la o versiune anterioară.

Sistemul trebuie să dețină facilități de restaurare a elementelor șterse (funcționalitate tip „Recycle Bin”).

6.2.6. Cerințe privind importul și exportul datelor în bloc

6.2.6.1 Interfața de import în bloc și șabloane

Componenta MPC va cuprinde de o interfață de utilizator prin care utilizatorii autorizați vor putea să importe, să editeze și să exporte seturi mari de date nu doar înregistrare cu înregistrare, ci și în mod agregat (bulk).

Se va asigura funcționalitatea de import a datelor stocate în fișiere .CSV / .XLS / .XLSX, etc.. În acest sens datele trebuie să fie organizate astfel încât să poată fi mapate corespunzător la modelele de resurse și structurile de date aferente acestora.

Pentru a facilita structurarea corespunzătoare a datelor în fișierele de importat, soluția va permite descărcarea unui fișier-șablon .csv / .xls / .xlsx pentru fiecare model de resurse selectabil dintr-o listă derulantă cu toate modelele de resurse configurate în aplicație.

Șabloanele vor include:

- foi de lucru (worksheets) corespunzătoare ramurilor utilizate în modelul de resurse;
- grupuri de câmpuri aferente fiecărei ramuri;

- o foaie distinctă cu tipurile de date și restricțiile asociate fiecărui câmp (nod).

Componenta MPC va asigura totodată și funcționalitatea de import individual și în mod agregat (bulk) a fișierelor de tip imagine, fișier media și 3D, asociindu-le URL-uri statice și mapându-le corespunzător la modelele de resurse și structurile de date aferente acestora.

6.2.6.2 Importarea și validarea datelor și interoperabilitate

Soluția va asigura mecanisme de validare a datelor și a fișierelor utilizate pentru import, înainte și în timpul procesului de încărcare, astfel încât să fie identificate și semnalate detaliat utilizatorului erorile de structură, de tip de date, de referință sau de conformitate cu modelele de resurse, vocabularele controlate, regulile de mapare și constrângerile definite în sistem.

Pentru resursele care includ fișiere asociate (de exemplu imagini, documente, fișiere media sau alte fișiere digitale), sistemul va permite importul acestora împreună cu fișierul care conține metadatele aferente (de exemplu Excel, CSV, JSON), fie prin arhive de tip ZIP, fie prin referințe de cale relativă sau identificatori de fișier, în mod agregat (bulk).

În cazul fișierelor utilizate pentru import și schimb de date, validarea va include, după caz, cel puțin următoarele:

- verificarea coerenței structurii fișierelor .csv în raport cu antetul;
- validarea completă prin parsare a fișierelor .xlsx, inclusiv sub aspectul compatibilității de format și al eventualelor macro-uri;
- verificarea faptului că fișierele .csv și .json sunt parsabile și conforme cu modelul de date, după caz;
- verificarea arhivelor .zip, care vor fi acceptate numai dacă sunt integrale, nu conțin alte arhive, nu includ fișiere executabile și respectă limitele de dimensiune.

În cazul identificării unor erori sau neconformități, sistemul va avertiza utilizatorul, va furniza informații suficiente pentru corectarea acestora și va permite, după caz, respingerea importului integral sau parțial.

Soluția va expune o interfață programatică (API) pentru importuri automate controlate, cu autentificare și jurnalizare a operațiunilor.

6.2.6.3 Editarea în bloc a datelor

Soluția va permite utilizatorilor autorizați să efectueze modificări în bloc ale datelor pentru mai multe instanțe de resurse, conform permisiunilor de acces definite.

Pentru câmpurile de tip String, soluția va asigura cel puțin următoarele tipuri de modificări în bloc:

- Ștergere
- Schimbarea capitalizării (majuscule, litere mici)

- Înlocuire text
- Eliminarea spațiilor goale de la începutul, mijlocul sau sfârșitul șirurilor de text
- Operațiuni de tip „Find and Replace”

Pentru alte tipuri de date, soluția va permite, după caz și în funcție de tipul câmpului, cel puțin setarea, înlocuirea sau ștergerea valorii, precum și actualizarea controlată a valorilor selectate din nomenclatoare, vocabulare sau liste configurate în sistem.

Operațiunile de editare vor putea fi aplicate pentru:

- un set de instanțe de resurse rezultat în urma unei căutări sau filtrări.
- toate instanțele de resurse ale unui model de resurse
- valoarea unui nod din fiecare instanță de resursă
- limba care urmează a fi actualizată în fiecare nod.
- înlocuirea textului prin „Find & Replace”

Sistemul va permite previzualizarea modificărilor înainte de aplicare și va înregistra automat un jurnal al operațiunilor (data, utilizator, acțiune, număr de înregistrări afectate).

6.2.6.4 Exportul în bloc al datelor

Soluția va permite exportul masiv al datelor instanțelor de resurse, cu înregistrarea automată a jurnalelor pentru fiecare operațiune de import / export (data, utilizator, rezultat, erori etc).

Datele exportate vor fi furnizate sub formă de fișiere .CSV / .XLS / .XLSX etc.

Soluția va permite exportul datelor fie în format structurat pe ramuri (reflectând stocarea logică a datelor - relații ierarhice între entități și noduri), fie în format structurat pe blocuri de date (reflectând stocarea fizică a datelor - entități și attribute grupate conform schemei interne a bazei de date).

Pentru instanțele de resurse cu noduri de tipul „file-list”, fișierele asociate acestor noduri vor fi exportate într-un fișier ZIP, fie împreună cu fișierul Excel, fie în arhive distincte, conform setărilor definite de administrator.

Exportul datelor în formatele „Bloc de date” și „Ramură” se va realiza exact în aceeași structură ca și la operațiunile de import, facilitând astfel modificarea datelor exportate și apoi reimportul datelor care nu pot fi editate cu ușurință în interfața grafică.

Pe lângă formatele tabelare utilizate pentru operațiuni de lucru în masă, soluția va permite și exportul datelor modelate conform ontologiei implementate în formate RDF standard, pentru utilizare în contexte de interoperabilitate semantică, publicare și reutilizare a datelor. Exportul va putea fi realizat atât la nivel de resursă individuală, cât și pentru seturi de resurse, cu păstrarea relațiilor semantice definite în ontologia de referință și a mapărilor aplicabile. Vor fi suportate cel puțin formate precum

RDF/XML și JSON-LD, precum și alte serializări RDF deschise, dacă sunt necesare pentru integrările prevăzute în cadrul contractului.

Pentru operațiunile de import, export și editare în masă, soluția va utiliza mecanisme de procesare asincronă a sarcinilor (working queues) care vor permite executarea în fundal a operațiunilor fără a afecta performanța generală a aplicației. Utilizatorii vor fi notificați la finalizarea fiecărei operațiuni și va păstra un jurnal detaliat al execuțiilor, incluzând durata, statusul și eventualele erori.

În cadrul contractului Prestatorul va importa toate resursele culturale, cu toate metadatele aferente și fișierele de tip imagine, media, 3D, etc. din SIPCI, Culturalia, DocPat, eGISpat, RAN, Acera, clasate.cimec.ro etc..

6.2.7. Cerințe privind interfața de căutare

Sistemul digital va dispune de o interfață de căutare care va include o secțiune cu instrucțiuni de utilizare privind căutarea.

Interfața de căutare va permite realizarea de căutări de tip text, prin care se vor găsi și afișa sub formă de listă și concomitent pe hartă, în același ecran, toate resursele care conțin textul respectiv în orice ramură din compunerea instanțelor de resurse.

6.2.7.1 Căutare și analiză distribuită

Pentru a asigura o căutare eficientă, scalabilă și configurabilă a datelor din Componenta MPC gestionate prin instanțele de resurse, sistemul va include un motor de căutare și analiză distribuită care permite indexarea, stocarea și interogarea rapidă a datelor structurate, semi-structurate și nestructurate. Sistemul va asigura indexarea datelor aferente instanțelor de resurse și va permite interogarea avansată prin căutare fațetată (Faceted Search), oferind funcționalități de filtrare, agregare și analiză a datelor pe categorii dinamice (ex. tip, perioadă, locație, material, instituție deținătoare, etc.), facilitând generarea de statistici, rapoarte și vizualizări geospațiale.

6.2.7.2 Motorul de căutare

Va cuprinde următoarele funcționalități:

- Va indexa datele stocate în baza de date relațională, sincronizându-le prin procese de tip worker, gestionate prin managementul sarcinilor la salvarea instanțelor sau la reindexare manuală, atunci când este necesar;
- Va permite căutări multilingve full-text și filtrări dinamice avansate pe volume mari de date, ceea ce este esențial pentru managementul patrimoniului cultural care include mii de instanțe de resurse (ex. clădiri, situri arheologice);
- Va indexa nodurile cu tipuri de date geospațiale, permițând afișarea straturilor de resurse pe hărți interactive;

- Va asigura realizarea de interogări avansate, inclusiv căutări pe mai multe câmpuri, agregări și filtrări configurabile;
- Va permite utilizatorilor să combine criterii (ex. „clădire gotică” + „secol XII”) și să vizualizeze rezultatele în timp real;
- Va include funcționalități de căutare fuzzy (toleranță la greșeli de tastare sau diferențe minore, de ex. Arad vs. Aradd)
- Va include caching inteligent pentru interogări recurente, reducând timpii de răspuns.
- Va indexa datele din blocurile de date în funcție de stările ciclului de viață (de exemplu: „draft”, „activă”, „retrasă”, etc.) și de permisiunile asociate (ex. „Fără acces”, „Vizualizare”, etc.). Acest lucru va permite afișarea doar a datelor autorizate pentru fiecare utilizator;
- Va asigura scalabilitatea pe orizontală, permițând gestionarea de baze mari de date fără a compromite performanța.
- Va distribui datele pe mai multe noduri de procesare asigurând continuitatea serviciului și reziliența la erori;
- Va fi utilizat inclusiv pentru validarea și indexarea datelor importate/exportate în bloc (ex. CSV, Excel), permițând editări masive și reindexare eficientă.

6.2.7.3 Statistici, căutări salvate și export

Componenta MPC va cuprinde următoarele funcționalități:

- va cuantifica numărul de vizualizări ale fiecărei resurse culturale în parte și numărul de accesări totale ale platformei (unice, țară, județ, etc). Lista completă a detaliilor legate de afișare date trafic/vizualizări va fi stabilită în perioada de analiză.
- va permite salvarea unei căutări și prezentarea acesteia ca o facilitate pentru utilizatori. Căutările salvate vor fi afișate ca opțiuni de căutare pe pagina principală de căutare.
- va permite stabilirea numărului maxim de resurse returnat în urma unei operațiuni de căutare, care pot fi exportate (CSV, JSON sau GeoJSON).
- va dispune de un instrument de vizualizare integrat în pagina de căutare, care grupează datele temporale ale resurselor (de exemplu, situri arheologice sau monumente) pe baza distribuției lor cronologice. Acesta va permite interogările temporale și afișarea rapidă a datelor pe nivele temporale (mileniul, secolul, deceniul etc.).
- va permite configurarea parametrilor de grupare a datelor pe număr de ani sau pe intervale de timp.

6.2.7.4 Operatori de căutare

Componenta MPC va pune la dispoziție cel puțin următorii operatori pentru căutare:

- **Căutare exactă:** prin plasarea termenului de căutare între ghilimele se vor returna doar valorile care se potrivesc complet, inclusiv majusculile și minusculele.
- **Căutare parțială:** reprezintă o căutare bazată pe prefix, prin care se vor identifica termeni care încep cu fiecare cuvânt din termenii de căutare, indiferent de ordinea lor, cu condiția ca fiecare cuvânt să aibă o potrivire. Nu este o căutare de tip „conține” (care ar include termenul oriunde în text). De exemplu, dacă termenul de căutare este „ca li”, aplicația va găsi „... carte liberă ...” sau „... librărie cu cărți ...”. Nu va găsi o valoare doar cu „carte” sau valoarea „lucrare” (unde „lucrare” se termină în „re” dar nu începe cu „ca”).
- **Căutare de frază:** reprezintă o căutare de tip frază completă, prin care se vor găsi doar cuvinte complete în ordinea exactă dată. De exemplu, dacă termenul de căutare este „castel medieval”, aplicația va găsi valoarea „Castelul Bran medieval”. Nu va găsi „... medieval în castel ...” sau „... castelul medieval nou ...”.
- **Căutare cu caractere speciale:** utilizatorul va furniza o frază de căutare exact așa cum o dorește. De exemplu, o căutare pentru „ca?t” va găsi valorile „cast” sau „cart”. Nu va găsi „Cărțile sunt în castel”, deoarece „castel” este înconjurat de alte cuvinte. Dacă este nevoie de o interogare de tip „conține”, trebuie puse asteriscuri la început și la sfârșit. Astfel, „ca?t” va găsi „Cărțile sunt în castel”.

6.2.7.5 Căutări avansate și dezambiguizare

Interfața sistemului va permite utilizatorilor să configureze căutări avansate care sunt aplicabile pe ramuri sau câmpuri specifice ale modelelor de resurse (ex. „Material”, „Autor”, „Epocă”), pentru a găsi instanțe de resurse.

De exemplu, pentru resursele care conțin atât ramura „Culoare”, cât și ramura „Material”, o căutare pentru „aur” în ramura „Material” va returna doar resursele cu materialul „aur”, nu și pe cele care au culoarea „aurie”.

Utilizatorii vor putea combina criterii multiple prin operatori logici (AND, OR, NOT) și vor putea aplica filtre și sortări (alfabetice, cronologice, tematice).

În cazul în care termenul căutat are mai multe semnificații, sistemul digital va furniza un link către o pagină de „dezambiguizare” unde utilizatorul poate selecta semnificația / domeniul dorită/dorit. Formularea pentru pagina de dezambiguizare va fi: „Pentru alte utilizări, consultați [termen căutat], [domeniu] (dezambiguizare).”

Interfața va oferi sugestii de completare automată (auto-complete) pe baza celor mai frecvente termeni și a vocabulelor controlate.

Rezultatele vor putea fi filtrate, sortate și exportate în funcție de criteriile selectate.

Sistemul va asigura performanța și scalabilitatea căutării pentru volume mari de date, oferind rezultate în timp real și integrare cu motorul de analiză distribuită descris în secțiunile anterioare.

6.2.7.6 Caracteristici ortografice

Sistemul digital va avea implementate caracteristicile ortografice specifice limbii române actuale. Astfel, la tratarea cuvintelor cheie din interogări / căutări, sistemul va trebui:

- să echivaleze automat literele „ș” și „ț” codate conform standardului românesc SR 13411/1999 (i.e. cu virguliță dedesubt) cu cele nestandard (dar încă foarte răspândite, datorită folosirii pachetelor de litere nestandard), i.e. „s” și „t” (i.e. cu sedilă dedesubt);
- să echivaleze cuvintele scrise (conform ortografiei vechi) cu „î” din „i”, cu cele scrise (conform ortografiei curente) cu „â” din „a” (e.g. „cuvînt” cu „cuvânt”);
- să ofere utilizatorului sugestii și în cazul în care cuvântul-cheie folosit este scris fără diacritice, mai ales de către utilizatori din afara României (e.g. pentru interogarea cu „Romania” să sugereze și rezultate pentru „România”, sau la interogarea cu „Brancusi” să sugereze și rezultate pentru „Brâncuși”).

6.2.8 Cerințe privind instrumentul de afișare și filtrare dinamică a datelor

Sistemul digital va oferi, pentru toate paginile și interfețele în care utilizatorii pot vizualiza sau explora date, un instrument unitar de afișare și filtrare sub formă de tabel dinamic personalizabil. Acesta va permite selectarea, rearanjarea, adăugarea și ascunderea coloanelor, aplicarea de filtre multiple (text, numeric, interval temporal, vocabular controlat etc.) și ordonarea datelor după criterii definite de utilizator.

Tabelul dinamic va fi complet integrat cu motorul de căutare și cu mecanismele de filtrare existente, oferind actualizarea în timp real a datelor afișate și posibilitatea de a salva configurațiile utilizatorului (seturi de coloane, filtre, mod de afișare). Interfața va asigura utilizare intuitivă, inclusiv pe dispozitive mobile, și va respecta cerințele de accesibilitate WCAG.

Utilizatorii vor putea exporta datele afișate în forma personalizată curentă, în funcție de tipul de date, în formate standardizate precum CSV, XLSX, JSON, GeoJSON sau altele aplicabile. Exportul va respecta permisiunile și rolurile utilizatorilor, fiind disponibil doar pentru datele la care aceștia au acces. Modulul va fi reutilizabil pentru toate componentele de explorare (management patrimoniu cultural, e-guvernare, rapoarte, analize), pentru a asigura consistență și întreținere facilă.

6.2.9 Cerințe privind vizualizarea imaginilor, materialelor audio-video și a obiectelor 3D

Sistemul digital trebuie să ofere posibilitatea de vizualizare a imaginilor, obiectelor 3D și a materialelor audio-video aferente resurselor culturale.

6.2.9.1 Imagini și documente digitale

Pentru a afișa obiectele digitale se va folosi standardul IIIF [International Image Interoperability Framework - <https://iiif.io/>], asigurându-se compatibilitate cu IIIF Image API și IIIF Presentation API (versiunea 3.0 sau ulterioară) .

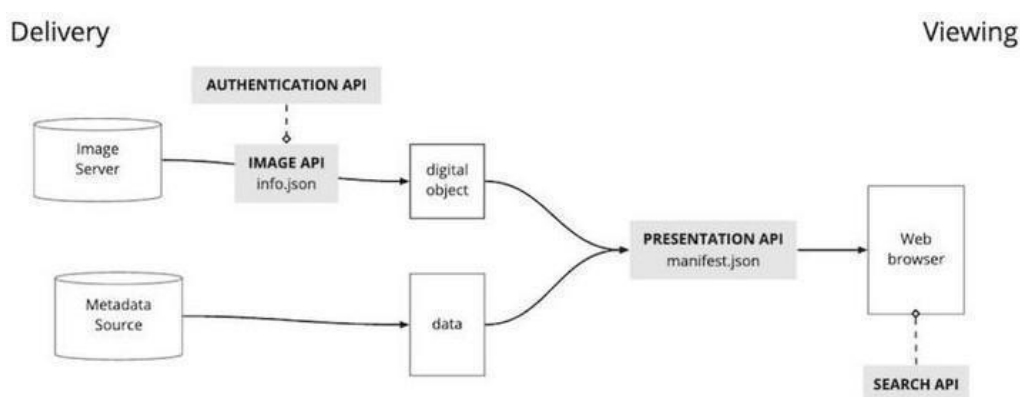


Figura 4 - Diagrama ce ilustrează cum API-urile de bază ale IIIF lucrează împreună
Acesta implică cel puțin:

- materiale de înaltă calitate și metadata despre structură;
- imaginile și materiale audio / video servite folosind un „Image API” și un server de imagini IIIF;
- imaginile și datele structurale combinate într-un Manifest IIIF folosind „Presentation API”;
- un vizualizator (viewer) va afișa obiectele în browser-ul web.

Vizualizatorul compatibil IIIF va fi instalat și integrat local astfel încât să nu existe dependențe față de terțe părți.

Vizualizatorul IIIF integrat în platformă va permite:

- zoom, panoramare, rotație și comparare de imagini;
- navigare în documente multi-pagină (ex. manuscrise, volume scanate);
- afișarea metadatelor asociate (titlu, descriere, autor, sursă, drepturi).

Documentele digitale (de ex. o carte în format .pdf) vor putea fi descărcat integral (dacă administratorul dă această permisiune), dar și vizualizate filă cu filă, direct în pagină,

prin încorporare (embed), iar utilizatorul va avea posibilitatea de a căuta în textul fișierelor.

6.2.9.2 Obiecte 3D

Platforma va permite afișarea obiectelor 3D printr-un vizualizator web instalat local (de tip Online3DViewer¹ sau Google Model Viewer² sau echivalent compatibil cu standardele WebGL / glTF 2.0).

Vizualizatorul 3D va oferi funcționalități de rotire 360°, mărire / micșorare și navigare liberă pe toate axele.

Soluția va suporta cel puțin următoarele formate de fișiere 3D: .3dm, .3ds, .3mf, .amf, .bim, .brep, .dae, .fbx, .fcstd, .gltf, .ifc, .iges, .step, .stl, .obj, .off, .ply, .wrl, lista completă urmând a fi stabilită în faza de analiză și în faza de dezvoltare.

Afișarea obiectelor 3D se va putea face prin încorporare (iframe) în paginile platformei.

6.2.9.3 Realitate Augmentată (AR) și Realitate Virtuală (VR)

Prin implementarea acestor funcționalități, sistemul digital va oferi o modalitate inovatoare și accesibilă de valorificare digitală a patrimoniului cultural, permițând publicului larg să descopere și să exploreze obiecte de patrimoniu într-un mod interactiv, tridimensional și imersiv, contribuind la creșterea atractivității, a gradului de interacțiune și a nivelului de imersiune al utilizatorilor, indiferent de tipul de dispozitiv utilizat.

Obiectele 3D vor putea fi vizualizate în modul AR (Realitate Augmentată), atât pe dispozitive mobile cu Android, cât și cu iOS, direct din browser, fără a fi necesară instalarea unei aplicații suplimentare, ci doar folosind uneltele implicite puse la dispoziție de aceste sisteme de operare.

- o Pentru Android, obiectele 3D vor fi automat convertite în formatul glTF³ pentru a fi folosite de către „Scene Viewer-ul”⁴ echipamentului mobil compatibil;
- o Pentru iOS, obiectele 3D vor fi automat convertite în formatul USDZ⁵ pentru a fi folosite de către „AR Quick Look”⁶ de pe echipamentul mobil compatibil;

¹ <https://github.com/kovacsv/Online3DViewer>

² <https://github.com/google/model-viewer>

³ <https://en.wikipedia.org/wiki/GLTF>

⁴ <https://developers.google.com/ar/develop/scene-viewer>

⁵ https://en.wikipedia.org/wiki/Universal_Scene_Description

⁶ https://developer.apple.com/documentation/arkit/arkit_in_ios/previewing_a_model_with_ar_quick_look

Pentru dispozitivele sau browserele care nu dispun de suport AR nativ, sistemul va oferi automat o vizualizare 3D standard, interactivă, în care utilizatorul poate roti, mări sau examina obiectul 3D direct pe ecran.

Obiectele 3D vor putea fi vizualizate în modul VR (Realitate Virtuală), compatibil cu căști de realitate virtuală (WebXR). Experiența VR va fi disponibilă tot direct din browser și va permite utilizatorului să se deplaseze sau să interacționeze cu obiectele 3D într-un mod natural, prin mișcarea capului sau folosind controlerele specifice echipamentului. Sistemul va asigura o redare fluentă, cu o rată de cadre adecvată pentru o experiență confortabilă vizual (minimum 30 Frames Per Second-FPS), acesta fiind optimizat pentru performanță, folosind modele 3D de dimensiuni reduse, cu texturi comprimate și încărcare progresivă (lazy loading), pentru a asigura timpi scurți de încărcare și o funcționare fluidă pe orice dispozitiv.

Funcționalitățile de vizualizare AR/VR vor fi integrate nativ în sistemul digital ePatrimoniu, astfel încât administratorii sau utilizatorii autorizați să poată adăuga, configura și gestiona modele 3D prin interfețele de administrare ale sistemului, fără cunoștințe tehnice avansate. Fiecare model va putea fi însoțit de metadate descriptive (de exemplu nume, autor, descriere, dimensiuni etc.), iar sistemul va genera automat identificatori sau linkuri unice de acces și partajare pentru vizualizarea 3D, AR și/sau VR, în funcție de drepturile de acces și politicile de publicare aplicabile.

Obiectele 3D vor include ancure informative interactive – puncte de interes vizuale („hotspots”) amplasate strategic pe suprafața modelului –, care vor oferi utilizatorului posibilitatea de a accesa informații suplimentare despre contextul istoric, artistic sau tehnic al obiectului. La selectarea unei ancure, se vor putea afișa texte explicative, imagini de arhivă, fișiere audio sau materiale video, contribuind la o înțelegere mai profundă și atractivă a patrimoniului digitalizat.

6.2.9.4 Coduri QR

Sistemul digital ePatrimoniu va permite generarea, asocierea și tipărirea de coduri QR pentru identificarea unică a resurselor culturale.

Fiecare cod QR va fi asociat dinamic unei resurse și va conduce, prin scanare, către pagina dedicată obiectului respectiv din sistemul digital ePatrimoniu.

Codurile QR vor fi generate în conformitate cu standardele internaționale de calitate a imaginii (ISO/IEC 18004), având o rezoluție minimă recomandată de 300 dpi pentru imprimare și un contrast optim între fundal și modelul codului.

Se va urmări asigurarea unei lizibilități ridicate la scanare, atât cu dispozitive mobile, cât și cu cititoare dedicate, inclusiv în condiții de uzură fizică, praf, variații de iluminare sau expunere la intemperii. În acest sens, formatul grafic al codului (dimensiuni, margini, culori) va fi adaptat cerințelor de lizibilitate și mediului de utilizare.

Înainte de implementarea finală, codurile QR vor fi supuse unei proceduri de testare pentru verificarea lizibilității și acurateții redirectionării către resursele digitale aferente.

6.2.9.5 Cerințe tehnice suplimentare

Vizualizatoarele integrate vor funcționa pe toate platformele majore (desktop, tabletă, mobil) și în browsere moderne compatibile HTML5.

Sistemul digital va asigura performanța și scalabilitatea redării fișierelor media, inclusiv streaming adaptiv pentru conținut video și cache local pentru imagini de înaltă rezoluție.

Sistemul va permite gestionarea metadatelor tehnice și descriptive pentru toate fișierele media (ex. EXIF, IPTC, Dublin Core).

6.2.9.6 Stocare fișiere

Sistemul digital trebuie să permită stocarea unei varietăți de formate de fișier: de exemplu fișier-text, fișiere-imagine, fișiere-audio și fișiere-video, fișiere-3D etc.

Acesta va utiliza ca standarde pentru setul caracterelor (stocarea datelor) UTF-8/UTF-16.

Sistemul va stoca fișierele media digitale (imagini, videoclipuri, documente, modele 3D etc.) asociate instanțelor de resurse, într-un sistem de fișiere, nu în baza de date relațională.

Sistemul trebuie să permită stocarea fișierelor media digitale (imagini, videoclipuri, documente, modele 3D etc.) asociate instanțelor de resurse, direct pe echipamente de stocare de tip object care permit accesul nativ prin protocol S3, fără a necesita infrastructură suplimentară.

6.2.10 Cerințe privind submodulul GIS și gestionarea datelor geospațiale

6.2.10.1 Cerințe generale

Submodulul GIS din cadrul sistemului digital ePatrimoniu va include:

- (a) o componentă server (bază de date spațială și servicii geospațiale),
- (b) o interfață WebGIS pentru vizualizare și interacțiune (desktop și mobil)
- (c) o aplicație mobilă pentru colectare de date în teren. Analizele și operațiile geospațiale cu impact asupra integrității datelor (ex. intersecări, buffer, reguli de topologie, raportări) se vor executa pe server; interfața WebGIS va realiza redarea, filtrarea și comenzi către server.

Submodulul va suporta sistemul de proiecție național Stereo 1970 și WGS 84 (World Geodetic System 1984) și va asigura interoperabilitatea cu serviciile de hărți (WMS / WFS) furnizate de ANCPI, astfel încât să asigure amplasarea exactă a geometriilor și a coordonatelor geografice, specifice elementelor de patrimoniu imobil (monumente istorice), a siturilor arheologice și a zonelor de protecție, etc.. Pentru resursele fără localizare unică (ex. patrimoniu mobil și imaterial), submodulul va permite asocierea unor repere spațiale (punct / linie / poligon) relevante (ex. loc de păstrare, loc de descoperire, areal de practică, etc.), cu indicarea tipului de localizare și a gradului de precizie. De asemenea va fi asigurată și reproiectarea datelor din cele 2 sisteme de proiecție în timp real (on the fly).

Submodulul va permite afișarea utilizatorilor autorizați suprapunerea straturilor de date cadastrale cu precizia furnizată de serviciile ANCPI, prin transformări de coordonate gestionate la nivel server și fără a introduce erori de reproiecție mai mari de 10 cm⁷, pentru a face posibilă acordarea / gestionarea de avize pe baza suprapunerii exacte a informațiilor spațiale cu hărțile cadastrale ale ANCPI.

Submodulul va permite utilizatorilor autorizați suprapunerea și interogarea pe hartă a straturilor de risc seismic furnizate de Institutul Național pentru Fizica Pământului (INFP) și a Hărților de Hazard și de Risc la Inundații (HHRI), prin consum de servicii geospațiale publicate de instituțiile sursă (preferabil OGC WMS / WMTS / WFS sau OGC API). Pe baza acestor straturi, submodulul va permite marcarea distinctă a resurselor afectate și generarea de rapoarte, iar în cazul în care serviciile nu sunt disponibile sau nu oferă nivelul necesar de detaliu, submodulul va permite, opțional, importul și actualizarea periodică a data-seturilor furnizate, cu mecanisme de versionare și audit.

Submodulul va permite utilizatorilor autorizați definirea și administrarea unor trasee/itinerarii tematice (linie + puncte de interes) pentru scopuri de inventariere, interpretare și prezentare, inclusiv asocierea acestora cu resursele din MPC. Integrarea cu platforme externe cu rol similar (ex.: Via Transilvanica, România Atractivă) se va realiza prin import/consum de date în formate standard și va fi tratată ca funcționalitate opțională, detaliată în faza de analiză. Datele vor cuprinde informații legate de patrimoniul cultural, conform legislației în vigoare.

Submodulul va integra rutele turistice / istorice (GeoJSON LineString), segmentate pentru mentenanță, și un inventar de POI (GeoJSON Point) cu tipuri controlate: patrimoniu imobil/patrimoniu mobil/arheologic / tehnic-industrial / imaterial și servicii (parcare, cazare, alimentare). Gestionarea, validarea și versionarea acestor date se vor realiza la nivelul serverului GIS, care va aplica reguli de schemă, constrângeri de integritate și validări topologice. Fiecare POI va include metadata: cod oficial LMI/RAN

⁷ Toleranța admisă la determinarea punctelor de contur pentru imobile împrejmuite conform normelor ANCPI - Regulament din 13 octombrie 2006 privind conținutul și modul de întocmire a documentațiilor cadastrale în vederea înscrierii în cartea funciară, Cap. 2 Art. 7, (2):
<https://legislatie.just.ro/Public/DetaliiDocumentAfis/78307>

unde există, descriere, accesibilitate, licență, sursă, data ultimei actualizări etc., aceste informații fiind administrate și auditate la nivel backend.

Regulile de generalizare / deplasare vor fi configurabile și aplicate diferențiat pe roluri și canale de publicare (interfață publică vs. dashboard intern), cu păstrarea coordonatelor exacte în mediul securizat. Aplicarea acestor reguli va fi auditabilă (autor, dată, regulă aplicată).

Interfața WebGIS (desktop și mobil) va avea rol de vizualizare și interacțiune în cadrul dashboard-ului intern, oferind hărți interactive cu funcționalități de filtrare, clustering, afișare profil de elevație, estimare a timpului de parcurgere și export în formate standard (GPX, KML, GeoJSON). Procesele de analiză spațială cu relevanță administrativă sau juridică vor fi executate la nivel server, iar interfața client va consuma rezultatele acestora prin servicii securizate. Suportul offline în interfața web va fi implementat prin mecanisme de tip PWA, cu stocare locală temporară a datelor publicate și utilizare limitată în absența conexiunii la internet, fără a substitui procesarea oficială realizată pe server, iar colectarea și editarea în teren (captare geometrii / atribute și sincronizare) se va realiza prin aplicația mobilă nativă descrisă la secțiunea 6.2.10.5.

6.2.10.2 Hărți de bază

Submodulul va fi livrat cu cel puțin un set de hărți/straturi de bază furnizate de servicii cartografice precum Google Maps Platform, OpenStreetMap, Microsoft Bing Maps, Esri, Mapbox, MapTiler sau echivalente și le va afișa în interfața web (desktop și mobil) utilizând biblioteci JavaScript dedicate (ex. MapLibre GL JS, Leaflet sau echivalente). Alegerea serviciilor cartografice va respecta condițiile de licențiere și de utilizare aplicabile fiecărui furnizor.

Serviciile vor furniza cel puțin următoarele tipuri de hartă de bază:

- strat de imagini satelitare / ortoimagini;
- strat cartografic rutier/urban (drumuri, clădiri, etichete, puncte de interes);;
- strat cartografic topografic (accent pe relief/altitudine)

Submodulul va permite utilizatorilor autorizați adăugarea de alte hărți de bază, precum ortofotoplanuri, ortomozaicuri, hărți topografice, hărți cadastrale, planuri de parcelare, hărți administrative, modele digitale (DEM / DTM / DSM), rețele rutiere sau hidrografice generalizate.

Submodulul va suporta configurarea și administrarea resurselor asociate hărților, inclusiv chei API, tokenuri de acces, stiluri cartografice, colecții de pictograme și fonturi utilizate pentru etichete. În cazul serviciilor externe care necesită autentificare, chei API, tokenuri, subscripții sau mecanisme de billing, soluția va permite gestionarea securizată a acestora, cu măsuri de limitare a expunerii (de ex. proxy la nivel server, restricții de domeniu, restricții de utilizare, rotația cheilor), pentru a reduce riscul de

acces neautorizat. Ofertantul va descrie în propunerea tehnică și financiară modul de asigurare a acestor servicii și eventualele costuri recurente asociate.

Resursele grafice ale hărților (pictograme, fonturi) vor fi administrate centralizat și utilizate în frontend doar pentru randare vizuală.

Pentru îmbunătățirea performanței, submodulul va suporta, la nivel server, generalizarea și agregarea vizuală a rezultatelor (ex. clustering, grid/heatmap sau simplificarea geometriei la niveluri mici de zoom), inclusiv prin livrare optimizată de tip vector tiles, reducând volumul de date livrat către client. Parametrii acestor mecanisme (ex. praguri de zoom, dimensiunea grilei, toleranța de simplificare) vor fi configurabili.

6.2.10.3 Afișarea datelor geospațiale și zone de protecție

Submodulul va genera automat straturi tematice de resurse (Resource Layers⁸) pentru afișarea pe hărți interactive a datelor geospațiale asociate instanțelor (ex. clădiri, situri, alte entități) și a zonelor relevante de reglementare / protecție.

Submodulul va permite utilizatorilor autorizați definirea, editarea și administrarea unor zone de protecție / reglementare sub formă de poligoane geospațiale, inclusiv suprapunerea mai multor poligoane asociabile aceleiași resurse (element de patrimoniu) sau aceluiași teritoriu. Sistemul va asigura vizualizarea, evidențierea și interogarea acestor zone pe hartă, împreună cu metadatele aferente (ex. tip/regim, sursă, perioadă de valabilitate, nivel de încredere/precizie, referințe către resursele asociate, după caz).

La nevoie, submodulul va permite configurarea de reguli / șabloane de delimitare (de exemplu prin buffer față de limita resursei / terenului), conform normelor aplicabile și practicilor curente, precum și ajustarea manuală a limitelor de către utilizatori autorizați.

6.2.10.4 Configurarea straturilor de resurse, interoperabilitate și importul datelor spațiale

Submodulul va permite personalizarea straturilor de resurse, inclusiv:

- definirea aspectului marcatorilor (culoare, simboluri);
- clusterizare parametrizabilă pentru zoom scăzut (distanța de agregare, prag de zoom, număr minim de entități). Pentru randare eficientă la volume ridicate, se vor utiliza vector tiles.

Submodulul trebuie să suporte importul datelor spațiale din diverse surse și formate (vector și raster), precum: Shapefile (.shp), GeoPackage (.gpkg), GeoParquet

⁸ Prin Resource Layers se înțeleg straturi tematice generate pe baza tipurilor/modelelor de resurse din MPC și a regulilor configurabile de simbolizare, filtrare, niveluri de zoom și permisiuni.

(.parquet) GeoTIFF (.tif), tabele textuale cu coordonate (.csv), fișiere Google Earth (.kml/.kmz), fișiere GPS (.gpx), GeoJSON (.geojson), xlsx etc.

Submodulul va permite utilizatorilor avansați adăugarea de straturi suplimentare (overlays) din fișiere și servicii web de hartă terțe. Utilizatorii vor putea activa simultan oricâte straturi doresc și vor putea modifica transparența acestora. De asemenea, submodulul va permite salvarea straturilor configurate și, opțional, publicarea acestora pentru reutilizare de către alți utilizatori ai platformei (ex. la nivel de instituție sau la nivel național), printr-un mecanism de moderare/aprobare realizat de utilizatori autorizați, cu păstrarea trasabilității (autor, dată, descriere).

Submodulul va suporta publicarea și consumul de servicii cartografice conforme OGC⁹: WMS / WMTS¹⁰, WFS¹¹ / OGC API – Features, OGC API – Tiles, pentru interoperabilitate cu sisteme terțe (INFP, HHRI etc.) și pentru integrare în alte aplicații.

Submodulul va oferi instrumente de analiză (executate pe server): buffer, intersect, nearest neighbour, filtrare spațială/atribut și șabloane predefinite pentru evaluări de risc (seism/inundații).

Pentru utilizatorii autorizați și doar pentru datele geospațiale în cadrul platformei, submodulul va include editor de geometrii cu reguli de topologie, audit și versionare, cu posibilitatea revenirii la versiuni anterioare.

Accesul la straturi și la elementele geospațiale asociate resurselor va fi controlat prin mecanismele standard de autentificare, roluri și drepturi ale platformei (utilizatori / grupuri / roluri), aplicabile atât la nivel de strat, cât și, unde este necesar, la nivel de instanță. Submodulul va jurnaliza accesul și operațiile efectuate asupra datelor geospațiale, în conformitate cu cerințele generale de audit.

6.2.10.5 Aplicație mobilă

Submodulul va integra o aplicație mobilă (Android, iOS) atașată modulului GIS, cu rol principal de colectare de date în teren: captarea de geometrii punct/linie/poligon, completarea de atribute și transmiterea (sincronizarea) către baza de date a modulului GIS. Aplicația va colecta coordonatele în WGS84, iar submodulul va asigura transformarea controlată și stocarea în sistemul de referință utilizat de platformă (inclusiv Stereo 1970) la nivel server, cu păstrarea metadatelor de precizie. De asemenea, aplicația va suporta lucrul offline cu sincronizare ulterioară, atunci când conectivitatea este disponibilă.

⁹ Open Geospatial Consortium: [Advancing Geospatial Standards and Technology | OGC](#)

¹⁰ Web Map Service/Web Map Tile Service

¹¹ Web Feature Service

6.2.11 Cerințe privind funcționalitățile de prezentare și valorificare atractivă a resurselor culturale digitale

Sistemul digital ePatrimoniu va cuprinde cel puțin de următoarele funcționalități pentru integrarea de narațiuni digitale (storytelling) și narațiuni prin derulare (scrollytelling):

- va permite afișarea textului în ordine secvențială, declanșată de acțiunile utilizatorului (ex. derulare sau click), pentru a povesti istoria unei resurse (ex. „Biserica Stavropoleos”). Textul trebuie să fie configurabil prin interfața de administrare;
- va suporta animarea treptată a elementelor (ex. imagini, titluri) care apar sau dispar la derulare, sincronizată cu poziția cursorului utilizatorului, pentru a evidenția aspecte cheie ale patrimoniului (ex. detalii arhitecturale ale „Bisericii Stavropoleos”);
- va include un efect de parallax scrolling, unde fundalul (ex. o fotografie a „Palatului Parlamentului”) se deplasează mai lent decât elementele din prim-plan (ex. text descriptiv), oferind o experiență vizuală captivantă;
- va permite definirea secțiunilor fixe care rămân vizibile pe ecran pe măsură ce utilizatorul derulează (ex. o hartă interactivă a „Castelului Bran”), cu tranziții controlate între secțiuni;
- va oferi o cronologie interactivă care se actualizează, afișând evenimente asociate resurselor (ex. construcția „Palatului Parlamentului” în 1984-1990), cu marcaje temporale ajustabile;
- va integra hărți interactive bazate pe datele geospațiale ale instanțelor de resurse, permițând zoom, pan și afișarea straturilor de resurse;
- va permite crearea de expoziții virtuale tematice (ex. „Arhitectura gotică”), utilizând instanțe de resurse și relații personalizate pentru a structura narațiunile;
- va suporta tururi virtuale navigabile, integrate cu datele 3D și geospațiale ale resurselor (ex. un tur al „Bisericii Stavropoleos”), utilizând fișiere media;
- va include infografice animate (ex. evoluția „Palatului Parlamentului” în timp), sincronizate cu textul narativ, configurabile prin interfața;
- va integra secțiuni cu imagini, galerii foto, fișiere video și audio asociate resurselor (ex. un videoclip despre restaurarea „Catedralei Notre-Dame”), accesibile prin noduri file-list;
- va permite utilizarea unui video pe fundal (ex. un tur video al „Castelului Bran”), cu control frame-by-frame sincronizat cu derularea, implementat prin JavaScript personalizat;
- va suporta experiențe 3D interactive (ex. un model 3D al „Bisericii Stavropoleos”), activate la derulare, utilizând fișiere media 3D încărcate în aplicație;

- va afișa un indicator de progres (ex. o bară procentuală) care se actualizează pe măsură ce utilizatorul derulează narațiunea (ex. turul virtual al „Palatului Parlamentului”);

Toate implementările de storytelling trebuie să fie optimizate pentru performanță (ex. încărcare lentă imaginilor), accesibilitate (ex. compatibilitate WCAG AA) și compatibilitate cross-device (responsive design), testate pe dispozitive mobile și desktop.

Autoritatea Contractantă, prin designerul propriu de interfață (ex. un specialist intern sau Prestator extern), poate transmite propuneri concrete, în format web, de astfel de componente UI. Codul sursă ce vizează exclusiv interfața web (fișiere HTML, CSS și JavaScript) va fi furnizat Prestatorului, în vederea utilizării ca sursă de referință și pentru integrarea în sistem.

Sistemul digital va dispune cel puțin de următoarele funcționalități interactive pentru utilizatori:

- va permite utilizatorilor autentificați să creeze colecții personalizate (ex. „Favorite”, „Liste de vizitare”, „Recomandări”), salvate ca instanțe de resurse, accesibile doar utilizatorului care le-a creat. De asemenea, utilizatorii autorizați (care dețin roluri și drepturi de publicare / administrare) vor putea crea și gestiona colecții destinate vizitatorilor platformei, disponibile în interfața publică a sistemului digital;
- va include quiz-uri și jocuri educaționale (ex. un quiz despre „Biserica Stavropoleos”), implementate ca module interactive, configurabile prin secțiuni de formular;
- va oferi un sistem de comentarii, recenzii sau aprecieri (ex. „Îmi place” pentru „Biserica Stavropoleos”), moderate de către un utilizator autorizat;
- va permite partajarea resurselor (ex. „Castelul Bran”) pe rețele sociale (Facebook, Twitter) prin link-uri generate din interfața, cu opțiuni de personalizare a mesajului

Sistemul digital trebuie să ofere un grad ridicat de configurabilitate la nivel de interfață și funcționalități pentru utilizatorii care creează conținut, permițând adaptarea narativelor digitale (ex. scrollytelling, hărți interactive) și a funcționalităților interactive (ex. colecții, quiz-uri) prin configurarea secțiunilor de formular, grafurilor și API-urilor.

Prestatorul va configura în perioada contractuală pentru fiecare funcționalitate de mai sus minim 2 exemple operaționale.

Sistemul digital trebuie să ofere posibilitatea ca utilizatorii să creeze, prin interogări specifice dedicate, galerii/expoziții cu material specific unei anumite comunități etnice, unui autor, perioade etc. Rezultatele acestor interogări specifice să poată fi publicate pe în interfața publică pentru a putea fi consultate de către orice utilizator interesat.

Prestatorul va configura pentru fiecare domeniu stabilit în perioada de analiză minim 2 galerii/expoziții cu material specific unei anumite comunități etnice, unui autor, perioade etc., material furnizat de Autoritatea Contractantă. Rezultatele acestor galerii/expoziții - interogări specifice - vor fi disponibile publicului.

6.2.12 Cerințe privind analiza datelor / dovezilor referitoare la patrimoniul cultural (existente în baza de date) și generarea de statistici și rapoarte în funcție de diverse criterii

Sistemul digital trebuie să cuprindă interogări complexe, în funcție de mai multe criterii selectate de utilizatori, în acord cu rolurile și permisiunile de acces ale acestora, ale informațiilor din Componenta MPC în vederea generării de date cu relevanță statistică, necesare pentru fundamentarea strategiilor și politicilor în domeniul cultural. Sunt necesare procese de cercetarea și analiză, monitorizare și cartografiere a zonelor de risc, planificare pentru investigare, cercetare, conservare / restaurare, finanțare etc.

Sistemul trebuie să cuprindă generarea de rapoarte automate printr-un modul de raportare unde se pot prescrie caracteristici personalizate ale raportului și se pot genera rapoarte (indicatori, algoritmi, formate de raport) în funcție de categoriile de utilizatori și de privilegiile utilizatorului. Lista cu tipurile de rapoarte va fi determinată în faza de analiză, în faza de dezvoltare, migrare și testare și după faza de punere în producție a primei versiuni.

6.2.13 Generare automată a descrierilor pentru resurse

Sistemul digital va integra un modul de generare a descrierilor pentru resurse, disponibil atât din interfața de editare (roluri interne), cât și din interfața de explorare (public). În interfața de editare, utilizatorul autorizat poate lansa generarea unui text pe baza metadatelor resursei și a relațiilor din ontologie; textul este afișat ca propunere editabilă și poate fi revizuit / acceptat înainte de salvare. În interfața de explorare, utilizatorii vor avea un buton de tip „Află mai multe”, care generează la cerere o descriere scurtă, lizibilă (fără a o salva), adaptabilă limbii, nivelului de detaliu și complexitate selectat (ex. mai generică, prietenoasă pentru publicul general, mai tehnică pentru specialiști).

Modulul va fi capabil să producă texte constrânse la datele existente (titlu, tip, perioadă, material, localizare etc.), vocabularele controlate și relațiile din ontologie.

6.2.14 Cerințe privind integrarea componentei e-Guvernare cu componenta MPC

Componenta MPC trebuie să asigure legătura și accesul direct la documente (de exemplu, PDF-uri, imagini sau alte formate) încărcate în cadrul fluxurilor din Componenta e-Guvernare, astfel încât să se poată urmări istoricul și proveniența acestora, precum și asigurarea că documentele sunt legate de resursele culturale

relevante¹² și, eventual, de alte entități (cum ar fi procese de avizare sau actori implicați), pentru a permite urmărirea relațiilor și a stării lor în timp.

În acest sens, se va realiza configurarea unui Model de Resurse care să permită stocarea și gestionarea acestor documente, împreună cu metadatele asociate, utilizând funcționalitățile soluției pentru gestionarea fișierelor și a relațiilor dintre resurse, în cadrul ontologiei CIDOC CRM.

În acest sens se vor utiliza funcționalitățile solicitate astfel:

- Tipul de date file-list: Permite încărcarea unuia sau mai multor fișiere (cum ar fi documente PDF sau imagini).
- Noduri și secțiuni de formular: Pentru a configura interfața de încărcare a documentelor.
- Relații resursă-la-resursă: Pentru a conecta documentele la clădiri sau alte entități.
- Cicluri de viață: Pentru a gestiona starea documentelor (de exemplu, draft, activă, retrasă).

Sistemul digital trebuie să asigure specificarea formatelor acceptate (de exemplu, `.pdf`, `.jpg`, `.docx`) și dimensiunea maximă a fișierelor, dacă este cazul.

Sistemul va permite modelarea documentelor ca instanțe de resurse distincte, cu metadate, cicluri de viață, permisiuni și relații proprii, iar fișierele aferente acestora vor fi gestionate ca fișiere asociate resursei.

Sistemul digital trebuie să asigure spre exemplu conectarea instanțelor de „Documente de avizare” la instanțele de „Clădiri” prin relații resursă-la-resursă. Se va crea o secțiune de formular „Documente de avizare” pentru grupul de noduri care include nodul „Documente de avizare”. Se va crea un widget de tip „file-upload” pentru nodul „Documente de avizare”, care permite utilizatorilor să încarce fișiere prin interfața. Se vor configura metadate suplimentare, cum ar fi:

- „Titlu document” (tip „string”).
- „Data emiterii” (tip „date”).
- „Tip document” (tip „Custom field values-list” valori: „Autorizație”, „Raport inspecție”, „Plan restaurare”).
- Se vor configura stări ale ciclului de viață pentru instanțele de resurse (atât „Clădiri”, cât și „Documente de avizare”), astfel:
- „Draft”: Documentele sunt încărcate și în curs de verificare.
- „Activă”: Documentele sunt validate și disponibile pentru acces public.

¹² cu metadate (cum ar fi titlul, data emiterii) și gestionate conform ciclurilor de viață (draft, activ, retras).

- „Retrasă”: Documentele nu mai sunt relevante (de exemplu, o autorizație expirată).

Se vor adăuga funcții personalizate (dacă este cazul) pentru a înregistra data tranziției între stări sau pentru a notifica utilizatorii implicați (de exemplu, angajați ai compartimentelor funcționale competente pentru avizare).

Se vor configura metadate pentru trasabilitate pentru a înregistra informații precum:

- „Autor emitent” (tip „string” sau „resource-instance” pentru a lega un actor).
- „Număr autorizație” (tip „string”).
- „Data modificării” (tip „date”).

Se vor configura permisiuni la nivelul secțiunilor de formular pentru a restricționa accesul la documente sensibile (de exemplu, „Fără acces” pentru public).

Pentru a asigura transmiterea automată a documentelor (cum ar fi documentele de avizare pentru lucrări asupra clădirilor) între componenta e-Guvernare (în care se realizează încărcarea/emiterea aceste documente) și componenta MPC, se va realiza o integrare la nivel API. Această abordare va permite transferul de date și fișiere între cele două componente în mod programatic, utilizând interfețe de programare a aplicațiilor (API).

Integrarea va respecta cerințele de securitate (autentificare, SSL) și ontologia CIDOC CRM.

Pentru realizarea integrării, API-ul componentei de e-Guvernare ePatrimoniu trebuie să permită exportul documentelor (ca fișiere sau URL-uri) și al metadatelor asociate (titlu, dată, ID clădire, etc.), asigurând:

- Suport pentru formate comune, cum ar fi JSON pentru metadate și fișiere (PDF, JPG).
- Autentificare securizată (de exemplu, OAuth 2.0 sau chei API).

Componenta MPC va fi prevăzută cu un API pentru gestionarea resurselor, inclusiv crearea de Resource Instances și încărcarea fișierelor.

Se va realiza o integrare „real-time” sau „bazată pe webhooks” pentru transfer automat fără intervenția operatorului, astfel:

- „Real-time”: Componenta e-Guvernare emitentă trimite documentele către Componenta MPC imediat ce sunt generate, folosind un endpoint API.
- „Webhooks”: Componenta e-Guvernare emitentă notifică Componenta MPC printr-un webhook atunci când un document este disponibil, declanșând transferul.

Finalizarea unui proces în modulul e-Guvernare va conduce, în funcție de tipul procesului și de actul administrativ rezultat, la actualizarea automată a bazei de date aferente modulului MPC, prin preluarea și înregistrarea informațiilor relevante rezultate

din procesul respectiv, în vederea populării anumitor nomenclatoare sau structuri de date, acolo unde acest lucru este aplicabil din punct de vedere funcțional.

Totodată, atribuirea codurilor și numerelor actelor generate în cadrul procesului se va realiza automat de către sistem, pe baza unor reguli de numerotare predefinite, menite să asigure unicitatea, coerența și trasabilitatea numerelor generate, în funcție de tipul actului și de contextul emiterii acestuia.

Alte integrări între componente vor fi definite în faza de analiză, în faza de dezvoltare, migrare și testare și după faza de punere în producție a primelor versiuni.

6.3 Componenta Gestiunea identității și accesul utilizatorilor (IAM) (componentă suport)

Sistemul digital ePatrimoniu va include o soluție de gestiune a identității utilizatorilor, asigurând administrarea centralizată a rolurilor și permisiunilor utilizatorilor, provizionarea identității și a conturilor de utilizator în sistemul digital.

Sistemul trebuie să ofere posibilitatea de a rula pe infrastructura pusă la dispoziție în cadrul proiectului. Componenta de management centralizat a identității utilizatorilor trebuie să îndeplinească următoarele cerințe funcționale:

- Stochează informații despre profilul utilizatorilor precum și conturile, permisiunile acestora în raport cu funcția pe care o au în cadrul instituției/organizației;
- Oferă o interfață unică de tip self-service pentru utilizatori prin care aceștia pot solicita conturi și permisiuni în sistemul digital;
- Oferă capabilități de monitorizare și auditare a accesului și identității utilizatorilor.

Sistemul va implementa un model de control al accesului bazat pe RBAC (Role-Based Access Control) – definirea drepturilor pe roluri preconfigurate și gestionate centralizat;

Pentru a crește eficiența operațiilor de administrare a utilizatorilor, componenta trebuie să includă mecanisme care să permită provizionarea simultană de conturi și drepturi de acces pentru mai mulți utilizatori. Rolurile și drepturile de acces în sistemul digital vor fi administrate prin interfața modulului de administrare din dashboard-ul intern, descris la subcapitolul 7.1.2.1, gestionat de către administratorul platformei.

Componenta trebuie să ofere posibilitatea de a defini politici asociate parolelor utilizatorilor în funcție de cerințele specifice de securitate ale componentelor și secțiunilor adresabile acestora, având criterii precum:

- Număr minim, maxim de caractere;
- Număr minim de caractere numerice, alfanumerice;
- Lista caractere obligatorii, permise sau interzise;
- Număr minim de caractere speciale;

- Posibilitatea de a interzice folosirea anumitor cuvinte în definirea parolei precum nume, prenume.

În acest sens, pentru toate tipurile de conturi, politicile de parolă vor respecta următoarele cerințe minime, definite în mod programatic:

- lungime minimă de 8 caractere;
- includerea de caractere speciale, numerice, majuscule și minuscule;
- expirare periodică configurabilă;
- interzicerea reutilizării parolelor anterioare;
- blocarea automată a contului după un număr configurabil de autentificări eșuate;
- parola nu poate fi similară sau să conțină id-ul utilizatorului;

Componenta trebuie să includă un framework pentru dezvoltarea de conectori specifici pentru integrarea cu modulul de administrare.

Soluția trebuie să includă un sistem centralizat de management a accesului la componentele sistemului și să ofere funcționalități de single sign-on, autentificare, autorizare, administrare centralizată, managementul agenților de autorizare și al politicilor de acces, management în timp real al sesiunilor de aplicații și audit. Pentru protecția împotriva atacurilor automate, mecanismele de securitate, precum CAPTCHA, trebuie să fie implementate într-un mod non-intruziv, fiind prezentate doar la nevoie, astfel încât să nu afecteze experiența utilizatorului.

Rolul acestui sistem este de creștere a securității prin politici globale de securitate și eliminarea riscurilor potențiale, prevenirea accesului neautorizat la sisteme și aplicații, simplificarea operațiilor de administrare.

Componenta de control acces va identifica utilizatorul la începutul sesiunii de lucru prin redirectarea către un ecran de autentificare. Ca și mecanisme de autentificare, soluția va suporta minim următoarele:

- utilizator și parola
- X.509 Digital certificates
- Federated tokens – SAML (Security Assertion Markup Language)
- Autentificare de tip multi-factor prin introducerea unui mecanism secundar de autentificare.

Acțiunile de autentificare efectuate de către utilizatori precum și activitățile administrative precum creare, modificare, vizualizare, ștergere scheme de autentificare, module și politici de acces vor trebui să fie auditate platforma colectând minim adresa IP, data acțiunii și ID login. Complementar, componenta va permite filtrarea autentificării și autorizării pe baza unor reguli avansate utilizând diverse criterii: adresa IP, dispozitivul folosit, tipul de browser folosit, interval orar.

Pentru managementul și monitorizarea sesiunilor deschise de către utilizatori, platforma trebuie să implementeze un mecanism de caching date sesiune utilizatori. Mecanismul de caching trebuie să asigure confidențialitatea datelor prin criptare automată, având și capabilități de failover automat și reconciliere. Sistemul de caching va conține, pe lângă datele de sesiune, și informații despre configurarea sistemului și politicile de acces la sistemele protejate. De asemenea, mecanismul de caching trebuie să asigure disponibilitate ridicată printr-o arhitectura de tip cluster activ-activ.

Stocarea configurațiilor și a politicilor de acces la resursele web trebuie să se realizeze în baza de date a sistemului, fără a exista necesitatea unui depozitar proprietar de date.

Soluția trebuie să suporte procesul de federalizare între furnizori de identitate utilizatori diferiți, facilitând schimbul de informații despre profilul utilizatorilor între furnizori diferiți. În acest sens, trebuie să suporte standardele SAML 1.1 și SAML 2.0, OPEN ID 2.0.

Componenta de federalizare a identității trebuie să suporte următoarele scenarii de implementare:

- distribuirea datelor de sesiune între domeniile de identitate fără să fie nevoie de trimiterea sau consumul informațiilor de identitate utilizatori;
- schimbul de informații despre profilul utilizatorilor și maparea informațiilor de profil între 2 furnizori de identitate;
- permite accesul la resursele protejate pe baza de politici de acces la nivel de atribute despre profilul utilizatorilor.

Nivelul de auditare trebuie să fie configurabil (succes, nereușita).

Soluția implementată va fi conformă cu standardele și bunele practici internaționale aplicabile în domeniul securității identității digitale și cu prevederile Regulamentului (UE) nr. 910/2014 (eIDAS) privind identificarea electronică și serviciile de încredere.

Soluția trebuie să asigure stocarea standardizată a profilelor de utilizatori.

Administrarea și editarea profilelor de utilizatori trebuie să se realizeze printr-o interfață web accesibilă doar administratorilor de sistem. Soluția oferă o flexibilitate maximă prin includerea unor mecanisme de schimb al identității, SCIM sau REST API precum și posibilitatea de a efectua operațiuni de administrare și configurare prin REST API. De asemenea, oferă suport pentru TLS 1.3.

Parolele stocate în cadrul directorului vor fi criptate, stocarea datelor trebuie să se realizeze într-o structură de tip bază de date. Profilele de utilizator vor putea fi extinse prin adăugarea de noi atribute, acestea putând fi administrate și editate la nivel individual.

Soluția va oferi mecanisme de extindere a funcționalităților standard utilizând plug-in-uri și REST APIs.

În vederea creșterii nivelului de flexibilitate în administrarea soluției, aceasta va trebui să ofere o componentă de tip command line interface (CLI).

Componenta IAM va fi configurată într-o arhitectură de înaltă disponibilitate atât la nivelul centrului de date principal, dar și în mod redundant, cu replicare în centrul de date secundar, pentru a asigura continuitatea serviciilor de autentificare și autorizare în caz de dezastru.

Sistemul va menține un RPO (Recovery Point Objective) de maximum 2 ore și un RTO (Recovery Time Objective) de maximum 4 ore pentru restaurarea serviciilor IAM în caz de incident major.

6.4 Componenta Middleware unificat de integrare (componentă suport)

Sistemul digital ePatrimoniu va include o componentă Middleware unificat de integrare, destinată asigurării interoperabilității între componentele software interne ale sistemului și sistemele informatice externe, precum și guvernancei traficului, securizării comunicațiilor și procesării fluxurilor de date.

Componenta va include cel puțin următoarele capabilități:

A. Capabilități de API Gateway și API Management

Componenta va asigura expunerea, securizarea și guvernarea serviciilor API, prin:

- gestionarea traficului de intrare și ieșire (traffic governance);
- mecanisme de throttling și rate limiting configurabile pe utilizator, aplicație sau serviciu;
- controlul accesului și autentificare prin mecanisme standard (ex.: OAuth2, OpenID Connect, JWT, certificat X.509);
- protecție împotriva accesului neautorizat și a abuzurilor de consum API;
- terminarea și gestionarea comunicațiilor securizate SSL/TLS;
- monitorizarea și jurnalizarea apelurilor API;
- mecanisme de caching pentru reducerea traficului către backend;
- posibilitatea definirii politicilor de acces și rutare;
- portal dedicat dezvoltatorilor (Developer Portal) pentru publicarea documentației API, gestionarea cheilor de acces și monitorizarea consumului.

B. Capabilități de Enterprise Service Bus (ESB)

Componenta va asigura medierea și orchestrarea serviciilor prin:

- orchestrarea fluxurilor de servicii și compunerea acestora în procese logice;
- transformarea mesajelor între formate diferite (ex.: XML ↔ JSON);
- conversia protocoalelor (ex.: REST ↔ gRPC);
- rutare inteligentă a mesajelor pe baza regulilor definite;

- agregarea sau fragmentarea cererilor;
- monitorizarea disponibilității serviciilor integrate;
- gestionarea erorilor și mecanisme de retry.

C. Capabilități de integrare și procesare date (ETL / Data Pipeline)

Componenta va permite integrarea și sincronizarea datelor prin:

- procesarea datelor în loturi (batch) pentru importul inițial al registrelor existente;
- sincronizarea periodică a datelor cu sisteme externe și registre administrative (ex.: ONRC, ANCPI, alte registre naționale);
- validarea, filtrarea și normalizarea datelor înainte de integrare;
- transformarea și maparea modelelor de date între sisteme;
- programarea și monitorizarea fluxurilor de integrare;
- gestionarea traficului de ieșire către sisteme externe.

Componenta Middleware va asigura disponibilitatea în modulul de administrare a unui jurnal al apelurilor de integrare și al fluxurilor de procesare date, accesibil utilizatorilor cu drepturi. Jurnalul va include cel puțin: data și ora apelului, tipul apelului (manual/automat/programat), serviciul apelat, statusul execuției, codul de răspuns, eventualele mesaje de eroare și referința la procesul sau entitatea afectată.

Sistemul digital va permite vizualizarea stării job-urilor programate, inclusiv frecvența de execuție, ultima rulare, rezultatul acesteia și eventualele erori. În cazul apariției unor erori sau disfuncționalități în apelurile de integrare sau în execuția job-urilor programate, sistemul va genera notificări vizibile în interfața de administrare.

6.5 Componenta Backup și restaurare (componentă suport)

Prestatorul are obligația de a implementa în cadrul sistemului digital ePatrimoniu măsuri și controale pentru asigurarea backup-ului și a redundanței sistemelor critice, în conformitate cu cerințele ISO/IEC 27001, corelate cu prevederile privind securitatea stocării conform ISO/IEC 27040. Scopul acestor măsuri este de a asigura disponibilitatea, integritatea și posibilitatea de recuperare a datelor și configurațiilor folosite, în cazul unor incidente, defecțiuni sau pierderi de informații.

Componenta de backup și restaurare trebuie să respecte în integralitate următoarele cerințe minime:

- să fie flexibilă și scalabilă, permițând implementarea într-o arhitectură distribuită (agenți de backup, server(e) de management, server(e) media sau echivalent).

- să permită administrarea din interfața GUI și să ofere mecanisme de automatizare prin CLI și RESTful API.
- să poată funcționa independent de o anumită tehnologie hardware.
- să poată fi instalată pe medii fizice, virtuale cât și pe medii cloud.
- să permită instalarea cel puțin pe următoarele sisteme de operare: Windows și Linux cu distribuții precum RHEL, SUSE Linux Enterprise Server, CentOS, Ubuntu sau alte distribuții Linux populare utilizate inclusiv în medii enterprise sau cloud.
- să suporte integrarea cu medii de stocare de tip DAS, NAS, SAN, cloud pentru stocarea fișierelor de backup.
- să suporte integrarea cu echipamente de stocare, în mod nativ sau prin protocoale standard de interoperabilitate.
- să identifice segmentele de date unice la nivelul agenților de backup, pentru optimizarea traficului prin rețea.
- să suporte transferul datelor pentru mediile on-premises și cloud.
- să permită reluarea unui backup nefinalizat cu succes de la ultimul checkpoint.
- să permită reluarea unei restaurări nefinalizate de la ultimul checkpoint.
- să ofere capabilități pentru efectuarea de backup-uri sintetice.
- să suporte verificarea automată a integrității backup-urilor și a restaurărilor.
- să automatizeze crearea de multiple copii ale backup-urilor pe diferite medii de stocare cu politici diferite de retenție.
- să permită crearea de backup-uri prin politici sau manual.
- să asigure asistență pentru operațiile importante: instalare, creare activități de salvare / restaurare, formatare și configurare medii de stocare etc.
- să ofere posibilitatea de restaurare completă a sistemelor fizice, virtuale și cloud, inclusiv restaurarea fișierelor, volumelor și instanțelor complete, precum și a aplicațiilor containerizate și a volumelor persistente asociate.
- să asigure suport complet pentru protecția aplicațiilor containerizate, inclusiv backup și restaurare a containerelor, protecția datelor persistente și integrare cu sistemele de orchestrare a containerelor. continuitatea operațională și restaurarea rapidă.
- să ofere toate tipurile de backup: full, incremental și diferențial, precum și metode de optimizare a backup-ului care permit reducerea volumului de date transferate și stocate, fără a compromite integritatea sau posibilitatea de restaurare completă.
- să permită integrarea cu sisteme de tip LDAP (Lightweight Directory Access Protocol) pentru autentificarea utilizatorilor

- să asigure suport pentru execuția paralelă a operațiilor de backup și multistreaming sau mecanisme echivalente funcțional.
- să permită restaurarea rapidă a datelor, permițând recuperarea selectivă a fișierelor, volumelor, containerelor sau instanțelor complete, fără a fi necesară restaurarea integrală a întregului backup, inclusiv pentru medii cloud și containere.
- să permită actualizarea automată a tuturor clienților de backup, inclusiv agenții instalați pe sisteme fizice, virtuale și în cloud, asigurând compatibilitatea cu toate versiunile suportate de sisteme de operare și fără a întrerupe procesele de backup active.
- să includă un modul centralizat de monitorizare și administrare, care să asigure alertare și raportare pentru toate funcțiile și componentele sistemului. Modulul trebuie să ofere rapoarte și alerte predefinite, dar și posibilitatea de a crea rapoarte personalizate prin interfața vizuală (point-and-click sau drag-and-drop) asupra repository-ului sau catalogului soluției. Modulul trebuie să asigure vizibilitate și control complet asupra infrastructurii de backup. Platforma trebuie să permită backup-ul mașinilor virtuale fără instalarea niciunui agent, permanent sau temporar, utilizând acces agentless prin hypervisor sau API-urile platformei cloud, pentru a proteja VM-urile fără a afecta performanța sau configurația acestora.
- să salveze blocurile modificate și să permită combinarea acestora cu backup-urile anterioare pentru optimizarea restaurării. Platforma de backup trebuie să asigure deduplicarea datelor la sursă și la nivelul stocării backup-urilor, folosind segmente de dimensiuni variabile, inclusiv pentru sisteme fără agenți dedicați. Deduplicarea trebuie să permită replicarea datelor deduplicate în diverse topologii („one-to-one”, „one-to-many”, „many-to-one” și cascade), pentru asigurarea continuității și protecției datelor în medii hibride și cloud.
- să asigure criptarea datelor replicate, în vederea securizării acestora pe perioada transferului între locații.
- să prevină accesului neautorizat la aplicația de backup prin mecanisme de control acces bazate pe roluri.
- să asigure suport pentru criptarea datelor, atât cele aflate în tranzit, cât și celor salvate. Soluția trebuie să includă propriile mecanisme pentru administrarea cheilor de criptare.
- să permită autentificarea utilizatorilor prin intermediul IAM
- să asigure protecție împotriva Ransomware, inclusiv prin păstrarea backup-urilor în mod imutabil, și mecanisme de obfuscare a datelor sensibile.
- să permită scalarea numărului de clienți de backup conform arhitecturii, indiferent de tipul acestora.

- să permită aplicarea de mecanisme de throttling pentru limitarea traficului de rețea și să ofere control asupra utilizării resurselor sistemului (CPU, memorie, I/O) de către procesele de backup și restaurare, atât pentru medii fizice, virtuale, cloud, per job sau per agent.

Componenta de backup va permite Autorității Contractante efectuarea actualizărilor (update-uri) conform politicilor producătorului și accesul direct la portalul acestuia pentru deschiderea cazurilor de suport tehnic.

6.6 Componenta Managementul incidentelor (ticketing) (componentă suport)

Sistemul digital ePatrimoniu va include o aplicație software de management a incidentelor (ticketing) semnalate de către utilizatorii interni ai sistemului digital (precum angajați ai Ministerului Culturii, DJC, INP) și destinate Prestatorului.

Aplicația va putea fi accesată din orice browser web.

Din punctul de vedere al licențierii, soluția trebuie să permită un număr nelimitat de utilizatori raportori și să permită extinderea numărului de agenți/membri suport.

Aplicația va cuprinde cel puțin următoarele funcționalități pe care Prestatorul le va configura în perioada de analiză și proiectare:

- După crearea din aplicație a unui tichet nou acesta va fi alocat automat către echipa Prestatorului pentru rezolvarea incidentului.
- Toate notificările sistemului (exemple: alocare tichet, modificare stare, închidere, redeschidere etc), vor fi transmise atât către echipa Prestatorului, cât și către utilizatorii interni ai Sistemului Digital, vor fi transmise via e-mail.
- Identificarea câmpurilor necesare astfel încât să fie colectate toate informațiile pentru documentarea corespunzătoare a tichetului, inclusiv prin posibilitatea de încărcare a unor fișiere ce pot reprezenta capturi de ecran sau similar. Această selecție de câmpuri va fi actualizată pe întreg SDLC (Software Development Life Cycle) și în perioada de mentenanță corectivă și evolutivă, conform cerințelor Autorității Contractante.
- Definirea nivelurilor de prioritate ale tichetelor în funcție de severitate, conform timpilor de răspuns și remediere detaliați în capitolul 8.
- Configurarea unui workflow specific incidentelor (ex. to do, in progress, done, reopen, closed, etc.)
- Generarea rapoartelor statistice în funcție de stare, prioritate, componenta asociată, perioadă de implementare depășită, etc.
- Organizarea și urmărirea activităților de dezvoltare și implementare în cicluri de lucru (iterații/sprinturi) cu durată fixă, configurabilă, care să susțină planificarea, prioritizarea și alocarea sarcinilor, monitorizarea progresului pe parcursul

ciclului și evaluarea rezultatelor la finalul fiecărei iterații, inclusiv prin rapoarte și indicatori de progres.

6.7. Componenta Monitorizare a performanței și disponibilității (componentă suport)

Componenta Monitorizare a performanței și disponibilității va facilita supravegherea continuă a performanței și disponibilității platformei, asigurând următoarele capacități ce vor fi configurate și personalizate de Prestator:

- Monitorizarea performanței Mașinilor Virtuale (VM-uri) prin colectarea de metrice precum utilizarea CPU, memorie RAM, spațiu pe disc și trafic de rețea pentru instanțele Nova din OpenStack, inclusiv componentele aplicative rulate pe aceste VM-uri. Aceasta include declanșatoare (triggers) pentru alerte la depășirea pragurilor de utilizare, cum ar fi peste 80% pentru vCPU sau RAM;
- Monitorizarea disponibilității VM-urilor prin verificarea stării instanțelor (activ/inactiv), a zonelor de disponibilitate, cu alerte automate pentru downtime sau stări dezactivate care afectează componentele aplicative;
- Monitorizarea performanței containerelor prin monitorizarea de metrice la nivel de container, inclusiv utilizarea CPU (mod kernel/user), memorie (utilizare maximă și commit), rețea (bytes/pachete RX/TX) și procese (număr PID-uri) asociate componentelor aplicative;
- Monitorizarea disponibilității containerelor prin verificarea stării containerelor (rulare, pauză, restart, OOMKilled), health checks și coduri de eroare la oprire, cu declanșatoare pentru stări nesănătoase persistente peste 2 minute, ținând cont de impactul asupra componentelor aplicative.
- Monitorizare hibridă integrată prin agregarea datelor din ambele medii (VM-uri și containere), permițând vizualizarea unificată prin dashboard-uri, cu suport pentru filtrare și grupare, nume de containere sau componente aplicative specifice.

În cazul depășirii pragurilor sau identificării unor anomalii, sistemul va putea executa acțiuni automate predefinite, precum închiderea sesiunilor inactive, izolarea serviciilor afectate, repornirea controlată a componentelor, declanșarea procedurilor de failover sau ajustarea dinamică a resurselor pentru restabilirea funcționării optime. Aceste acțiuni pot fi setate / redefinite de către administratori dintr-o interfață de tip web.

6.8. Componenta Managementul evenimentelor de securitate (SIEM)

Sistemul digital ePatrimoniu va include o soluție de monitorizare evenimente de securitate care trebuie să fie instalată pe infrastructura sistemului, să suporte implementare în arhitectură distribuită și să îndeplinească următoarele cerințe minimale:

- va asigura colectarea, indexarea, analizarea și corelarea tuturor log-urilor (ex: server de aplicații, web, sisteme de operare, aplicații, etc) și de la soluțiile de securitate cibernetică, cu scopul de a detecta și alerta în cazul apariției amenințărilor de securitate.
- trebuie să asigure capacitatea de ingerare, procesare și stocare online a tuturor log-urilor generate de toate tehnologiile de securitate și aplicațiile informatice implementate la nivelul componentelor interne a sistemului pentru o perioadă de minim 12 luni.
- nu trebuie să limiteze capacitatea de stocare a log-urilor de securitate colectate.
- transferul log-urilor către componenta de procesare/componenta centrală trebuie să se facă în mod securizat folosind protocolul SSL sau TLS.
- trebuie să asigure în mod implicit colectarea și interpretarea oricărui tip de log (de exemplu evenimente generate de: soluții de securitate, aplicații informatice sau sisteme de operare).
- va fi configurată să colecteze cel puțin următoarele tipuri de loguri:
 - autentificările reușite și nereușite cu origine, timp, utilizator, succes/eșec evidențiate;
 - modificare a rolurilor, permisiunilor sau a nivelului de acces.;
 - accesările neautorizate;
 - acțiunile administrative asupra utilizatorilor și asupra sistemului - toate modificările de configurare care să evidențieze schimbări ale resurselor sau politicilor – cine, ce, când și traseul de aprobare;
 - evenimente Firewall/IDS - atacuri detectate și blocate, cu corelarea incidentelor;
 - loguri Cloud / Endpoint: accesul API, servicii care pot afecta resurse.
- trebuie să fie scalabilă astfel încât să ofere posibilitatea de a mări performanța de corelare/procesare/stocare prin adăugarea unor resurse hardware suplimentare.
- trebuie să ofere o consolă de management de tip web-based care nu necesită instalarea unui software adițional și prin care sunt accesate toate funcționalitățile acesteia.
- trebuie să asigure facilități de indexare a datelor obținute de la surse diferite de log.
- trebuie să ofere un mecanism integrat de compresie a datelor, iar după expirarea perioadei de retenție a log-urilor online stocarea log-urilor compresate să se facă într-o structură, alta decât bază de date relațională, și care trebuie să poată fi accesate în orice moment de timp.

- trebuie să asigure vizualizarea/analiza/interpretarea log-urilor printr-o consolă/interfață unică.
- trebuie să asigure mecanisme de protecție a integrității datelor stocate prin intermediul algoritmilor de tip hash.
- trebuie să asigure exportarea log-urilor colectate în format CSV, JSON.
- trebuie să asigure un pachet predefinit de reguli de corelare și alertare.
- trebuie să asigure generarea automată a unui scor de severitate al alertelor.
- trebuie să asigure execuția de corelări bazate pe anumite condiții specifice și să permită definirea unor acțiuni de răspuns ce includ cel puțin:
 - crearea unei alerte,
 - transmiterea unui email
 - execuția unei acțiuni
- trebuie să asigure investigarea incidentelor de securitate pornind de la log-ul corelat până la identificarea log-urilor primare ce au generat alerta.
- trebuie să asigure utilizarea expresiilor regulate și operatori logici de tip Boolean (AND, OR, NOT) în aplicația de căutare
- trebuie să asigure geolocalizarea adreselor IP identificate în cadrul log-urilor colectate.
- autentificarea utilizatorilor pentru acces la administrarea soluției trebuie să se poată realiza pe baza de conturi de utilizatori definiți prin IAM, precum și integrare cu LDAP.
- trebuie să poată să fie integrată cel puțin cu soluții tip SOAR, Platforma Threat Intelligence, soluție ticketing via metode specifice de API.
- trebuie să ofere un panou central pentru filtrarea și corelarea în timp real a evenimentelor.
- trebuie să asigure generarea de rapoarte pe baza unor interogări, cât și exportul acestora în format CSV, PDF, XLS etc. Platforma va oferi un modul de rapoarte avansat ce asigură:
 - Rapoarte preconfigurate : soluția trebuie să include rapoarte standard pentru "Best Practices" și conformitate (GDPR, ISO 27001, COBIT,).
 - Personalizare și creare: Utilizatorii pot crea noi rapoarte, edita pe cele existente și planifica rularea/transmiterea acestora.
 - Funcționalități avansate: soluția trebuie să ofere opțiuni de exportare a rezultatelor rapoartelor pentru analize ulterioare.

Implementarea funcționalităților și configurările necesare bunei funcționări a componentei Managementul evenimentelor de securitate conform cerințelor descrise anterior cade în responsabilitatea Prestatorului.

În faza de analiză Prestatorul va propune structuri de dashboard-uri ale componentei.

6.9 Componenta de protecție servicii web (componentă suport)

Componenta de protecție a serviciilor web are rolul de a asigura securitatea, disponibilitatea și vizibilitatea asupra traficului către serviciile web publice și interne ale sistemului digital.

În acest sens, componenta de protecție servicii web va fi furnizată sub formă de appliance virtual, asigurând următoarele capabilități:

- Soluția WAF trebuie să permită definirea, modificarea și gestionarea regulilor de securitate într-un mod intuitiv și eficient, cu suport pentru atât reguli predefinite cât și personalizate, fără a impune utilizarea exclusivă a expresiilor regulate sau a modului de învățare automată.
- Sa ofere o interfață grafică intuitivă de tip web based pentru:
 - a) Adăugarea de noi reguli, fără a fi nevoie de codare
 - b) Vizibilitate asupra informațiilor despre atacuri
 - c) Tablouri de bord grafice pentru monitorizarea atacurilor și monitorizarea în timp real
 - d) Crearea și modificarea regulilor folosind API-ul
- WAF-ul trebuie sa suporte următoarele moduri de operare:
 - o Mod de blocare: Detectarea atacurilor, logare și blocarea lor
 - o Mod non-blocant: Doar detectarea și logarea atacurilor.
- Suport pentru IPv4 și IPv6
- Suport pentru redundanță și disponibilitate ridicată (High Availability) în mod Active-Active sau în mod Active-Standby, pentru a garanta filtrarea neîntreruptă a traficului în cazul defectării unei instanțe.
- Soluția trebuie sa proceseze tot traficul „on-prem” în modul reverse proxy

Soluția trebuie sa protejeze atât servicii web publice (publicate pe Internet), cât și aplicațiile web interne, fără a fi nevoie sa trimită trafic în afara infrastructurii în care e instalat.

Atât jurnalele de atac, cât și jurnalele de audit trebuie păstrate timp de cel puțin 30 de zile în consola de administrare a soluției.

Evenimentele suspecte ar trebui sa includă auditarea lor completă, inclusiv:

- a) Acțiuni întreprinse de WAF
- b) Sursa incidentelor de securitate pe tari
- c) Tipul atacului
- d) Durata atacului
- e) Serii temporale, date și ore
- f) URL-uri și subdirectoare compromise de un atac
- g) Detalii despre mesaj sau comanda, cum ar fi anteturi, corp și atribute, unde sunt disponibile
- h) Coduri CVE asociate atacului, atunci cand sunt relevante și disponibile

Soluția trebuie să ruleze pe un sistem de operare securizat, suportat de furnizor, cu actualizări regulate și optimizări pentru performanța și securitatea WAF-ului.

Soluția trebuie să asigure:

- Suport pentru multiple interfețe de rețea
- Stocare locală pentru jurnale și evenimente de securitate
- Management prin interfață web securizată (HTTPS), acces CLI securizat (SSH) și suport pentru monitorizare prin SNMP.

Soluția trebuie să suporte un volum de trafic adecvat serviciilor web protejate, cu posibilitate de scalare prin instanțe virtuale.

Soluția trebuie să garanteze un throughput Layer 4 de minimum 10 Gbps. Această resursă trebuie să fie divizibilă și partajabilă între mai multe instanțe virtuale independente, permițând alocarea dinamică a lățimii de bandă în funcție de necesitățile specifice ale serviciilor web protejate.

Soluția nu trebuie să se licențieze în funcție de numărul servicii web deservite.

Funcționalități minime solicitate în ceea ce privește livrarea serviciilor web:

- Suport IPv4 si IPv6
- Server load balancing Layer 4 și Layer 7 cu suport:
 - Fast HTTP, Full HTTP proxy, HTTP/2, HTTP/3
 - pentru persistența sesiunilor de nivel Layer 7

- pentru comutare Layer 7 bazată pe reguli și șabloane, cu posibilitatea de manipulare a headerelor HTTP URL-urilor și domeniului
- Load balancing DNS
- Layer 4 (UDP/TCP) și Layer 7 (DNS-UDP/DNS-TCP)
- Recursive DNS lookup
- DNS firewall/RPZ
- DNS cache
- Metode balansare: Round robin, least connections, weighted round robin, weighted least connections, fastest response
- Monitorizare stare
- Traffic steering/service chaining
- Suport pentru Internet content adaptation protocol (ICAP)

Funcționalități minime solicitate în ceea ce privește accelerarea aplicațiilor:

- Optimizare Protocol: Suport nativ pentru HTTP/2 și HTTP/3 (QUIC) pentru reducerea latenței;
- Eficientizarea Conexiunilor: Multiplexare TCP (connection reuse) și optimizare TCP (window scaling, keep-alive) pentru minimizarea numărului de sesiuni deschise către servere;
- Accelerare SSL/TLS: SSL Offloading și SSL Termination pentru descărcarea procesării criptografice de pe serverele de aplicație;
- Managementul Conținutului: RAM Caching pentru obiecte statice și compresie HTTP pentru reducerea volumului de date transferat.

Funcționalități minime solicitate în ceea ce privește securitatea serviciilor web:

- Criptare și Certificate: Suport pentru protocoale TLS actuale și gestionarea automată a certificatelor digitale.
- Protecție la nivel de Protocol: Apărare integrată împotriva atacurilor de tip DDoS, HTTP Request Smuggling și detectarea anomaliilor de IP.
- Controlul Traficului: Posibilitatea de a limita rata de conexiuni (rate limiting) și de a gestiona dinamic listele de acces (Blacklist/Whitelist) pe baza comportamentului sursei.

Soluția trebuie să asigure disponibilitatea aplicațiilor prin atenuarea atacurilor volumetrice și de protocol:

- Protecție la nivel de Protocol (L3/L4): Detectarea și blocarea automată a anomaliilor de rețea, inclusiv: pachete IP fragmentate, pachete cu opțiuni IP invalide, atacuri de tip Land-attack, Ping of Death și pachete TCP cu flag-uri invalide sau incomplete (TCP-no-flag, SYN-FIN, SYN-frag).
- Atenuare SYN Flood: Implementarea mecanismelor de tip SYN Cookies pentru protecția resurselor serverelor în timpul atacurilor de tip TCP handshake flood.
- Controlul Fluxului (Rate Limiting): Limitarea ratei pentru protocolul ICMP (IPv4/v6);
- IP Source Rate Limiting: Capacitatea de a limita numărul de conexiuni simultane și rata de cereri per IP sursă;
- Suport pentru politici de limitare bazate pe clase de trafic sau priorități.
- Managementul Incidentelor DDoS: Posibilitatea de a redirecționa, loga sau bloca automat adresele IP care depășesc pragurile de trafic stabilite, pentru intervale de timp configurabile.
- Protecție DDoS la nivel de Aplicație (L7): Detectarea atacurilor de tip HTTP Flood prin analiză comportamentală și limitarea ratei de cereri pe URL-uri specifice.

Funcționalități minime solicitate în ceea ce privește regulile și politicile de securitate:

- Protecție împotriva atacurilor de tip bot (spammeri, scraperi etc.)
- Protejarea paginilor de autentificare și înregistrare a utilizatorilor împotriva atacurilor Account-Takeover (ATO).
- Protecție API dedicată; REST, SOAP, JSON, XML si GraphQL.
- Prevenirea atacurilor de tip API Abuse.
- Inspecția și protejarea cererilor prin Websockets.
- Protecție împotriva atacurilor OWASP Top 10
- Protecție împotriva atacurilor WEB cunoscute: SQL Injection, Cross Site Scripting (XSS), Command Execution/Injection, Path Traversal, fișiere Backdoor, atacuri Brute Force, cookie poisoning etc.
- Protecție împotriva celor mai recente amenințări, cum ar fi Server-Side Request Forgery (SSRF) și Log4J JNDI.
- Protecție împotriva anomaliilor de protocol în cererile și răspunsurile HTTP:

- Integritatea Căii (Path Anomaly): Detectarea și blocarea căilor de acces anormale sau neconforme cu standardul RFC;
 - Tehnici de Evasion: Detectarea tentativelor de ocolire a securității prin utilizarea caracterelor de tip Null byte, Double encoding sau codificări invalide;
 - Validarea Antetelor (Headers): Identificarea anomaliilor în headerele HTTP (headere duplicate, lipsa User-Agent-ului, headere malformate);
 - Controlul Protocolului: Prevenirea atacurilor de tip HTTP Response Splitting și Request Smuggling;
 - Analiza Erorilor de Server: Monitorizarea și corelarea codurilor de eroare (4xx, 5xx) pentru identificarea tentativelor de scanare forțată sau de tip brute-force;
 - Identificarea Instrumentelor de Scanare: Detectarea semnelor specifice uneltelor automate de scanare a vulnerabilităților;
 - Securitate Transport: Capacitatea de a forța utilizarea protocolului HTTPS și de a refuza versiuni învechite de protocoale (TLS 1.0, 1.1) sau cifruri nesigure.
- Suport pentru marcarea adresei IP sursa ca fiind rău intenționată (blocare sau logare) dacă acestea depășesc un prag configurabil (rata de atac per sursa). WAF-ul ar trebui să prezinte IP-uri suspecte care nu au atins încă „pragul de atac” definit, așa cum s-a menționat anterior.
 - IP-urile rău intenționate identificate, utilizate pentru a ataca alte aplicații / clienți, ar trebui aplicate automat în componentă pentru blocare sau monitorizare.
 - Blocarea doar a cererilor etichetate ca atacuri: Traficul curat ar trebui transmis normal, chiar dacă provine de la aceeași adresă IP ca și atacatorul (pentru a evita rezultatele fals pozitive).
 - Regulile ar trebui să suporte orice parametru de header HTTP atât în cerere, cât și în răspuns. Mai jos sunt valorile posibile care pot fi combinate în definiția unei reguli. Regula ar trebui să suporte condiții logice folosind atât operatorii „SI”, cât și „SAU”:
 - Țara
 - Domeniu
 - Adresa IP
 - Metoda
 - Cale
 - Parametru POST

- Parametru interogare
 - Request cookie
 - Request header
 - Response code
 - Response header
 - Scheme (http, https)
 - Signal
 - User agent
- Suport pentru crearea de liste de elemente comune (șabloane) care să fie reutilizate în cadrul regulilor.
 - Regulile trebuie să suporte expresii regulate.
 - Regulile trebuie să suporte blocarea (geolocația) anumitor țări sau regiuni.
 - WAF-ul trebuie să identifice solicitările din rețelele TOR, centrele de date sau IP-urile rău intenționate, conform Institutului SANS.
 - Regulile trebuie să se actualizeze automat cu noile CVE-uri și atacurile 0-day care apar.

Funcționalități minime solicitate în ceea ce privește monitorizarea:

- Suport pentru tablouri de bord în timp real pentru a furniza starea fiecăreia dintre aplicațiile protejate, inclusiv:
 - Trafic în timp real.
 - Numărul de clienți care accesează aplicațiile.
 - Numărul de solicitări.
 - Alerte de securitate pentru OWASP Top 10.
 - Alerte de stare și atacuri.
 - Audit al modificărilor de configurație.
 - Incidente de securitate în funcție de aplicație:
 - Incidente de securitate în funcție de țară.
 - Tip de atac.
 - Durata unui atac.
 - Serii temporale, date și ore.
 - URL-uri și directoare compromise de un atac.
 - Detalii despre mesaj sau comandă, cum ar fi anteturi, corp și atribute.
 - Coduri CVE asociate atacului, atunci când sunt relevante.

- Soluția ar trebui să permită investigarea evenimentelor de securitate în timp real, inclusiv:
 - Căutare și filtrare după diferite criterii și evenimente.
 - Date despre solicitări individuale (URI/URL) și mesaje (cum ar fi anteturi, corp și attribute) care au fost blocate sau permise.
 - Date despre IP-ul sursa cu geolocație.
 - Anomalie potențială identificată de WAF.

Funcționalități minime solicitate în ceea ce privește integrarea cu soluții terțe:

- Integrare SIEM: Soluția trebuie să permită exportul datelor către sisteme de management al evenimentelor de securitate (SIEM) prin API sau protocoale standard. Configurarea log-urilor trebuie să fie granulară, permițând selectarea nivelului de detaliu transmis (de la jurnale de erori critice până la jurnale de tranzacții HTTP complete).
- Sisteme de Alertare: Posibilitatea de a transmite alerte automate către platforme de colaborare și management al incidentelor prin utilizarea mecanismelor de tip Webhook, Email sau conectori dedicați.
- Automatizare: Integrare completă cu soluții externe de orchestrare și automatizare prin interfață programabilă (RESTful API).

Sistemul va include funcționalități de filtrare și cenzurare a datelor sensibile (Data Masking). Se va garanta că informațiile de identificare personală (PII) și credențialele utilizatorilor sunt protejate prin mascare, astfel încât să nu fie vizibile în clar în jurnalele de audit, rapoarte sau exporturi.

Specificațiile de conformitate și certificare pentru soluția oferită vor asigura alinierea cu standarde recunoscute internațional pentru securitate, protecția datelor și integritatea operațională, astfel:

- conformitate cu OWASP Top 10
- conformitate cu SOC 2 (System and Organization Controls 2)

Cerințe minime privind licențierea:

- Soluția va fi licențiată pentru toate funcționalitățile solicitate

Cerințe minime privind suportul:

- Suportul va fi asigurat pe perioada mentenanței și garanției, acoperind dreptul de a face actualizări (firmware/sistem de operare – versiuni minore și majore, pachete software de la producător etc).
- Va fi asigurat acces 24x7x365 (24 de ore pe zi, 7 zile pe săptămână, 365 zile pe an) în centrul de suport al producătorului, cu posibilitatea raportării

problemelor apărute în funcționare și solicitarea rezolvării acestora în funcție de severitate.

7. Cerințe funcționale și nefuncționale transversale ale Sistemului digital ePatrimoniu

7.1 Niveluri de prezentare ale Sistemului digital ePatrimoniu

Sistemul digital va avea o zonă publică, accesibilă oricărui solicitant, fără a avea nevoie de autentificare în prealabil, în care vor fi expuse informații despre elementele de patrimoniu cultural gestionate în componenta de management de patrimoniu cât și informații privind serviciile de e-Guvernare furnizate de către Autoritatea Contractantă și de către instituțiile subordonate și compartimentele funcționale responsabile de furnizarea serviciilor.

Accesul la zonele cu acces controlat se va realiza printr-un mecanism securizat de autentificare, diferențiat în funcție de nivelul de sensibilitate al datelor și de categoria de utilizator.

Sistemul va suporta următoarele mecanisme de autentificare:

- autentificare cu un singur factor (utilizator/parolă) pentru rolurile cu nivel redus de acces la date sensibile;
- autentificare cu 2 factori (2FA) pentru utilizatorii cu drepturi administrative, pentru funcționarii publici cu rol decizional sau pentru fluxurile care implică aprobare, avizare ori semnătură digitală;
- autentificare unificată Single Sign-On (SSO), integrată cu servicii de identitate externe, în conformitate cu standardele precum SAML 2.0, OpenID Connect și eIDAS.

Sistemul va permite autentificarea prin serviciul național de identitate digitală ROeID precum și autentificarea cu certificate digitale calificate, utilizând validarea automată a acestora prin mecanismul OCSP (Online Certificate Status Protocol).

Pentru utilizatorii externi, autentificarea se va realiza prin cele două condiții de mai jos

- prin nume de utilizator și parolă, completate cu un cod OTP transmis prin e-mail sau SMS;
- prin ROeID sau certificat digital calificat.

7.1.1 Interfața publică

Interfața publică reprezintă zona de acces deschis a sistemului digital ePatrimoniu, destinată informării, transparenței și valorificării patrimoniului cultural național, fără a necesita autentificarea utilizatorilor. Aceasta oferă publicului larg acces la informații structurate despre elementele de patrimoniu cultural gestionate în sistem, la anumite secțiuni din registrele relevante pentru patrimoniul cultural, precum și la date relevante

privind serviciile de e-Guvernare furnizate de Autoritatea Contractantă și instituțiile subordonate.

Interfața publică are rolul de a asigura o prezentare coerentă, unitară și accesibilă a informațiilor, prin mecanisme moderne de navigare, căutare și explorare, adaptate atât utilizatorilor nespecializați, cât și celor cu interese profesionale, academice sau de cercetare. Aceasta este proiectată astfel încât să susțină descoperirea contextuală a resurselor culturale, evidențiind relațiile tematice, geografice și cronologice dintre acestea, precum și legăturile cu evenimente, persoane, instituții sau colecții relevante.

Din punct de vedere funcțional, interfața publică integrează datele și resursele expuse din Componenta MPC, respectând regulile de vizibilitate, clasificare și acces stabilite la nivelul sistemului. Afișarea informațiilor se realizează diferențiat, în funcție de tipul resursei, statutul acesteia și politicile de publicare, fiind susținută de suport multimedia avansat (imagini, materiale audio-video, modele 3D, hărți interactive), pentru o experiență de utilizare intuitivă și atractivă.

Interfața publică este concepută ca un instrument de promovare, educație și valorizare culturală, respectând standardele de accesibilitate, interoperabilitate și design centrat pe utilizator. Prin conținut editorial, narațiuni digitale, expoziții virtuale și mecanisme de recomandare, aceasta contribuie la creșterea vizibilității patrimoniului cultural, la stimularea interesului public și la facilitarea accesului deschis la resurse culturale digitale, în conformitate cu principiile guvernării deschise și ale reutilizării informațiilor publice.

7.1.1.1 Cerințe privind informațiile afișate din componenta MPC în interfața publică

Prestatorul va realiza dezvoltarea funcționalităților sistemului digital ePatrimoniu pentru a îndeplini următoarele cerințe:

- a) Navigarea și descoperirea resurselor.** Platforma oferă utilizatorilor o experiență de explorare intuitivă, bazată pe mai multe moduri complementare de navigare și descoperire a resurselor culturale. Scopul este de a facilita accesul rapid la informație, dar și de a permite o explorare liberă, bazată pe curiozitate și conexiuni tematice.
- b) Navigare prin categorii.** Resursele sunt grupate în categorii principale: **Tip** (ex: obiecte, clădiri, documente, evenimente, actori), **Colecții**, **Tematică**, **Locație** (ex: Transilvania), **Perioadă** (ex: 1600 - 1700) Etc. În interiorul fiecărei categorii, resursele pot fi sortate și filtrate după criterii specifice (de exemplu: tipul, perioada istorică, locația geografică, materialul, instituția deținătoare sau tema). Sistemul va cuprinde configurări în care obiecte conexe să fie grupate și prezentate într-un mod care evidențiază legăturile tematice, contextuale sau cronologice, cu posibilitatea navigării directe între entitățile asociate.

- c) **Căutare, filtrare și sortare.** Utilizatorul poate descoperi resurse folosind o căutare liberă, cu completare automată și sugestii relevante. Interfața oferă și un sistem de filtrare dinamică, în care utilizatorul poate combina mai multe criterii pentru a rafina rezultatele. De exemplu, poate selecta toate obiectele fizice din perioada medievală, aflate în zona Transilvaniei și realizate din metal. Sistemul va fi optimizat (încărcare progresivă a rezultatelor, optimizare bază de date, caching etc) astfel încât rezultatele căutărilor / filtrărilor / sortărilor să fie afișate rapid, indiferent de volumul total al bazei de date sau de complexitatea căutării / filtrării.
- d) **Navigare contextuală.** De pe pagina unei resurse individuale, utilizatorul poate continua explorarea prin legături contextuale: către alte resurse asociate (de exemplu, obiecte din aceeași colecție, evenimente legate de același loc, sau persoane implicate). Astfel, navigarea devine o experiență fluidă, bazată pe conexiuni între entități culturale.
- e) **Explorare vizuală.** Pentru o experiență interactivă, resursele pot fi explorate și prin vizualizări tematice: hărți interactive, pentru resurse geolocalizate, cronologie pentru evenimente și perioade istorice, o galerie vizuală, pentru imagini și obiecte cu reprezentare grafică. Aceste moduri alternative de navigare permit descoperirea intuitivă a patrimoniului, chiar și fără o intenție de căutare precisă.
- f) **Recomandări, actualizări și explorare ghidată.** Platforma va integra un set avansat de mecanisme pentru facilitarea descoperirii de conținut relevant și pentru stimularea explorării continue a colecțiilor culturale. Sistemul de recomandări afișează, pe paginile de prezentare ale obiectelor, resurse conexe sau similare, pe baza istoricului de navigare, preferințelor tematice, popularității generale sau a colecțiilor promovate editorial. În plus, platforma evidențiază permanent secțiuni cu ultimele resurse adăugate, permițând utilizatorilor să rămână conectați la noutăți. Pentru a susține navigarea fluidă prin patrimoniu, interfața include selecții editoriale ce scot în evidență cele mai relevante și interesante obiecte din colecții, vizibile în zone strategice ale platformei, precum paginile principale. De asemenea, platforma poate adapta conținutul afișat pe prima pagină în funcție de context: evenimentele culturale ale zilei, aniversări, comemorări la data vizitării sistemului digital, oferind un strat suplimentar de relevanță temporală.
- g) **Afișarea resurselor culturale.** Fiecare resursă culturală va avea o pagină separată identificată printr-un URL static. Soluția trebuie să ofere posibilitatea de vizualizare a imaginilor, obiectelor 3D și a materialelor audio-video aferente resurselor de patrimoniu (conform prevederilor din subsecțiunea 6.2.9) și hărților (conform prevederilor din subsecțiunea 6.2.10).

Va fi proiectat un layout optim pentru prezentarea intuitivă și ușor accesibilă a metadatelor complete ale fiecărei resurse și a informațiilor esențiale despre context și proveniență. Se va pune accentul pe media (imagini, clipuri audio,

clipuri video, modele 3D, etc.) și asigurarea unei experiențe vizuale captivante. Vor fi implementate și funcționalități avansate precum vizualizarea la rezoluție înaltă, secvențe video alternative, moduri de vizualizare AR/VR.

Resursele culturale din sistem pot să fie afișate public sau nu, iar afișarea informațiilor aferente fiecărei resurse culturale se face diferențiat în funcție de tipul de utilizator.

- h) **Optimizarea pentru motoarele de căutare, generative și de răspuns (SEO, GEO, AEO).** Pentru a crește vizibilitatea în ecosistemul digital și accesibilitatea patrimoniului cultural, se vor implementa strategii de SEO (Search Engine Optimization) pentru poziționarea în primele rezultate afișate de motoarele de căutare, GEO (Generative Engine Optimization) optimizarea conținutului astfel încât să fie corect înțeles, citat și utilizat de motoarele de căutare și sistemele AI generative, AEO (Answer Engine Optimization) optimizarea conținutului pentru a fi selectat și afișat ca răspunsuri directe la întrebări, în căutări vocale, răspunsuri sintetizate de AI.

7.1.1.2 Prezentarea și valorificarea atractivă a resurselor culturale digitale

Pentru a prezenta istoria și evoluția unor resurse culturale selectate de Autoritatea Contractantă într-un mod atractiv, sistemul digital va conține pagini dedicate cu narațiuni digitale (storytelling) și narațiuni prin derulare (scrollytelling), pentru o explorare imersivă a patrimoniului cultural. Printre funcționalitățile esențiale ce trebuie dezvoltate se numără:

- a) afișarea secvențială a textului;
- b) animarea treptată a elementelor vizuale;
- c) efectele de tip „parallax scrolling”;
- d) secțiunile fixe la derulare;
- e) comparatoarele de imagini „înainte/după”;
- f) cronologii interactive;
- g) hărți geospațiale;
- h) expoziții virtuale tematice;
- i) tururi virtuale 3D sau VR;
- j) infografice animate;
- k) galerii foto, fișiere video și audio;
- l) narațiuni audio generate automat din text;
- m) utilizarea unui video pe fundal sincronizat cu derularea paginii;
- n) indicator de progres vizual care reflectă parcurgerea narațiunii.

7.1.1.3 Profilurile publice ale direcțiilor județene de cultură (DJC)

Direcțiile județene de cultură (DJC) vor putea activa și gestiona profiluri publice (instanțe instituționale) în cadrul sistemului digital ePatrimoniu. Practic, aceste profiluri vor fi spații publice online / website-uri oficiale, prin intermediul cărora instituțiile vor putea publica informații de interes despre activitatea curentă.

Structura acestor pagini (meniul, submeniurile și tipurile de conținut disponibile) va fi stabilită în urma unor consultări directe cu DJC-urile. Această abordare participativă are rolul de a asigura că organizarea informațiilor respectă atât nevoile specifice ale instituțiilor, cât și cerințele impuse de legislația în vigoare. Definirea finală a structurii va avea loc în perioada de analiză/implementare a contractului.

Pentru a răspunde nevoilor variate ale direcțiilor județene, se va dezvolta un template modular, gândit ca un website personalizabil. Fiecare DJC va putea adapta acest șablon în funcție de specificul propriu, păstrând însă o coerență generală în cadrul sistemului digital ePatrimoniu.

Acest template va include:

- Prezentări generale despre activitatea și rolul direcției județene de cultură;
- Pagini cu structură standard, în care va exista posibilitatea inserării de texte, imagini, grafice sau alte tipuri de conținut multimedia, pentru a face informațiile mai accesibile și mai atractive;
- O zonă interactivă, destinată utilizatorilor externi, prin care aceștia vor putea urmări în timp real stadiul cererilor depuse la DJC (de exemplu cereri de avize, proceduri de clasare a monumentelor, autorizări sau alte solicitări similare).

Editarea și actualizarea conținutului acestor pagini vor fi concepute ca procese simple și intuitive, realizabile fără cunoștințe tehnice avansate. Sistemul digital va pune la dispoziția utilizatorilor din cadrul direcțiilor județene de cultură instrumente de administrare prietenoase, care vor permite gestionarea facilă a informațiilor publicate. Astfel, persoanele desemnate din cadrul fiecărei DJC vor putea crea, modifica și publica conținut în mod autonom, asigurând menținerea la zi a informațiilor și o comunicare eficientă cu publicul, fără a fi necesară intervenția unui administrator tehnic central.

Prin acest modul, sistemul digital ePatrimoniu va contribui la creșterea transparenței, eficienței și accesibilității în relația dintre instituțiile de cultură și public, oferind în același timp un instrument unitar de prezentare și comunicare pentru toate direcțiile județene de cultură.

7.1.1.4 Registre naționale pentru patrimoniu

Sistemul digital va conține o zonă de interes public în care se vor publica toate registrele relevante pentru patrimoniu, cum ar fi, dar fără a ne limita la:

- Lista monumentelor istorice: conține informații despre monumentele istorice clasate oficial
- Registrul bunurilor culturale mobile clasate în Patrimoniul Cultural Național:
- Registrul specialiștilor în domeniul protejării monumentelor istorice
- Registrul arheologilor
- Repertoriul Arheologic Național

- Rapoarte de cercetare relevante pentru domeniul patrimoniului cultural,
- etc.

7.1.2 Dashboard-ul intern

Destinat utilizatorilor autentificați, **dashboard-ul intern este structurat în module și submodule¹³** și reprezintă interfața centrală de lucru a sistemului digital ePatrimoniu pentru utilizatorii autentificați, fiind punctul centralizat de facilitare a activităților de administrare, e-Guvernare, management al patrimoniului și de guvernanță digitală. **Va fi asigurat un acces unificat, securizat și personalizat la funcționalitățile operaționale ale sistemului, în funcție de drepturile de acces/rolurile asociate tipului de cont.**

Funcționalitățile dashboard-ului vor fi disponibile exclusiv în mediul autentificat și vor fi adaptate responsabilităților specifice fiecărei categorii de utilizatori. În acest mod, utilizatorul va putea vizualiza atât informațiile publicate cu caracter general (valabile pentru toți utilizatorii autentificați), cât și pe cele cu caracter specific, valabile pentru unitatea organizatorică din care face parte.

Interfața dashboard-ului va fi organizată modular, incluzând următoarele module principale: **Administrare, e-Guvernare, Management Patrimoniu Cultural**, la care se vor adăuga module precum: Rapoarte, Date cont, Activități etc. Structura modulelor și submodulelor dashboardului intern va fi stabilită în faza de analiză, pe baza cerințelor utilizatorilor și a proceselor administrative identificate, urmând a fi proiectate conform principiilor de uzabilitate și design centrat pe utilizator.

Din punct de vedere al interfeței, dashboard-ul intern va fi realizat pe o structură bazată pe module și submodule, în conformitate cu subcapitolele 7.1.2.1–7.1.2.3, fiecare dispunând de ecrane dedicate pentru gestionarea funcționalităților specifice. Interfața va asigura o navigare intuitivă și o actualizare în timp real a conținutului afișat, în funcție de acțiunile utilizatorului, utilizând mecanisme de tabelare dinamică acolo unde este necesar.

Funcționalități generale disponibile în dashboardul intern:

- ecranele vor permite afișarea dinamică a informațiilor în funcție de criteriile selectate și vor integra funcționalități de filtrare, sortare și căutare a datelor, precum și opțiuni de export al listelor și rapoartelor în formate uzuale
- va exista posibilitatea de a exporta sau printa înregistrările selectate prin filtrare direct din ecranele aferente în diferite formate uzuale (pdf., html, word, excel etc.), fără a accesa, în mod necesar, modulul de Rapoarte

¹³ **Modulul** este o unitate funcțională majoră a dashboardului intern, care grupează un set coerent de funcționalități și procese asociate unui domeniu specific de activitate, având un scop bine definit și putând funcționa independent sau integrat cu alte module ale sistemului. **Submodulul** reprezintă o subdiviziune funcțională a unui modul, care implementează funcționalități specifice, detaliate sau specializate, contribuind la realizarea scopului modulului din care face parte și fiind accesibil în funcție de rolurile și drepturile utilizatorilor.

- se va implementa personalizarea tuturor mesajelor de eroare din sistem și afișarea cauzei. Se vor dezvolta și implementa soluțiilor tehnice optime pentru reducerea timpului de realizare a unei acțiuni
- se va implementa funcționalitatea *drag and drop* pentru încărcarea fișierelor.

7.1.2.1 Zona pentru gestionarea conturilor de utilizator și a entităților organizaționale

Zona de gestionare a conturilor și a entităților organizaționale reflectă modul în care este organizată și administrată asocierea unei persoane fizice cu o entitate organizațională, așa cum este descrisă în capitolul 3.2.

Sistemul va implementa un model de acces bazat pe asocierea unui utilizator la una sau mai multe entități organizaționale, cu roluri distincte definite pentru fiecare entitate.

Această zonă este reprezentată de o interfață clar structurată, în care utilizatorul poate vedea lista entităților organizatorice asociate.

Fiecare entitate va apărea cu datele de identificare esențiale și cu indicația administratorului curent, iar lângă fiecare utilizator asociat vor exista opțiuni pentru a vizualiza sau modifica drepturile și rolurile acestuia. Utilizatorul va putea adăuga o entitate nouă completând câmpurile pentru denumire, tipul organizației și datele de identificare, iar documentele justificative vor putea fi încărcate direct din același ecran.

Pentru fiecare utilizator asociat unei entități, administratorul va putea, printre altele: adăuga sau elimina utilizatori asociați, atribui roluri predefinite, configura permisiuni personalizate și vizualiza istoricul modificărilor drepturilor de acces.

Interfața va include și un panou de filtre și căutare pentru a găsi rapid conturi sau entități și va oferi acces direct la procesele inițiate în numele entităților, precum completarea fișelor de patrimoniu sau solicitarea/acordarea de avize.

Toate acțiunile realizate în această zonă vor fi jurnalizate, fiind asigurată trasabilitatea la nivel de persoană fizică, chiar și atunci când sunt efectuate în numele unei entități, asigurând transparență și responsabilitate.

Modelul de acces va permite o separare clară, vizualizabilă între identitatea individuală a utilizatorului și contextul operațional aferent entității organizaționale în numele căreia acesta acționează. Astfel, administratorii vor putea gestiona în mod eficient atât conturile personale, cât și operațiunile realizate în numele entităților, menținând simultan securitatea și integritatea datelor.

7.1.2.2 Pagina Home „Acasă”

Pagina Home „Acasă” a dashboard-ului intern va fi populată cu cele mai relevante și actuale informații pentru majoritatea utilizatorilor platformei. De asemenea, dashboard-ul va include pagini (secțiuni, tab-uri) unde vor fi încărcate informații relevante. Exemple de categorii de informații: regulamente, proceduri, ordine cu

caracter normativ, ordine și/sau dispoziții cu caracter intern pentru informarea tuturor angajaților, informări, situații statistice, propuneri de modificare a actelor normative, anunțuri de formare profesională. Publicarea conținutului general, care va fi disponibil tuturor utilizatorilor sau la nivel individual, respectiv de grup, în pagini ale dashboardului intern se va realiza de către administratorii de conținut desemnați, prin intermediul modului de Administrare.

Prima pagină a dashboard-ului intern Home „Acasă” va oferi utilizatorilor autentificați o prezentare sintetică a informațiilor relevante pentru activitatea acestora, personalizată în funcție de rolurile și drepturile de acces atribuite. Conținutul afișat pe dashboard va fi configurabil și va include elemente informative și funcționale specifice utilizatorului și proceselor inițiate sau gestionate, care vor fi stabilite în faza de analiză.

Componenta Activități aferentă paginii Home va afișa doar fluxurile și pașii din flux pentru care utilizatorul autentificat este responsabil, având următoarele funcționalități:

- vor fi afișați exclusiv pașii din fluxurile de lucru pentru care utilizatorul este desemnat ca responsabil unic sau co-responsabil;
- pentru fiecare activitate vor fi afișate: numele fluxului, pasul, link către flux și pas, afișarea clară a datei limită pentru finalizarea pasului, starea pasului (neînceput, în progres, întârziat, finalizat);
- marcarea vizibilă a pașilor cu date limită depășite;
- auditarea privind statusul pașilor.

Dashboard-ul Home „Acasă” va include funcționalități avansate de vizualizare a datelor operaționale, cu afișare aproape în timp real a indicatorilor relevanți pentru activitatea utilizatorilor, pe baza informațiilor din sistem. Datele vor fi prezentate sub formă de grafice, diagrame și alte elemente vizuale interactive, configurate în funcție de rolurile și drepturile de acces ale utilizatorilor.

Componenta de vizualizare va permite interacțiunea directă cu elementele grafice, astfel încât utilizatorii să poată explora datele afișate prin acțiuni de selecție (de tip click sau echivalent) asupra segmentelor de interes. Această interacțiune va facilita navigarea contextuală de la nivel agregat (indicatori, statistici, distribuții) către nivelul detaliat al datelor subiacente. În acest sens, selecția unui element dintr-un grafic sau diagramă va conduce utilizatorul către o vizualizare tabelară detaliată, prefiltrată automat conform criteriilor corespunzătoare selecției efectuate, permițând analiza directă a înregistrărilor care compun indicatorul respectiv.

Funcționalitățile de interactivitate și navigare contextuală vor sprijini monitorizarea operațională, identificarea rapidă a situațiilor relevante și analiza eficientă a fluxurilor administrative, fără a necesita reconfigurări manuale sau cunoștințe tehnice avansate din partea utilizatorilor.

Detaliile privind tipurile de grafice, nivelurile de agregare, mecanismele de interacțiune și corelarea acestora cu tabelele de date vor fi stabilite în faza de analiză, în faza de dezvoltare, migrare și testare și după faza de punere în producție a primei versiuni, în

concordanță cu arhitectura platformei și cu cerințele funcționale definite în capitolul 7.2.

7.1.2.3 Modulul de administrare

Modulul de administrare va permite gestionarea principalelor funcționalități de administrare integrate din componentele sistemului digital, **accesibile prin dashboardul intern**, în conformitate cu rolurile și drepturile atribuite administratorilor de sistem. Disponibilitatea acestor funcționalități într-un modul centralizat este importantă pentru ca administratorii de sistem să poată configura, monitoriza și controla în mod unitar utilizatorii, rolurile, fluxurile, setările operaționale și de securitate ale sistemului digital ePatrimoniu, asigurând funcționarea coerentă, sigură și eficientă a acestuia.

Submodule principale:

- gestionare utilizatori;
- gestionare unități organizaționale;
- gestionare nomenclatoare;
- gestionare șabloane și modele de documente;
- gestionare drepturi de acces pe module, submodule, acțiuni;
- gestionare notificări;
- gestionare parametri arhivare electronică;
- audit și jurnalizare;
- gestionare model AI;
- gestionare rapoarte și analize;
- gestionare probleme raportate de utilizatori;
- gestionare valorificare resurse culturale (informații publicate în interfața publică);
- administrarea spațiilor publice online ale instituțiilor (DJC) etc.;
- gestionarea apelărilor privind interoperabilitatea cu alte sisteme;
- administrarea operațională a schimburilor de date și a integrărilor cu sisteme externe.

Detaliile privind structura și funcționalitățile interfeței modulului de administrare vor fi stabilite în faza de analiză (vezi 8.1), pe baza cerințelor utilizatorilor și a proceselor administrative identificate și cu respectarea funcționalităților obligatorii prevăzute în prezentul caiet de sarcini, urmând a fi proiectate conform principiilor de uzabilitate și design centrat pe utilizator. Acestea vor putea fi modificate în faza de dezvoltare, migrare și testare și după faza de punere în producție a primei versiuni.

Administratorii vor putea efectua operațiuni de configurare, întreținere și monitorizare a sistemului, după cum urmează (listă neexhaustivă):

- gestionarea utilizatorilor, rolurilor și permisiunilor de acces, pe baza modelului RBAC (Role-Based Access Control);
- administrarea unităților organizatorice (Ministerul Culturii, Institutul Național al Patrimoniului, direcțiile județene pentru cultură, alte instituții înrolate) și a ierarhiei instituționale;
- configurarea registrelor publice asociate patrimoniului cultural, inclusiv lista monumentelor istorice, și gestionarea versiunilor acestora;
- configurarea de rapoarte complexe și grafice pe baza seturilor din baza de date;
- configurarea de alerte și notificări specifice/generale;
- monitorizarea stării componentelor sistemului (serve, servicii, baze de date, containere, API-uri, resurse de stocare);
- gestionarea și notificarea expirării certificatelor digitale, printr-un parametru de sistem: ex. perioada atenționare expirare - x zile;
- vizualizarea alertelor, incidentelor și jurnalelor de sistem;
- generarea rapoartelor de activitate și performanță pentru administratori;
- configurarea unei modalități de raportare a problemelor de către utilizatori și comunicare a soluțiilor de către administratori.

Submodulul privind administrarea utilizatorilor și a drepturilor de acces

Administrarea utilizatorilor și a drepturilor de acces și a nivelului de gestiune a unităților organizaționale în cadrul sistemului digital ePatrimoniu are ca scop garantarea unui nivel înalt de securitate și control asupra resurselor informaționale, asigurând accesul doar persoanelor, entităților și proceselor autorizate, în conformitate cu rolurile și responsabilitățile atribuite. Această funcționalitate se realizează prin integrarea și coordonarea cu **componenta suport pentru Gestiunea identității și accesul utilizatorilor - IAM (Identity and Access Management)**, descrisă în capitolul 6.3, care oferă mecanisme centralizate pentru gestionarea identităților, autentificarea utilizatorilor și definirea politicilor de acces pe baza rolurilor și privilegiilor specifice.

Sistemul va implementa un proces complet, unitar și auditabil de **identificare, autentificare, autorizare și auditare** a tuturor utilizatorilor, conform principiilor *least privilege* și *need-to-know*, astfel încât fiecare utilizator să poată accesa doar resursele strict necesare îndeplinirii atribuțiilor sale.

Toate entitățile care interacționează cu sistemul – persoane fizice, persoane juridice, procese automate, aplicații interne sau externe – vor fi identificate în mod unic, pentru a asigura trasabilitatea completă a acțiunilor efectuate. Administrarea utilizatorilor se va realiza centralizat, printr-o interfață unificată, cu control complet asupra ciclului de viață al conturilor (creare, modificare, suspendare, ștergere) și asupra drepturilor de acces asociate.

Soluția va permite definirea și gestionarea unui set extensibil de roluri și permisiuni, configurabile în funcție de tipul de utilizator și de nivelul de acces la funcționalitățile sistemului. Modelul de acces va respecta principiul segregării responsabilităților, asigurând separarea funcțiilor și acțiunilor critice, astfel încât rolurile incompatibile să nu poată fi atribuite aceleiași entități, prevenind conflictul de interese și riscurile de securitate.

Modalitatea de gestionare a relațiilor dintre utilizatorii persoane fizice și entitățile pe care le reprezintă va fi stabilită în faza de analiză.

Conturile cu rol de administrator al platformei vor putea crea, modifica, suspenda sau revoca drepturile de acces pentru orice utilizator, printr-o interfață grafică intuitivă, fără a fi necesare cunoștințe de programare. În acest sens, interfața trebuie să ofere posibilitatea de a defini în mod grafic attribute asociate utilizatorilor, rolurilor, precum și tipul de date al atributelor (ex: minim șir de caractere, numeric, lista de valori, tip data).

Soluția va include o consolă web care să ofere posibilitatea configurării granulare a politicilor de acces la nivel de resursă web sau adresă URL. Definirea acestor politici se va realiza exclusiv prin interfață grafică, fără a fi necesare cunoștințe de programare sau rularea de scripturi pe server.

În plus, sistemul trebuie să permită definirea politicilor de acces în funcție de attributele utilizatorilor, attributele cererilor de acces, precum și informații din contextul sesiunii.

Componenta trebuie să ofere capabilități de grupare politici de acces pe zona funcțională și să permită delegarea procesului de administrare a politicilor de acces către administratori locali, fiecare administrator local putând să gestioneze doar grupul de politici de acces alocate. Soluția va include și un instrument grafic de testare politici de acces pe resursele protejate prin care administratorul platformei să identifice rapid politicile de autorizare aplicate pe fiecare adresă web.

Componenta trebuie să captureze evenimentele administrative și de utilizator, inclusiv modificări ale rolurilor, permisiunilor și profilurilor utilizatorilor. Acestea vor putea fi configurate pentru a înregistra tentative de acces neautorizat sau violări de politici.

Sistemul va permite asocierea multiplă între utilizatori, roluri și entități organizaționale (de exemplu: direcții județene, comisii de specialitate, instituții subordonate, persoane juridice).

Aplicarea principiului **segregării responsabilităților (SoD)** va fi obligatorie. În consecință, sistemul nu va permite asocierea simultană a rolurilor considerate incompatibile (de exemplu: aprobare și validare în același flux procedural).

Toate politicile de acces vor fi documentate, configurabile și versionate. Sistemul va permite exportul și auditarea acestor politici în formate standard (PDF, CSV, JSON).

Submodul privind administrarea fluxurilor, șabloanelor și nomenclatoarelor

Submodulul va permite gestionarea completă a fluxurilor de lucru electronice, a formularelor și a șabloanelor utilizate în procesarea cererilor din componenta de e-

Guvernare [a se consulta secțiunea 6.1 a prezentului caiet de sarcini]. Acestea vor putea fi create, modificate și publicate prin instrumente vizuale low-code/no-code, fără a necesita cunoștințe de programare. Pentru fiecare flux, sistemul va păstra istoricul modificărilor (versiuni, autor, dată, descriere modificare), permițând revenirea la versiuni anterioare. Vor fi implementate mecanisme de aprobare a modificărilor asupra fluxurilor înainte de activarea lor în mediul de producție, pentru a asigura coerența și controlul calității.

Administrarea nomenclatoarelor, vocabularelor controlate și tezaurelor terminologice se va realiza centralizat. Prestatorul va asigura posibilitatea importului, exportului și actualizării acestor resurse, cu versiuni bilingve (română/engleză) și compatibilitate cu standardele internaționale (Getty, CIDOC CRM, EDM). Soluția va permite validarea automată a consistenței datelor din nomenclatoare, precum și corelarea acestora cu ontologia sistemului.

Submodul privind administrarea registrelor publice

Sistemul va asigura gestionarea registrelor publice aferente patrimoniului cultural. Administratorii vor putea actualiza, valida și publica versiunile registrelor în format deschis, respectând principiile FAIR și Linked Open Data. Pentru fiecare registru vor fi definite reguli de actualizare, frecvență, structură a datelor, drepturi de vizualizare și import / export. Soluția va asigura, totodată, trasabilitatea completă a tuturor modificărilor realizate asupra registrelor și va genera automat loguri și rapoarte de audit.

Fiecare registru va avea configurate niveluri de confidențialitate, iar accesul la date va fi restricționat utilizatorilor în conformitate cu acesta. Vor fi definite roluri distincte pentru actualizare, validare și publicare. Submodulul va permite selecția coloanelor din registre care vor fi publicate în interfețe.

Submodulul dedicat administrării componentei de inteligență artificială

Submodulul va integra funcționalități de tip MLOps, cu scopul de a asigura robustețea, trasabilitatea și calitatea continuă a răspunsurilor generate de sistemul AI, pe întreaga durată de viață a platformei.

Acest submodul va permite, prin interfață grafică, fără intervenție directă asupra codului sau infrastructurii tehnice:

- implementarea mecanismelor de **Data Versioning**, pentru urmărirea și gestionarea seturilor de date utilizate la indexare și în procesele RAG, cu evidența versiunilor și trasabilitatea modificărilor;
- rularea și vizualizarea rezultatelor proceselor de **Model Evaluation**, prin testare automată a acurateții răspunsurilor generate, utilizând seturi de date de referință validate (golden truth), în scopul prevenirii regresiei calității și a apariției halucinațiilor;

- gestionarea mecanismului de **Feedback Loop**, care permite marcarea, analizarea și corectarea răspunsurilor incorecte sau ambigue, precum și reintegrarea controlată a corecturilor în baza de cunoștințe;
- administrarea versiunilor bazei de cunoștințe utilizate în procesele RAG;
- monitorizarea indicatorilor de performanță AI.

Submodulul va asigura evidența completă a modificărilor realizate asupra modelelor, seturilor de date și parametrilor de funcționare, inclusiv identificarea utilizatorului care a efectuat modificarea, data și justificarea acesteia, în vederea auditării și conformității cu cerințele de guvernare AI.

7.1.2.4 Modulul MPC

Modulul Management Patrimoniu Cultural (MPC) reprezintă componenta operațională a dashboard-ului intern destinată gestionării, administrării și valorificării datelor referitoare la patrimoniul cultural mobil, imobil, arheologic și imaterial. Acesta oferă utilizatorilor autentificați acces controlat la funcționalități avansate de creare, editare, corelare și analiză a resurselor culturale, în conformitate cu rolurile și drepturile de acces definite la nivelul sistemului digital ePatrimoniu.

Modulul MPC este construit pe baza modelelor de date, ontologiilor și vocabularelor controlate descrise în capitolul 6.2 și funcționează ca nucleu informațional al platformei, asigurând consistența semantică și interoperabilitatea datelor. Informațiile gestionate în MPC constituie sursa principală de date pentru fluxurile de e-Guvernare, pentru registrele publice și pentru interfața publică, fiind utilizate atât în scop administrativ, cât și pentru analiză, raportare și fundamentarea deciziilor.

În mod particular, modulul MPC va permite configurarea și modificarea fișelor/formulelor de catalogare (secțiuni, câmpuri, validări, valori controlate și relații între resurse) din editoare / panouri de administrare. Structura acestor fișe va fi corelată cu ontologiile și vocabularele controlate utilizate în platformă, iar schimbările vor fi gestionate prin versionare și publicare controlată (draft/publicat), cu trasabilitate.

Prin intermediul MPC, utilizatorii instituționali și specialiștii autorizați pot gestiona ciclul de viață al resurselor culturale, incluzând stările de lucru, validare, publicare și arhivare, cu mecanisme de trasabilitate și audit. Modulul permite atașarea și gestionarea documentațiilor, materialelor multimedia, datelor geospațiale și a relațiilor dintre resurse, facilitând o viziune integrată asupra patrimoniului cultural la nivel național.

Modulul MPC este integrat nativ cu celelalte componente ale sistemului digital ePatrimoniu, în special cu componenta de e-Guvernare, astfel încât datele existente în MPC să poată fi utilizate direct în fluxurile administrative (avizare, autorizare, certificare). Această integrare elimină redundanțele, reduce riscul de erori și asigură coerența informațiilor utilizate în procesul decizional.

Interfața modulului MPC din cadrul dashboard-ului intern va fi configurabilă și adaptată tipurilor de utilizatori, permițând personalizarea vizualizărilor, filtrelor și instrumentelor de lucru. Modulul va respecta principiile de securitate, accesibilitate și performanță definite la nivelul întregului sistem și va permite extinderea funcționalităților în faza de analiză și în faza de proiectare, fără modificarea arhitecturii de bază.

Detaliile privind structura și funcționalitățile interfeței modulului management patrimoniu vor fi stabilite în faza de analiză, pe baza cerințelor utilizatorilor și a proceselor administrative identificate, urmând a fi proiectate conform principiilor de uzabilitate și design centrat pe utilizator.

7.1.2.5 Modulul e-Guvernare

Modulul e-Guvernare reprezintă componenta din dashboard-ul intern prin care sunt implementate și operate serviciile publice digitale furnizate de sistemul ePatrimoniu. Acesta asigură suportul necesar pentru inițierea, gestionarea, analizarea și soluționarea solicitărilor administrative aferente patrimoniului cultural, în conformitate cu cadrul legal aplicabil și cu fluxurile definite la nivelul Ministerului Culturii și al instituțiilor subordonate.

Prin intermediul modulului e-Guvernare, utilizatorii autentificați pot iniția și gestiona procese administrative digitale, pot încărca documentații, pot formula solicitări, pot participa la etapele de analiză și avizare și pot emite sau primi documente oficiale în format electronic. Modulul asigură trasabilitatea completă a fiecărui proces, de la inițiere până la soluționare, inclusiv evidența intervențiilor, deciziilor și termenelor.

Modulul e-Guvernare este strâns integrat cu componenta Management Patrimoniu Cultural, utilizând datele existente în MPC ca suport informațional pentru procesele administrative. Această integrare permite corelarea automată a solicitărilor cu resursele culturale relevante și elimină necesitatea introducerii repetitive a informațiilor, contribuind la eficientizarea activităților administrative și la creșterea calității deciziilor.

Funcționalitățile modulului includ gestionarea circuitelor interne de aprobare, organizarea activității comisiilor de specialitate, formularea observațiilor și deciziilor, precum și emiterea documentelor finale semnate electronic. Modulul va permite configurarea și adaptarea fluxurilor de lucru, a șabloanelor și a regulilor de procesare, în conformitate cu prevederile capitolului 6.2 și cu mecanismele low-code/no-code ale platformei.

Modulul e-Guvernare va respecta cerințele de securitate, confidențialitate și auditabilitate prevăzute în capitolul 7.5 și va asigura interoperabilitatea cu alte sisteme informatice publice relevante. Interfața sa din dashboard-ul intern va fi unitară și intuitivă, facilitând utilizarea eficientă de către toate categoriile de utilizatori instituționali implicați în furnizarea serviciilor publice digitale din domeniul patrimoniului cultural.

Detaliile privind structura și funcționalitățile interfeței modulului de e-Guvernare vor fi stabilite în faza de analiză, pe baza cerințelor utilizatorilor și a proceselor administrative identificate, urmând a fi proiectate conform principiilor de uzabilitate și design centrat pe utilizator.

7.1.2.6. Modulul de notificări

Modulul de notificări va asigura informarea în timp real și asincronă a utilizatorilor autentificați în platformă cu privire la evenimentele, acțiunile și modificările relevante care au loc în cadrul sistemului digital ePatrimoniu, în funcție de rolurile, drepturile de acces și preferințele configurate. Acesta va putea fi accesat de către utilizatorii logați din butonul aferent disponibil în interfața de lucru.

Modulul va funcționa integrat cu toate modulele și funcționalitățile sistemului (de exemplu e-Guvernare, Managementul Patrimoniului Cultural) și va permite generarea automată de notificări ca urmare a unor evenimente sau declanșatori predefiniți.

Sistemul va realiza cel puțin următoarele tipuri de notificări pentru utilizatorii autentificați:

- notificări operaționale (ex: cereri atribuite, solicitări de validare/aprobare, termene limită);
- notificări de sistem (ex: modificări de roluri sau drepturi de acces, suspendarea/activarea conturilor);
- notificări privind fluxurile de lucru (ex: schimbarea stadiului unei cereri, finalizarea unui proces, respingerea/ acceptarea unei solicitări);
- notificări administrative și de audit (ex: modificări asupra registrelor, nomenclatoarelor, fluxurilor sau politicilor de acces).

Modulul va permite livrarea notificărilor prin următoarele canale, configurabile per utilizator și per tip de eveniment: notificări în interfața web a platformei (prin prezentul modul de notificări) și notificări prin e-mail.

Sistemul va oferi prin interfața specifică un centru dedicat de notificări care va asigura vizualizarea atât a notificărilor active, cât și a istoricului acestora. Funcționalitatea va permite gestionarea stării notificărilor prin marcarea acestora ca citite sau necitite, precum și organizarea lor prin mecanisme de filtrare și sortare după criterii precum tipul, data, prioritatea sau componenta sursă. Din cadrul fiecărei notificări, utilizatorul va putea accesa în mod direct elementul sau acțiunea corespunzătoare din sistem, inclusiv cereri sau procese de lucru.

Administratorii platformei vor avea la dispoziție o interfață grafică pentru:

- definirea tipurilor de evenimente care generează notificări;
- configurarea regulilor de declanșare a notificărilor în funcție de roluri, stări ale proceselor, niveluri de confidențialitate sau alte attribute contextuale;
- stabilirea nivelului de prioritate (informativ, avertizare, critic);
- definirea șabloanelor de notificare (titlu, conținut).

Notificările vor respecta politicile de securitate și confidențialitate ale sistemului, fiind afișate exclusiv utilizatorilor autorizați. Conținutul notificărilor va fi adaptat nivelului de acces al utilizatorului și nu va expune date sensibile către persoane neautorizate. Modulul de notificări va asigura jurnalizarea tuturor notificărilor generate și transmise, incluzând informații privind sursa evenimentului, tipul evenimentului, momentul generării și canalul de livrare utilizat.

7.1.2.7. Rapoarte

Modulul Rapoarte reprezintă componenta din dashboard-ul intern prin care utilizatorii autorizați pot accesa, genera și analiza informațiile consolidate din toate modulele platformei. Acesta oferă o interfață unificată pentru vizualizarea, filtrarea și exportul datelor relevante pentru activitatea fiecărui utilizator sau pentru unitatea organizațională din care face parte, în acord cu funcționalitățile descrise în capitolul 7.2.

Utilizatorii vor putea accesa și genera diverse rapoarte în funcție de rol și drepturi, care oferă o perspectivă asupra datelor și activităților din sistem. Panoul principal va prezenta o colecție de rapoarte organizate pe categorii și surse de informații, astfel încât utilizatorul să poată accesa rapid date relevante pentru rolul său.

Printre rapoartele disponibile se numără rapoarte tematice și comparative, care permit analiza diferitelor procese administrative. Acestea pot include informații despre intervenții asupra patrimoniului, activitatea instituțiilor sau specialiștilor acreditați, precum și comparații între perioade sau categorii de obiecte, oferind o imagine contextualizată și utilă pentru luarea deciziilor.

Sistemul va pune la dispoziția utilizatorilor rapoartele standard care oferă o privire rapidă și detaliată asupra activității instituțiilor și a patrimoniului cultural. Aceste rapoarte permit urmărirea proceselor administrative, analiza intervențiilor asupra bunurilor culturale, evaluarea activității specialiștilor și compararea datelor între perioade sau regiuni.

Sistemul va permite configurarea de rapoarte dinamice, personalizate, printr-o interfață intuitivă, care nu va presupune cunoștințe de programare, această configurare fiind realizată de utilizatori cu rol de administrator. Administratorul va defini structura, conținutul și parametrii rapoartelor, precum și categoriile de utilizatori care au dreptul de acces la acestea. Rapoartele astfel configurate vor fi puse la dispoziția utilizatorilor interni sub forma unei colecții de rapoarte predefinite, relevante pentru rolul și funcția deținute în cadrul instituției, utilizatorii având posibilitatea de a selecta câmpurile permise, de a aplica filtre și agregări și de a vizualiza datele sub formă de tabele sau grafice, fără a putea modifica structura de bază a rapoartelor.

Astfel, fiecare utilizator va putea accesa setul de rapoarte adaptat atât necesităților generale ale entității, cât și cerințelor specifice ale activității sale, în funcție de drepturile și responsabilitățile deținute.

În momentul accesării modulului Rapoarte, utilizatorul va avea acces la un panou central, unde toate rapoartele disponibile vor fi afișate sub formă de carduri sau liste, organizate pe categorii și surse de date. Fiecare raport este prezentat cu titlu, descriere scurtă și indicatori cheie care permit identificarea rapidă a conținutului și relevanței sale. Rapoartele pe care utilizatorul le poate accesa sunt adaptate în funcție de drepturile de acces, astfel încât fiecare să vadă doar informațiile pentru care are autorizație.

Panoul va include filtre vizuale și butoane rapide care permit sortarea rapoartelor după categorie, perioadă sau relevanță, precum și opțiuni pentru exportul datelor în diferite formate. Utilizatorul poate marca rapoartele frecvent utilizate ca favorite, pentru acces rapid, și poate naviga între secțiuni intuitiv, fără a părăsi contextul analizei.

Rapoartele generate vor putea fi descărcate în formate standard, precum XLSX, PDF, CSV, JSON, HTML în conformitate cu tipul și scopul raportului. Structura vizuală și conținutul rapoartelor descărcabile vor respecta șabloane prestabilite, care vor fi definite și aprobate în faza de analiză, în vederea asigurării coerenței, lizibilității și utilizării unitare a rapoartelor la nivelul instituțiilor beneficiare.

Detaliile privind organizarea interfeței modulului Rapoarte, inclusiv modul de afișare și filtrare a informațiilor, vor fi definite în faza de analiză, pentru a asigura o integrare coerentă cu arhitectura generală a sistemului digital ePatrimoniu și cu funcționalitățile celorlalte module.

7.1.2.8. Documente

Modulul Documente reprezintă componenta centralizată de accesare și vizualizare a tuturor documentelor asociate activității utilizatorilor în cadrul sistemului digital ePatrimoniu. Acesta va fi disponibil exclusiv utilizatorilor autentificați, prin intermediul dashboard-ului intern, și va asigura o evidență unitară a documentelor generate, încărcate sau procesate în cadrul tuturor modulelor platformei la care aceștia au acces (e-Guvernare, Management Patrimoniu Cultural etc.).

Modulul va permite fiecărui utilizator să vizualizeze și să gestioneze:

- documentele proprii încărcate în sistem;
- documentele generate automat de sistem sau încărcate, aferente cererilor și proceselor administrative în care utilizatorul este implicat, în conformitate cu rolurile și drepturile de acces atribuite;
- documentele asociate entității organizaționale pe care utilizatorul este autorizat să le reprezinte.

Utilizatorii vor putea vizualiza exclusiv documentele pentru care au drepturi explicite, iar orice acces sau acțiune asupra unui document va fi înregistrată și auditabilă.

Modulul Documente va oferi cel puțin următoarele funcționalități:

- listarea documentelor într-o interfață unificată, sub formă de tabel dinamic, cu posibilități de filtrare, sortare și căutare după criterii precum: tip document, proces asociat, status, dată, instituție, autor, nivel de confidențialitate;
- vizualizarea documentelor direct în interfața web (pentru formate uzuale: PDF, imagini, documente text), fără a necesita descărcarea locală;
- descărcarea documentelor, în conformitate cu drepturile de acces ale utilizatorului;
- încărcarea de documente suplimentare în cadrul proceselor active, acolo unde fluxurile definite permit acest lucru;
- afișarea metadatelor asociate fiecărui document (tip, versiune, autor, dată creare/încărcare, proces asociat, instituție, status);
- versionarea documentelor, cu păstrarea istoricului modificărilor și posibilitatea de consultare a versiunilor anterioare;
- corelarea automată a documentelor cu cereri, procese sau entitățile organizaționale relevante.

Documentele vor fi organizate într-o structură logică și coerentă, în funcție de data creării sau a încărcării, de apartenența la procesele administrative și fluxurile de lucru corespunzătoare, precum și de tipologia documentului (cereri, avize, autorizații, fișe de patrimoniu, rapoarte, documente justificative etc.), astfel încât utilizatorii autorizați să poată identifica și accesa rapid informațiile relevante.

Documentele vor fi accesibile și consultabile atât în modulul Documente, unde pot fi vizualizate în ansamblu, cât și în contextul fiecărei instanțe din platformă legate de procesele în care sunt implicate. Această abordare permite utilizatorilor să gestioneze și să urmărească documentele exact acolo unde sunt relevante, dar și să aibă o vedere de ansamblu asupra tuturor informațiilor. Astfel, se asigură coerența datelor, urmărirea completă a documentelor în funcție de contextul lor operațional și o transparență sporită a tuturor acțiunilor și stadiilor proceselor administrative.

Sistemul va asigura trasabilitatea completă a documentelor, prin înregistrarea informațiilor privind persoana care a creat, încărcat, modificat sau accesat fiecare document, momentul în care a fost realizată fiecare acțiune, precum și contextul în care documentul a fost utilizat (proces, cerere sau flux de lucru), aceste date fiind disponibile pentru audit și raportare.

Structura detaliată a interfeței modulului Documente, precum și modul de organizare și prezentare a informațiilor, vor fi definite în faza de analiză, în corelare cu arhitectura generală a sistemului digital ePatrimoniu și cu funcționalitățile celorlalte module, astfel încât să fie asigurată o integrare coerentă și unitară.

7.2 Realizare de interogare și analiză rapoarte pe baza datelor din sistem

Modulul de interogare și analiză a rapoartelor pe baza datelor reprezintă un element transversal al sistemului digital ePatrimoniu, care are rolul de a colecta, corela, analiza și prezenta într-o manieră structurată și vizuală informațiile provenite din toate

modulele platformei: e-Guvernare, Managementul Patrimoniului Cultural (MPC), administrarea utilizatorilor și drepturilor de acces, submodulul GIS, registrele naționale etc.

Scopul acestei componente este de a oferi **instrumente avansate de analiză**, care să susțină procesul decizional strategic, operațional și administrativ la nivelul Ministerului Culturii, al instituțiilor subordonate și al altor actori autorizați, precum și de a permite generarea de **rapoarte dinamice, statistici și indicatori de performanță** privind activitățile și datele gestionate de sistem.

Prestatorul va configura în timpul implementării un număr de minim 50 tipuri de rapoarte, care vor fi definite în faza de analiză.

7.2.1. Surse de date și integrare

Sistemul va integra un mecanism centralizat de colectare și agregare a datelor din toate modulele și componentele platformei, precum și din bazele de date externe interoperabile.

Informațiile pentru rapoarte vor fi extrase din bazele de date interne ale sistemului prin intermediul API-urilor dedicate, pentru a asigura acces rapid, sigur și coerent la date.

Sursele de date care vor alimenta componenta de raportare includ, fără a se limita la:

- fluxurile electronice din Componenta e-Guvernare (cereri depuse, stadii de procesare, avize și autorizații emise, timpi de răspuns, statusuri etc.);
- registrele naționale administrate de Ministerul Culturii și instituțiile subordonate (Registrul Specialiștilor, Lista Monumentelor Istorice, Registrul bunurilor clasate, Registrul Arheologilor etc.);
- datele și metadatele din Componenta Management Patrimoniu Cultural (obiecte culturale, instituții, locații, evenimente, fișe descriptive etc.);
- datele provenite din submodulul GIS (distribuții spațiale, zone de risc, amplasamente, corelări teritoriale);
- informațiile privind activitatea utilizatorilor (accesări, roluri, acțiuni, sesizări și incidente);
- date provenite din sistemele externe interconectate prin API-uri (de ex. ANCPI, Europeana, INFP, HHRI, ROeID).

Integrarea datelor se va realiza automat, prin procese programate de tip ETL (Extract – Transform – Load), asigurând consistența, deduplicarea și validarea datelor provenite din surse multiple.

7.2.2. Funcționalități generale de raportare

Componenta de raportare va permite utilizatorilor autorizați să genereze, vizualizeze și exporte rapoarte și statistici personalizate, bazate pe datele din toate componentele sistemului (e-guvernare, management patrimoniu, GIS, AI, administrare etc.), asigurând o perspectivă unitară asupra întregului ecosistem ePatrimoniu.

Funcționalitățile minime care trebuie implementate includ:

- rapoarte standard predefinite, livrate împreună cu sistemul, configurabile de către administrator (ex.: număr cereri procesate, durata medie de soluționare, număr bunuri clasate, statistici privind patrimoniul imobil/mobil/imaterial, distribuții teritoriale, situații comparative între instituții etc.);
- rapoarte dinamice (ad-hoc), configurabile de către utilizatori autorizați printr-o interfață grafică intuitivă (ex. secvențiere de pași), care permite selecția câmpurilor, aplicarea de filtre, agregări și sortări;
- corelarea datelor între componente (de exemplu, analiza relației dintre numărul de cereri de avizare și tipologia bunurilor culturale implicate, sau distribuția geografică a bunurilor clasate în raport cu riscurile seismice și de inundație);
- vizualizare interactivă sub formă de tabele dinamice, filtrabile, grafice, hărți, diagrame și dashboard-uri personalizabile;
- rapoarte tematice generate pe baza registrelor publice și a fluxurilor administrative (ex.: rapoarte de clasare, declasare, autorizare intervenții, acreditare specialiști etc.);
- rapoarte comparative cu posibilitatea de a selecta perioade de timp, regiuni, instituții sau tipuri de patrimoniu;
- rapoarte agregate pentru managementul sistemului (număr total utilizatori, sesiuni active, incidente, timpi medii de răspuns, performanță componente etc.);
- rapoarte cu criterii de selecție flexibile asupra datelor specifice sistemului, de ex. valori provenite din liste derulante, fluxuri, etape aferente, coloane, stări ale etapelor, etc.;
- proiectare rapoarte solicitate de AC, cu posibilitatea aplicării de filtre multiple și utilizând template-uri construite conform regulilor de identitate vizuală ale Ministerului Culturii, în format PDF, tabelar (XLS/ XLSX), CSV, XML, DOCX, etc. Totodată, se impune implementarea de a putea genera rapoarte în mod dinamic, adăugând sau renunțând la anumite coloane / câmpuri;
- pentru rapoarte, în special pentru cele care necesită un timp mare de generare, se impune posibilitatea de a fi generate și în mod asincron și totodată dezvoltat un modul pentru managementul acestora;
- notificare cu privire la finalizarea generării unui raport asincron;
- numele fișierelor rezultate în urma generării rapoartelor trebuie să fie parametrizate;
- salvarea fișierelor generate și vizualizarea istoricului rapoartelor generate (data executării, statusul generării, formatul, parametri, utilizator, etc.)

Funcționalități extinse suplimentare:

- **rapoarte de vizualizare per resursă**, inclusiv topuri dinamice („cele mai vizualizate bunuri”, „resurse cu cele mai multe descărcări”, „cele mai accesate fișe de monumente” etc.);

- **rapoarte complexe de activitate**, cum ar fi generarea automată a raportului anual de activitate al unei Direcții Județene pentru Cultură (DJC), prin agregarea automată a indicatorilor operaționali (număr cereri, avize, intervenții, clasări, inspecții, controale, situații pe tipuri de patrimoniu etc.);
- **analize geospațiale interactive**, care să permită introducerea coordonatelor unui traseu (de exemplu, pentru o lucrare de infrastructură) sau a unei clădiri și identificarea automată a zonelor și bunurilor de patrimoniu pentru care este necesară obținerea de avize, folosind integrarea cu sistemul GIS și regulile teritoriale privind zonele de protecție;

Funcționalități complementare: posibilitatea programării automate a generării periodice de rapoarte, transmiterea lor prin e-mail utilizatorilor autorizați.

În modul de configurare a unui raport, utilizatorul autorizat va putea defini atât conținutul acestuia (câmpuri, filtre, agregări, surse de date), cât și structura și prezentarea la nivel de pagină, inclusiv stabilirea poziționării elementelor (titluri, tabele, grafice, subrapoarte), configurarea antetelor și subsolurilor, numerotarea paginilor, reguli de paginare, inserarea de secțiuni repetitive și utilizarea unor șabloane prestabilite. Configurarea va permite controlul detaliat al aspectului final al documentului, astfel încât rapoartele generate să poată respecta o structură formală și un format prestabilit, adecvate utilizării în documente oficiale și raportări instituționale.

Toate rapoartele vor putea fi exportate în formatele PDF, XLSX, CSV, JSON și HTML, iar dashboard-urile vor fi salvabile și reutilizabile. Înainte de exportul unui raport în format final, sistemul va permite utilizatorului vizualizarea unei versiuni de tip preview, generată pe baza parametrilor și filtrelor selectate, cu posibilitatea ajustării acestora înainte de confirmarea exportului.

7.2.3. Funcționalități avansate și vizualizare

Sistemul va permite vizualizarea datelor prin interfețe grafice intuitive, integrate în platformă sau prin componente software compatibile, configurate în funcție de nevoile beneficiarului.

Funcționalitățile vor permite cel puțin:

- filtrarea și gruparea datelor după criterii relevante (de exemplu: instituție, tip patrimoniu, status, perioadă, județ, categorie);
- afișarea rezultatelor în formă tabelară și grafică;
- realizarea de dashboard-uri și vizualizări tematice pentru monitorizarea activităților și a datelor din sistem;
- afișarea pe hartă a datelor care au componentă geospațială, prin integrarea cu modulul GIS;
- exportul rezultatelor și rapoartelor în formate uzuale.

Tipurile exacte de vizualizări, nivelul de interactivitate și scenariile de utilizare vor fi detaliate în etapa de analiză, în funcție de prioritățile operaționale ale beneficiarului.

7.3 Interoperabilitate și integrare cu alte sisteme

7.3.1 Cerințe de implementare a API-urilor dezvoltate

Soluția va dispune de „RESTful” API ce va putea fi folosit de toate sistemele informatice care doresc să utilizeze informații privind patrimoniul cultural (de exemplu enciclopedii online, expoziții virtuale, biblioteci digitale specializate).

Soluția va utiliza și returna codurile de stare HTTP într-un mod corect și aliniat arhitecturii RESTful, respectând scopul definit de standardele oficiale pentru fiecare clasă de coduri (1xx- Informational, 2xx- Success, 3xx- Redirection, 4xx- Client Error, 5xx- Server Error).

Utilizarea acestor coduri trebuie să reflecte fidel situația întâmpinată: de exemplu, codul 401 Unauthorized va fi utilizat exclusiv în cazurile în care autentificarea este necesară, dar nu a fost furnizată sau nu este validă, iar codul 403 Forbidden va fi rezervat situațiilor în care autentificarea a avut loc, dar accesul la resursă este interzis din motive de permisiuni insuficiente și nu invers.

7.3.2 Autentificare și autorizare

Sistemul trebuie să pună la dispoziție un serviciu web de tip REST API care să permită înregistrarea unei aplicații OAuth de către un utilizator autorizat, generând un client ID pentru configurarea controlului accesului și care va fi utilizat la autentificare în serviciile web securizate.

Sistemul trebuie să pună la dispoziție un serviciu web de tip REST API care să permită autentificarea și care în urma autentificării să genereze un token/ticket care să se utilizeze la apelarea altor servicii web.

7.3.3 Operații CRUD pe resurse

Sistemul trebuie să pună la dispoziție servicii web de tip REST API care să permită:

- a) obținerea unui singur termen de vocabular prin GET, returnând un obiect JSON cu detalii despre termen, relații și valori.
- b) obținerea unei liste paginate de ID-uri de instanțe de resurse prin GET, returnând un obiect JSON cu containere de ID-uri de resurse.
- c) obținerea unei instanțe de resursă prin GET, returnând un obiect JSON cu date aferente instanței de resursă.
- d) actualizarea totală unei instanțe de resurse prin PUT.

- e) actualizarea parțială a unei instanțe de resurse prin PATCH.
- f) introducerea unei noi instanțe de resurse prin metoda POST.
- g) ștergerea unei instanțe de resurse prin DELETE.
- h) obținerea unei colecții JSON a modificărilor resurselor (Create, Update, Delete) prin GET, returnând un obiect cu numărul total de elemente și link-uri către prima și ultima pagină.
- i) obținerea unei pagini, pentru un număr de pagină prin GET, returnând o listă de elemente ordonate cu detalii despre actor, obiect și tipul modificării.

Pentru resursele care conțin informații geospațiale, soluția va utiliza formatul GeoJSON pentru reprezentarea datelor, oferind suport pentru paginare, filtrare și metadata. În completare, se va asigura publicarea unui endpoint conform standardului OGC API – Features pentru aceleași seturi de date, cu suport pentru filtrare și paginare standard OGC și descrierea colecțiilor, precum și expunerea prin servicii WMS/WMTS în regim read-only pentru compatibilitate cu aplicații GIS existente.

7.3.4 Design și standarde de implementare

API-urile vor fi documentate complet, furnizând descrieri clare ale endpoint-urilor, parametrilor, codurilor de răspuns, schemelor de date și exemple de utilizare, pentru a facilita interoperabilitatea și integrarea altor sisteme informatice.

Endpoint-urile vor fi structurate ierarhic, reflectând corect relațiile dintre resurse, evitând rute ambigue sau redundante.

Toate metodele HTTP vor respecta semantica standard: GET fără efecte colaterale, folosirea corectă și conformă arhitecturii “RESTful API” a metodelor POST, PUT și PATCH.

Se va evita supraîncărcarea unui endpoint cu mai multe scopuri.

7.3.5 Cerințe privind integrarea cu alte servicii publice

Pentru simplificarea proceselor administrative, reducerea sarcinilor administrative și validarea automată a datelor furnizate de utilizatori, se vor lua în considerare integrări și/sau interogări cu alte baze de date și sisteme informatice naționale, administrate de instituții publice. Autoritatea Contractantă va realiza acordurile cu terțele-părți pe baza analizei efectuate de Prestator cu privire la datele existente în aceste sisteme și necesare pentru sistemul digital. Prestatorul va fi responsabil cu implementarea/dezvoltarea de cod pentru a realiza această integrare; numărul integrărilor va fi stabilit în faza de dezvoltare, migrare și testare și după faza de punere în producție a primelor versiuni.

Lista de instituții publice, sisteme și baze de date vizate include:

- Agenția Națională de Cadastru și Publicitate Imobiliară (ANCPI) - Sistemul integrat de cadastru și carte funciară și Registrul electronic național al nomenclaturilor stradale, prevăzute în Legea nr. 7/1996, republicată, cu modificările și completările ulterioare; – pentru interogarea datelor relevante în cazul bunurilor culturale imobile (informații legate de cartea funciară, cadastru, hărți cadastrale etc),
- Ministerul Afacerilor Interne (MAI) – pentru informații referitoare la circulația bunurilor, bunuri furate/distruse, sancțiuni,
- Ministerul Apărării Naționale (MapN) – pentru hărți, alte date și servicii,
- Ministerul Mediului, Apelor și Pădurilor (MMAP), Administrația Națională „Apele Române” (ANAR) și Institutul Național de Hidrologie și Gospodărire a Apelor (INHGA) – pentru zone Natura 2000 și Hărți de Hazard și de Risc la Inundații (HHRI),
- Ministerului Dezvoltării, Lucrărilor Publice și Administrației (MDLPA) – pentru informații din registrul clădirilor și observatorul teritorial,
- Sistemul informatic al Ministerului Finanțelor / ANAF – pentru obținerea informațiilor fiscale necesare în procesele administrative, acolo unde este cazul,
- Sistemul informatic național de plăți electronice (ghiseul.ro) – pentru facilitarea plății online a taxelor aferente serviciilor furnizate prin platformă,
- Institutul Național pentru Fizica Pământului (INFP) – pentru integrare cu informații/hărțile ce conțin riscurile seismice,
- Platforma Națională de Adaptare la Schimbările Climatice, RO-ADAPT (<https://www.roadapt.ro>),
- Direcția Generală pentru Evidența Persoanelor (DGEP) - Sistemul național informatic de evidență a persoanelor, prevăzut în Ordonanța de urgență a Guvernului nr. 97/2005 privind evidența, domiciliul, reședința și actele de identitate ale cetățenilor români, republicată, cu modificările și completările ulterioare – pentru validarea automată a datelor de identificare ale persoanelor fizice,
- Registrul central al comerțului, ținut de către Oficiul Național al Registrului Comerțului și registrele comerțului ținute de oficiile registrului comerțului organizate în fiecare județ și în municipiul București, prevăzute în Legea nr. 26/1990 privind registrul comerțului, republicată, cu modificările și completările ulterioare – pentru verificarea și preluarea datelor privind persoanele juridice (denumire, cod unic de înregistrare, statut juridic etc.)
- Platforma Națională de Interoperabilitate (PNI), Platforma de Jurnalizare și Notificare (PJN)
- Registrul Asociațiilor și Fundațiilor;

- Primării (emitere autorizație construire, PUG-uri, PUZ-uri etc),
- Baza de date a portalului instanțelor de judecată; (proces referitoare la monumente istorice, bunuri culturale),
- Registrul contribuabililor persoane fizice,
- Registrul contribuabililor persoane juridice,
- Registrul de date privind resursele minerale, perimetrele de prospecțiune, explorare, exploatare de resurse minerale,
- Alte baze de date sau registre electronice naționale relevante, în funcție de specificul fluxurilor și serviciilor digitalizate.

Componenta de e-Guvernare se va integra prin REST API cu platforma ghiseul.ro în scopul facilitării plății tarifelor asociate serviciilor furnizate de Ministerul Culturii către persoanele fizice și juridice. *Componenta de e-Guvernare* va dispune de interfețe standardizate care să permită includerea în fluxurile de lucru aferente serviciilor electronice a unui pas ce presupune efectuarea și confirmarea unei plăți electronice.

În dezvoltarea funcționalităților de e-guvernare se va avea în vedere integrarea/interoperabilitatea cu PCUe - Punctul de Contact Unic Electronic / PDURo – Portalul Digital Unic al României și publicarea serviciilor electronice în PCUe/PDURo.

7.3.6 Cerințe privind interconectarea cu Biblioteca digitală Europeană (Europeana.eu)

Componenta MPC va fi interconectată cu Biblioteca Digitală Europeană (europeana.eu) – pentru transmiterea de informații despre resursele culturale. Soluția va încărca în mod automat fișierele EDM în europeana.eu, dar va oferi și posibilitatea de descărcare a lor pentru a putea fi introduse manual în europeana.eu.

Astfel, se vor exporta metadata și linkuri în formatul curent folosit de sistem - RDF (Resource Description Framework) pentru exportul obiectelor „raw”, dar și în formatul European Data Model [EDM], folosind „European Record API” în toate cele 3 structuri documentate: JSON16, JSON-LD17, RDF/XML18.

EDM este un standard conceput pentru a facilita colectarea, organizarea și partajarea datelor culturale în format digital la nivel european. EDM permite reprezentarea complexă a obiectelor culturale, inclusiv a relațiilor dintre acestea și a meta-datelor asociate. Înainte de a trimite metadata, este esențial să fie înțelese structura și specificațiile EDM și modul în care acestea se interconectează. Documentația oficială Europeană oferă ghiduri detaliate și exemple.

Prestatorul va configura în cadrul soluției regulile de mapare, transformare și validare necesare pentru conversia datelor din modelul curent al sistemului în schema European Data Model (EDM), astfel încât datele trebuie să fie curățate, normalizate și structurate conform specificațiilor EDM. Pe baza acestor reguli, sistemul va genera

fișiere conforme cu specificația EDM și va asigura completarea și asocierea corespunzătoare a elementelor de metadate necesare exportului.

Sistemul va realiza alimentarea schemei EDM printr-un mecanism de selecție a metadatelor conform cerințelor EDM.

În cadrul procesului de interconectare, Prestatorul va configura și mecanisme de aliniere a termenilor (descriptorilor) românești utilizați în sistem la termenii relevanți din vocabularele Getty, astfel încât sistemul să poată utiliza aceste corespondențe pentru creșterea consistenței semantice și a interoperabilității datelor exportate..

7.3.7 Alte cerințe privind interoperabilitatea

Sistemul digital trebuie să permită schimbarea de informații cu alte sisteme/platforme prin folosirea de standarde open source universal recunoscute.

În acest scop, pentru datele modelate conform ontologiei implementate, sistemul va permite și schimbul de informații în formate RDF standard, pe baza regulilor de mapare și a structurilor semantice configurate în cadrul soluției.

Prestatorul va face un număr de maxim 50 implementări cu instituțiile/organizațiile cu care Autoritatea Contractantă va decide conectarea în perioada de implementare a contractului.

Sistemul va cuprinde un API configurat pentru a furniza diverse informații de interes public (statistici, diverse informații publice legate de serviciul de e-guvernare.). Lista informațiilor puse la dispoziție prin API se va decide în faza de analiză, faza de dezvoltare, migrare și testare și după faza de punere în producție a primelor versiuni.

Sistemul va cuprinde un API configurat pentru administrare cu scopul de a facilita împrumuturile inter-bibliotecare sau inter-muzeale, dar și de a ușura munca utilizatorilor autorizați prin oferirea posibilității conectării sistemului de gestiune a acestuia la platformă.

Sistemul va cuprinde un API configurat pentru conectarea cu data.gov.ro și data.europa.eu și pentru furnizarea de seturi de date în format deschis pentru aceste platforme.

7.4 Inteligență artificială

Componenta de inteligență artificială constituie o parte transversală a sistemului digital ePatrimoniu, menită să valorifice volumele mari de date administrative, culturale și geografice gestionate de MC și instituțiile subordonate, prin aplicarea unor tehnologii avansate de analiză automată, procesare a limbajului natural (NLP), învățare automată și analiză predictivă.

Această componentă va sprijini atât procesele administrative curente (e-guvernare), cât și activitățile de analiză strategică și suport decizional necesare fundamentării

politicilor publice în domeniul patrimoniului cultural. Sistemele dezvoltate vor respecta cerințele *Regulamentului (UE) 2024/1689 al Parlamentului European și al Consiliului din 13 iunie 2024 de stabilire a unor norme armonizate privind inteligența artificială* (AI Act), principiile „AI de încredere” (implicare și supraveghere umană; robustețe tehnică și siguranță; respectarea vieții private și guvernanta datelor; transparență; diversitate, nediscriminare și echitate; bunăstare societală și de mediu; responsabilizare) și prevederile aplicabile privind protecția datelor personale (GDPR).

Sistemul de inteligență artificială va utiliza o arhitectură de tip Retrieval-Augmented Generation (RAG) pentru a asigura fundamentarea răspunsurilor generate în principal pe datele încărcate în baza de cunoștințe a sistemului, precum documente, metadate și ontologiile specifice patrimoniului cultural. Prestatorul va livra un sistem complet funcțional, bazat pe modele preantrenate, pe care le va integra, configura și adapta cerințelor funcționale și lingvistice ale platformei. Sistemul va putea utiliza, pe lângă datele furnizate de Autoritatea Contractantă, și alte resurse, precum corpusuri lingvistice, date publice sau modele preexistente, pentru a crește acuratețea răspunsurilor și a susține generarea de rezultate verificabile.

Prestatorul va realiza procesul de configurare, testare, validare și optimizare a soluției, inclusiv implementarea și ajustarea parametrilor de funcționare și a mecanismelor RAG. Autoritatea Contractantă va primi documentația aferentă implementării sistemului, incluzând arhitectura soluției, metodologia de configurare și integrare, sursele de date furnizate de Autoritatea Contractantă utilizate în procesul de retrieval, parametrii relevanți de configurare și rezultatele evaluării performanței.

Prestatorul își asumă responsabilitatea integrală pentru corectitudinea, acuratețea și conformitatea răspunsurilor generate de sistemul AI, inclusiv pentru adaptarea acestora în funcție de complexitatea și profilul utilizatorului. Prestatorul va asigura implementarea unui proces riguros de validare, testare și monitorizare continuă a calității răspunsurilor, precum și mecanisme eficiente de corectare și actualizare a conținutului furnizat.

7.4.1 Funcționalități de sprijin pentru e-guvernare și procese administrative

Prestatorul va proiecta și implementa funcționalități bazate pe AI care să contribuie la automatizarea și eficientizarea fluxurilor de lucru interne și la creșterea calității serviciilor electronice oferite publicului, asigurând cel puțin următoarele:

7.4.1.1 Extracție automată de date din documente scanate

Această funcționalitate are ca obiectiv implementarea unui mecanism automatizat de identificare, recunoaștere și extragere a informațiilor textuale din documente fizice scanate cu diferite grade de structuralitate (nestructurate, parțial structurate) ca de exemplu documente, fișe, formulare, manuscrise, corespondență.

Soluția va utiliza tehnologii de recunoaștere optică a caracterelor (OCR) pentru conversia conținutului grafic în text digital, precum și metode de procesare a limbajului natural (NLP) pentru interpretarea și structurarea conținutului extras. De asemenea, soluția va include capabilități de **HTR (Handwritten Text Recognition)** pentru procesarea manuscriselor și a documentelor completate olograf (ex: fișe de inventar vechi, registre, corespondență).

Rezultatul procesării va consta în text digitalizat și metadate asociate (de exemplu: titlu, autor, dată, locație, tip de document, cuvinte-cheie, entități denumite etc.), care vor fi stocate în sistemul ePatrimoniu și asociate resurselor digitale corespunzătoare. De asemenea, sistemul va permite preluarea informațiilor relevante identificate în conținutul documentelor, în vederea completării automate sau semiautomate a câmpurilor predefinite din aplicație (de exemplu, extragerea automată a numelui, adresei, datei sau altor date din formulare vechi). Această funcționalitate are rolul de a reduce volumul de muncă manuală al personalului implicat, de a crește acuratețea datelor introduse și de a accelera procesele de digitizare și actualizare a bazelor de date instituționale.

Suplimentar față de recunoașterea textului, soluția va implementa module avansate de **Analiză a Layout-ului (Document Layout Analysis)** capabile să identifice automat structura complexă a paginilor, inclusiv tabele, semnături, ștampile, adnotări marginale și fotografii atașate. În cazul tabelelor, sistemul trebuie să garanteze păstrarea relației logice între rânduri și coloane, asigurând o mapare semantică corectă în baza de date.

Implementarea acestei componente are drept scop îmbunătățirea calității și accesibilității informației, facilitând căutarea, indexarea și valorificarea digitală a resurselor culturale.

7.4.1.2 Asistent conversațional intern (chatbot instituțional), destinat sprijinirii personalului în activitățile zilnice, care va răspunde la întrebări referitoare la proceduri, legislație, norme interne, stadiul documentelor sau instrucțiuni de utilizare a sistemelor informatice, integrându-se cu knowledgebase și aplicațiile existente.

Exemple de funcționalități:

- Oferirea de ghidaje și instrucțiuni pentru personalul care utilizează sistemele informatice din cadrul proiectului ePatrimoniu ex. "Cum încarc informațiile despre o resursă culturală în sistemul ePatrimoniu?"
- Asistentul ar putea oferi acces rapid la arhivele istorice, localizare sau documentele specifice din cadrul ministerului pentru cercetători sau angajați, evitând astfel căutările manuale în baze de date voluminoase ex. "Unde pot găsi documentația originală privind restaurarea monumentului X?"

7.4.1.3 Asistent conversațional public (chatbot public), care va oferi sprijin interactiv în navigarea serviciilor electronice.

Modulul de chatbot va avea rolul de a asista utilizatorii platformei ePatrimoniu în navigarea sistemului și completarea formularelor web, oferind răspunsuri contextuale, ghidare în timp real și suport proactiv. Integrarea nativă în interfața aplicației va permite reducerea erorilor de completare și a timpului necesar desfășurării proceselor administrative.

Asistentul virtual va fi programat să desfășoare conversații într-un mod cât mai apropiat de comportamentul uman, utilizând tehnologii moderne de procesare, înțelegere și generare a limbajului natural (NLP, NLU, NLG), cu scopul de a livra o experiență conversațională coerentă, precisă și adaptivă.

Modulul chatbot va îndeplini următoarele cerințe tehnice minime:

- funcționare exclusivă on-premise, fără dependențe de servicii externe;
- capacitatea de a răspunde unui set extins de întrebări predefinite și dinamice dintr-o bază de date de tip knowledgebase implementată ca Vector Store;
- persistență a sesiunii de chat la schimbarea paginii, tab-ului sau ferestrei;
- suport conversațional complet pentru limbile: română și engleză;
- suport pentru cel puțin 100 sesiuni concurente online;
- proiectat pentru scalare, astfel încât să poată susține creșterea numărului de sesiuni simultane și a volumului de procesare, în funcție de extinderile viitoare ale infrastructurii.

Knowledgebase și gestiune dinamică:

- Baza de date cu întrebări și răspunsuri va fi definită central, la nivelul modulului de administrare.
- Aceasta va fi gestionată dinamic, printr-un flux de aprobare în mai multe etape: solicitare modificare, validare conținut, solicitare punct de vedere, aprobare finală și publicare;
- Actualizarea bazei de date va genera modificări automate în chatbot și în sistem, prin API-uri sau mecanisme M2M (machine-to-machine);
- Sistemul va genera rapoarte de utilizare și performanță, inclusiv: cele mai frecvente întrebări, timpi de răspuns minim/mediu/maxim, evaluări de satisfacție, etc.;
- Răspunsurile pot conține text, imagini, linkuri interne și externe.
- Oferă prompt-uri succinte de:
 - 1-100 cuvinte (Întrebări Simple). Pentru întrebări directe care necesită o explicație scurtă sau informații succinte;

- 100-300 cuvinte (Întrebări Moderat de Complexe). Pentru întrebări care au nevoie de puțin mai multe detalii și context, dar sunt încă relativ directe;
- 300-500 cuvinte (Întrebări Complexe sau Detaliat). Pentru subiecte care necesită explicații detaliate, perspective multiple sau context extins;
- prompt-urile vor fi adaptate și nivelului de complexitate logică.
- Detecția automată a limbajului licențios va închide conversația și/sau va afișa un mesaj generic care îndeamnă la reformularea întrebării într-un limbaj adecvat. Modulul va menține un ton politicos, neutru și empatic, indiferent de conținutul sau tonul mesajelor primite de la utilizator.
- Chatbot-ul va păstra și utiliza contextul conversației pe durata sesiunii active pentru a genera răspunsuri relevante și coerente.
- Contextul reținut va include informații esențiale din prompturile și răspunsurile anterioare, evitând repetările inutile.
- Chatbot-ul va permite direcționarea către submodulul de raportare probleme, în cazul în care întrebarea nu poate fi soluționată automat.

Funcționalități pentru utilizatori:

- Autentificarea în sistemul ePatrimoniu implică și autentificarea automată în chat, în mod securizat;
- Utilizatorii logați pot:
 - vizualiza istoricul complet al conversațiilor;
 - închide manual o conversație;
- La scrierea unei întrebări, sistemul va afișa completări automate în funcție de conținutul deja configurat în sistem.

7.4.1.4 Sistem de recomandare a resurselor similare bazat pe algoritmi de inteligență artificială explicabili cu următoarele cerințe:

- prezintă primele 3 resurse cele mai apropiate de cea afișată curent;
- resursele sunt afișate în sistem top 3 în baza unor criterii precum: cele mai relevante rezultat, cele mai populare resurse similare, cele mai vizualizate resurse similare;
- algoritmi vor oferi un scor de similitudine și vor pune la dispoziția utilizatorului explicația privind cum a fost compus acest scor;
- pe lângă cele mai similare 3 resurse, sistemul poate sugera și o opțiune de explorare surpriză („descoperă și alt stil / altă regiune”);
- recomandările trebuie generate într-un interval de timp rezonabil pentru a nu întrerupe experiența utilizatorului; intervalul de timp rezonabil va fi stabilit în faza de analiza.

- recomandările vor fi calculate pe baza mai multor tipuri de similitudine (stil arhitectural, epocă, locație, comportament utilizatori etc.) și vor afișa un scor detaliat, inclusiv explicații vizuale privind factorii care au contribuit la scor;
- sistemul de recomandare să se bazeze pe ontologia patrimoniului (ex. CIDOC-CRM, European Data Model).

7.4.1.5 Sistem speech to text pentru transcrierea automată a fișierelor audio încărcate care:

- folosește biblioteci de machine learning, modele și motoare de speech to text de tip open-source disponibile offline și on-premise (ex. DeepSpeech, Tensorflow, Kaldi, Whisper sau echivalent);
- oferă o similaritate de cel puțin 95% între conținutul audio și cel text;
- permite simultan online cel puțin 10 de sesiuni;
- proiectat pentru scalare, astfel încât să poată susține creșterea numărului de sesiuni simultane și a volumului de procesare, în funcție de extinderile viitoare ale infrastructurii;
- are capabilități de detecție și deduplicare pentru fișiere deja încărcate. Deduplicarea este validată de utilizator și aprobată de administrator înainte de ștergerea fișierului încărcat;
- are suport minim pentru următoarele limbi: română, engleză;
- acceptă cel puțin fișiere de tip mp3, flac, aac, ...". Lista completă se va stabili în faza de analiză, respectiv în implementare;
- după transcriere, sistemul oferă sugestii de corecții automate (spell-check, grammar-check).

7.4.1.6 Sistem text to speech pentru crearea automată a versiunilor audio ale textelor

- folosește motoare de text to speech de tip open-source disponibile offline și on-premise (ex. coqui TTS, Mozilla TTS sau echivalent);
- oferă o similaritate de cel puțin 95% între conținutul text și cel audio;
- permite simultan online cel puțin 10 sesiuni;
- proiectat pentru scalare, astfel încât să poată susține creșterea numărului de sesiuni simultane și a volumului de procesare, în funcție de extinderile viitoare ale infrastructurii;
- permite citirea paginilor afișate către utilizator;
- are suport minim pentru următoarele limbi: română, engleză,
- acceptă fișiere de tip txt, docx, odt, pdf. Lista completă se va stabili în faza de analiză, respectiv în faza de dezvoltare.

7.4.1.7 Traducerea automată a conținutului între mai multe limbi

- folosește motoare LLM de traducere automată de tip open-source disponibile offline și on-premise (ex. variante Mistral AI, Phi-2, Eagle 7B, Gemma sau echivalent);
- are suport minim pentru următoarele limbi: română, engleză, germană, franceză. Lista completă se va stabili în faza de analiză, respectiv în faza de dezvoltare;
- permite simultan online cel puțin 100 sesiuni;
- proiectată pentru scalare, astfel încât să poată susține creșterea numărului de sesiuni simultane și a volumului de procesare, în funcție de extinderile viitoare ale infrastructurii;
- glosar controlat (exemplu: stiluri arhitecturale) cu reguli de înghețare a termenilor (nu se traduc anumite nume proprii);
- panou de feedback pe pagini: „Propune corectura” legat la glosar

7.4.1.8 Image to Text pentru extragerea textului din obiectele digitale

- funcționare exclusivă on-premise, fără dependențe de servicii externe;
- să extragă textul din imagini pentru a fi stocat ulterior ca metadate asociate acelui obiect;
- permite simultan online cel puțin 50 de sesiuni;
- proiectat pentru scalare, astfel încât să poată susține creșterea numărului de sesiuni simultane și a volumului de procesare, în funcție de extinderile viitoare ale infrastructurii;
- acceptă fișiere de tip png, jpg, etc. Lista completă a tipurilor de fișiere/formatelor acceptate se va stabili în faza de analiză, respectiv în faza de implementare.

7.4.2 Cerințe generale de conformitate și interoperabilitate

- Se va implementa un mecanism de guvernare AI, incluzând evidența modelelor și datelor utilizate, versiuni, performanțe și audituri de conformitate, conform cerințelor AI Act;
- Arhitectura va permite scalabilitate și reutilizare, pentru extinderea ulterioară către noi domenii de analiză și alte instituții publice din ecosistemul guvernamental digital.

7.4.3 Considerente de implementare

Sistemul de inteligență artificială va utiliza modele preantrenate open-source, adaptate nevoilor Autoritatea Contractantă prin mecanisme de generare a răspunsurilor pe baza recuperării și utilizării controlate a informațiilor din bazele de cunoștințe, configurare comportamentală, reguli de utilizare și, după caz, fine-tuning controlat. Sistemul nu va fi antrenat de la zero, ci va valorifica modele existente, validate și utilizate pe scară largă, pentru a asigura eficiență, robustețe și sustenabilitate pe termen lung.

În acest sens, Prestatorul va implementa o **bază de date vectorială (Vector Store)** pentru indexarea semantică a resurselor, permițând AI-ului să furnizeze referințe precise către documentele sursă pentru fiecare răspuns generat.

Aceasta va presupune:

- **Vectorizarea datelor:** Transformarea metadatelor, a textelor din ontologie și a documentelor de referință în embeddings stocate într-o bază de date vectorială (ex: pgvector, Milvus sau similar).
- **Recuperarea Contextului (Retrieval):** La fiecare cerere de generare, sistemul va identifica și va furniza modelului LLM fragmentele de informație relevante și verificate din baza de date ePatrimoniu.
- **Generare Constrânsă:** Modelul LLM va fi configurat să genereze textul **exclusiv** pe baza contextului recuperat, refuzând să furnizeze informații care nu se regăsesc în sursele oficiale

Componenta de stocare vectorială (Vector Store) va suporta:

- stocarea unui număr de vectori (embeddings) adaptat la volumul de date necesar platformei (minim 10.000.000), cu dimensiuni de până la 1536 dimensiuni per vector, asigurând căutări rapide și scalabilitate pentru creșterea datelor și complexitatea interogărilor;
- indexare ANN, utilizând algoritmi ce garantează căutări rapide, cu latență de sub o secundă;
- executarea de interogări hibride, permițând filtrarea simultană pe baza similarității vectoriale și a metadatelor scalare;
- interoperabilitate cu sistemul RAG.

Interfețele platformei ePatrimoniu ce vor beneficia de funcționalitățile de inteligență artificială vor consuma serviciile AI exclusiv prin API-uri, fără a permite modificarea directă a modelelor, regulilor sau bazei de cunoștințe. Administrarea modului se va face din submodulul dedicat, parte a modului de administrare detaliat în capitolul 7.1.2.

Autoritatea Contractantă va putea menține și îmbunătăți sistemul AI pe toată durata de viață a sistemului digital prin intermediul interfeței dedicate, în special prin:

- actualizarea bazei de cunoștințe;

- validarea feedback-ului utilizatorilor;
- ajustarea regulilor și comportamentului AI.

7.4.4 Indicatori de Performanță AI

Componentele de AI vor fi supuse următoarelor praguri de performanță (KPI), a căror monitorizare va fi disponibilă în secțiunea *Audit și Jurnalizare și Gestionare model AI* din Dashboard-ul Intern:

- **Acuratețe factuală (RAG):** Min. 95% (măsurată prin compararea răspunsului generat cu sursa din Knowledge Base).
- **Timp de răspuns (Latență):** < 3 secunde pentru prima interacțiune a Chatbot-ului.
- **Rata de respingere a întrebărilor out-of-scope:** 100% (sistemul nu trebuie să răspundă la întrebări care nu sunt legate de patrimoniul cultural).

7.5 Securitate și confidențialitate

Scopul formulării cerințelor de securitate este de a defini cadrul general prin care se asigură confidențialitatea, integritatea, disponibilitatea datelor și sistemelor informatice și de comunicații destinate operaționalizării sistemului digital ePatrimoniu. Acest obiectiv se realizează de către Prestator prin implementarea unor măsuri adecvate, încă din faza de proiectare, în conformitate cu cerințele legale aplicabile (inclusiv dar fără a se limita la Regulamentul (UE) 2016/679 (GDPR), Legea nr. 190/2018, Directiva (UE) 2022/2555 (NIS2) și legislația națională de transpunere a acesteia; Regulamentul (UE) 2019/881 – Cybersecurity Act), și cu cele mai bune practici recunoscute în domeniul securității cibernetice (ex: familia de standarde ISO27K, OWASP, NIST SP, CIS sau ghiduri ENISA). Astfel:

- Prestatorul trebuie să furnizeze dovezi despre politica sa internă de securitate care asigură securitatea și reziliența serviciilor oferite pentru implementarea sistemului digital. **Înțelegerea adecvată a cadrului legal de conformitate necesar sistemului digital va fi asigurată prin certificarea ISO 27001 a Prestatorului sau un standard internațional echivalent privind managementul securității informațiilor, emis de un organism de certificare acreditat.**
- Controlul accesului la rețele și sisteme trebuie să fie implementat și controlat riguros, cu identificare, autentificare și segregare a drepturilor.

7.5.1 Controale de securitate

Sistemul digital trebuie să asigure mecanisme robuste pentru autentificare, autorizare și control al responsabilităților, asigurând confidențialitatea, integritatea,

disponibilitatea datelor și non-repudierea acțiunilor, precum și trasabilitate și mecanisme de audit. Arhitectura trebuie să fie flexibilă și să permită eliminarea sau atenuarea riscurilor identificate, să implementeze principiile de protecție a datelor și securitate prin concepție (privacy & security by design) și pe întreg ciclul de viață a sistemului digital.

Sistemul va include mecanisme și controale pentru asigurarea următoarelor **principii fundamentale de securitate a informațiilor**:

- Confidențialitatea – asigurarea faptului că datele sunt accesibile, vizibile sau disponibile numai utilizatorilor autorizați, atât în cazul datelor stocate, cât și al celor care tranzitează sistemul;
- Integritatea – asigurarea faptului că datele nu pot fi modificate, alterate sau distruse în mod neautorizat și că acestea își păstrează acuratețea și completitudinea;
- Disponibilitatea – asigurarea faptului că resursele sistemului digital sunt accesibile și utilizabile, la cerere, de către personalul autorizat, în momentul în care acestea sunt necesare;
- Autentificarea și autorizarea – asigurarea faptului că un utilizator sau o entitate demonstrează identitatea proprie și dreptul de a accesa anumite resurse ale sistemului;
- Non-repudierea – asigurarea faptului că sunt implementate mecanisme care previn negarea ulterioară a unei acțiuni efectuate în cadrul sistemului digital, asigurând dovada originii și a integrității datelor transmise sau modificate;
- Trasabilitatea – asigurarea faptului că sunt implementate mecanismele care permit monitorizarea, înregistrarea și corelarea tuturor acțiunilor efectuate de utilizatori sau de componentele sistemului, în scopul auditului, analizei incidentelor și erorilor și asigurării responsabilității (accountability).

Sistemul digital va fi conceput și dezvoltat astfel încât să asigure și:

- **Protecția datelor în tranzit și în repaus**, utilizând protocoale moderne de criptare și algoritmi de hashing acolo unde este necesar,
- **Aplicarea principiului privilegiului minim**, conform căruia utilizatorii, procesele și sistemele trebuie să aibă doar accesul strict necesar pentru îndeplinirea atribuțiilor sau funcțiilor specifice alocate, pe baza “nevoii de a cunoaște”, pentru a reduce riscurile de compromitere;
- **Aplicarea principiului segregării responsabilităților**, conform căruia niciun utilizator, proces sau sistem nu va deține control complet asupra unui flux critic care ar putea afecta oricare dintre principiile securității cibernetice enumerate mai sus sau cerințe ale fluxurilor implementate;
- **Managementul vulnerabilităților și a actualizărilor de securitate**, constând în implementarea de mecanisme, pentru actualizarea periodică a

componentelor software (patch-uri) și pentru gestionarea vulnerabilităților, în vederea menținerii unui nivel adecvat de protecție; Se va avea în vedere managementul efectiv al patch-urilor și vulnerabilităților și controlul responsabil asupra schimbărilor (change management) așa cum este definit acesta în controlul A8.32 din ISO 27001. Prestatorul trebuie să asigure Autoritatea Contractantă că aplicațiile software utilizate în cadrul Sistemului Digital sunt actualizate la zi, beneficiază de suport tehnic, au actualizările automate activate acolo unde este posibil sau, în caz contrar, sunt actualizate manual ori de câte ori este necesar (de exemplu, în cazul vulnerabilităților critice de securitate) pe întreaga durată a contractului, inclusiv în perioada mentenanței și a garanției.

- **Asigurarea continuității operaționale și recuperarea în caz de dezastru**, care implică pe lângă existența unui backup al datelor și al sistemelor critice complet, testat și funcțional și elaborarea unui plan/procedură (recovery plan) care să permită menținerea funcționării și în situații neprevăzute (ex. întreruperi de alimentare, atacuri cibernetice, dezastru naturale) și reluarea rapidă a activităților în condiții de siguranță, cu pierderi minime de date sau funcționalitate.

Sistemul digital trebuie să îndeplinească și **următoarele cerințe**:

- să fie livrat cu o configurație securizată implicită, inclusiv cu posibilitatea de a reseta produsul la starea sa inițială, însă fără a șterge datele aplicației;
- să asigure protecția împotriva accesului neautorizat prin mecanisme de control adecvate, inclusiv, dar fără a se limita la sistemele: de autentificare, de gestionare a identității sau a accesului;
- să protejeze integritatea datelor, a comenzilor, a programelor și a configurației împotriva oricărei manipulări sau modificări neautorizate și să semnaleze și să blocheze fișierele corupte;
- să protejeze disponibilitatea funcțiilor esențiale, inclusiv reziliența împotriva atacurilor care vizează blocarea accesului la servicii (inclusiv atacuri de tip Denial of Service);
- să își reducă la minimum propriul impact negativ asupra disponibilității serviciilor furnizate de alte dispozitive sau rețele;
- să fie proiectat, dezvoltat și implementat astfel încât să reducă suprafața (inclusiv interfețele externe) și vectorii de atac;
- să fie proiectat, dezvoltat și implementat astfel încât să reducă probabilitatea unui incident prin utilizarea de mecanisme și tehnici adecvate de prevenire a exploatarei vulnerabilităților;
- serviciile și porturile de comunicație folosite vor fi documentate într-o listă a serviciilor utilizate. Serviciile și porturile neutilizate vor fi dezactivate;

- să furnizeze jurnalizarea evenimentelor - informații legate de securitate, erori, anomalii prin înregistrarea și/sau monitorizarea activității interne relevante, inclusiv accesul la date, servicii sau funcții sau modificarea acestora;

Mecanismele de transfer menite să faciliteze schimburile de informații între sistemul digital și alte sisteme trebuie să fie:

- înregistrate și verificate, astfel încât atât expeditorul, cât și destinatarul să fie identificați și autentificați prin mecanisme și proceduri adecvate;
- criptate, astfel încât să asigure confidențialitatea datelor tranzitate;
- marcate temporal, pentru a indica ora exactă a transferului documentelor electronice și a accesului;
- jurnalizate, pentru arhivarea înregistrărilor electronice în scopul de a se conserva o dovadă cu valoare juridică.

Sistemul digital trebuie să fie protejat împotriva **încercărilor deliberate sau accidentale de acces neautorizat la datele** pe care acesta le înmagazinează. Astfel, sistemul trebuie să asigure și următoarele cerințe:

- securitatea datelor printr-un sistem de control al accesului bazat pe drepturi (roluri) și credențiale unice, defalcat pe mai multe niveluri de acces și securitate. Drepturile de acces ale utilizatorilor vor putea fi configurate din interfața aplicației de utilizatorii cu privilegii administrative;
- împiedicarea utilizatorilor de a se conecta la sistem dacă acesta este în stare de eroare sau mentenanță;
- închiderea automată a sesiunilor de lucru ale utilizatorilor în caz de inactivitate pe o anumită durată predeterminată de timp, stabilită în faza de analiză;
- jurnalizarea operațiilor zilnice, individual pentru fiecare utilizator, cu marcarea orei la care a fost executată fiecare operație, a tipului operației, a adresei IP, precum și a identității utilizatorului care a inițiat-o;
- jurnalizarea evenimentelor semnificative legate de controlul accesului:
 - înregistrarea în jurnal a autentificărilor cu succes și a autentificărilor fără succes (dată, oră, adresa IP);
 - jurnalele vor fi disponibile în aplicație pentru vizualizare de către administratorii sistemului.
- detecția și raportarea tentativelor de acces neautorizat și generarea de alerte către administratorii de securitate.
- autentificarea utilizatorilor trebuie să se poată realiza printr-o soluție centralizată și să permită integrarea cu alte soluții externe de identitate și autentificare (de exemplu, SAML, OAuth2, OpenID Connect).

- cerințele referitoare la definirea identităților și rolurilor, nivelul de complexitate al mecanismelor de autentificare, precum și timpul de propagare a eliminării drepturilor de acces sunt stabilite prin politicile de securitate aplicabile infrastructurii de bază și sunt implementate prin sistemul Identity and Access Management (IAM). Aceste politici sunt definite de Prestator în faza de analiză și sunt aprobate de Autoritatea Contractantă;
- stabilirea unei sesiuni de lucru va consta în operațiunea de autentificare (login) a utilizatorului curent;
- autentificarea unică a utilizatorilor și autorizarea acestora se vor realiza o singură dată pe sesiune, prin mecanisme de tip Single Sign On (SSO), prin intermediul rolurilor și privilegiilor;
- autentificarea și asocierea permisiunilor / privilegiilor funcție de rolurile prestabilite vor fi realizate cu ajutorul unor instrumente specializate (ex. Identity and Access Management (IAM));
- nu se va permite accesul neautentificat la date și informații (mai puțin secțiunea publică a sistemului). Orice acces în aplicație, atât la nivelul utilizatorilor cât și la nivelul altor module de aplicație, este precedat de identificarea, autentificarea și autorizarea accesului;
- vizualizarea istoricului complet al activității pe fiecare cont cu posibilitatea filtrării tranzacțiilor după anumite criterii:
 - perioadă de timp;
 - tip de acțiune;
 - dispozitiv folosit;
 - locație (dacă este disponibilă).
- istoricul activităților, cu toate detaliile aferente, va fi păstrat pe termen lung într-o aplicație specializată de tip log management, pentru a permite analize corelate și activități de audit și investigare. Se vor avea în vedere în mod special detaliile de audit pe operațiunile de avizare/semnare, mai ales cea calificată (unde și acestea trebuie să fie semnate calificat). Jurnalul de acces și de activitate va fi filtrabil în raport cu scopuri determinate, explicite și legitime, precum securitatea sistemului, investigarea incidentelor, auditul și asigurarea trasabilității. Categoriile de date jurnalizate, persoanele care au acces la acestea, termenele de păstrare și regulile de extragere, consultare și reutilizare vor fi stabilite prin politici interne documentate, cu respectarea principiilor reducerii la minimum a datelor, limitării stocării și accesului strict pe baza necesității de a cunoaște. Datele din jurnale nu vor fi utilizate în scopuri incompatibile cu cele pentru care au fost colectate.

- Eliminarea și dezactivarea privilegiilor speciale de acces atunci când nu mai sunt necesare (ex. când un membru al echipei Prestatorului este înlocuit)
- Prestatorul va utiliza conturi separate pentru a efectua activități administrative (fără e-mail-uri, navigare pe web sau alte activități standard care pot expune privilegiile administrative la riscuri cibernetice)
- Nu se vor utiliza conturi generice precum "Admin", "Tester", "GlobalAdmin".

Securitatea de perimetru va fi asigurată prin infrastructura centrului de date STS, astfel:

- prin implementarea segmentelor de rețea, a unui sistem de tip firewall care va proteja rețeaua internă de trafic nedorit. Astfel, acest sistem va bloca traficul care vine dinspre Internet și care nu se supune politicii aplicate (atacuri din Internet, scanări, exploatare vulnerabilități cunoscute), dar va bloca și traficul utilizatorilor interni care nu va fi acceptat de politică internă (de exemplu utilizatorii interni nu pot avea acces direct pe baza de date);
- prin implementarea unor echipamente/ soluții software ce permit detectarea/ prevenirea intruziunilor;
- securitate la nivelul tuturor resurselor IT - prin instalarea unei soluții sau a mai multor soluții de software antivirus / anti-malware / anti-wiper / anti-locker care va proteja toate resursele ce alcătuiesc sistemul informatic; Prestatorul trebuie să dea asigurări Autorității Contractante că pe toate sistemele informatice și dispozitivele folosite pentru dezvoltarea Sistemului Digital are instalat, este activ și actualizat un mecanism de protecție împotriva programelor malware;
- implementare VPN - altor instituții / administrații locale li se va permite accesul la infrastructura ce susține sistemul digital numai prin tehnologii de tip VPN (canale de comunicații criptate care asigură confidențialitatea datelor manipulate) ce necesită MFA.

La nivel de integrare, sistemul digital va asigura funcționalitățile de protecție menționate pentru toate mediile virtuale în care sunt inițializate aplicațiile web, cu posibilitatea scalării.

Sistemul digital ePatrimoniu și componentele acestuia se vor instala și configura numai pe sisteme care au aplicat ultimele patch-uri de securitate. Aceste patch-uri vor fi actualizate pe toată perioada contractului, și în perioada de garanție, dar acest proces va fi monitorizat pentru a nu genera incompatibilități sau downtime. Patch-urile trebuie testate în mediul de test înainte de a fi implementate în producție.

Prin implementarea *Politicii de securitate a sistemului digital, care va fi definită de Prestator (după analiza riscurilor) dar aprobată de Autoritatea Contractantă*, parolele folosite pentru tipurile de conturi care au acces la datele cu caracter personal, vor fi conforme cu cele mai bune practici din prezent, cu o entropie mai mare de 60 biți.

De asemenea, soluția va permite actualizarea semnăturilor și a patch-urilor de securitate în mediu on-premises, prin descărcarea acestora din surse oficiale ale producătorului și instalarea lor locală.

În cadrul componentelor aplicative ale sistemului digital, se vor avea în vedere următoarele cerințe generale privind securitatea și integritatea datelor:

- Implementarea unor mecanisme robuste de validare a fișierelor încărcate (ex: antivirus, sandbox, validare semnături digitale, monitorizare și alertare, carantină până la validare etc.), astfel încât aplicația să permită exclusiv tipurile de fișiere aprobate prin specificațiile tehnice. Validarea va include, fără a se limita la, verificarea extensiei fișierului, a tipului MIME (media type) și a semnăturii binare (magic numbers), în vederea prevenirii încărcării de fișiere neconforme sau potențial periculoase.
- Implementarea unor mecanisme complete de validare a datelor introduse de utilizatori, aplicabile tuturor formularelor și punctelor de introducere a datelor din cadrul aplicației, pentru a preveni transmiterea de conținut malițios (de tip injecții de cod, comenzi neautorizate, scripturi etc.), precum și introducerea de date care depășesc dimensiunile sau formatele acceptate. Validarea va include atât controale sintactice, cât și semantice, în conformitate cu bunele practici de securitate aplicațională.

Aceste mecanisme de validare trebuie implementate la nivelul întregii arhitecturi aplicaționale, inclusiv la nivelul serviciilor și interfețelor de tip REST API, nu doar la nivelul interfeței web (front-end), astfel încât să fie asigurată o protecție unitară și coerentă a sistemului împotriva accesului sau utilizării neautorizate, indiferent de modalitatea de interacțiune cu aplicația.

Orice mecanism de hashing sau criptare folosit pentru parole, date sensibile, integritate sau comunicații va fi implementat utilizând algoritmi considerați siguri și eficienți și va respecta standardele actuale de securitate cibernetică, în conformitate cu bunele practici publicate de organizații de referință, cum este OWASP.

Interfețele Web și porturile de administrare aferente acestora, deserving sistemul digital nu vor fi expuse în rețele publice (inclusiv rețeaua Internet). Accesul la aceste interfețe de administrare va fi permis doar dintr-un segment de rețea controlat prin whitelisting-ul adreselor IP. Protecția traficului HTTP și HTTPS către aplicațiile web se va realiza printr-o soluție de tip Web Application Firewall (WAF), care va detecta și bloca traficul malițios, inclusiv SQL Injection, Cross-Site Scripting (XSS), Command Injection, Brute Force, URL Fuzzing și alte atacuri specifice aplicațiilor web (referință: OWASP Top 10 și/sau MITRE CWE Top 25). Soluția va permite utilizarea regulilor predefinite și crearea de politici personalizate, aplicând principiul „deny all, allow only known good”. WAF-ul va opera la nivel Layer 7 (aplicație) și va asigura protecția traficului către servere și API-uri.

Înainte de punerile în producție Prestatorul va realiza testări de securitate pentru a se identifica și elimina orice vulnerabilitate care ar putea afecta sistemul. Testele vor

respecta cel puțin metodologiile OSSTM (Open Source Security Testing Methodology) sau OWASP (Open Web Applications Security Project). Rapartele finale de testare de securitate rezultate vor cuprinde vulnerabilitățile existente în cadrul sistemului și componentelor acestuia și vor fi structurate astfel:

- Sumar Executiv;
- Obiectivele și scopul evaluării;
- Prezentare succintă a metodologiei utilizate;
- Descrierea contextului în care s-a desfășurat evaluarea;
- Lista testelor de securitate / simulări ale unor atacuri cibernetice efectuate.

Prezentarea individuală a vulnerabilităților descoperite după cum urmează:

- Descrierea vulnerabilității;
- Catalogarea vulnerabilității;
- Descrierea tehnică;
- Analiza severității și probabilității;
- Calcularea riscului;
- Contramăsuri recomandate pentru remediere;
- Alte detalii și recomandări.

Scanarea de vulnerabilitati se va realiza prin utilizarea de aplicații dedicate și actualizate la momentul realizării scanărilor. În acest sens se vor utiliza aplicații care să conțină baze de date de vulnerabilități la nivel de rețea, sisteme de operare, aplicații/servicii, care, pe de-o parte, trebuie să permită auditarea activităților realizate astfel încât să poată fi demonstrată efectuarea acestor activități și, pe de altă parte, să conțină baze de date actualizate cu exploit-uri (coduri care demonstrează că o vulnerabilitate poate fi exploatată însă fără ca sistemul să fie propriu-zis compromis).

Prestatorul are obligația tratării cu celeritate a tuturor vulnerabilități identificate de auditul extern sau de către STS.

Prestatorul are obligația testării securității pe întreg ciclul de viață de dezvoltare și punere în producție al sistemului digital.

7.5.2 Confidențialitatea și protecția datelor cu caracter personal

Implementarea și operarea sistemului digital se va realiza cu respectarea integrală a legislației naționale și europene aplicabile în materie de protecție a datelor cu caracter personal și a vieții private, inclusiv a dispozițiilor Regulamentului (UE) 2016/679 (GDPR) și a legislației subsecvente. Măsurile din OUG nr. 155/2024, aprobată și modificată prin Legea nr. 124/2025 și legislația subsecventă acestor acte normative care transpun în legislația națională Directiva (UE) 2022/2555 (NIS 2) privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, vor fi aplicate și pentru asigurarea protecția datelor cu caracter personal.

Sistemul digital va include funcționalități tehnice care să permită punerea în aplicare, după analiza juridică a fiecărei solicitări, a drepturilor persoanelor vizate, inclusiv a

dreptului la ștergere și, după caz, a măsurilor de anonimizare, restricționare sau arhivare, în condițiile și limitele prevăzute de Regulamentul (UE) 2016/679 și de legislația aplicabilă privind arhivarea, evidențele publice și alte obligații legale de păstrare.

Sistemul trebuie să asigure aplicarea principiilor de protecție a datelor încă din faza de concepție și în mod implicit (*privacy by design, privacy by default*) și să includă mecanisme tehnice și organizatorice adecvate pentru garantarea confidențialității, integrității și disponibilității datelor cu caracter personal.

Toate datele cu caracter personal ale utilizatorilor vor fi confidențiale în limitele stabilite printr-o *Politică de confidențialitate cu limite definite în faza de proiectare*. Aceste limite vor fi stabilite în funcție de rolul pe care îl are fiecare utilizator în cadrul sistemului digital.

Vor fi încheiate cu Prestatorul acorduri de confidențialitate și, după caz, acordul prevăzut la art. 28 din Regulamentul (UE) 2016/679, atunci când Prestatorul prelucrează date cu caracter personal în numele și pe baza instrucțiunilor documentate ale Autorității Contractante, în calitate de persoană împuternicită. Numai în situația în care, pentru operațiuni distinct determinate, rezultă din analiza factuală și juridică faptul că părțile stabilesc în comun scopurile și mijloacele esențiale ale prelucrării, raportul juridic va fi calificat și reglementat distinct în condițiile art. 26 din Regulamentul (UE) 2016/679.

În ipoteza în care Prestatorul are calitatea de persoană împuternicită, acesta va prelucra datele numai pe baza instrucțiunilor documentate ale Autorității Contractante, va asigura confidențialitatea persoanelor autorizate, nu va recurge la alți împuterniciți fără autorizarea prealabilă scrisă, specifică sau generală, a Autorității Contractante, va sprijini operatorul în îndeplinirea obligațiilor privind securitatea prelucrării, notificarea încălcărilor de securitate, evaluările de impact și exercitarea drepturilor persoanelor vizate și, la încetarea raportului contractual, va returna sau șterge datele, conform instrucțiunilor operatorului și obligațiilor legale aplicabile.

Prestatorul se va asigura că persoanele autorizate să prelucreze datele și toți subcontractanții implicați în prelucrare au obligații de confidențialitate și obligații contractuale echivalente celor stabilite în sarcina Prestatorului, iar desemnarea unui alt împuternicit se va putea realiza numai cu autorizarea prealabilă scrisă a Autorității Contractante și cu impunerea acelorași obligații în materia protecției datelor. Accesul la datele cu caracter personal va fi strict controlat și limitat doar la persoanele împuternicite care au contracte de confidențialitate semnate cu Prestatorul astfel încât să se respecte toate măsurile de protecție a datelor cu caracter personal începând cu momentul conceperii și implicit în tot procesul de prelucrare a datelor cu caracter personal;

Prestatorul va notifica fără întârzieri nejustificate Autoritatea Contractantă cu privire la orice incident de securitate care afectează sau este susceptibil să afecteze datele cu caracter personal prelucrate în cadrul sistemului și va furniza, de îndată, toate

informațiile și suportul necesare pentru evaluarea incidentului, adoptarea măsurilor de remediere și îndeplinirea obligațiilor legale de notificare.

Sistemul va utiliza cel puțin următoarele mecanisme pentru a asigura **protecția datelor cu caracter personal - plan de măsuri P2**:

- **P2.1:** Toate datele cu caracter personal procesate de sistem vor fi identificate, cartografiate și clasificate în funcție de nivelul de sensibilitate și confidențialitate, în conformitate cu cerințele Regulamentului (UE) 2016/679 (GDPR) și ale Legii nr. 190/2018. Prestatorul va sprijini Autoritatea Contractantă, în faza de analiză a fluxurilor și ori de câte ori intervin modificări relevante în procesele de prelucrare, la identificarea operațiunilor de prelucrare, a fluxurilor de date și a măsurilor tehnice și organizatorice aferente, în vederea întocmirii și actualizării de către Autoritatea Contractantă a evidenței activităților de prelucrare prevăzute la art. 30 din Regulamentul (UE) 2016/679. În măsura în care are calitatea de persoană împuternicită, Prestatorul va menține propria evidență a categoriilor de activități de prelucrare efectuate în numele Autorității Contractante, în condițiile art. 30 alin. (2) din Regulamentul (UE) 2016/679. Fiecare operațiune de prelucrare va fi documentată distinct, cu indicarea scopului, a categoriilor de date, a categoriilor de persoane vizate și a temeiului juridic aplicabil, stabilit în raport cu natura fluxului de prelucrare. În cazul prelucrărilor efectuate de Autoritatea Contractantă în exercitarea atribuțiilor sale legale, temeiurile juridice vor fi identificate și documentate în mod corespunzător, în special în raport cu art. 6 alin. (1) lit. c) și e) din Regulamentul (UE) 2016/679, după caz. Datele vor fi colectate și utilizate numai pentru scopuri specifice, explicite și legitime, respectând principiile de prelucrarea a datelor cu caracter personal din Regulamentul GDPR (ex. principiul de minimizare a datelor, principiul stocării minime).
- **P2.2:** Sistemul va implementa politici și mecanisme de retenție controlată a datelor în conformitate cu legislația aplicabilă privind protecția datelor și arhivarea documentelor, asigurându-se că datele cu caracter personal sunt păstrate doar pe durata necesară îndeplinirii scopurilor pentru care au fost colectate, conform principiului limitării stocării prevăzut la art. 5 alin. (1) lit. e) din Regulamentul (UE) 2016/679 (GDPR).
- **P2.3:** Acolo unde cerințele de business permit, datele cu caracter personal vor fi anonimizate și/sau pseudonimizate, pentru a reduce riscul de identificare a persoanelor vizate. Toate procesele de prelucrare a datelor cu caracter personal vor respecta principiile esențiale din Regulamentul GDPR, precum legalitate, echitate, limitarea scopului, transparența, integritatea și confidențialitate, minimizarea, limitarea stocării, responsabilitatea prelucrărilor. Astfel se vor dezvolta mecanisme de ștergere și/sau arhivare a datelor cu caracter personal (considerate procese critice), care vor putea fi activate în condiții foarte stricte (ex. aplicând principiul „separării responsabilităților”).
- **P2.4:** Sistemul Digital va include funcționalități care să permită publicarea și actualizarea de către Autoritatea Contractantă a informațiilor de transparență și a

notificărilor privind prelucrarea datelor cu caracter personal, redactate într-un limbaj clar și accesibil, în conformitate cu art. 12, 13 și 14 din Regulamentul (UE) 2016/679. Prestatorul va asigura suportul tehnic necesar pentru configurarea, afișarea și actualizarea acestor informații în interfața sistemului. Sistemul digital va include, la nivelul interfeței, un meniu vizibil și accesibil prin care persoanele vizate pot transmite solicitări privind exercitarea drepturilor prevăzute de Regulamentul (UE) 2016/679. Interfața va permite inițierea facilă a cererilor, înregistrarea lor automată, urmărirea stadiului soluționării și păstrarea unei evidențe a solicitărilor și răspunsurilor, în vederea asigurării conformității și auditului. Cererile vor fi direcționate către structurile competente desemnate de Autoritatea Contractantă, cu informarea responsabilului cu protecția datelor potrivit procedurilor interne aplicabile.

- **P2.5:** Politica de cookies va fi publicată, transparent și folosind un limbaj non-tehnic. Sistemul va avea un banner sau modalitate vizibilă de consimțământ, care să permită utilizatorului: acceptarea tuturor cookie-urilor; refuzul tuturor cookie-urilor non-esențiale; personalizarea alegerilor pentru tipuri de cookie-uri (ex. analitice, marketing). Cookie-urile strict necesare funcționării serviciului vor putea fi utilizate fără consimțământ, în limitele prevăzute de normele aplicabile în materie de comunicații electronice și protecția vieții private, iar toate celelalte categorii de cookie-uri sau tehnologii similare vor fi activate numai după obținerea consimțământului valabil al utilizatorului. Sistemul va permite, în orice moment, retragerea consimțământului cel puțin la fel de facil cum a fost acordat și modificarea granulară a preferințelor.
- **P2.6:** Introducerea unor noi componente software, servicii externe, integrări sau tehnologii de urmărire care implică prelucrarea datelor cu caracter personal va fi supusă unei analize prealabile de conformitate și de risc, realizată inițial de Prestator și prezentată Autorității Contractante. În măsura în care analiza preliminară indică faptul că prelucrarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, implementarea se va realiza numai după efectuarea unei evaluări a impactului asupra protecției datelor, în condițiile art. 35 din Regulamentul (UE) 2016/679. Orice transfer de date cu caracter personal în afara Spațiului Economic European se va realiza numai cu respectarea capitolului V din Regulamentul (UE) 2016/679. Orice divulgare sau punere la dispoziție a datelor către alți destinatari se va face numai în temeiul unui scop determinat, al unui temei juridic aplicabil și cu respectarea principiului reducerii la minimum a datelor.
- **P2.7:** Accesul la datele stocate în sistem va fi protejat adecvat, iar accesul va fi auditat permanent;

Securitatea și **confidențialitatea** sunt preocupări de bază în furnizarea de servicii publice. Atât pe parcursul conceperii, dezvoltării, implementării cât și pe toata durata perioadei de garanție oferite de Prestator, sistemul digital trebuie să asigure:

- că urmează abordarea securității prin concepție și implicită pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- că nu este vulnerabil la atacuri care ar putea să-i întrerupă funcționarea și ar putea provoca furtul sau alterarea datelor;
- că respectă cerințele și obligațiile legale privind protecția și confidențialitatea datelor și a datelor cu caracter personal, recunoscând riscurile la adresa confidențialității care reies din analiza și prelucrarea avansată a datelor.
- utilizarea unor servicii calificate de asigurare a încrederii în conformitate cu regulamentul eIDAS pentru a asigura integritatea, autenticitatea, confidențialitatea și nerepudiarea datelor, permițând verificarea identității părților și protejarea datelor de alterare sau acces neautorizat.

De asemenea, pentru a asigura respectarea cerințelor de conformitate cu NIS2 pentru acest sistem digital, Prestatorul va îndeplini și următoarele cerințe:

- va furniza un Plan de minimizare a riscurilor provenite din lanțul de aprovizionare ce va include o listă completă a tuturor componentelor software din care este alcătuit sistemul (Software Bill of Materials - SBOM), incluzând toate bibliotecile open-source, framework-urile și componentele COTS, cu specificarea versiunilor exacte utilizate. Pentru fiecare componentă, Prestatorul va descrie modul în care monitorizează, evaluează și aplică patch-urile de securitate pentru aceste componente pe întreaga durată a contractului, inclusiv pe perioada de garanție;
- în cazul unui incident de securitate, pe lângă respectarea timpilor de remediere, Prestatorul se obligă să furnizeze Autorității Contractante (Ministerul Culturii) toate informațiile necesare și suportul tehnic pentru ca aceasta să își poată îndeplini obligațiile legale de notificare a incidentelor conform Directivei NIS2 și legislației naționale de transpunere;
- având în vedere că STS furnizează infrastructura cloud în model IaaS (Infrastructure as a Service), Prestatorul va fi responsabil cel puțin pentru, dar fără a se limita la:
 - Securitatea și configurarea sistemelor de operare și a aplicațiilor instalate;
 - Implementarea mecanismelor sigure de gestiune a identității și a accesului utilizatorilor;
 - Implementarea mecanismelor pentru protecția, integritatea și confidențialitatea datelor gestionate;
 - Implementarea controalelor de securitate la nivel de aplicație, inclusiv firewall, criptare și audit;
 - Realizarea configurărilor software și definirea și implementarea politicilor de acces.

De asemenea Sistemul Digital va respecta și cerințele din OUG 89/2022 și legislația subsecventă prin care se cere ca sistemele informatice utilizate de către autoritățile și

instituțiile publice centrale să fie dezvoltate astfel încât să fie apte pentru migrarea în Cloud-ul Privat Guvernamental sau interconectate cu acesta (Art.1 alin.7).

7.6 Accesibilitate și UI/UX

Pentru a realiza un sistem digital accesibil, intuitiv și ușor de utilizat, care să răspundă nevoilor reale ale utilizatorilor și să garanteze incluziunea acestora, Prestatorul va realiza activități de accesibilitate și UI/UX, în cadrul fazei de proiectare, ale căror rezultate vor fi reflectate în **Raportul de proiectare (L2)** și **Prototipul vizual al principalelor fluxuri de utilizare (L3)** (vezi 9.1 Documente), în conformitate cu următoarele cerințe:

1. Cercetare bazată pe nevoile utilizatorilor

- a) Vor fi implicați tipuri de utilizatori diferiți în toate etapele de design pentru optimizarea UI/UX.
- b) Vor fi colectate propuneri și vor fi testate interfețele, cu posibilitatea reluării dezvoltării dacă soluția nu este aprobată.
- c) Va fi stabilit modul de evaluare și nivelul de implicare a utilizatorilor în faza de analiză.

2. Testare și îmbunătățire continuă

- a) Vor fi realizate teste iterative de utilizabilitate pe tot parcursul dezvoltării.
- b) Va fi colectat feedback-ul prin interviuri, observații și analize de utilizare.
- c) Vor fi identificate problemele și va fi ajustat constant designul UI/UX pe durata contractului, inclusiv după recepționarea intermediară a unei componente.

3. Validarea soluțiilor cu utilizatori reali

- a) Vor fi testate interfața, navigarea și fluxurile de lucru cu utilizatori reali.
- b) Vor fi măsurați indicatorii de performanță, precum rata de succes a sarcinilor, timpul de completare și scorul System Usability Scale.
- c) Va fi colectat feedback-ul calitativ și va fi îmbunătățit designul pe baza rezultatelor obținute.

4. Arhitectura informației, navigare și experiența utilizatorului

- a) Va fi creată o structură logică și intuitivă pentru accesarea și organizarea conținutului.
- b) Va fi implementată o navigare clară și consecventă, care să includă filtre, funcții de căutare, breadcrumb-uri și secțiuni relevante.
- c) Vor fi proiectate fluxurile și interfața pentru a minimiza efortul cognitiv și pentru a asigura consistență, previzibilitate și ergonomie.

- d) Va fi monitorizată continuu experiența utilizatorului și va fi ajustat designul UI/UX pentru a asigura eficiență și confort.

7.6.1 Accesibilitate

7.6.1.1 Standarde și reglementări internaționale

Sistemul digital va fi dezvoltat cu un accent major pe accesibilitate, incluziune și ușurință în utilizare, asigurând acces egal la patrimoniul cultural digital pentru toți utilizatorii, indiferent de vârstă, nivel de competență digitală sau tip de dizabilitate.

Interfețele publice ale sistemului digital vor fi multilingve (cel puțin în limbile română și engleză) și vor respecta standardele internaționale de accesibilitate web, în conformitate cu recomandările W3C (World Wide Web Consortium) și inițiativa WAI (Web Accessibility Initiative).

Interfața portalului web de servicii va fi proiectată astfel încât să respecte prevederile OUG 112/2018 privind transpunerea Directivei (UE) 2102/2016 privind accesibilitatea site-urilor web și a aplicațiilor mobile ale organismelor din sectorul public, precum și respectarea prevederilor Directivei (UE) 2019/882 a Parlamentului European și a Consiliului din 17 aprilie 2019 privind cerințele de accesibilitate aplicabile produselor și serviciilor.

Sistemul va îndeplini pentru toate interfețele de utilizator accesibile publicului cerințele definite în Web Content Accessibility Guidelines (WCAG) 2.2 – nivel minim AA, recunoscute la nivel global drept referință pentru proiectarea conținuturilor digitale accesibile.

Principalele caracteristici de accesibilitate vor include, fără a se limita la:

- a) Structurarea paginilor prin etichete HTML semantice, compatibile cu cititoarele de ecran (ex. NVDA, JAWS, VoiceOver);
- b) Navigare completă prin tastatură, cu tabulare logică și previzibilă;
- c) Gestionarea corectă a focalizării, mai ales în interacțiunea cu ferestre modale, panouri glisante și meniuri derulante;
- d) Contrast suficient între text și fundal (minim 4.5:1 conform WCAG AA);
- e) Redimensionare corectă a interfeței pe dispozitive mobile sau la aplicarea unui zoom de până la 400%, fără pierdere de conținut sau funcționalitate;
- f) Dimensionare relativă a textului, pentru a permite utilizatorului să-și ajusteze preferințele vizuale;
- g) Text alternativ (alt text) pentru toate imaginile relevante din punct de vedere informativ;
- h) Subtitrări și/sau transcrieri pentru conținutul audio-video;

- i) Evitarea elementelor care pot provoca disconfort (ex. clipiri rapide, animații excesive, contrast intermitent);
- j) Compatibilitate cu dispozitive de asistență (cititoare de ecran, comenzi vocale, tehnologii de acces alternativ).

7.6.1.2 Testare și evaluare a accesibilității

Sistemul digital va fi supus unui proces continuu de evaluare a accesibilității, care include:

- testare automată prin instrumente de validare WCAG 2.2 AA (ex. WAVE, Axe, Lighthouse);
- testare manuală pe eșantioane reprezentative de conținut;
- implicarea utilizatorilor cu dizabilități în fazele de testare și feedback, pentru verificarea reală a experienței de utilizare.

7.6.1.3 Accesibilitate continuă

Pentru a asigura menținerea conformității în timp, sistemul digital ePatrimoniu va include proceduri de monitorizare și actualizare periodică a interfețelor, pe măsură ce apar noi cerințe legislative sau versiuni actualizate ale standardelor WCAG. În faza de proiectare vor fi integrate reguli clare privind accesibilitatea by design, astfel încât orice nouă funcționalitate sau componentă să respecte principiile „Design for All”.

7.6.2 UI/UX

7.6.2.1 Manual de identitate vizuală ePatrimoniu

Autoritatea Contractantă va pune la dispoziția Prestatorului identitatea vizuală dedicată proiectului, structurată conform **Manualului de identitate vizuală ePatrimoniu**. Pentru a asigura coerența și unitatea designului, cerințele din acest manual se aplică, unitar și în mod obligatoriu, interfeței publice, a dashboardului intern și a ambelor componente aplicative ale sistemului digital ePatrimoniu.

Manualul de identitate vizuală ePatrimoniu va include **elementele esențiale de identitate grafică și de comunicare** (logo primar și variante adaptative, sistem tipografic, paletă cromatică, ilustrații esențiale, pictograme relevante, declinări grafice pe materiale promoționale), precum și regulile de utilizare a acestora. Prestatorul are obligația de a respecta întocmai identitatea vizuală și instrucțiunile din Manualul de identitate vizuală ePatrimoniu în toate activitățile de proiectare, dezvoltare și implementare a sistemului digital ePatrimoniu, pentru a asigura coerența și unitatea imaginii proiectului în mediul digital și în materialele de comunicare asociate.

7.6.2.2 Design de sistem ePatrimoniu

Autoritatea Contractantă va elabora și va pune la dispoziția Prestatorului un **Design de sistem** bazat pe Manualul de identitate vizuală ePatrimoniu, asigurând un sistem de design unitar, coerent vizual și funcțional, în conformitate cu principiile UI/UX actuale.

Designul de sistem ePatrimoniu va integra principalele componente UI ale sistemului digital și va include reguli de utilizare, recomandări, restricții, precum și exemple de scenarii de aplicare pentru fiecare componentă.

Exemple de componente UI ce vor fi incluse în **Designul de sistem ePatrimoniu**:

- sistem tipografic: fonturi principale și secundare, dimensiuni titluri/ subtitluri/ text normal, reguli privind folosirea unităților de măsură;
- paletă cromatică: culori primare și secundare, variațiuni, exemple de combinații permise;
- iconografie: un set consistent de iconițe, care ajută la navigare, feedback și înțelegerea acțiunilor;
- elemente de afișare de date: tabele, liste, carduri cu texte/imagini, galerii multimedia, etc;
- elemente de introducere de date: formulare, tipuri de inputuri (text, search, dropdown list, checkbox, radio, etc);
- elemente de navigare: meniuri, filtre, butoane, etc;
- layout și structură: un sistem de grid (care va asigura că platforma este responsive), structura tipică a paginilor, spațiere / margini / aliniere.

Codul sursă pe care Designul de sistem ePatrimoniu este bazat va fi alcătuit din fișiere ce țin strict de interfața web (precum HTML, CSS și JavaScript), structurate într-un mod modular, clar și scalabil, pentru a menține organizarea, performanța, ușurința de întreținere și posibilitatea dezvoltării de noi componente UI. Prestatorul va avea acces la codul sursă și poate colabora în mod continuu cu designerul de interfață al Autorității Contractante pentru a găsi soluții optime și fezabile.

7.6.2.3 Suită de prototipuri de interfață, în format web

Interfața web va fi dezvoltată în conformitate cu Designul de sistem ePatrimoniu. Autoritatea Contractantă, prin intermediul designerului propriu de interfață, are posibilitatea de a transmite și **propuneri concrete, în format web**, bazate pe Designul de sistem ePatrimoniu, de layout-uri pentru modulele care urmează a fi realizate sau pentru pagini care exemplifică fluxuri complexe de interacțiune în platformă. În acest caz, Autoritatea Contractantă va pune la dispoziția Prestatorului și codul sursă pentru aceste propuneri. Acesta poate fi integrat ulterior în platformă sau poate fi folosit doar ca sursă de referință. Întregul cod sursă propus de Autoritatea Contractantă va viza

exclusiv interfața web, pentru a separa complet componenta front-end de logica back-end și a preveni potențialele probleme de securitate ale platformei. Propunerile urmează a fi integrate de către Prestator după validarea de către Autoritate.

Pentru Dashboardul Intern, Prestatorul va livra o interfață grafică, modernă și intuitivă, aliniată la Manualul de identitate vizuală al proiectului. Designul va facilita identificarea rapidă a modulelor disponibile, asigurând o tranziție vizuală fluidă către componente.

8 Implementare, mentenanță, garanție și suport tehnic

Prestatorul va realiza dezvoltarea și implementarea sistemului digital ePatrimoniu printr-o metodologie de dezvoltare **incrementală și iterativă** (conform prevederilor din secțiunea 4.1 din prezentul caiet de sarcini), care presupune analiza, proiectarea, dezvoltarea, configurarea, testarea, livrarea, validarea și punerea în producție graduală a componentelor, modulelor și funcționalităților sistemului, asigurând adaptabilitate și control al calității pe tot parcursul contractului.

Abordarea incrementală presupune livrarea succesivă de versiuni parțiale, complet funcționale, testate și documentate (incrementuri), ale componentelor în mediul de producție. Incrementurile acceptate de Autoritatea Contractantă vor fi implementate în mediul de producție, fără a afecta funcționarea generală a sistemului. Această metodologie permite Autorității Contractante validarea continuă a rezultatelor, ajustarea rapidă a specificațiilor și reducerea riscurilor aferente implementării unui sistem complex și integrat.

Utilizarea metodologiei de dezvoltare incrementală și iterativă nu exonerează contractantul de obligația de a respecta integral cerințele funcționale și nefuncționale stabilite și nu poate constitui motiv pentru livrarea incompletă sau neconformă a sistemului.

Etapele sunt structurate după cum urmează:

Stadiu	Fază
Preimplementare	8.0 Faza de pre-analiză
Implementare	8.1 Faza de analiză
	8.2 Faza de proiectare
	8.3 Faza de dezvoltare, migrare și testare
	8.4 Faza de punere în producție
	8.5 Instruire pentru utilizatori și administratori

	8.6 Faza de stabilizare operațională a sistemului
Post-implementare	8.7 Mentenanță
	8.8 Garanția și suportul tehnic

Fiecare fază de implementare reprezintă o parte integrată a procesului general de dezvoltare și implementare și se va desfășura în strânsă colaborare cu Autoritatea Contractantă, în baza unei planificări agreeate și a unor jaloane intermediare de verificare și validare.

Toate fazele vor respecta principiile metodologiei de dezvoltare **incrementală și iterativă**, cu livrări intermediare supuse procesului de validare de către Autoritatea Contractantă. Fiecare fază va avea obiective măsurate prin livrabile clar definite, conform capitolului 9. Punerea în producție se va realiza gradual, bazat pe jaloane critice (*Key Milestones*)¹⁴, pentru a asigura valorificarea timpurie a funcționalităților și reducerea riscurilor de implementare. Instruirea, testarea și validarea vor fi activități recurente, realizate pentru fiecare increment funcțional livrat. Toate livrabilele vor fi documentate, gestionate versionat și aprobate formal de către Autoritatea Contractantă, în condițiile prezentului Caiet de sarcini.

Având în vedere complexitatea și caracterul inovator al contractului, precum și abordarea de dezvoltare incrementală și iterativă, în fazele de analiză, proiectare și dezvoltare și stabilizare, precum și în urma activităților de testare și validare desfășurate cu beneficiarii finali ai platformei, pot fi identificate cerințe suplimentare sub forma unor **ajustări / completări** sau **implementarea de noi funcționalități**, care nu au fost explicit specificate în prezentul caiet de sarcini, dar care sunt necesare pentru asigurarea unei funcționalități complete, coerente și centrate pe utilizator a sistemului, în conformitate cu obiectivele asumate ale proiectului și cu scopul / obiectul și rezultatele contractului.

Cerințele suplimentare din partea autorității contractante sunt justificate de necesitatea asigurării operabilității, interoperabilității, compatibilității tehnice, securității, accesibilității, adaptării la nevoi reale identificate în urma testării, alinierii la standarde tehnice noi sau actualizate, precum și a conformității legale sau de alte motive similare și rezonabile.

Prin **ajustare** se înțelege „orice modificare de detaliu aplicată unor elemente deja prevăzute în documentația de atribuire sau în soluția tehnică, realizată cu scopul de a optimiza, adapta sau clarifica implementarea acestora, fără a altera obiectul principal

¹⁴ Repere semnificative în cronologia unui contract care marchează puncte de progres importante sau completarea unor etape / activități cheie, folosite ca instrument de planificare și control pentru a monitoriza evoluția contractului și pentru a facilita comunicarea cu părțile interesate. În metodologiile PMI, un jalon nu implică durată de execuție, ci este un eveniment de referință pe linia de timp a contractului.

(sursa: <https://www.pmi.org/learning/library/manage-milestone-managing-deliverables-10437>)

al contractului, fără a introduce cerințe esențial diferite și fără impact semnificativ asupra prețului, duratei sau echilibrului economic al contractului. Ajustările pot include adaptări de parametri tehnici, configurări, setări sau modalități de prezentare și nu reprezintă modificări substanțiale ale obligațiilor contractuale.

Prin **completare** se înțelege orice adăugare sau detaliere suplimentară, identificată pe parcursul derulării contractului, care are ca scop asigurarea funcționalității complete și coerente a sistemului, fără a modifica obiectul principal al contractului și fără a afecta echilibrul economic inițial al acestuia. Completările nu reprezintă modificări substanțiale ale cerințelor inițiale, ci elemente rezonabile și proporționale, necesare pentru operabilitate, interoperabilitate, securitate, conformitate legală, accesibilitate sau adaptare la nevoi reale constatate în etapa de testare și validare.

Atât ajustările, cât și completările se vor integra în soluția finală fără costuri suplimentare, în măsura în care acestea sunt necesare pentru atingerea obiectivelor proiectului.”

Prin **funcționalitate suplimentară** se înțelege orice caracteristică sau modul adițional care nu a fost prevăzut inițial în documentația de atribuire sau în soluția tehnică, dar care trebuie implementat cu scopul de a completa, optimiza sau îmbunătăți funcționalitatea platformei, fără a altera obiectul principal al contractului, fără a introduce cerințe esențial diferite și fără a avea un impact semnificativ asupra prețului, duratei sau echilibrului economic al contractului. Funcționalitățile suplimentare pot include module opționale, notificări, rapoarte adiționale sau alte facilități similare și nu reprezintă modificări substanțiale ale obligațiilor contractuale.

Pe parcursul întregului contract, în toate fazele, inclusiv în faza de mentenanță și în perioada de garanție, pentru fiecare tichet (indiferent dacă este de tip eroare, deficiență, neconformitate etc.) înregistrat în *Componenta de management al incidentelor* se va stabili unul dintre nivelurile de prioritate de mai jos:

Nivel de Prioritate	Descriere
Urgent	Impact Major asupra funcționării sistemului. Problema împiedică desfășurarea activității unităților organizaționale înrolate, procesul de activitate este serios afectat și nu mai poate continua, pierderea funcționalităților devenind critică.
Critic	Impact Semnificativ asupra funcționării sistemului. Problema împiedică desfășurarea în condiții normale a activității utilizatorilor. Nicio soluție alternativă nu este disponibilă, iar activitatea utilizatorilor poate continua, însă într-un mod restrictiv.
Major	Impact Mediu asupra funcționării sistemului. Problema afectează minor funcționalitățile sistemului. Impactul reprezintă un inconvenient care necesită soluții alternative pentru refacerea funcționalităților.
Minor	Impact Minim asupra funcționării sistemului. Problema nu afectează funcționalitățile sistemului. Rezultatul este o eroare minoră care nu împiedică desfășurarea în bune condiții a activității utilizatorilor.
Scăzut	Problema nu afectează desfășurarea activității utilizatorilor și nu produce blocaje, restricții funcționale sau erori semnificative în utilizarea curentă a sistemului. Poate viza aspecte izolate, situații cu frecvență redusă, neconformități de prezentare, ajustări minore sau solicitări care pot fi tratate planificat, fără impact asupra operării normale a sistemului.

În cazul situațiilor semnalate în tichete cu nivel de prioritate "urgent", asistența va fi asigurată 24x7, fiind disponibilă până când problema va fi rezolvată. Pentru aceasta, Autoritatea Contractantă va furniza o persoană de contact, disponibilă 24x7, care să furnizeze informații, să testeze soluții și să aplice soluțiile furnizate.

Timpi de răspuns și rezoluții

Timp de Răspuns: Timpul scurs de la înregistrarea tichetului în Componenta de management incidente până la răspunsul primit de la echipa Prestatorului. În răspunsul inițial prestatorul confirmă faptul că a luat la cunoștință despre problemă și precizează resursele alocate ce intervin imediat pentru rezolvarea problemei.

Remediere Provizorie: O modificare temporară în cadrul procedurilor sau a datelor, menită să prevină sau să atenueze efectele erorilor, fără a afecta funcționarea corectă și sigură a sistemului digital.

Timp de Remediere: Durata de timp până la punerea în producție a soluției finale.

Remediarea reprezintă implementarea soluției definitive pe mediul de producție, acceptată de Autoritatea Contractantă în urma parcurgerii cu succes a tuturor testelor conform cerințelor din Caietul de sarcini și documentată în detaliu, care elimină complet problema.

Prestatorul va respecta următorii timpi de răspuns, în corelație cu nivelul de prioritate:

Nivel prioritate	Timp de răspuns	Timp remediere provizorie	Timp de remediere
Urgent	1 oră	4 ore	12 ore
Critic	2 ore	12 ore	24 ore / 1 zi
Major	4 ore	1 zi	48 ore / 2 zile
Minor	8 ore	48 ore / 2 zile	72 ore / 3 zile
Scăzut	2 zile	4 zile	14 zile

La sfârșitul fiecărui caz deschis, Prestatorul va efectua o analiză a cauzelor care au dus la producerea deranjamentului și o va fi include în recomandarea finală.

Depășirile timpilor de răspuns / remediere de mai sus dau dreptul Autorității Contractante de a calcula și aplica penalizări. Un punct de penalizare valorează 200 lei. Punctele de penalizare sunt cuantificate astfel:

- Pentru depășirea termenului de răspuns și a termenului de soluționare provizorie / remediere aferente tichetelor cu nivel de prioritate urgent, se vor aplica 3 puncte de penalizare pentru fiecare oră de depășire a termenului;
- Pentru depășirea termenului de răspuns și a termenului de soluționare provizorie / remediere aferente tichetelor cu nivel de prioritate critic, se vor aplica 2 puncte de penalizare pentru fiecare oră de depășire a termenului;
- Pentru depășirea termenului de răspuns și a termenului de soluționare provizorie / remediere aferente tichetelor cu nivel de prioritate major, se va aplica 1 punct de penalizare pentru fiecare oră de depășire a termenului;
- Pentru depășirea termenului de răspuns și a termenului de soluționare provizorie / remediere aferente tichetelor cu nivel de prioritate minor sau scăzut, se va aplica 1 punct de penalizare pentru fiecare zi de depășire a termenului;

8.0 Faza de pre-analiză

În vederea înțelegerii contextului organizațional, procedural și tehnic, Autoritatea Contractantă va derula o **fază de pre-analiză**. Scopul acestei etape este realizarea **Documentației de pre-analiză** și a **Manualului de identitate vizuală ePatrimoniu**, a **Designului de sistem ePatrimoniu** și a **Suitei de prototipuri de interfață**, care vor sta la baza începerii fazelor de analiză și de proiectare cu focus pe îndeplinirea primelor două jaloane.

Documentația preliminară de pre-analiză este elaborată de către echipa internă a Autorității Contractante, formată din specialiști cu roluri complementare (analști de business și/sau sistem, specialiști în procese și fluxuri operaționale, specialiști de date, programatori, designeri de interfață, precum și alți experți tehnici și funcționali relevanți).

Obiectivele acestei etape premergătoare presupun înțelegerea proceselor și a structurilor organizaționale, reducerea riscului de interpretare diferită a cerințelor și structurarea în mod eficient a fazelor de analiză și de proiectare.

Faza de pre-analiză va fi fundamentată pe:

- interviuri și/sau întâlniri de lucru cu utilizatori-cheie, factori decizionali și alți stakeholderi relevanți;
- analiza documentelor și a procedurilor interne existente;
- inventarierea preliminară a sistemelor informatice și a bazelor de date existente;
- eșantionare reprezentativă pentru principalele tipuri de resurse;
- maparea relațiilor dintre bazele de date existente și fluxurile în care sunt implicate;
- evaluare preliminară a necesarului de integrări și interoperabilitate cu alte sisteme;
- identificarea cerințelor privind accesibilitatea (inclusiv standarde aplicabile, după caz);
- identificarea constrângerilor legale, operaționale și tehnice.

Structura și conținutul orientativ al **Documentației de pre-analiză** va fi:

A. pentru **Componenta Gestiunea identității și accesul utilizatorilor (IAM)**

- Inventar preliminar al actorilor și tipurilor de cont relevante pentru platformă (utilizatori instituționali, administratori, utilizatori externi etc.) și mapare ale tipurilor de entități organizaționale, ca bază pentru definirea rolurilor și accesului.
- Catalog preliminar de roluri funcționale și responsabilități (la nivel de „cine face ce”), corelat cu modulele principale și cu fluxurile operaționale descrise în document.
- Matrice preliminară rol–permisiuni (RBAC), la nivel de principii și operațiuni standard (vizualizare / creare / modificare / avizare / aprobare / publicare / administrare), cu marcarea zonelor unde sunt necesare clarificări/decizii.
- Delimitarea preliminară a nivelurilor de vizibilitate asupra datelor (public / intern / restricționat) și reguli orientative de diferențiere a accesului în funcție de instituție/structură și context.
- Lista preliminară a funcțiilor IAM necesare în dashboard-ul intern (administrare utilizatori/entități, atribuire roluri/drepturi, jurnalizare/audit la nivel de acces și modificări), descrise la nivel de nevoi operaționale (nu soluție tehnică)

B. pentru **Componenta de e-Guvernare**

1. **Documentație preliminară de analiză a proceselor administrative** vizate în jalonul 1 (capitolul 9.2.), incluzând:
 - definirea cadrului conceptual (proces, flux administrativ, etapă, actor) și descrierea scopului proceselor și a fluxurilor componente,

- actorii implicați: cine sunt utilizatorii (persoane fizice, juridice, personalul MC, DJC, INP, etc.) și ce roluri specifice au;
- etapele fiecărui flux: documentarea detaliată a fiecărui pas, de la inițierea solicitării până la transmiterea răspunsului. De exemplu, pentru o cerere de avizare, se vor detalia pașii de la depunerea documentației, la distribuirea internă, avizare, aprobare, semnare electronică și transmiterea răspunsului;
- diagrama de proces, incluzând evidentierea fluxurilor, formularelor asociate fiecărei etape și notificărilor primite de utilizatori;
- documentele și datele necesare: pentru fiecare serviciu, trebuie specificate exact documentele solicitate (ex. copii CI, autorizații, planuri de construcție etc.);
- reguli de business și validări: identificarea constrângerilor și a regulilor specifice fiecărui serviciu (ex. condiții pentru validarea semnăturii electronice, reguli de obligativitate pentru anexarea documentelor, validări ale datelor introduse);
- șabloane aferente etapelor de proces și analiză structurată a câmpurilor (tip câmp, reguli de validare, sursă de preluare a datelor, nomenclatoare asociate, condiții de completare etc.);
- definirea tipurilor de notificări, a direcției acestora și a conținutului orientativ;
- identificarea și definirea tuturor nomenclatoarelor necesare, cum ar fi tipurile de servicii, tipurile de documente, compartimentele funcționale, tipurile de bunuri culturale etc.;

2. Arhivare electronică:

- estimarea volumului preliminar de documente și cereri pentru a dimensiona procesul de arhivare electronică;
- descrierea principalelor tipuri de documente generate sau gestionate în cadrul fluxurilor administrative;
- evidențierea formatelor de fișiere utilizate sau acceptate în cadrul fluxurilor administrative, inclusiv indicarea etapelor în care acestea sunt încărcate, generate sau arhivate;
- descrierea modului de grupare a documentelor în colecții, în corelare cu fluxurile administrative și cu structura registrelor;
- definirea metadatelor arhivistice relevante în funcție de tipul documentului (identificator, dată, autor, tip document);

3. Registre publice despre patrimoniu

- structura de date a registrelor (câmpuri, categorii, clasificări utilizate);
- mapări ale structurilor de date
- relațiile dintre registre și fluxurile administrative;

- eșantioane de date reprezentative din registre;
- descrierea fluxurilor administrative care conduc la introducerea, actualizarea sau modificarea înregistrărilor din registre;
- matricea rolurilor și acțiunilor utilizatorilor referitoare la administrarea registrelor, descrierea modului de vizualizare și administrare a registrelor de către utilizatorii interni ai sistemului (ex. personal MC, INP), incluzând funcționalități de căutare, filtrare, editare, versionare și audit a modificărilor.
- descrierea modului de publicare și afișare a registrelor în interfața publică a platformei, inclusiv definirea câmpurilor publice, a nivelurilor de vizibilitate, a mecanismelor de căutare și filtrare disponibile publicului, precum și a eventualelor restricții privind accesul la anumite categorii de date

C. Pentru **componenta de Management Patrimoniu Cultural**:

- Structură conceptuală preliminară a modelului semantic de referință, indicând clasele / entitățile principale și tipurile de relații avute în vedere, precum și sursa / versiunea (unde este cazul).
- Reguli operaționale minimale pentru utilizarea MPC: roluri implicate și responsabilități (creare / validare / publicare), respectiv niveluri de vizibilitate (intern / public / restricționat), în forma disponibilă la momentul semnării.
- Inventar preliminar al surselor de date existente relevante pentru MPC și conexe (Culturalia, LMI (SIPCI), RAN, DOCPAT, eGISPat, ACERA, Bunuri culturale mobile clasate în Patrimoniul Cultural Național, Bunuri culturale mobile distruse, furate, dispărute sau exportate ilegal etc.), cu descriere: proprietar, format, mod de acces, frecvență de actualizare și câmpuri / identificatori-cheie.
- Eșantioane reprezentative de date pentru principalele tipuri de resurse (menționate la punctul anterior), inclusiv exemple cu probleme, pentru evaluarea calității și a regulilor de validare.
- 50 de seturi de nomenclatoare tematice disponibile și/sau utilizate curent, cu sursa și versiunea.
- Set preliminar de straturi GIS relevante pentru MPC: geometrii pentru patrimoniu imobil / arheologic și zone de protecție, cu surse și condiții de utilizare, plus date de referință furnizate de instituții terțe (ex. ANCPI, INFP, HHRI, etc.), disponibile prin standarde OGC (ex. WMS/WFS), dacă sunt contractate/permise.

D. Pentru **cerința de interoperabilitate**

- identificarea preliminară a unei serii de sisteme externe relevante cu care platforma urmează să interacționeze (ex. sisteme naționale, registre externe, servicii de identitate digitală etc.);
- descrierea tipurilor de schimburi de date preconizate (interogare date, transmitere date, validare date, sincronizare periodica etc.);

- o mapare preliminară neexhaustivă a tipurilor de date ce urmează a fi schimbate și a corelării acestora cu structurile interne ale sistemului.

E. pentru **modulul de Rapoarte**

- structurarea tipurilor de rapoarte avute în vedere (rapoarte operaționale, rapoarte statistice, rapoarte de management, rapoarte publice etc.);
- definirea orientativă a structurii în funcție de tipul de raport (indicatori principali, agregări relevante, perioade de raportare, eventuale secțiuni distincte);
- corelarea tipurilor de rapoarte cu rolurile de utilizator, în vederea delimitării accesului și a nivelului de detaliu vizibil;
- definirea orientativă a indicatorilor operaționali relevanți pentru fiecare categorie de rol;
- propuneri de structuri de dashboard adaptate pe roluri (de management, dashboard de monitorizare activitate), cu evidențierea principalelor zone de interes.

UI/ UX Design

În etapa de pre-analiză, Autoritatea Contractantă va pune la dispoziția Prestatorului documentațiile aferente componentei de UI/UX, care vor constitui baza pentru proiectarea și implementarea interfețelor sistemului digital: **Manualul de identitate vizuală ePatrimoniu**, **Designul de sistem ePatrimoniu** și **Suita de prototipuri de interfață** (conform capitolului 7.6.2 UI/UX).

Manualul de identitate vizuală ePatrimoniu va defini elementele de identitate grafică și regulile de utilizare ale acestora. Pe baza acestuia, **Designul de sistem ePatrimoniu** va descrie principalele componente UI ale platformei, regulile de utilizare și exemplele de aplicare și va fi constituit dintr-o colecție în format web de componente, prezentate generic: butoane, input-uri, carduri, grid-uri și alte tipuri de elemente care pot apărea în platforma. **Suita de prototipuri de interfață**, realizată în conformitate cu **Designul de sistem ePatrimoniu**, va cuprinde propuneri de layout-uri pentru module selectate sau pentru pagini care exemplifică fluxuri complexe de interacțiune în sistemul digital.

Un exemplu concret de prototip de interfață îl reprezintă pagina principală a componentei de Management Patrimoniu Cultural. Aceasta va evidenția multiple modalități de explorare a resurselor culturale: căutare principală, navigare pe categorii (Tip, Subiect, Perioadă, Locație etc.) și acces către modulul Hartă. În plus, vor fi integrate mecanisme de explorare secundară, precum secțiuni de recomandări, „Astăzi” (evenimente, aniversări, comemorări, etc.), muzee și cele mai recente resurse adăugate.

Toate elementele din prototipurile de interfață vor fi aplicate atât pentru componenta de e-Guvernare cât și pentru componenta de Management Patrimoniu Cultural.

Suita de prototipuri de interfață va utiliza exclusiv tehnologii web standard: HTML pentru structurarea semantică, CSS pentru stilizare și layout și JavaScript pentru comportament și interacțiuni client-side. Această abordare elimină dependența de framework-uri specifice și permite Prestatorului integrarea și adaptarea ușoară a prototipurilor în diferite arhitecturi frontend. Codul sursă va viza strict interfața web, va fi organizat modular, pe o structură clară și scalabilă și va fi pus integral la dispoziția Prestatorului.

Manualul de identitate vizuală, Designul de sistem și Suita de prototipuri de interfață constituie livrabile inițiale ale Autorității Contractante în etapa de pre-analiză și pot fi revizuite sau completate ulterior, în funcție de evoluția cerințelor și rezultatele activităților etapelor următoare.

Documentația rezultată în etapa de pre-analiză are rolul de **material orientativ de lucru** și de **intrare** pentru faza de analiză realizată de Prestator, fără a substitui activitățile, responsabilitățile și livrabilele specifice acestei faze. Documentul de pre-analiză poate constitui un punct de plecare pentru elaborarea **Documentului de Analiză**, iar **Manualul de identitate vizuală ePatrimoniu, Designul de sistem ePatrimoniu și Suita de prototipuri de interfață** au rol de referință pentru definirea și rafinarea interfețelor care vor fi proiectate și implementate de Prestator; acestea nu reprezintă specificații finale și nu limitează soluțiile tehnice sau de arhitectură propuse de Prestator, care rămâne responsabil pentru proiectarea completă, conformă și optimă a soluției, în acord cu caietul de sarcini. În cadrul fazei de analiză, Prestatorul are obligația de a **revizui, verifica și valida** informațiile și propunerile din pre-analiză (inclusiv fluxuri, roluri, reguli și prototipuri), de a identifica neclarități, inconsecvențe sau riscuri, de a formula clarificări și propuneri de îmbunătățire și de a formaliza, împreună cu Autoritatea Contractantă, varianta finală a cerințelor în Documentul de Analiză, care constituie reperul contractual pentru dezvoltarea și acceptanța soluției.

8.1 Faza de analiză

Faza de analiză are ca obiectiv identificarea, definirea, documentarea și validarea înțelegerii cerințelor funcționale și nefuncționale ale sistemului digital, precum și a cerințelor tehnice, organizaționale, operaționale, de interoperabilitate, de securitate și de conformitate juridică ale acestuia, astfel încât acesta să răspundă nevoilor specifice ale utilizatorilor și ale instituțiilor responsabile.

Rezultatele fazei de analiză, astfel cum sunt documentate și aprobate, constituie baza obligatorie pentru etapele ulterioare de proiectare, dezvoltare și implementare, toate cerințele, specificațiile și soluțiile definite urmând a fi transpuse integral în sistemul livrat.

Prestatorul are obligația de a realiza o analiză completă și coerentă, care să asigure că soluția propusă răspunde integral cerințelor prevăzute în prezentul caiet de sarcini, este conformă cu legislația națională și europeană aplicabilă, este interoperabilă cu sistemele relevante și este scalabilă, securizată și sustenabilă pe termen lung.

Faza de analiză are ca livrabil **Documentul de analiză a sistemului digital**, structurat pe capitole, conform metodologiei iterative.

Informațiile care stau la baza procesului de analiză includ, fără a se limita la:

- a. Contractul de achiziție (termene și condiții);
- b. Caietul de sarcini și propunerea tehnică;
- c. Documentația de pre-analiză (descrișă în subcapitolul 8.0)
- d. Manualul de identitate vizuală, Designul de sistem și Suita de prototipuri de interfață (descrișe în subcapitolul 8.0)
- e. Alte informațiile furnizate de Autoritatea Contractantă și beneficiari;
- f. Cadrul legislativ aplicabil (patrimoniu cultural, arhivare, interoperabilitate, protecția datelor, securitate cibernetică, eIDAS etc.).

Activitățile desfășurate în faza de analiză se vor concentra inițial pe completarea informațiilor prezentate în caietul de sarcini, astfel încât Prestatorul să poată avea o imagine corectă și completă a domeniilor de aplicabilitate.

Faza de analiză are ca livrabil **Documentul de analiză a sistemului digital (L1)**, care sintetizează arhitectura propusă, interfețele, cerințele funcționale și nonfuncționale. Descrierea detaliată a acestuia se regăsește în secțiunea 9.1.

Autoritatea Contractantă poate solicita înlocuirea unor tehnologii dacă acestea generează risc major de lock-in și Prestatorul este obligat să vină cu soluții alternative.

Pe parcursul implementării contractului, **Prestatorul are obligația de a actualiza Documentul de analiză**, inclusiv matricele, fluxurile, modelele și specificațiile asociate, în oricare dintre următoarele situații:

- apariția unor modificări legislative relevante;
- identificarea unor neconformități sau riscuri majore;
- modificări aprobate ale cerințelor;
- constatări rezultate în urma testării (neconformități, erori sau oportunități de îmbunătățire);
- necesitatea clarificării unor specificații incomplete;
- identificarea de cerințe suplimentare, ajustări sau completări necesare, inclusiv implementarea de noi funcționalități, în condițiile descrise în prezentul Caiet de sarcini;
- ori de câte ori situația o impune, pentru asigurarea conformității soluției cu cerințele contractuale, obiectivele proiectului și cadrul legal aplicabil.

În **faza de analiză**, Prestatorul este responsabil pentru identificarea oricăror lacune, neclarități sau contradicții și are obligația de a solicita clarificări. Lipsa unor clarificări solicitate în această fază nu poate fi invocată ulterior ca motiv de întârziere sau cost suplimentar.

Documentul de analiză, inclusiv versiunile sale ulterioare actualizate, va fi supus unei **proceduri formale de verificare și recepție**.

Autoritatea Contractantă are dreptul de a respinge, total sau parțial, livrabilul în următoarele cazuri, exemplificative, dar nu limitative:

1. Documentul este incomplet sau nu acoperă integral cerințele Caietului de sarcini ori cele comunicate de Autoritatea Contractantă în scris sau în cadrul întâlnirilor de lucru.
2. Cerințele sunt formulate ambiguu sau generic.
3. Lipsesc diagramele, modelele sau matricele necesare sau obligatorii.
4. Nu sunt respectate cele mai bune practici din domeniu.
5. Nu este demonstrată trasabilitatea cerințelor.
6. Nu sunt identificate și tratate riscurile majore.
7. Documentul conține contradicții interne.
8. Nu sunt documentate mecanismele de securitate și protecție a datelor.

Prestatorul are obligația de a remedia neconformitățile în termenul comunicat de Autoritatea Contractantă, care nu poate fi mai mic de 3 zile lucrătoare de la notificare, fără costuri suplimentare în sarcina Autorității Contractante.

Aprobarea Documentului de analiză nu exonerează Prestatorul de răspunderea pentru eventuale omisiuni, erori sau neconformități identificate ulterior.

Prestatorul nu poate invoca ambiguități ale Documentului de analiză aprobat pentru a limita obligațiile contractuale sau a justifica nerespectarea termenelor asumate.

Propunerea tehnică trebuie să cuprindă metodologia detaliată pentru desfășurarea activităților de analiză, precum și descrierea instrumentelor utilizate pentru colectarea, gestionarea și evidențierea cerințelor.

8.2 Faza de proiectare

Faza de proiectare stabilește fundamentul tehnic, arhitectural și funcțional al sistemului digital ePatrimoniu.

În cadrul acestei faze, Prestatorul are obligația de a adopta o **abordare de tip prototip evolutiv**, prin configurarea preliminară a sistemului, astfel încât să asigure Autorității Contractante un suport vizual și funcțional concret pentru validarea modului de implementare a proceselor viitoare.

Prototipul va fi **dezvoltat în mod iterativ** și va fi supus procesului de **verificare și validare** de către Autoritatea Contractantă până la obținerea acceptării finale scrise. Prestatorul are obligația de a colecta, documenta și integra în prototip toate observațiile, recomandările și solicitările formulate de Autoritatea Contractantă sau de persoanele desemnate de aceasta pe parcursul procesului de analiză și validare. În măsura în care sunt formulate observații sau solicitări de modificare, Prestatorul va proceda la actualizarea corespunzătoare a prototipului și îl va retransmite spre validare. Procesul de validare se va relua ori de câte ori este necesar până la obținerea validării finale scrise a prototipului, aceasta constituind **condiție pentru acceptarea fazei de proiectare**.

În cadrul fazei de proiectare, Prestatorul are obligația de a livra **Raportul de proiectare (L2)** - descris în 9.1, **Prototipul vizual al principalelor fluxuri de utilizare (L3)** - descris în 9.1.

Prestatorul are obligația de a respecta **Manualul de identitate vizuală și Designul de sistem ePatrimoniu** puse la dispoziție de Autoritatea Contractantă. Pentru a respecta o identitate vizuală unitară, Prestatorul va consulta constant Manualul de identitate vizuală și Designul de sistem ePatrimoniu, puse la dispoziție de Autoritatea Contractantă. Prestatorul va ține cont, de asemenea, de propunerile în format web transmise de Autoritatea Contractantă, care exemplifică module sau pagini ale sistemului digital. Mai multe detalii se regăsesc în capitolul 7.6.2 UI/UX.

Prestatorul are obligația de a pregăti și pune la dispoziția Autorității Contractante infrastructura pentru mediile de dezvoltare, testare și de producție: pregătire mediu de dezvoltare și testare (obiectele din baza de date, instalare și configurare servere de aplicații și rapoarte, configurații de înaltă disponibilitate, etc); pregătire mediu de producție (obiectele din baza de date, instalare și configurare servere de aplicații și rapoarte, configurații de înaltă disponibilitate etc); pregătire mediu de gestionare și întreținere automată a versiunilor de aplicație (mediu de "continuous integration").

8.3 Faza de dezvoltare, migrare și testare

În această fază, Prestatorul va desfășura activități de configurare, parametrizare, personalizare, dezvoltare software, migrare date și testare.

Totodată, Prestatorul va realiza instalarea și configurarea tuturor produselor software pe baza arhitecturii de deploy în cloud aprobate prin **Raportul de proiectare (L2)**. Orice abatere de la arhitectura validată va putea fi realizată exclusiv cu acordul prealabil scris al Autorității Contractante.

Instalarea și configurarea vor fi efectuate astfel încât să asigure funcționarea corespunzătoare, securitatea, stabilitatea și performanța sistemului în mediile configurate.

La finalizarea activității, Prestatorul va elabora un **Raport de instalare și configurare a componentelor software (L4)**, descris în capitolul 9.1.

Prestatorul are obligația de a se asigura că informațiile privind autentificarea sunt transmise în condiții de securitate și că Autoritatea Contractantă dobândește control deplin asupra mediilor instalate.

În cazul în care, în urma verificărilor efectuate de Autoritatea Contractantă, se constată că procesul de instalare și/sau configurare nu a fost realizat conform cerințelor aprobate, conține erori, vulnerabilități sau abateri de la arhitectura validată, sau că Raportul de instalare și configurare este incomplet, conține informații eronate sau nu reflectă în mod fidel instalarea și configurarea efectivă a componentelor software, ori în cazul în care se constată neconformități față de arhitectura aprobată sau cerințele contractuale, Autoritatea Contractantă are dreptul de a respinge, total sau parțial, atât

procesul de instalare și configurare, cât și Raportul aferent și de a solicita remedierea neconformităților constatate.

Respingerea va fi comunicată în scris, cu indicarea neconformităților constatate, iar Prestatorul are obligația de a remedia deficiențele, respectiv de a reconfigura componentele afectate și de a retransmite livrabilul.

În situația în care, după remediere, se constată în continuare neconformități sau deficiențe majore, Autoritatea Contractantă își rezervă dreptul de a aplica toate măsurile prevăzute în contract pentru neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor de către Prestator.

8.3.1. Dezvoltare

Întrucât sistemul informatic integrat va trebui să respecte cerințele funcționale și nefuncționale specifice Autorității Contractante, Prestatorul va desfășura activități de configurare, parametrizare, personalizare, dezvoltare software și testare. Aceste activități se vor desfășura pe mediile de testare și dezvoltare, pe baza prototipului validat și pe feedback-ul colectat în faza de proiectare.

Prestatorul va asigura acces în regim *read-only* la mediul de versionare al codului sursă (ex. Git, SVN, etc.), pentru părțile desemnate de Autoritatea Contractantă, în scopul verificării și auditării activităților de dezvoltare.

Prestatorul va pune la dispoziția Autorității Contractante acces la platforma de ticketing internă, limitat la drepturi de vizualizare asupra tichetelor, pentru membrii desemnați de către Autoritatea Contractantă.

De asemenea, în cadrul platformei se va implementa o zonă dedicată modificărilor asupra codului sursă. Prestatorul va asigura integrarea automată a notelor de versiune (release notes) cu modulul dedicat administratorilor de sistem din platformă. Modulul va permite afișarea versiunilor publicate, a listei de modificări (commit-uri) asigurând trasabilitatea completă între codul sursă și versiunilor livrate. Lista de modificări poate fi doar vizualizată, nu se poate interveni asupra ei prin procesul de editare. Nu va fi permisă ștergerea acestor elemente din sistem.

Prestatorul va asigura Autorității Contractante o cât mai bună vizibilitate asupra stadiului implementării sistemului, printr-o abordare de implementare flexibilă, iterativă, bazată pe un feedback rapid și o disponibilitate sporită.

Planul de implementare a activităților contractului (anexă la Ofertă) va fi actualizat pentru a cuprinde fazele / etapele identificate ca urmare a fiecărei iterații a fazei de analiză aferente jaloanelor, conform metodologiei de dezvoltare a sistemelor informatice de tip iterativ. Acestea vor fi structurate în sprinturi, conform metodologiei de dezvoltare, cu o durată între 2 și 4 săptămâni.

Fiecare sprint (iterație) de implementare va adăuga funcționalități noi și le va rafina / modifica / actualiza pe cele existente.

Fiecare versiune livrată va avea un număr de versiune unic, conform schemei de versionare agreate:

Tip versiune	Exemplu	Semnificație
Majoră	3.0.0	Structuri de date modificate, rescrieri module, schimbări majore
Minoră	3.4.0	Funcționalități noi, compatibile cu versiunile anterioare
Patch	3.4.21	Bugfix-uri, optimizări, fără schimbări funcționale

Prestatorul are obligația de a livra, la finalul fiecărui sprint, o versiune funcțională a sistemului digital, care să includă integral funcționalitățile asumate în acel sprint și să fie pusă în producție.

Versiunea livrată la finalul sprintului trebuie să respecte criteriile de acceptanță definite pentru fiecare set de funcționalități din sprint (agreate la începutul fiecărui sprint cu Autoritatea Contractantă și acceptate de către aceasta) și să nu conțină defecte critice sau blocante, altfel, sprintul nu poate fi considerat livrat, iar Prestatorul are obligația de a remedia neconformitățile în următorul sprint. Semnarea procesului-verbal de predare primire aferent livrărilor cuprinse în fiecare jalon este condiționată de acceptarea a către AC a sprinturilor realizate de Contractant.

La sfârșitul fazei de dezvoltare, Prestatorul are obligația de a se asigura că toate cerințele și specificațiile prevăzute în Caietul de sarcini, cele definite în fazele de analiză și proiectare, precum și optimizările identificate pe parcursul dezvoltării sunt integral implementate, funcționale și conforme cu standardele și criteriile de calitate agreate, astfel încât să permită validarea de către Autoritatea Contractantă.

Autoritatea Contractantă are dreptul de a verifica și valida îndeplinirea tuturor cerințelor și specificațiilor, iar în cazul constatării unor neconformități sau deficiențe, le va comunica Prestatorului, care are obligația de a le remedia.

Înainte de punerea în producție, versiunile trebuie să primească validarea AC.

8.3.2. Migrarea datelor

Migrarea datelor din sistemele existente este o etapă a fazei de dezvoltare, migrare și testare și va fi realizată de Prestator astfel încât toate datele să fie corect, complet și consistent transferate către modelul de date al sistemului digital ePatrimoniu. În acest sens, Prestatorul va elabora un Plan și proceduri de migrare a datelor (metodologii detaliate de import, mapare și validare).

Prestatorul va testa corectitudinea, completitudinea și consistența datelor migrate și va documenta integral procesul.

Prestatorul va asigura Autorității Contractante vizibilitate asupra stadiului migrării și va integra observațiile și recomandările acesteia pe tot parcursul procesului.

Activități principale:

- testarea corectitudinii, completitudinii și consistenței datelor migrate;
- testarea unitară, de integrare și de acceptanță pentru fiecare increment livrat;
- implementarea mecanismelor de versionare și actualizare controlată a componentelor sistemului;
- documentarea completă a soluției, incluzând ghiduri de instalare, administrare și utilizare.

Procedura de migrare va fi implementată și testată. Importul va presupune minimum preluarea metadatelor și a fișierelor binare asociate bunurilor culturale digitalizate, cu respectarea categoriilor, formatelor, ontologiilor, structurilor de date implementate / disponibile în aplicație.

Livrabilul aferent procesului de migrare este documentul **Plan și proceduri de migrare a datelor (metodologii detaliate de import, mapare și validare) - (L5)** - descris în capitolul 9.1.

Prestatorul este obligat să realizeze migrarea integrală și corectă a datelor. În cazul identificării de neconformități sau erori de către Autoritatea Contractantă, Prestatorul va remedia aceste deficiențe.

8.3.3. Testare

Prestatorul este responsabil pentru planificarea, pregătirea, executarea, documentarea și actualizarea activităților de testare a sistemului, în vederea demonstrării îndeplinirii tuturor cerințelor funcționale, nefuncționale și de securitate, precum și a compatibilității cu specificațiile de interfațare cu sistemele externe.

Testarea se va desfășura continuu, pe întreaga durată a procesului de dezvoltare, pentru a permite identificarea și remedierea timpurie a neconformităților și pentru a asigura stabilitatea și calitatea sistemului până la livrarea finală și după punerea în producție.

Testarea va fi realizată de către Prestator pentru toate implementările noi și înaintea fiecărei lansări de versiune în mediul de producție.

Activitățile de testare vor include, după caz, abordări de tip white-box, grey-box și black-box, corespunzător nivelului de acces la informații și obiectivelor fiecărei etape de testare, inclusiv în cadrul testării de securitate și al testelor de penetrare.

Prestatorul are obligația de a elabora o **Matrice de conformitate (L6)**, descrisă în capitolul 9.1, având ca scop demonstrarea trasabilității dintre cerințele prevăzute în Caietul de Sarcini și funcționalitățile implementate și testate ale sistemului.

Draftul matricei de conformitate va fi întocmit de către Prestator și va fi supus aprobării Autorității Contractante în perioada de analiză.

Matricea de conformitate va fi actualizată de Prestator pentru fiecare livrare de jalon și va fi transmisă Autorității Contractante împreună cu rapoartele de testare internă pe componentele care fac obiectul livrărilor.

Autoritatea Contractantă are dreptul de a solicita clarificări, remedieri, dovezi de conformitate sau testări suplimentare, la prezentarea fiecărei versiuni a matricei de conformitate.

Prestatorul va elabora un **Plan de Testare (L7)** descris în capitolul 9.1, care va fi supus aprobării Autorității Contractante înainte de începerea activităților de dezvoltare.

1. Testare funcțională

Aceasta va include, fără a se limita la:

- Unit Testing - testarea unităților sau componentelor individuale ale aplicației;
- Integration Testing - verificarea funcționării corecte a interacțiunilor dintre componente și module;
- System Testing - testarea sistemului ca ansamblu, pentru a confirma îndeplinirea tuturor cerințelor funcționale.

Testele funcționale vor acoperi toate funcționalitățile prevăzute în Caietul de Sarcini, pentru fiecare modul și componentă a sistemului, având ca scop verificarea respectării fluxurilor de lucru pentru toți actorii implicați, a corectitudinii procesării și generării datelor, a validării datelor de intrare și a corectitudinii datelor de ieșire, precum și a gestionării și personalizării corespunzătoare a erorilor și a mesajelor de alertă. De asemenea, testele funcționale vor confirma aplicarea corectă a regulilor de business definite în Caietul de Sarcini și în fluxurile de business definite în perioada de analiză. Testele funcționale vor include și testarea integrării între componente și modulele sistemului, precum și interacțiunile cu sistemele externe, cu respectarea specificațiilor de interfațare. Testarea sistemului, în ansamblul său funcțional, va include scenarii și cazuri de testare menite să demonstreze conformitatea cu toate cerințele prevăzute în prezentul Caiet de Sarcini, precum și buna funcționare end-to-end a tuturor fluxurilor de business și operaționale definite.

2. Testare non-funcțională

Aceasta va include, cel puțin:

- Performance Testing - evaluarea performanței sistemului în condiții normale de utilizare;
- Load Testing - verificarea comportamentului sistemului sub sarcini de lucru așteptate;
- Stress Testing - evaluarea comportamentului sistemului în condiții extreme sau neprevăzute;
- Security Testing - identificarea vulnerabilităților și a riscurilor de securitate.

Testarea non-funcțională are ca scop evaluarea caracteristicilor de calitate ale sistemului, altele decât funcționalitatea propriu-zisă. Testele non-funcționale trebuie

să acopere cerințele de disponibilitate, scalabilitate, fiabilitate, robustețe, salvare și restaurare, recuperare în caz de dezastru, estimări capacitate și planificare, performanță, management configurații, extensibilitate / flexibilitate, siguranță în funcționare, reziliență, securitate, management și monitorizare sistem, conectivitate și calitate servicii.

Testarea securității (Security Testing) presupune, dar fără a se limita la: identificarea vulnerabilităților (ex. SQL injection, XSS, autentificare slabă, acces neautorizat, evaluarea riscurilor, simularea atacurilor (penetration testing), respectarea cerințelor de securitate în legislație (ex. ISO 27001, OWASP Top 10), precum și testarea mecanismelor de protecție (autentificare, autorizare, criptare, audit, logare, etc.).

În cadrul testării non-funcționale, Prestatorul va realiza și activități de evaluare a utilizabilității interfețelor sistemului digital (usability testing). Testele de utilizabilitate vor urmări măsura în care interfața sistemului este intuitivă, eficientă și ușor de utilizat pentru actorii definiți în cadrul sistemului. Prestatorul va planifica și executa teste de utilizabilitate cu utilizatori reprezentativi utilizând metode calitative și cantitative (de exemplu: scenarii de utilizare, task-based testing, observație directă, chestionare de satisfacție etc.). Rezultatele testelor vor fi documentate și vor fundamenta îmbunătățirea continuă a soluțiilor de design UI/UX ale sistemului digital.

Activitățile de testare de utilizabilitate se vor aplica tuturor componentelor sistemului digital care includ interfețe destinate utilizatorilor.

Testele de performanță, încărcare și acceptanță (UAT) se vor executa și pe platforma de producție.

3. Testare de regresie

Este un proces continuu care se adaptează la modificările din software și cerințele contractului.

Mediul și instrumentele de testare

Prestatorul trebuie să precizeze în propunerea tehnică, conform structurii definite în cadrul capitolului 12.1 din prezentul Caiet de Sarcini, toate instrumentele de testare utilizate, inclusiv aplicații, scripturi etc. destinate a fi utilizate în timpul procesului de testare. Prestatorul trebuie să pună la dispoziția Autorității Contractante, la cerere, instrumentele, mediile și datele de testare utilizate, precum și documentația aferentă, în condiții care să permită reproducerea integrală și verificarea independentă a rezultatelor consemnate în raportul de testare intern.

Mediul de testare nu trebuie să fie reutilizat sau integrat în alt mod în mediul de producție.

Pe întreg ciclul de dezvoltare al sistemului digital, Prestatorul va realiza activitățile de testare corespunzătoare și va întocmi **Rapoarte de testare - L8**, descrise în capitolul 9.1.

Autoritatea Contractantă își rezervă dreptul de a solicita Prestatorului prezentarea rapoartelor de testare, la orice moment, ori de câte ori consideră necesar, pe durata derulării contractului.

Testarea funcțională de acceptanță

Testarea funcțională de acceptanță se va realiza de către Autoritatea Contractantă, în prezența Prestatorului, după finalizarea testelor și remedierea tuturor vulnerabilităților identificate folosind Planul de Testare, Rapoarte de Testare Internă ale Prestatorului, Manuale de utilizare (actori interni și actori externi ai Sistemului Digital), Manualul de administrare, dar fără a se limita strict la acestea.

Testarea de acceptanță va avea ca obiectiv verificarea îndeplinirii integrale a cerințelor funcționale și nefuncționale prevăzute în prezentul Caiet de Sarcini, din perspectiva utilizatorilor finali și a scenariilor reale de utilizare.

Scenariile, cazurile și criteriile de testare funcțională de acceptanță vor fi propuse și/sau validate de Autoritatea Contractantă, pe baza cerințelor din Caietul de Sarcini, instruirea livrabilelor contractuale și a rezultatelor fazelor anterioare de analiză și proiectare. Prestatorul va avea obligația de a asigura suportul tehnic necesar desfășurării testelor și de a pune la dispoziție toate informațiile, documentațiile și mediile necesare testării.

Pentru fiecare livrare intermediară (de jalon) și anterior acceptanței finale, Prestatorul va furniza rapoarte interne de testare complete, precum și versiunea actualizată a Matricei de Conformitate, din care să rezulte corelarea explicită a cerințelor din prezentul Caiet de Sarcini cu funcționalitățile implementate, stadiul de maturitate tehnică, funcțională și operațională a componentelor livrate, în vederea punerii în exploatare.

Acceptanța funcțională finală este acordată exclusiv de Autoritatea Contractantă și este condiționată cumulativ de:

- marcarea cu „pass” a tuturor cazurilor de testare funcțională de acceptanță stabilite de Autoritatea Contractantă;
- implementarea integrală și demonstrabilă a tuturor cerințelor din prezentul Caiet de Sarcini;
- inexistența oricăror neconformități critice sau majore care afectează utilizarea sistemului în exploatare;
- respectarea cerințelor de securitate conform 7.5 și a celor de accesibilitate și UI/UX conform 7.6,

Neîndeplinirea oricăruia dintre criteriile de mai sus atrage neacceptarea livrării, fără a genera drepturi suplimentare de plată pentru Prestator.

Prestatorul va produce și preda următoarele livrabile, care vor reflecta complet implementarea, configurarea, testarea și pregătirea sistemului pentru exploatare: **Manualul de administrare a sistemului (L9), Manualul de utilizare a sistemului (L10), Planul de măsuri privind protecția datelor cu caracter personal (L11),**

Planul de minimizare a riscurilor provenite din lanțul de aprovizionare (L12), Documentația tehnică pentru avizarea ADR a sistemului electronic de arhivare (L25) și Procedură de efectuare a copiilor de siguranță și restaurare (L26) descrie în capitolul 9.1.

8.4. Faza de punere în producție

În cadrul acestei faze, Prestatorul va realiza toate activitățile necesare pentru operaționalizarea sistemului digital în mediul de producție, în condiții de siguranță, performanță și continuitate operațională.

Activitățile includ:

- configurarea mediului de producție și replicarea parametrilor de testare validați, respectiv migrarea soluțiilor implementate din mediul de testare/dezvoltare în mediul de producție, cu respectarea configurațiilor validate;
- încărcarea datelor finale migrate și verificarea acurateței, consistenței și integralității acestora, cu efectuarea ajustărilor necesare pentru alinierea completă la datele sursă și la cerințele sistemului;
- realizarea testelor finale de performanță, disponibilitate și securitate în mediu real;
- implementarea sistemului de monitorizare și alertare;
- asigurarea asistenței tehnice pentru lansarea oficială și pentru perioada de stabilizare a sistemului;
- elaborarea procedurilor de backup, restaurare și recuperare în caz de dezastru (DR).

Ca parte integrantă a acestei faze, Prestatorul are obligația de a elabora și preda **Documentația „as-built” a sistemului digital (L17)**. Aceasta va actualiza și consolida toate specificațiile din faza de proiectare pentru a reflecta cu exactitate configurația finală din mediul de producție.

Prestatorul are obligația de a asigura migrarea completă, corectă și verificabilă a datelor din sistemele sursă în mediul de producție, fără pierderi de informații, coruperi de date sau alterări neautorizate ale structurii și conținutului acestora. Orice pierdere de date, trunchiere, mapare eronată sau neconformitate structurală identificată ulterior punerii în producție va fi remediată de îndată de Prestator, fără costuri suplimentare.

Activitățile se vor desfășura în conformitate cu **Planul de punere în producție (L18)** realizat de Prestator și agreeat de Autoritatea Contractantă.

Prestatorul are obligația de a transmite informațiile privind autentificarea (conturi administrative, credențiale, chei de acces, certificate digitale etc.) în condiții de securitate, prin mecanisme protejate.

Autoritatea Contractantă trebuie să dobândească control deplin și exclusiv asupra mediilor instalate, inclusiv drepturi de administrare complete.

Nu este permisă existența unor conturi ascunse, mecanisme de acces neautorizate sau configurări care să permită accesul unilateral al Prestatorului fără acordul explicit al Autorității Contractante.

La finalul procesului, Prestatorul va furniza un **Raport de punere în producție (L19)**.

Recepția fazei de punere în producție și declararea jaloanelor aferente ca fiind realizate vor fi condiționate de îndeplinirea cumulativă a tuturor cerințelor prevăzute în prezentul caiet de sarcini și în **Planul de punere în producție (L18)** acceptat de Autoritatea Contractantă.

Recepția va fi condiționată, în mod obligatoriu, de:

- operaționalizarea sistemului în mediul de producție conform arhitecturii aprobate și cerințelor contractuale;
- finalizarea și validarea testelor de performanță, securitate și disponibilitate;
- implementarea și testarea procedurilor de backup și recuperare în caz de dezastru;
- predarea și acceptarea Documentației „as-built”, completă și conformă;
- predarea și acceptarea Raportului de instalare și configurare, care trebuie să reflecte în mod fidel configurația efectivă a sistemului.

În cazul în care, în urma verificărilor efectuate de Autoritatea Contractantă, se constată că procesul de punere în producție nu a fost realizat conform cerințelor aprobate, datele migrate prezintă erori, lipsuri, inconsistențe sau abateri de la structura validată, există vulnerabilități de securitate sau abateri de la arhitectura aprobată sau există alte neconformități față de cerințele contractuale, Autoritatea Contractantă are dreptul de a respinge, total sau parțial, procesul de punere în producție, precum și livrabilele aferente.

Prestatorul are obligația de a remedia toate deficiențele, de a reconfigura componentele afectate și de a retransmite livrabilele corespunzătoare.

În situația în care, după remediere, se constată în continuare neconformități sau deficiențe majore, Autoritatea Contractantă își rezervă dreptul de a aplica toate măsurile prevăzute în contract pentru neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor contractuale.

8.5 Instruire pentru utilizatori și administratori

Obiectivul serviciilor de instruire îl constituie asigurarea unui transfer structurat de cunoștințe și competențe necesare către personalul Ministerului Culturii și al entităților aflate în subordinea sau coordonarea acestuia (direcțiile județene de cultură, Institutul Național al Patrimoniului etc.), precum și către alte persoane interesate desemnate de Autoritatea Contractantă, în vederea utilizării, administrării și operării autonome, eficiente și în condiții de securitate a sistemului digital ePatrimoniu.

Se urmărește ca prin participarea la cursurile de instruire, cursanții să dobândească un nivel de cunoștințe teoretice și competențe practice referitoare la funcționalitățile soluției dezvoltate, care să le permită să desfășoare în cele mai bune condiții activitățile curente ce presupun utilizarea soluției. Astfel, Prestatorul va asigura dobândirea de către participanți cel puțin a competențelor necesare pentru: utilizarea funcționalităților operaționale ale sistemului în conformitate cu rolurile și drepturile de acces atribuite, gestionarea fluxurilor de lucru și a proceselor specifice, administrarea configurațiilor și a componentelor sistemului, pentru utilizatorii cu atribuții specifice, aplicarea măsurilor și procedurilor privind securitatea informațiilor și protecția datelor cu caracter personal.

Pentru a asigura exploatarea în bune condiții a sistemului digital, Prestatorul va elabora un **Plan de instruire (L13)**, structurat pe **tipuri de utilizatori**, după cum urmează:

- a. **Administratori (personal tehnic)** – aprox. 10 persoane, cu durata minimum 5 zile*;
- b. **Utilizatori avansați** (personal operațional din cadrul Ministerului Culturii, INP, DJC, membrii Comisiilor de specialitate) – aprox. 150 de persoane, cu durata minimum 5 zile*, aprox. 15 - 20 participanți/sesiune;
- c. **Utilizatori standard** (personalul instituțiilor culturale și ai altor entități relevante etc.) – aprox. 100 de persoane, cu durata minimum 2 zile*, aprox. 15 - 20 participanți/sesiune;

*zilele nu vor fi consecutive, ci vor fi corelate cu punerile în producție ale versiunilor, conform Capitolului 9.2. Fără realizarea instruirii, jaloanele nu va fi considerat finalizate de Prestator și acceptate de Autoritatea Contractantă.

Administratorii și utilizatorilor avansați vor beneficia de instruire adaptate rolurilor și responsabilităților specifice fiecărei categorii.

Cursurile vor fi organizate în **format classroom** (sesiuni teoretice și demonstrative, cu explicații detaliate privind funcționalitățile, fluxurile operaționale, rolurile și drepturile de acces) și **hands-on** (sesiuni practice, în care cursanții vor aplica cunoștințele și competențele dobândite prin realizarea de activități reale sau simulate, conform scenariilor standardizate, sub supravegherea formatorului), astfel încât să combine prezentarea teoretică a funcționalităților sistemului cu exerciții practice efectuate direct în mediul de test al platformei.

Instruirea trebuie să fie realizată de experții cheie și/sau non-cheie alocați contractului, în funcție de decizia Prestatorului.

Conținutul și durata fiecărei sesiuni vor fi adaptate în funcție de complexitatea funcționalităților abordate și de profilul participanților, astfel încât să se asigure dobândirea competențelor necesare pentru utilizarea autonomă, eficientă și sigură a sistemului.

Instruirea administratorilor (personal tehnic) se va realiza în format fizic și are ca obiectiv dobândirea următoarelor cunoștințe și competențe minime:

- administrarea utilizatorilor și a permisiunilor asociate acestora în cadrul aplicației;
- operarea interfețelor grafice ale sistemului;
- administrarea și particularizarea sistemului, inclusiv configurarea componentelor;
- consultarea jurnalelor de audit privind accesul și operațiunile desfășurate în sistem;
- întreținerea aplicației, cu toate componentele sale;
- definirea și întreținerea nomenclatoarelor la nivel central și județean;
- definirea și dezvoltarea de rapoarte și analize;
- procedura de import al resurselor;
- configurarea șabloanelor standard și personalizate.
- operarea tuturor softurilor utilizate în sistemul digital (baze de date, servere de aplicații, servere rapoarte etc).

Pentru administratori, se vor furniza manuale de administrare pentru toate softurile utilizate în sistemul digital care să trateze inclusiv cazurile cele mai uzuale de erori, proceduri de lucru, ghid de mentenanță etc.

Instruirea utilizatorilor avansați va urmări dobândirea cunoștințelor și competențelor necesare pentru:

- utilizarea generală și specifică a sistemului, a componentelor și a funcționalităților sale;
- adăugarea, modificarea și ștergerea datelor în sistem, conform rolurilor și drepturilor de acces;
- respectarea fluxurilor operaționale și procedurilor standard;
- utilizarea rapoartelor și a analizelor, în funcție de rol și responsabilități;
- aplicarea măsurilor de securitate a informațiilor și protecția datelor cu caracter personal.

Suportul de curs va consta în **manualele de utilizare a sistemului (L10)**, redactate în limba română, livrate în format digital și care vor reflecta conținutul ultimei versiuni a sistemului acceptate de Autoritatea Contractantă. Pentru principalele cazuri de utilizare, Prestatorul va crea **tutoriale video dedicate (L14)**, prin intermediul cărora vor fi prezentate principalele funcționalități ale sistemului. Durata tutorialelor va varia în funcție de complexitatea cazului de utilizare. Tutorialele vor fi realizate **separat pentru utilizatorii interni și pentru utilizatorii externi**, astfel încât să reflecte specificul rolurilor și nivelurilor de acces. Lista tutorialelor video va fi stabilită în faza de dezvoltare, migrare și testare.

Modalitatea de desfășurare a cursurilor (format online, fizic sau hibrid) va fi stabilită în perioada de pregătire a activității, în acord cu Autoritatea Contractantă. Prestatorul va suporta integral costurile legate de instructori și costurile materialelor asociate desfășurării sesiunilor de instruire.

Sesiunile de instruire organizate în **format clasic** (cu prezența fizică a tuturor participanților) se vor realiza într-o locație pusă la dispoziție și echipată corespunzător de către prestator. Locația aleasă pentru desfășurarea sesiunilor de instruire trebuie să fie amplasată pe o rază de 3 km față de Biblioteca Națională a României (km 0) în vederea facilitării deplasării participanților.

Pentru derularea în condiții optime a sesiunilor de instruire ce trebuie organizate în format clasic, Prestatorul trebuie să asigure:

- toate condițiile logistice și tehnice necesare derulării sesiunilor de instruire (videoproiector, flipchart, ecran de proiecție, accesul la internet în sistem wireless etc);
- participarea cel puțin a unui membru din echipa de implementare, cu rol de observator, la sesiunile de instruire, în aceleași condiții ca și un participant.

Pentru cursurile organizate în format online, Prestatorul va asigura toate condițiile logistice și tehnice necesare derulării sesiunilor de instruire, inclusiv softul utilizat în sistemul de videoconferință, care trebuie să fie agreat de către beneficiar și să poată fi utilizat pe o gamă largă de terminale și sisteme de operare, ținând cont de faptul că mediile de lucru ale cursanților sunt eterogene.

Sesiunile de instruire se vor derula în limba română. Materialele de curs vor fi redactate în limba română și se vor referi la soluția / funcționalitățile implementate.

Ofertanții trebuie să prezinte procedurile după care vor realiza programul de instruire. Procedurile vor conține cel puțin următoarele informații:

- a. Descrierea cursurilor de instruire și a rezultatelor așteptate;
- b. Modalitatea de evaluare a programului de instruire;
- c. Formulare utilizate.

Prestatorul răspunde pentru caracterul adecvat, complet și proporțional al programului de instruire în raport cu complexitatea, funcționalitățile și nivelul tehnologic al sistemului dezvoltat și implementat, astfel încât instruirea să permită utilizarea autonomă a acestuia de către personalul desemnat de Autoritatea Contractantă.

Prestatorul va asigura un **mecanism de transfer de cunoștințe** către personalul desemnat de Autoritatea Contractantă (materiale reutilizabile, proceduri/ ghiduri metodologice), astfel încât acesta să poată asigura ulterior instruirea noilor utilizatori fără dependență operațională de Prestator.

Prestatorul va furniza un **Raport de instruire - L15** care va fi însoțit de înregistrările sesiunilor (pentru instruirile online), respectiv de fotografii cu participanții din timpul desfășurării sesiunilor (pentru instruirile în format fizic), precum și de acordurile participanților privind prelucrarea datelor cu caracter personal, colectate în conformitate cu legislația aplicabilă. Raportul de instruire va include și lista de prezență nominală a participanților pentru fiecare sesiune desfășurată.

Serviciile de instruire vor fi considerate îndeplinite dacă sunt respectate cumulativ următoarele condiții:

- realizarea tuturor instruirilor planificate, cu respectarea cerințelor prevăzute în prezentul caiet de sarcini;
- punerea la dispoziție a materialelor și tutorialelor conform cerințelor;
- predarea documentației finale actualizate (e.g. manuale, materiale suport, ghiduri metodologice, proceduri);
- predarea raportului de instruire și aprobarea acestuia de către Autoritatea Contractantă.

8.6 Faza de stabilizare operațională a sistemului

După finalizarea jalonului 4, Prestatorul va derula o fază de stabilizare operațională, desfășurată în mediul de producție, având ca scop consolidarea funcționării soluției și confirmarea comportamentului stabil al acesteia în condiții reale de exploatare.

În cadrul fazei de stabilizare, Prestatorul va asigura monitorizarea intensivă a sistemului, verificarea funcționării integrate a componentelor, serviciilor și fluxurilor operaționale, urmărirea indicatorilor de performanță, disponibilitate, securitate, accesibilitate, UI/UX, AI, continuitate, integritate și consistență a datelor, precum și identificarea, analizarea și remedierea disfuncționalităților și neconformităților constatate în exploatarea curentă.

Faza de stabilizare poate include, fără a se limita la acestea, următoarele activități:

- optimizare operațională a sistemului;
- ajustarea parametrilor de configurare;
- calibrarea mecanismelor de monitorizare, alertare, backup și restaurare;
- verificarea și consolidarea integrărilor și a schimburilor de date cu alte sisteme;
- remedierea disfuncționalităților apărute în exploatare;
- acordarea de suport operațional Autorității Contractante pentru utilizarea curentă a sistemului.

Faza de stabilizare reprezintă etapa anterioară recepției calitative finale a sistemului digital.

Recepția calitativă finală a sistemului digital se va realiza numai după finalizarea fazei de stabilizare și după confirmarea, de către Autoritatea Contractantă, a faptului că sistemul funcționează stabil în mediul de producție, fără disfuncționalități majore care să afecteze utilizarea normală a componentelor și fluxurilor operaționale.

8.7. Mentenanță corectivă și evolutivă

De la data semnării **procesului-verbal de recepție calitativă finală a sistemului digital ePatrimoniu**, Prestatorul va asigura servicii de mentenanță corectivă pentru o perioadă de minimum 36 de luni.

În cadrul acestei faze se operează modificări asupra platformei, pentru a se corecta defecte, pentru a se extinde setul de funcționalități oferite de aceasta, pentru a implementa optimizări de natură să îmbunătățească performanța platformei și calitatea serviciilor oferite utilizatorilor săi.

Prestatorul are obligația de a asigura funcționarea continuă, stabilă și conformă a sistemului, în parametrii funcționali, de performanță, securitate, disponibilitate și integritate a datelor agreeți prin contract.

Prestatorul are obligația de a transmite Autorității Contractante **rapoarte anuale de mentenanță (L22)**, în termen de 30 de zile de la încheierea fiecărui an contractual, precum și un **raport final de mentenanță (L23)**, în termen de 30 de zile de la expirarea perioadei de mentenanță.

Rapoartele vor include cel puțin: situația incidentelor gestionate, timpii de răspuns și remediere, actualizările și patch-urile aplicate, activitățile de mentenanță corectivă și evolutivă realizate (dacă este cazul), precum și eventualele recomandări privind funcționarea ulterioară a sistemului.

Raportul final constituie documentul suport pentru recepția finală a serviciilor de mentenanță.

Activitatea de mentenanță corectivă și evolutivă a sistemului informatic va fi asigurată de către Prestator fără costuri suplimentare pentru Autoritatea Contractantă, prin urmare aceasta va fi trecută cu 0 zile/ om.

8.7.1 Mentenanță corectivă

Mentenanța corectivă reprezintă procesul prin care se aduc modificări asupra sistemului ePatrimoniu ca urmare a unor defecțiuni sau funcționării în afara parametrilor optimi, cu scopul de a restabili capacitatea de funcționare optimă a acestuia.

Mentenanța corectivă va acoperi, pe cheltuiala Prestatorului, remedierea tuturor defecțiunilor, disfuncționalităților și incidentelor identificate în perioada de operare, asigurarea suportului necesar, precum și realizarea actualizărilor și patch-urile de securitate. Pentru toate componentele software constitutive ale sistemului digital ePatrimoniu se va asigura suport tehnic pe perioada mentenanței, începând cu data procesului verbal de recepție calitativă finală a sistemului. Pentru produsele COTS, suportul tehnic va include și dreptul Autorității Contractante de a face update-uri, precum și acces direct la site-ul producătorului pentru a deschide direct cazuri de suport cu acesta.

De maximă importanță este evitarea blocării sistemului, respectiv funcționarea lui continuă și optimă pentru desfășurarea activității curente a tuturor categoriilor de utilizatori.

Toate incidentele vor fi gestionate prin intermediul unei **aplicații software de gestionare a tichetelor**. Pentru fiecare incident vor exista minimum următoarele informații documentate: defectul semnalat, data intervenției, descrierea intervenției, modalitatea de rezolvare a intervenției, durata de intervenție și confirmarea remedierii defectului de către Prestator și Autoritatea Contractantă.

La finalul perioadei de mentenanță, Prestatorul are obligația de a elabora și de a transmite Achizitorului un **Raport final de mentenanță** (L23). Acest raport va centraliza toate incidentele, intervențiile, actualizările software și activitățile de mentenanță desfășurate pe întreaga perioadă de mentenanță și va constitui documentul suport obligatoriu pentru realizarea recepției finale a serviciilor.

În cadrul perioadei de mentenanță se vor asigura:

- rezolvarea bug-urilor care nu au fost identificate în timpul dezvoltării și care apar în faza de producție;
- menținerea funcționării sistemului furnizat în parametrii agreeți (funcțional, performanță, disponibilitate, integritatea datelor etc.);
- instalarea de noi versiuni ale sistemului digital în urma efectuării corecțiilor;
- instalarea de patch-uri de securitate;
- actualizarea manualelor de utilizare și a altor documente în urma efectuării corecțiilor;
- aplicarea modificărilor legislative componentelor software implementate și puse în producție;
- consistența și acuratețea mediilor de lucru și a configurațiilor sistemului digital;
- rezolvarea tuturor incidentelor apărute în sistemul informatic, (referitoare la aplicație, sistem, baza de date, comunicații, securitate etc), până la finalizarea contractului;
- asistență tehnică acordată utilizatorilor;
- comunicare și suport necesar pentru a răspunde incidentelor ridicate de utilizatorii finali cu referire la modul de funcționalitate al sistemului digital.

Nivelul de prioritate și termenii de răspuns aplicabili pentru incidentele semnalate sunt cei prezentați în prima parte a Capitolului 8.

8.7.2 Mentenanța evolutivă

Mentenanța evolutivă reprezintă procesul prin care se aduc modificări și optimizări asupra sistemului digital pentru îmbunătățirea funcționării acestuia, pentru a răspunde unor noi cerințe din partea AC și/sau implementarea unor noi funcționalități în sistem, astfel încât sistemul să răspundă mult mai bine așteptărilor utilizatorilor săi. Activitățile de mentenanță evolutivă se vor realiza de către experții Prestatorului la solicitarea scrisă a Autorității Contractante în limita a 12.000 ore.

Serviciile de mentenanță evolutivă se vor realiza la solicitarea scrisă a Autorității Contractante, în funcție de necesitățile acesteia. În vederea utilizării eficiente și controlate a volumului de ore alocat pentru mentenanța evolutivă, fiecare intervenție va face obiectul unei analize și aprobări prealabile din partea Autorității Contractante. În acest sens, Prestatorul va transmite, anterior demarării oricărei activități, o propunere detaliată care va include cel puțin: descrierea intervenției solicitate, estimarea efortului exprimată în ore/om, tipurile și numărul de experți implicați și impactul estimat asupra sistemului. Autoritatea Contractantă va avea dreptul de a accepta, respinge sau solicita modificarea propunerii (inclusiv ajustarea efortului sau a componenței echipei), iar activitatea va putea fi demarată exclusiv după aprobarea explicită a acesteia. Orele aferente intervențiilor neaprobată în prealabil nu vor fi considerate eligibile pentru decontare din plafonul de ore alocat mentenanței evolutive.

Toate propunerile vor fi gestionate prin intermediul componentei de gestionare a tichetelor. Nivelul de prioritate și termenii de răspuns aplicabili pentru incidentele semnalate sunt cei prezentați în prima parte a Capitolului 8.

8.8. Garanție și suport tehnic

Prestatorul are obligația de a acorda o garanție de **5 ani** pentru întregul sistem digital, începând cu **data procesului-verbal de recepție calitativă finală a serviciilor de mentenanță**.

Garanția va acoperi, pe cheltuiala Prestatorului, funcționarea sistemului în conformitate cu specificațiile tehnice, cerințele funcționale și nefuncționale, indicatorii de performanță și documentația aprobată la data recepției, precum și remedierea tuturor incidentelor identificate, precum și asigurarea suportului tehnic necesar. De maximă importanță este evitarea blocării sistemului. Prestatorul are obligația de a asigura funcționarea continuă, stabilă și sigură a sistemului, fără întreruperi nejustificate, astfel încât activitatea curentă a tuturor categoriilor de utilizatori să nu fie afectată.

Suportul tehnic va consta în remedierea defecțiunilor și anomaliilor apărute în cadrul sistemului, precum și realizarea de actualizări și patch-uri de securitate.

Pentru componentele software licențiate se va asigura suport tehnic pe perioada garanției, începând cu data procesului verbal de recepție calitativă finală a serviciilor.

Pentru produsele COTS, suportul tehnic va include și dreptul Autorității Contractante de a face update-uri precum și acces direct la site-ul producătorului pentru a deschide direct cazuri de suport cu acesta.

Toate incidentele vor fi gestionate prin intermediul unei aplicații software de gestionare a tichetelor. Nivelul de prioritate și termenii de răspuns aplicabili pentru incidentele semnalate sunt cei prezentați în prima parte a Capitolului 8.

La expirarea perioadei de garanție, Prestatorul are obligația de a transmite Autorității Contractante un **Raport final de suport tehnic aferent garanției (L24)**, în termen de 30 de zile de la data încetării garanției.

9. Managementul contractului

9.1 Documente

În tabelul de mai jos sunt sintetizate documentele solicitate:

Fază / Documente	Documente minime ale fazei
8.1. Faza de analiză	
Documentul de analiză a sistemului digital (L1)	Livrabilul va conține cel puțin următoarele informații, fără a se limita la: arhitectura logică a sistemului; modelul conceptual și modelul fizic de date; scenarii prioritare de implementare, specificații funcționale / nefuncționale detaliate; delimitarea funcționalităților componentelor; fluxurile de lucru și stările ciclului de viață al resurselor; diagramele fluxurilor de lucru, diagrama utilizatorilor (user diagram), actorii și rolurile implicate; matricea roluri-permisiuni; tipuri de date colectate; regulile de business; estimările de volum de resurse; criteriile și mecanismele de căutare; utilizatorii și permisiunile asociate; reguli de guvernanta a conținutului; plan de migrare sau import de date existente; metodologii de dezvoltare, testare; descrierea cazurilor de utilizare pentru fiecare flux de lucru, rapoartele generate prin aplicație (sincrone și asincrone), interoperabilitatea cu sisteme externe, descrierea API-urilor și a mecanismelor de integrare cu sisteme externe; analiză riscuri (tehnice, organizaționale, juridice, securitate) și măsuri de reducere / eliminare principii de arhivare electronică și stocare a documentelor; aspecte de securitate, conformitate și control al accesului (ex: autentificare/ autorizare, GDPR); scenarii de utilizare pentru rolurile diferite de utilizatori, lista completă a tehnologiilor utilizate; justificarea utilizării fiecărei tehnologii proprietare; analiza riscului de dependență tehnologică; standardizarea formatelor de date, planul de implementare a contractului. Prima versiune a documentului se va livra cel târziu la T0+3 luni. Frecvență actualizare: Documentul de analiză a sistemului digital va fi revizuit și actualizat înainte de predarea fiecărui jalon, pentru a reflecta evoluțiile, modificările de cerințe și deciziile tehnice asumate în cadrul contractului, dar și de fiecare dată când Autoritatea Contractantă o va cere.

Fază / Documente	Documente minime ale fazei
8.2 Faza de proiectare	
Raport de proiectare (L2)	Raportul de proiectare va conține, dar fără a se limita la: descrierea arhitecturii generale a soluției și a arhitecturii de deploy în cloud; arhitectura logică și funcțională (detalierea componentelor, modulelor și a interacțiunilor dintre acestea); arhitectura tehnică (tehnologii propuse, medii de dezvoltare, test, producție), formulare web reprezentative și reguli de validare de bază, principii generale de UI/UX și accesibilitate; Prima versiune a documentului se va livra cel târziu la T0+3 luni. Frecvență actualizare: Raportul de proiectare va fi revizuit și actualizat ori de câte ori intervin modificări semnificative asupra arhitecturii soluției, arhitecturii de deploy, componentelor sau tehnologiilor utilizate, precum și la începutul fiecărei etape majore de dezvoltare (jalon), pentru a reflecta în mod fidel evoluția tehnică și funcțională a sistemului.
Prototipul vizual al principalelor fluxuri de utilizare (L3)	Prototipul vizual al principalelor fluxuri de utilizare va include cel puțin următoarele elemente, dar fără a se limita la acestea: prototip vizual (pentru diverse ecrane și rolurile diferite de utilizatori), fluxuri de utilizare (ex: depunere cereri, procese de avizare / aprobare, înregistrare sau gestionare bunuri de patrimoniu), navigare și interacțiune (descrierea parcursului utilizatorilor pentru utilizarea platformei), aplicarea principiilor de UI/UX și accesibilitate în interfață, fonturi, utilizare diacritice, formate de tip dată, set de caractere, alinieri câmpuri în funcție de tip, condiționalități afișare acțiuni în funcție de diverse criterii, roluri, etc. Prima versiune a documentului se va livra cel târziu la T0+3 luni. Frecvență actualizare: Prototipul vizual va fi revizuit și actualizat ori de câte ori apar modificări semnificative ale cerințelor funcționale, ale modalităților de utilizare sau ale regulilor de interacțiune, precum și înaintea începerii dezvoltării fiecărui modul major, pentru a asigura validarea de către Autoritatea Contractantă a experienței utilizatorului și a logicii operaționale propuse.
8.3 Faza de dezvoltare, migrare și testare	
8.2.1. Dezvoltare	
Raport de instalare și configurare a	Livrabilul va conține cel puțin următoarele informații: un tabel cu produsele software livrate și instalate, cu versiuni și licențe (tip, durată, drept de utilizare); un tabel cu mașinile virtuale /

Fază / Documente	Documente minime ale fazei
componentelor software (L4)	containerele configurate; descrierea modului de instalare / configurare a fiecărei componente software (inclusiv cu capturi de ecran); o listă de verificare a instalării și configurării preliminare a componentelor software; datele de autentificare (user, parola), dacă este cazul. Se vor detalia instalările sistemului digital atât pe medii virtuale, cât și pe medii cloud. Frecvență actualizare: Raportul de instalare și configurare a componentelor software va fi actualizat ori de câte ori sunt instalate, configurate sau actualizate componente software, sunt create sau modificate mașini virtuale / containere, ori intervin schimbări privind versiunile, licențele sau parametrii de configurare, astfel încât documentația să reflecte permanent configurația reală a mediului implementat.
8.2.2. Migrare	
Plan și proceduri de migrare a datelor (metodologii detaliate de import, mapare și validare) - (L5)	Livrabilul va conține cel puțin următoarele informații: datele utilizate în procesul de migrare și tipurile de date preluate din fiecare sursă; rezultatele procesului de migrare; etapele și calendarul procesului de migrare; metodologia și instrumentele utilizate pentru migrare; regulile de transformare, mapare și validare a datelor; procedurile de testare și validare a rezultatelor migrării; responsabilitățile părților implicate în procesul de migrare, documentația de validare a integrărilor cu sisteme externe. Frecvență actualizare: Planul și procedurile de migrare a datelor vor fi revizuite și actualizate ori de câte ori intervin modificări în sursele de date, structura acestora, regulile de mapare și transformare, metodologia sau instrumentele utilizate pentru migrare, precum și înaintea fiecărei noi etape de migrare planificate, astfel încât documentația să reflecte în mod corect procesele, responsabilitățile și rezultatele asociate.
8.2.3. Testare	
Matricea de conformitate (L6)	Livrabilul va include, cel puțin, următoarele informații: identificatorul și descrierea fiecărei cerințe din Caietul de Sarcini; modulul sau componenta sistemului în care fiecare cerință este implementată; referința la cazul de testare din raportul de testare în care cerința a fost tratată; statusul cerinței (de implementat / în testare / conformă). Frecvență actualizare: Matricea de conformitate va fi revizuită și actualizată ori de câte ori este pus în producție o nouă componentă software, funcționalitate sau sunt implementate modificări relevante asupra sistemului, dar și la predarea fiecărui jalon, astfel încât aceasta să reflecte în mod fidel stadiul

Fază / Documente	Documente minime ale fazei
	de implementare, testare și conformitate al fiecărei cerințe din Caietul de Sarcini.
Plan de testare (L7)	Livrabilul va descrie strategia generală de testare, strategia de priorizare a testelor, și va include, cel puțin, dar fără a se limita la, tipurile de testare menționate în capitolul 8.3.3. Frecvență actualizare: Planul de Testare va fi revizuit și actualizat înaintea fiecărui jalon și ori de câte ori apar modificări ale cerințelor funcționale, nefuncționale sau de securitate, indicând referința spre Rapoartele de Testare aferente, pentru a asigura reflectarea fidelă a strategiei și priorizarea testelor.
Rapoarte de testare (L8)	Fiecare raport de testare întocmit de Prestator va include, cel puțin: scenariile de testare; cazurile de testare; tipul testelor efectuate; metoda de testare (manuală, automată); lista pașilor efectuați; rezultatele testelor (pass/fail); numărul de iterații, data și ora execuției; versiunea aplicației; numele persoanelor care au efectuat testarea; dovezi de testare (capturi de ecran, loguri sau alte artefacte relevante). Pentru fiecare caz de utilizare se vor completa cel puțin următoarele informații: ● id și nume caz de utilizare; ● componenta / modulul / funcționalitatea; ● descriere; ● evenimente de business; ● actori; ● precondiții; ● scenariu principal. Se va completa și cu informații privind: ○ condițiile de accesare a fiecărei componente / modul / funcționalitate, inclusiv cu informații referitoare la drepturile de acces ale utilizatorilor; ○ validările pentru fiecare câmp, mesaje de eroare și/sau de atenționare; ○ condiționările dintre câmpuri și obligativitatea impusă acestora (obligatoriu, opțional, condițional); ○ regulile și condițiile existente; ○ legături cu alte sisteme informatice de unde se preiau și unde se transmit informații și/sau se efectuează validări; ○ nomenclatoare utilizate, acolo unde este cazul; ○ tipuri de vizualizări ale informațiilor pe ecran și în rapoarte (în tipurile de fișiere solicitate), filtre și/sau criterii de căutare simple și complexe; ● scenarii alternative;

Fază / Documente	Documente minime ale fazei
	Frecvență actualizare: Rapoartele de testare vor fi întocmite și actualizate pentru fiecare livrare de jalon și înaintea punerii fiecărei versiuni a sistemului sau a unei noi funcționalități în mediul de producție, precum și la solicitarea Autorității Contractante, pentru a reflecta complet rezultatele testelor și stadiul de conformitate al componentelor livrate.
Operare (perioada de realizare continuă a livrabililor aferentă tuturor etapelor de dezvoltare, migrare și testare)	
Manual de administrare a sistemului (L9)	Livrabilul constituie documentația tehnică a sistemului care trebuie să asigure transferul complet de cunoștințe pentru instalarea, configurarea, administrarea, operarea, mentenanța și monitorizarea acestuia de către personalul IT autorizat al Autorității Contractante, fără suport suplimentar din partea Prestatorului. Acesta trebuie să includă cel puțin următoarele informații (listă neexhaustivă): descrierea generală a sistemului (arhitectura logică și fizică, diagrame de componente și fluxuri de date, descrierea mediilor - dezvoltare, testare, producție, dependențe externe și integrare cu alte sisteme etc.), cerințe tehnice (cerințe hardware și software, cerințe de rețea, versiuni și compatibilități etc.), instrucțiuni pentru instalare și configurare, gestionarea utilizatorilor și a permisiunilor, politici și mecanisme de control al accesului, gestionarea certificatelor digitale, configurarea permisiunilor și a fluxurilor, proceduri pentru backup și restaurarea datelor, ghiduri pentru monitorizarea performanței și a jurnalelor de sistem, precum și proceduri pentru aplicarea patch-urilor și actualizărilor. Manualul va include de asemenea și mecanismul de versionare a ontologiei, care va conține cel puțin următoarele informații (listă neexhaustivă): strategia de versionare, gestionarea modificărilor, regulile de introducere, modificare sau eliminare a claselor și proprietăților, reguli de migrare semantică inclusiv tratarea conceptelor marcate ca deprecated, reguli de validare și verificare a conformității, mecanisme de testare post migrare. Manualul trebuie să detalieze pașii pentru depanare, gestionarea incidentelor, procedurile de securitate și bune practici pentru menținerea integrității și disponibilității sistemului. Frecvență actualizare: Manualul de administrare a sistemului va fi revizuit și actualizat ori de câte ori apar modificări semnificative ale arhitecturii, configurației, funcționalităților sau procedurilor de operare și administrare, precum și înaintea fiecărei livrări de versiune în producție, pentru a reflecta corect

Fază / Documente	Documente minime ale fazei
	instrucțiunile privind instalarea, configurarea, administrarea, mentenanța, securitatea, monitorizarea, gestionarea utilizatorilor și permisiunilor, backup-urile, aplicarea patch-urilor, depanarea și gestionarea incidentelor.
Manuale de utilizare a sistemului (L10)	Livrabilele vor fi ghiduri complete pentru utilizatorii finali, atât interni, cât și externi, pentru operarea corectă a sistemului. Acestea vor include cel puțin următoarele informații: descrierea funcționalităților principale, instrucțiuni pas cu pas pentru realizarea activităților specifice, exemple și scenarii de utilizare. Manualul va include și documentarea extensiilor ontologice, care va conține cel puțin următoarele informații (listă neexhaustivă): diagrama ierarhică completă a extensiei ontologice, regulile de numire și namespace utilizate pentru definirea conceptelor, precum și descrierea modului de utilizare și gestionare a acestor extensii în cadrul sistemului. Manualele trebuie să conțină, de asemenea, informații despre fluxurile de lucru, precum și recomandări și bune practici pentru utilizarea eficientă și sigură a sistemului. Frecvență actualizare: Manualele de utilizare a sistemului vor fi revizuite și actualizate ori de câte ori apar modificări ale funcționalităților sistemului de natură să schimbe modul de desfășurare a activităților din platformă sau scenariilor de utilizare, precum și înaintea lansării fiecărei versiuni majore sau a unei noi funcționalități, pentru a asigura că ghidurile reflectă întotdeauna modul corect și eficient de operare a platformei.
Plan de măsuri privind protecția datelor cu caracter personal (L11)	Livrabilul va respecta cerințele descrise în capitolul 7.5.2 și va conține, dar fără a se limita la: politicile, procedurile și mecanismele operaționale privind confidențialitatea, controlul accesului, retenția și ștergerea datelor, anonimizarea și/sau pseudonimizarea, exercitarea drepturilor persoanelor vizate, gestionarea consimțământului și a incidentelor de securitate, în corelare cu cerințele NIS2, Regulamentul GDPR, eIDAS și legislația națională în vigoare. Frecvență actualizare: Planul de măsuri privind protecția datelor cu caracter personal va fi revizuit și actualizat ori de câte ori intervin modificări legislative sau de reglementare aplicabile (precum NIS2, GDPR, eIDAS sau legislația națională relevantă) schimbări în arhitectura sau funcționalitățile sistemului care implică prelucrarea datelor cu caracter personal, precum și în urma producerii unor incidente de securitate sau a rezultatelor evaluărilor periodice de conformitate.

Fază / Documente	Documente minime ale fazei
Plan de minimizare a riscurilor provenite din lanțul de aprovizionare (L12)	Livrabilul va conține, conform capitolului 7.5.2, dar fără a se limita la: lista completă a tuturor componentelor software care alcătuiesc sistemul (Software Bill of Materials – SBOM), incluzând biblioteci open-source, framework-uri și componente COTS, cu specificarea versiunilor exacte utilizate; descrierea procesului de identificare, monitorizare și evaluare a vulnerabilităților asociate componentelor software utilizate, inclusiv sursele de informare privind alertele de securitate; procedura de gestionare și aplicare a patch-urilor de securitate, inclusiv termenele de remediere și responsabilitățile aferente; măsurile de control și reducere a riscurilor generate de dependențele software din lanțul de aprovizionare; mecanismele de verificare și actualizare periodică a SBOM pe durata derulării contractului, inclusiv pe perioada de garanție; procedurile de notificare a Autorității Contractante în cazul identificării unor vulnerabilități critice sau incidente de securitate asociate lanțului de aprovizionare. Frecvență actualizare: Planul de minimizare a riscurilor provenite din lanțul de aprovizionare va fi revizuit și actualizat ori de câte ori sunt introduse, eliminate sau actualizate componente software în cadrul sistemului (inclusiv actualizarea versiunilor), la apariția unor vulnerabilități relevante sau a unor alerte de securitate care afectează componentele utilizate, precum și periodic, pe întreaga durată a contractului și a perioadei de garanție, pentru a asigura menținerea unui nivel adecvat de securitate și conformitate.
Documentația tehnică pentru avizarea ADR a sistemului electronic de arhivare (L25)	Livrabilul va include, fără a se limita la: descrierea arhitecturii sistemului de arhivare, specificațiile de securitate, mecanismele de asigurare a integrității, autenticității, confidențialității și disponibilității datelor, descrierea fluxurilor arhivistice, structura metadatelor arhivistice, precum și manualul de administrare aferent componentei de arhivare electronică. Documentația va fi elaborată astfel încât sistemul să fie pregătit pentru depunerea dosarului de avizare la Autoritatea pentru Digitalizarea României, în conformitate cu legislația aplicabilă în vigoare. Frecvență actualizare: Documentația tehnică pentru avizarea ADR va fi revizuită și actualizată ori de câte ori intervin modificări relevante asupra componentei de arhivare electronică (arhitectură, mecanisme de securitate, fluxuri arhivistice, metadata), precum și anterior depunerii dosarului de avizare sau redeunerii acestuia, astfel încât documentația să reflecte în mod fidel configurația și funcționarea efectivă a sistemului.

Fază / Documente	Documente minime ale fazei
Procedură de efectuare a copiilor de siguranță și restaurare (L26)	Livrabilul va descrie în mod detaliat politica și procedurile operaționale privind realizarea copiilor de siguranță și restaurarea datelor, incluzând cel puțin: tipurile de backup (complet, incremental, diferențial), frecvența realizării acestora, perioadele de retenție, locațiile de stocare, mecanismele de criptare și protecție, responsabilitățile aferente, scenariile de restaurare (la nivel de fișier, bază de date, sistem complet), precum și procedurile de testare periodică a restaurării pentru verificarea integrității și disponibilității datelor. Se vor include proceduri de operare a sistemului digital: pornirea și oprirea sistemului, proceduri de salvare și restaurare a sistemului din salvările de siguranță. Frecvență actualizare: Procedura de efectuare a copiilor de siguranță și restaurare va fi revizuită și actualizată ori de câte ori intervin modificări semnificative în arhitectura sistemului, infrastructura de stocare, mecanismele de backup sau politicile de securitate aplicabile, precum și în urma testelor periodice de restaurare care evidențiază neconformități sau a producerii unor incidente care afectează integritatea ori disponibilitatea datelor, dar și la cererea Autorității Contractante, astfel încât documentația să reflecte în mod fidel procedurile operaționale aplicate.
8.5 Instruire pentru utilizatori și administratori	
Plan de instruire (L13)	Livrabilul va conține toate serviciile solicitate pentru numărul specificat de utilizatori, va fi supus aprobării Autorității Contractante cu cel puțin 10 zile înainte de începerea instruirii și va conține cel puțin următoarele informații: detalierea modului de organizare și desfășurare; curricula cursurilor de instruire; materialele de curs (pentru fiecare tip de instruire), etc
Tutoriale video pentru principalele funcționalități (L14)	Livrabilele vor respecta următoarele cerințe tehnice minime: format digital standard, compatibil cu platforme comune (MP4 sau echivalent); rezoluție minimă Full HD; narare în limba română, clară și inteligibilă, fără erori gramaticale, de pronunție sau de exprimare, astfel încât informațiile să fie ușor de înțeles și aplicat de către utilizatori; structură modulară (un tutorial per caz de utilizare); accesibile prin platformă sau printr-un sistem de tip knowledge base, care să permită căutarea și consultarea rapidă a tutorialelor și a materialelor de suport. Frecvență actualizare: Tutorialele video vor fi actualizate sau suplimentate ori de câte ori intervin modificări semnificative asupra interfeței, procedurilor / metodelor de utilizare sau funcționalităților prezentate, precum și înaintea lansării fiecărei

Fază / Documente	Documente minime ale fazei
	versiuni majore a sistemului, astfel încât conținutul să reflecte în mod fidel funcționarea platformei.
Raport de instruire (L15)	Livrabilul va include cel puțin următoarele informații: calendarul sesiunilor de instruire; metodologia utilizată (se vor anexa materialele reutilizabile și ghidurile metodologice utilizate); lista participanților, cu indicarea instituției și a categoriei de utilizator, după caz; tematica abordată în cadrul fiecărei sesiuni, corelată cu obiectivele de învățare stabilite; rezultatele evaluărilor realizate (teste, exerciții practice, alte instrumente de verificare a cunoștințelor/ competențelor), inclusiv analiza gradului de atingere a obiectivelor; sinteza și evaluarea feedback-ului colectat de la participanți, precum și măsurile propuse pentru îmbunătățirea eventualelor deficiențe identificate. Frecvență actualizare: Raportul de instruire va fi întocmit după finalizarea fiecărei sesiuni sau serii de sesiuni de instruire, astfel încât să reflecte în mod complet activitățile desfășurate și rezultatele obținute.
8.4 Faza de punere în producție	
Documentația as-built a sistemului digital (L17)	Livrabilul va include obligatoriu, dar nu limitativ: arhitectura finală: diagrame logice și fizice actualizate, incluzând maparea finală a rețelei, adresarea IP, fluxurile de date și porturile de comunicație deschise; inventarul software: lista completă a componentelor software instalate, cu numerele exacte de versiune, patch-urile aplicate și configurațiile specifice (fișiere de configurare, parametri de start-up); configurări de securitate: detalierea politicilor de securitate implementate efectiv (configurații WAF, permisiuni IAM); dependențe: maparea dependențelor între servicii / microservicii, baze de date și sisteme externe; jurnalul modificărilor: o listă a devierilor aprobate față de Proiectul Tehnic inițial și justificarea acestora; date de autentificare (user, parola), dacă este cazul.
Plan de punere în producție (L18)	Livrabilul va cuprinde toate activitățile necesare pentru transferul sistemului în mediul de producție și va ține cont de legăturile logice dintre subsistemele / componentele sistemului, astfel încât să se asigure o trecere în producție coerentă și cu impact minim asupra activităților zilnice ale angajaților Autorității Contractante. Frecvență actualizare: Planul de punere în producție va fi revizuit și actualizat ori de câte ori apar modificări semnificative în arhitectura, componentele sau procedurile sistemului,

Fază / Documente	Documente minime ale fazei
	precum și la fiecare livrare către mediul de producție, indicând referința spre Raportul de punere în producție aferent, pentru a asigura o tranziție coerentă și cu impact minim.
Raport de punere în producție (L19)	Livrabilul care va include cel puțin calendarul și descrierea activităților efectuate; confirmarea migrației și validării datelor; configurările și parametrii finali ai sistemului; eventualele probleme identificate și măsurile aplicate; confirmarea că Autoritatea Contractantă deține control deplin asupra mediilor instalate și funcționale. Frecvență actualizare: Raportul de punere în producție va fi întocmit și actualizat la realizarea fiecărei activități de transfer în mediul de producție, pentru a reflecta complet calendarul și modul de execuție al activităților, validarea datelor, configurările finale ale sistemului, problemele identificate și măsurile aplicate, precum și confirmarea controlului deplin al Autorității Contractante asupra mediilor instalate și funcționale.
8.6. Faza de stabilizare operațională a sistemului	
Raport final de stabilizare operațională (L27)	Document elaborat de Prestator la finalul etapei de stabilizare operațională desfășurate în mediul de producție, prin care se evidențiază modul de derulare a activităților de stabilizare, disfuncționalitățile și neconformitățile identificate după punerea în producție, măsurile de remediere, reglaj, optimizare și configurare aplicate, precum și rezultatele verificărilor efectuate pentru confirmarea funcționării stabile, coerente și susținute a sistemului digital în condiții reale de exploatare. Raportul va include cel puțin situația problemelor identificate și modul de închidere a acestora, rezultatele monitorizării funcționării componentelor și fluxurilor operaționale esențiale, confirmarea stabilității operaționale a sistemului, precum și eventualele aspecte reziduale care nu afectează utilizarea normală a soluției. Raportul îl constituie documentul justificativ pentru finalizarea etapei de stabilizare operațională și pentru susținerea recepției calitative finale a sistemului digital. Frecvență actualizare: Raportul final de stabilizare operațională va fi întocmit la încheierea fazei de stabilizare,
Plan de mentenanță (L20)	Planul de mentenanță este livrabilul care definește strategiile, responsabilitățile și procedurile pentru asigurarea funcționării continue a sistemului incluzând și acțiunile corective și evolutive pentru menținerea performanței și disponibilității acestuia. Documentul va include cel puțin: tipurile de activități de mentenanță (preventivă, corectivă, evolutivă), responsabilitățile personalului tehnic, calendarul și periodicitatea intervențiilor,

Fază / Documente	Documente minime ale fazei
	procedurile de raportare și remediere a incidentelor, mecanismele de monitorizare a stării sistemului, criteriile de succes pentru activitățile de mentenanță și procedurile de testare a funcționalităților după intervenții. Planul va detalia, de asemenea, interacțiunea cu procedură de efectuare a copiilor de siguranță și restaurare și cu planul de suport tehnic, pentru a asigura integritatea și disponibilitatea continuă a sistemului. Frecvență actualizare: Planul de mentenanță va fi revizuit și actualizat ori de câte ori apar modificări semnificative în arhitectura, configurația, componentele sau procedurile sistemului care afectează activitățile de mentenanță, precum și înaintea fiecărei livrări de versiune majoră a sistemului, astfel încât să reflecte în mod fidel responsabilitățile, procesele și calendarul activităților de mentenanță planificate și corective.
Plan de suport tehnic în garanție (L21)	Planul de suport tehnic în garanție va defini modul de gestionare a incidentelor tehnice pe perioada de garanție, procedurile de raportare și escaladare, timpii de răspuns și remediere, responsabilitățile Prestatorului și mecanismele de comunicare cu Autoritatea Contractantă, pentru a asigura un suport tehnic eficient și conform cerințelor contractuale. Frecvență actualizare: Planul de suport tehnic în garanție va fi revizuit și actualizat ori de câte ori apar modificări ale procedurilor de suport, precum și la inițierea perioadei de garanție, pentru a reflecta corect modul de gestionare a incidentelor și timpii de răspuns și remediere prevăzuți.
8.7 Mentenanță corectivă și evolutivă	
Raport anual de mentenanță (L22)	Livrabile vor conține situația incidentelor gestionate, timpii de răspuns și remediere, actualizările și patch-urile aplicate, activitățile de mentenanță corectivă și evolutivă realizate (dacă este cazul), precum și eventualele recomandări privind funcționarea ulterioară a sistemului. Frecvență actualizare: Raportul anual de mentenanță va fi elaborat și transmis o dată pe an, la finalul fiecărui an contractual, incluzând situația cumulativă a activităților de mentenanță, precum și ori de câte ori este solicitat în mod justificat de către Autoritatea Contractantă.
Raport final de mentenanță (L23)	Livrabilul va conține situația incidentelor gestionate, timpii de răspuns și remediere, actualizările și patch-urile aplicate, activitățile de mentenanță corectivă și evolutivă realizate (dacă este cazul), precum și eventualele recomandări privind funcționarea ulterioară a sistemului.

Fază / Documente	Documente minime ale fazei
	Frecvență actualizare: Raportul final de mentenanță va fi întocmit la încheierea perioadei de mentenanță, concret după finalizarea tuturor activităților de mentenanță, pentru a reflecta complet situația incidentelor gestionate, timpii de răspuns și remediere, actualizările și patch-urile aplicate, activitățile corective și evolutive realizate, precum și recomandările privind funcționarea ulterioară a sistemului.
8.8 Garanție și suport tehnic	
Raport final de suport tehnic în garanție (L24)	Livrabilul va include cel puțin: lista completă a incidentelor înregistrate în perioada de garanție, nivelul de prioritate al fiecărui incident, timpii de răspuns și de remediere aferenți, descrierea soluțiilor aplicate, situația actualizărilor și patch-urilor de securitate implementate, confirmarea închiderii tuturor incidentelor, eventuale recomandări tehnice privind exploatarea ulterioară a sistemului Frecvență actualizare: Raportul final de suport tehnic în garanție va fi întocmit la finalul perioadei de garanție, pentru a reflecta complet situația incidentelor gestionate, timpii de răspuns și remediere, soluțiile aplicate, actualizările și patch-urile implementate, precum și recomandările tehnice privind exploatarea ulterioară a sistemului.

Toate livrabilele documente predate de Prestator:

- vor fi redactate în limba română, cu excepția terminologiei standard comune, acronimelor sau denumirilor tehnice internaționale utilizate în mod uzual în domeniu;
- vor fi furnizate în format editabil (DOCX) și în format PDF semnat electronic de reprezentantul legal sau persoana împuternicită;
- vor conține istoricul versiunilor;
- vor include următoarele informații: autor, dată, versiune, descrierea modificărilor;
- vor fi corelate explicit cu cerințele din prezentul Caiet de sarcini și, după caz, cu documentele de analiză și proiectare;
- vor avea caracter operațional, complet, coerent și aplicabil, reflectând configurația și implementarea efectivă a sistemului.

Documentele sunt supuse **actualizării** pe întreaga durată a contractului și a perioadei de garanție.

Prestatorul are obligația de a revizui și actualiza documentele ori de câte ori acest lucru este necesar, inclusiv, dar fără a se limita la următoarele situații:

- modificarea cerințelor sau implementarea unor cerințe suplimentare;
- actualizarea matricei de conformitate ca urmare a implementării sau testării funcționalităților;

- apariția unor modificări legislative relevante;
- identificarea unor neconformități, riscuri sau vulnerabilități;
- constatări rezultate în urma testării (erori, neconformități, necesitatea optimizării);
- modificări de arhitectură;
- actualizări de versiune;
- implementarea de patch-uri;
- modificări de configurare;
- integrarea unor noi componente;
- necesitatea alinierii la obiectivele proiectului sau la cadrul legal aplicabil;
- la solicitarea justificată a Autorității Contractante.

Versiunile actualizate ale documentelor vor reflecta permanent configurația efectivă și acceptată a sistemului.

Cu excepția situațiilor în care în cadrul secțiunii dedicate unui anumit document se prevede expres un alt termen, Prestatorul are obligația de a transmite versiunea actualizată în termenul comunicat de Autoritatea Contractantă.

9.2 Gantt orientativ pentru faze și etape majore

Prestatorul trebuie să demareze procedurile necesare dezvoltării sistemului digital în prima zi lucrătoare următoare constituirii garanției de bună execuție.

Activitățile în cadrul Contractului se vor desfășura conform unui **Plan de implementare a activităților contractului** propus de către Ofertant în cadrul ofertei, care trebuie să ia în considerare toate activitățile, fazele și jaloanele descrise în prezentul caiet de sarcini.

Autoritatea Contractantă își rezervă dreptul de a solicita, în etapa premergătoare semnării contractului ajustări și/sau modificări ale Planului de implementare propus de Ofertantul declarat câștigător, în vederea asigurării unei implementări etapizate mai eficiente, remedierii neconcordanțelor/inadvertențelor identificate în evaluare, optimizării succesiunii activităților și a alocării resurselor sau alinierii planului la constrângeri instituționale sau operaționale. Ofertantul declarat câștigător are obligația de a transmite versiunea revizuită a Planului de implementare în termenul stabilit de Autoritatea Contractantă. Planul de implementare astfel revizuit și agreat de părți va constitui anexă la Contract.

Ofertanții vor prezenta **Planul de implementare a contractului** în format Gantt în cadrul propunerii tehnice. Structura planului de implementare trebuie realizată conform capitolului 12.1.

Planul de implementare propus de Ofertant va include obligatoriu jaloanele critice (Key Milestones) și Livrabilele așa cum sunt descrise în tabelul de mai jos. Orice ofertă care propune un plan de implementare a contractului ce depășește termenele din tabelul de mai jos va fi declarată neconformă.

Jalon critic/ Livrabil	Termen și Descriere	Documente + Instruire
Jalon 1 - Termen: T0+9 luni Semnarea procesului verbal de predare - primire pentru punerea în producție a sistemului digital care include următoarele elemente:		
Configurare infrastructură hardware și software	Finalizarea configurării infrastructurilor hardware și software necesare funcționării sistemului digital	Documente: L1 - L19, L25, L26 Instruire
Componentele suport [6.3-6.9]	Operaționalizarea componentelor suport conform cerințelor funcționale solicitate: - 6.3 Componenta Gestiunea identității și accesul utilizatorilor (IAM) - 6.4 Componenta Middleware de integrare - 6.5 Componenta Backup și restaurare - 6.6 Componenta Managementul incidentelor - 6.7 Componenta Monitorizare a performanței și disponibilității - 6.8 Componenta Managementul evenimentelor de securitate (SIEM) - 6.9 Componenta de protecție servicii web	
Interfața publică [7.1.1] Ediția 1	Operaționalizarea interfeței publice a sistemului digital, cu acces deschis, destinată informării și prezentării patrimoniului cultural, inclusiv profilurile publice ale direcțiilor județene de cultură. Această versiune va include: navigare pe categorii, funcționalități de căutare, filtrare și sortare, pagini publice dedicate resurselor culturale, afișare multimedia de bază și publicarea registrelor naționale, în conformitate cu cerințele funcționale descrise. Interfața publică va include și implementarea și punerea în producție a primului set de funcționalități de valorificare digitală a patrimoniului cultural, utilizabile în interfața publică, pe baza datelor și resurselor gestionate prin MPC. De asemenea, va include mecanisme inițiale de storytelling, afișare multimedia,	

Jalon critic/ Livrabil	Termen și Descriere	Documente + Instruire
	colecții / expuneri digitale și componente interactive de bază, configurabile din zona de administrare, astfel încât să permită publicarea și prezentarea unor exemple funcționale de valorificare digitală a patrimoniului, conform cap. [6.2.11, 7.1.1.2];	
Dashboard intern [7.1.2] Ediția 1	Operaționalizarea proceselor de înrolare a utilizatorilor și a dashboard-ului intern pentru utilizatorii autentificați, cu acces personalizat pe roluri la modulele e-Guvernare, Management Patrimoniu Cultural, administrare, rapoarte, documente și notificări, conform cerințelor din cap. 7.1.2. Operaționalizarea funcționalităților descrise la 7.1.2.1, 7.1.2.2, 7.1.2.4, 7.1.2.5, 7.1.2.6, 7.1.2.8. Operaționalizarea Modulului administrare descris la cap. 7.1.2.3, cu excepția submodulelor de gestionare modelul AI și a celui de gestionare rapoarte și analize.	
Interoperabilitate și integrare cu alte sisteme [7.3]	Operaționalizarea funcționalităților descrise la cap. 7.3 care sunt necesare pentru operarea în producție a edițiilor componentelor aplicative aferente acestui jalon.	
Securitate și confidențialitate [7.5]	Operaționalizarea funcționalităților descrise la cap. 7.5	
Accesibilitate și UI/UX [7.6]	Operaționalizarea funcționalităților descrise la cap. 7.6	
Componenta e-Guvernare [6.1] Ediția 1	Operaționalizarea în producție a primei versiuni consolidate a componentei e-Guvernare ce include implementarea completă a zonei publice și private, a configuratorului de fluxuri și configurarea, testarea end-to-end și punerea în utilizare a unui prim pachet de 12 procese	

Jalon critic/ Livrabil	Termen și Descriere	Documente + Instruire
	digitale complete, conform cap. 6.1. Ediția va permite inițierea, depunerea, înregistrarea, analiza, avizarea / aprobarea, emiterea documentelor și notificarea utilizatorilor pentru procesele implementate, utilizând rolurile, regulile de validare, șabloanele și mecanismele de trasabilitate aferente conform capitolelor 6.1.3 și 6.1.4. Vor fi migrate și validate seturile de date necesare operării în producție a acestor procese. În cadrul acestei versiuni vor fi configurate și implementate, utilizând configuratorul dezvoltat, 12 procese digitale complete conform capitolului 6.1: P1, P5, P11, P24, P27, P34, P37, P47, P48, P49, P52, P53.	
Componenta Management Patrimoniu Cultural [6.2] Ediția 1	Operaționalizarea în producție a primei versiuni utilizabile a componentei MPC, care va asigura nucleul funcțional necesar administrării și consultării resurselor culturale în corelare cu procesele și fluxurile de e-Guvernare. Ediția va include cel puțin: modelul logic de date și ontologiile (6.2.2), nomenclatoarele, vocabularele controlate și tezaurele terminologice necesare primei etape (6.2.4); creare, editare, validare și administrare de resurse culturale pentru categoriile prioritare (6.2.3, 6.2.5); funcționalități de import inițial și actualizare controlată a datelor (6.2.6); căutare și filtrare de bază (6.2.7, 6.2.8); vizualizare de bază a fișelor și a conținutului multimedia (6.2.9); funcționalitățile GIS (6.2.10); mecanisme de relaționare între resurse și de expunere către interfața publică și către fluxurile relevante de e-Guvernare (6.2.14). Ediția trebuie să permită exploatarea reală în producție a componentei pentru seturile de date și scenariile prioritare stabilite în faza de analiză și proiectare. Vor fi migrate și validate seturile de date necesare operării în producție a acestor	

Jalon critic/ Livrabil	Termen și Descriere	Documente + Instruire
	funcționalități.	
Jalon 2 - Termen: T0+15 luni Semnarea procesului verbal de predare - primire pentru punerea în producție a sistemului digital care include următoarele elemente:		
Inteligență artificială [7.4] Ediția 1	Operaționalizare funcționalităților inițiale ale modulului de inteligență artificială, având ca scop asigurarea unei baze funcționale, după cum urmează: - implementarea mecanismelor de extragere automată a datelor din documente scanate (7.4.1.1); - sistemul speech to text (7.4.1.5) - sistemul text to speech (7.4.1.6) Asistentul conversațional instituțional (7.4.1.2) va fi disponibil într-o formă inițială funcțională, cu un set limitat de funcționalități de bază (răspunsuri text, detectarea limbajului licențios, oferirea de ghidaje etc).	Documente: L1 - L19 Instruire
Realizare de interogare și analiză rapoarte pe baza datelor din sistem [7.2]	Operaționalizare funcționalităților descrise la cap. 7.2	
Dashboard intern [7.1.2] Ediția 2	Operaționalizare tuturor funcționalităților descrise la 7.1.2, inclusiv a celor de la 7.1.2.7. Operaționalizare Modulului administrare cap. 7.1.2.3, inclusiv a submodulelor de gestionare modelul AI și a celui de gestionare rapoarte și analize.	
Jalon 3 - Termen: T0+21 luni Semnarea procesului verbal de predare - primire pentru punerea în producție a sistemului digital care include următoarele elemente:		
Componenta e-Guvernare [6.1] Ediția 2	Operaționalizarea în producție a versiunii finale a componentei e-Guvernare, prin acoperirea completă a cerințelor funcționale ale componentei prevăzute în caietul de sarcini,	Documente: L1 - L19 Instruire

Jalon critic/ Livrabil	Termen și Descriere	Documente + Instruire
	inclusiv configurarea și punerea în utilizare a tuturor fluxurilor digitale solicitate.	
Componenta MPC [6.2] Ediția 2	Operaționalizarea în producție a versiunii finale a componentei MPC, prin acoperirea completă a cerințelor funcționale ale componentei prevăzute în caietul de sarcini, inclusiv instrumentele de analiză și raportare (6.2.12) și generare automată a descrierilor pentru resurse (6.2.13).	
Interfața publică [7.1.1] Ediția 2	Operaționalizarea în producție a versiunii finale a Interfeței publice, prin extinderea și consolidarea funcționalităților de valorificare a patrimoniului cultural prin dezvoltarea narațiunilor digitale avansate (storytelling și scrollytelling), integrarea componentelor interactive complexe (expoziții virtuale tematice, tururi virtuale, hărți și cronologii interactive), optimizarea experienței utilizatorului, a performanței și a accesibilității, precum și configurarea de exemple suplimentare, conform cap. 6.2.11.	
Inteligență artificială [7.4] Ediția 2	Operaționalizarea completă a tuturor funcționalităților AI conform capitolului 7.4.	
Jalon 4 - Termen: T0+24 luni		
Semnarea procesului verbal de predare - primire pentru:		
Migrarea completă a datelor	Finalizarea migrării integrale, corecte, verificabile și recepționabile a datelor din toate sistemele sursă și registrele vizate de contract, inclusiv metadatele, relațiile dintre date și, după caz, fișierele binare asociate, cu validarea completitudinii, consistenței și acurateței acestora în mediul de producție. Acest jalon presupune închiderea tuturor activităților de mapare, transformare, încărcare, reconciliere și remediere a neconformităților identificate, astfel încât varianta finală integrată a sistemului să	Documente: L5

Jalon critic/ Livrabil	Termen și Descriere	Documente + Instruire
	poată fi recepționată fără rezerve din perspectiva datelor migrate. Migrarea se va face progresiv pe toată durata menționată și se vor înregistra progresele periodice, în funcție de nevoile punerilor în producție descrise mai sus și de punctele consemnate în Planul de implementare a contractului propus de Ofertanți. Finalizarea operaționalizării interoperabilității sistemului digital ePatrimoniu cu sistemele externe, cu toate API-urile funcționale și schimbul de date complet integrat, inclusiv metadatele, relațiile dintre date și fișierele asociate. Sistemul va asigura transferul complet și corect al datelor, astfel încât informațiile să fie accesibile, coerente și interoperabile cu toate sistemele externe identificate.	
Jalon 5 - Termen: T0+ max. 36 luni (dar nu mai târziu de 30 Noiembrie 2029) Semnarea procesului verbal de recepție calitativă finală a sistemului digital ePatrimoniu		
Stabilizarea operațională a sistemului digital	Confirmarea funcționării stabile, coerente și susținute a sistemului digital în condiții reale de exploatare prin monitorizarea intensivă a sistemului în producție, verificarea funcționării integrate end-to-end a componentelor și fluxurilor operaționale, urmărirea performanței, disponibilității, securității, accesibilității, UI/UX, AI, integrărilor și consistenței datelor, precum și analizarea și remedierea disfuncționalităților și neconformităților identificate la trecerea în exploatarea curentă. Sistemul digital funcțional integrat final este pus în producție, operațional și recepționabil din punct de vedere calitativ, în conformitate cu metodologia de implementare descrisă în secțiunile 8.6 și 9.2.	Documente: L1 - L21, L27

Jalon critic/ Livrabil	Termen și Descriere	Documente + Instruire
	Recepția calitativă finală a sistemului digital se va realiza numai după finalizarea etapei de stabilizare și după confirmarea faptului că sistemul funcționează stabil în mediul de producție, fără disfuncționalități majore care să afecteze utilizarea normală a componentelor și fluxurilor operaționale esențiale.	
Jalon 6 - Termen: PV recepție calitativă finală a sistemului digital ePatrimoniu + 3/4/5 ani Semnarea procesului verbal de recepție calitativă finală a serviciilor de mentenanță		
Mentenanță corectivă Mentenanța evolutivă	Asigurarea serviciilor de mentenanță corectivă post-implementare, prin remedierea neconformităților și incidentelor apărute în exploatare, aplicarea de corecții, patch-uri și actualizări necesare, pentru menținerea funcționării corespunzătoare, securității și performanței sistemului după recepția calitativă finală a sistemului ePatrimoniu. Realizarea de modificări și optimizări asupra sistemului digital pentru îmbunătățirea funcționării acestuia, pentru a răspunde unor noi cerințe din partea AC și/sau implementarea unor noi funcționalități în sistem, astfel încât sistemul să răspundă mult mai bine așteptărilor utilizatorilor săi după recepția calitativă finală a sistemului ePatrimoniu.	L22 L23
Jalon 7 - Termen: PV recepție calitativă finală a serviciilor + 5 ani Semnarea procesului verbal de recepție calitativă finală a serviciilor		
Garanție și suport tehnic	Asigurarea serviciilor de garanție și suport tehnic pentru sistemul ePatrimoniu, inclusiv gestionarea incidentelor prin sistem de ticketing, remedierea defecțiunilor și anomaliilor, furnizarea actualizărilor și patch-urilor de securitate, precum și suportul aferent componentelor licențiate / COTS, pe întreaga perioadă de garanție contractuală.	L24

Variabilele folosite în prezentul tabel au următorul înțeles:

- **T0** reprezintă data constituirii garanției de bună execuție;
- **E1 (prima ediție)** reprezintă prima versiune operațională a componentei, pusă în producție, utilizabilă de utilizatorii țintă pentru scenarii reale de lucru, cu funcționalitățile de bază, setul minim de integrări necesare, datele minime migrate și documentația / livrabilele aferente recepției intermediare.
- **E2 (a doua ediție)** versiunea completă și finală a componentei, pusă în producție, care acoperă integral cerințele din caietul de sarcini pentru componenta respectivă, inclusiv funcționalitățile avansate, optimizările, integrările complete și datele/mecanismele necesare exploataării finale.

Pentru fiecare jalon prevăzut în prezentul tabel, Prestatorul are obligația de a actualiza și transmite Autorității Contractante matricea de conformitate aferentă livrărilor realizate, documentată pe baza cerințelor în caietul de sarcini. Actualizarea matricii de conformitate va reflecta stadiul de implementare a componentelor livrate, gradul de îndeplinire a cerințelor asumate, precum și eventualele neconformități identificate, constituind condiție pentru evaluarea și acceptarea formală a fiecărui jalon de către Autoritatea Contractantă.

9.3 Gestionarea riscurilor și relația Prestator – Autoritate Contractantă

Ofertantul va identifica potențialele riscuri, pe baza experienței proprii din contracte similare. Se vor identifica riscuri din categorii diferite, care necesită abordări diferite și va detalia impactul riscurilor identificate și se va prezenta posibile măsuri de remediere în vederea micșorării acestui impact.

Riscurile ce au fost identificate de către Autoritatea Contractantă și pot apărea pe parcursul derulării Contractului inclusiv măsuri pentru diminuarea efectelor sau eliminarea riscurilor sunt:

Risc identificat	Măsuri propuse
Posibile întârzieri în procesul de încheiere a contractului de achiziție	Se va răspunde cu celeritate tuturor solicitărilor;
Neîndeplinirea la termen și în condiții corespunzătoare a contractului de către Prestator	Prin contract sunt prevăzute clauze privind aplicarea de dobânzi penalizatoare, precum și rezilierea contractului.
Lipsa unei comunicări adecvate	Prin clauze contractuale sunt stabilite mijloacele și formatul de comunicare a informațiilor
Calitate necorespunzătoare a livrabilelor	Au fost definite criterii clare de acceptanță și obligații de a respecta standarde tehnice și bune practici.

9.4 Conformitate legală, drepturi asupra codului sursă și licențiere

Toate livrabilele software realizate în cadrul prezentului contract, inclusiv, dar fără a se limita la cod sursă, cod obiect, scripturi, documentații, configurații și orice alte materiale dezvoltate sau personalizate de către Prestator (dezvoltări proprii), devin proprietatea exclusivă a Autorității Contractante de la momentul plății acestora. Prestatorul cedează către Autoritatea Contractantă toate drepturile patrimoniale de autor asupra dezvoltărilor proprii, pe durată nelimitată.

În măsura în care livrabilele includ componente software open source, acestea vor fi furnizate și utilizate în conformitate cu termenii și condițiile licențelor aplicabile. Prestatorul are obligația de a identifica și documenta toate componentele open source utilizate, inclusiv tipul licenței și obligațiile aferente. Autoritatea Contractantă beneficiază de drepturile de utilizare conferite de respectivele licențe, iar Prestatorul garantează că integrarea acestora nu impune restricții care să afecteze utilizarea normală a soluției pentru întreaga durată a contractului, inclusiv pe perioada de mentenanță evolutivă, corectivă și garanție.

Pentru componentele software de tip COTS (Commercial Off-The-Shelf) incluse în soluția tehnică implementată, Prestatorul asigură Autorității Contractante drept de utilizare neexclusiv, pe întreaga durată a contractului, inclusiv perioada de mentenanță evolutivă, corectivă și garanție, fără costuri pentru Autoritatea Contractantă. Acest drept de utilizare permite exploatarea completă a funcționalităților soluției, fără restricții care să împiedice utilizarea conform scopului contractului.

Prestatorul garantează că deține sau a obținut toate drepturile necesare pentru a transmite drepturile prevăzute mai sus și că utilizarea livrabilelor de către Autoritatea Contractantă nu încalcă drepturile de proprietate intelectuală ale unor terți.

Prestatorul nu va avea dreptul de a reproduce, reutiliza, modifica, ceda, publica sau distribui, în tot sau în parte, elemente ale soluției tehnice livrate, decât cu acordul expres, prealabil și scris al Autorității Contractante.

Sistemul digital va fi livrat sub licență EUPL v.1.2 (European Union Public License) sau o licență echivalentă permisivă, cu asigurarea posibilității de reutilizare, modificare, extindere și redistribuire de către Autoritatea Contractantă, fără restricții suplimentare. Prestatorul va asigura că toate componentele software, inclusiv cele open-source, integrate în livrabil sunt compatibile din punct de vedere licențial cu licența aplicabilă livrabilului final. În cazul identificării unor incompatibilități sau restricții de licențiere, Prestatorul are obligația de a remedia situația prin substituirea componentelor sau obținerea drepturilor / licențelor necesare, astfel încât să nu fie afectate drepturile Autorității Contractante prevăzute în prezentul Caiet de Sarcini. Remedierea nu va implica costuri suplimentare din partea Autorității Contractante și nu va afecta termenele asumate.

Codul sursă pentru sistemul digital și pentru toate aplicațiile dezvoltate și utilizate în implementarea contractului va fi publicat într-un depozit, cum ar fi GitHub sau Joinup

(<https://joinup.ec.europa.eu/>). Codul trebuie documentat și comentat astfel încât să fie ușor de înțeles și de modificat în viitor. Operatorul economic va livra Pipeline CI/CD (Continuous Integration/Continuous Delivery) integrată cu un Git repository unde documentația completă și codul sursă comentat va fi stocat. Această componentă trebuie să fie configurată astfel încât să suporte branching și pull requests.

Codul sursă pentru software-ul dezvoltat în cadrul contractului va fi livrat împreună cu o documentație completă de instalare, configurare, migrare (inclusiv în cloud), administrare și utilizare a sistemului, incluzând manuale de utilizare, instrucțiuni de instalare, operare și mentenanță, ghiduri de dezvoltare ulterioară și altele, astfel încât Autoritatea Contractantă să poată realiza modificarea / administrarea sistemului după finalizarea perioadei de garanție, fără intervenția Prestatorului.

În situația în care orice componentă software externă propusă nu beneficiază de garanții comerciale, suport activ sau angajamente de nivel de serviciu (SLA) din partea producătorului sau dezvoltatorului, Prestatorul va avea obligația de a-și asuma integral, prin declarație fermă, responsabilitatea privind funcționarea, securitatea, performanța și mentenanța acesteia, inclusiv remedierea eventualelor neconformități sau vulnerabilități apărute pe parcursul utilizării.

Prestatorul va declara în mod explicit utilizarea oricăror instrumente de inteligență artificială sau generare automată de cod în cadrul dezvoltării soluției software. Declarația va include descrierea modulelor, funcționalităților sau livrabilelor dezvoltate cu ajutorul acestor instrumente, distinct de cele dezvoltate exclusiv de către personalul propriu.

Utilizarea instrumentelor de inteligență artificială sau de generare automată de cod nu exonerează Prestatorul de nicio obligație contractuală. Prestatorul își asumă integral și în aceleași condiții răspunderea pentru codul generat cu ajutorul inteligenței artificiale ca și pentru codul dezvoltat exclusiv de personalul propriu, inclusiv, dar fără a se limita la conformitatea, funcționalitatea, securitatea, performanța și mentenanța soluției software livrate.

Cu excepția componentei de inteligență artificială incluse în soluția contractată și descrisă la capitolul 7.4, Prestatorul se obligă să nu utilizeze informații, date, documente sau materiale aparținând Autorității Contractante ca input pentru alte instrumente de inteligență artificială sau sisteme de generare automată de conținut, operate de terți sau utilizate în afara soluției contractate, fără aprobarea prealabilă, expresă și scrisă a Autorității Contractante.

În cazul în care pentru implementarea contractului sunt necesare și alte licențe/software pentru funcționarea sistemului digital ePatrimoniu decât cele prevăzute în prezentul caiet de sarcini, acestea vor fi descrise și incluse în ofertă, fără cheltuieli suplimentare din partea autorității contractante, iar ofertantul va justifica necesitatea acestora.

Orice activitate, componentă, cerință, funcționalitate, licență/software care se va dovedi ulterior necesară în vederea implementării contractului în conformitate cu

specificațiile din prezentul caiet de sarcini, se va furniza și pune în funcțiune fără costuri suplimentare pentru autoritatea contractantă.

Prestatorul are obligația ca în cazul folosirii de resurse software externe (de exemplu, dar fără a se limita la: componente, module, biblioteci etc.), acestea să fie mature, stabilizate, testate public și să dispună de suport activ sau comunități stabile de întreținere. Este interzisă utilizarea resurselor software externe aflate în fază experimentală, a versiunilor „beta” sau a modulelor fără suport oficial.

Toate componentele software utilizate, indiferent dacă sunt open-source, comerciale (COTS) sau dezvoltate intern, trebuie să respecte în totalitate regimul legal de licențiere și să nu impună obligații incompatibile cu drepturile de proprietate/ utilizare ale Autorității Contractante asupra soluției finale.

Prestatorul va acorda drepturi de acces reprezentanților Autorității Contractante în mediul versionat de dezvoltare/ testare, iar odată cu livrarea sistemului, va fi pregătit oricând să realizeze transferul de proprietate la cererea Autorității Contractante.

Prestatorul are obligația de a furniza, odată cu livrarea sistemului, o listă completă și actualizată a tuturor componentelor software utilizate, împreună cu specificarea versiunilor, tipului de licență și condițiilor aferente. În cazul oricăror modificări ulterioare ale regimului de licențiere sau al condițiilor de utilizare, în perioada de garanție, Prestatorul va notifica imediat Autoritatea Contractantă și va asigura, fără costuri suplimentare, actualizarea sau înlocuirea componentelor afectate, astfel încât funcționalitatea sistemului și drepturile de utilizare ale Autorității Contractante să nu fie afectate.

Prețul total al ofertei va include prețul licențelor și al componentelor software aferente, precum și toate cheltuielile de instalare, configurare, punere în funcțiune, testare, operaționalizare, integrare la nivel de servicii și instruire asociate, defalcat pentru fiecare în parte.

Componentele software de tip COTS (Commercial Off The Shelf), trebuie să beneficieze de suport activ din partea producătorului pe toată perioada de mentenanță și garanție a sistemului. În toate documentele de achiziție aferente componentelor software de tip COTS, Prestatorul va indica drept beneficiar final Autoritatea Contractantă, astfel încât aceasta să poată, la nevoie, comunica direct cu furnizorul componentelor respective și să poată deschide tichete de suport fără intermedierea Prestatorului.

Pentru a asigura predictibilitatea bugetară și sustenabilitatea sistemului pe termen lung, Ofertanții au obligația de a prezenta transparent costurile recurente estimate pentru produsele software comerciale (COTS) propuse. Ofertanții trebuie să furnizeze, cu titlu informativ, în cadrul Propunerii Financiare, estimarea costurilor anuale de subscripție/mentenanță/suport pentru fiecare produs COTS, aplicabile după expirarea perioadei de garanție.

Prestatorul garantează că soluția livrată este conformă din punct de vedere juridic și tehnic, fiind în deplină concordanță cu legislația privind drepturile de autor, protecția

proprietății intelectuale, protecția datelor și reglementările aplicabile în domeniul tehnologiei informației.

În cazul în care se constată existența unor încălcări ale regimului de licențiere sau a unor litigii privind drepturile de proprietate intelectuală asupra componentelor software utilizate, întreaga răspundere revine Prestatorului, care are obligația de a despăgubi Autoritatea Contractantă pentru eventualele prejudicii cauzate. Pe perioada garanției, Prestatorul va asigura, de asemenea, continuitatea operațională a sistemului în situația în care un furnizor extern sau o licență terță parte își modifică condițiile de utilizare, garantând funcționarea neîntreruptă a soluției livrate.

Prin semnarea contractului, Prestatorul confirmă că deține toate drepturile, licențele, acordurile și autorizările necesare pentru utilizarea, integrarea și distribuirea componentelor software incluse în soluție și își asumă întreaga responsabilitate pentru conformitatea legală a acestora. Toate prevederile referitoare la drepturile asupra codului sursă și la conformitatea legală se aplică în mod corespunzător și subcontractorilor sau terților implicați în execuția contractului, Prestatorul având obligația de a garanta respectarea integrală a acestora pe întreg lanțul de livrare.

10. Recepția și plata serviciilor

10.1 Recepția

Fiecare jalon va fi predat de Contractant către AC la termenele din cap 9.2 în baza unor **procese-verbale de predare-primire**. Fiecare jalon va fi acceptat de către AC prin verificarea existenței, conformității și completitudinii livrabilelor aferente, în baza unor **procese-verbale de recepție calitativă intermediară**. Jaloanele sunt detaliate în capitolul 9.2 al prezentului Caiet de sarcini.

În cadrul recepției, toate funcționalitățile aferente livrabilelor și toate documentele trebuie să fie verificate / testate, validate și recepționate de AC pentru a confirma conformitatea cu cerințele contractuale.

Autoritatea Contractantă are dreptul de a analiza fiecare livrabil și de a decide:

- acceptarea acestuia;
- acceptarea condiționată de remedierea unor neconformități;
- respingerea totală sau parțială.

Nerespectarea cerințelor stabilite prin caietul de sarcini, a ofertei sau a observațiilor formulate în procesul de validare obligă Prestatorul să refacă, completeze sau corecteze livrabilele, respectiv să remedieze neconformitățile comunicate, în termenul stabilit de Autoritatea Contractantă.

Livrabilul revizuit va fi retransmis spre analiză, iar procesul de verificare și revizuire se va relua până la obținerea recepției calitative scrise din partea Autorității Contractante. Recepția calitativă scrisă reprezintă condiție pentru considerarea livrabilului ca fiind recepționat.

Lipsa unui răspuns din partea Autorității Contractante nu echivalează cu acceptarea tacită a livrabilului.

În situația în care, după remediere, se constată în continuare neconformități sau deficiențe, Autoritatea Contractantă își rezervă dreptul de a aplica toate măsurile prevăzute în contract pentru neîndeplinirea sau îndeplinirea necorespunzătoare a obligațiilor de către Prestator.

Procedura de verificare și revizuire aplicabilă livrabilelor se aplică în mod corespunzător și jaloanelor, ținând cont de specificul acestora ca etape critice de implementare și punere în producție a componentelor sistemului.

Prestatorul nu poate condiționa continuarea sau desfășurarea activităților prevăzute în cadrul contractului de recepția sau plata unor livrabile sau jaloane anterioare. Obligațiile contractuale privind realizarea etapelor, livrabilelor și activităților se mențin independente și executarea lor nu poate fi suspendată sau întârziată ca urmare a disputelor privind alte livrabile, jaloane sau plăți.

În vederea încheierii **procesului-verbal de recepție calitativă intermediară**, Prestatorul are obligația de a implementa toate cerințele Autorității Contractante rezultate în urma testării/ analizei documentelor/ livrabilelor predate și a jaloanelorlor puse în producție.

În etapa de recepție, Autoritatea Contractantă poate utiliza auditori externi, experți independenți sau alte entități delegate pentru a verifica implementarea și îndeplinirea tuturor cerințelor din prezentul Caiet de Sarcini, inclusiv cele de securitate și cele privind protecția datelor cu caracter personal. În acest caz, Prestatorul are obligația de a asigura suport complet și disponibilitate necondiționată pe durata desfășurării auditului sau verificării și nu poate invoca secretul comercial, confidențialitatea sau alte motive pentru a refuza sau întârzia furnizarea suportului sau accesul la informații. Orice recomandare, observație sau neconformitate identificată în raportul de audit sau de verificare va fi implementată de Prestator în termenul stabilit de Autoritatea Contractantă. Nerespectarea acestei obligații constituie neîndeplinire a obligațiilor contractuale de către Prestator și poate atrage aplicarea sancțiunilor prevăzute în contract.

Varianta finală integrată a sistemului digital va fi acceptată de către AC în baza unui **proces-verbal de recepție calitativă finală a sistemului ePatrimoniu**, încheiat după semnarea tuturor proceselor-verbale de recepție calitativă intermediară aferente tuturor jaloanelor definite în capitolul 9.2 din prezentul caiet de sarcini.

Procesul-verbal de recepție calitativă finală nu va putea fi semnat decât după verificarea și validarea de către Autoritatea Contractantă (sau auditorii acestuia) a corespondenței dintre realitatea din teren (configurațiile din mediul de producție) și informațiile prezentate în Documentația As-Built (Livrabilul L17). Orice neconcordanță va fi considerată neconformitate și va bloca recepția finală până la remedierea documentației/ configurației.

Recepția serviciilor de mentenanță se va face astfel:

- anual pe baza unui raport de activitate întocmit de Prestator și aprobat de Autoritatea Contractantă printr-un Proces – verbal de recepție calitativă intermediară serviciilor de mentenanță.
- la finalizarea perioadei de mentenanță, pe baza unui raport de activitate întocmit de Prestator și aprobat de Autoritatea Contractantă printr-un Proces – verbal de recepție calitativă finală a serviciilor de mentenanță.

Recepția finală a serviciilor se face la finalul perioadei de garanție.

10.2 Plata

Plățile se vor face în tranșe corespunzătoare jaloanelor 1-5, după semnarea proceselor-verbale de recepție calitativă intermediară, respectiv a procesului-verbal de recepție finală a sistemului ePatrimoniu.

Se va avea în vedere că pentru punerea în producție a Ediției 1 a fiecărui livrabil se va achita 40% din valoarea acesteia, pentru punerea în producție a Ediției 2 a fiecărui livrabil se va achita 40% din valoarea acesteia, iar la recepția finală a sistemului se va achita diferența de 20%. Pentru livrabilele care nu au două ediții se va achita 80% din valoarea acestora la punerea în producție, iar la recepția finală a sistemului se va achita diferența de 20%.

Facturile pentru serviciile prestate în temeiul contractului de achiziție vor fi emise de către Prestator numai după semnarea de către AC a proceselor-verbale de recepție calitativă intermediară. Plățile se vor face prin trezorerie, în termen de cel mult 60 de zile de la data primirii facturii de către AC, în funcție de existența bugetului aprobat pe anul în curs.

11. Resurse umane și expertiza necesară pentru realizarea activităților contractului și obținerea rezultatelor

11.1 Experți cheie solicitați pe categorii de expertiză

În vederea implementării cu succes a contractului, Prestatorul va organiza și va pune la dispoziția autorității contractante o echipă de experți care, prin atribuțiile și pregătirea lor, vor realiza execuția tuturor activităților care trebuie realizate în cadrul contractului.

Prestatorul va pune la dispoziția Autorității Contractante lista completă a personalului său (inclusiv cel care aparține asociațiilor și subcontractanților, dacă este cazul) care va fi implicat în derularea contractului și prestarea serviciilor și care vor necesita acces în locațiile de instalare și acces la informații despre acestea. Datorită caracterului confidențial al informațiilor la care persoanele nominalizate vor avea acces, Autoritatea Contractantă își rezervă dreptul de a verifica personalul respectiv, conform normelor sale interne privind accesul la date și informații cu caracter confidențial și de a interzice accesul în amplasamente sau la informații legate de contract acelor persoane care nu îndeplinesc condițiile impuse de Autoritatea Contractantă.

Prestatorul se obligă să păstreze, atât el cât și resursele umane propuse, confidențialitatea asupra informațiilor primite de la Autoritatea Contractantă pe parcursul derulării contractului și asupra rezultatelor obținute în executarea contractului.

Echipa ce va fi prezentată de ofertant va trebui să aibă o vastă experiență în implementarea de sisteme informatice integrate. În acest sens, ofertantul trebuie să asigure pe întreaga perioadă de derulare a contractului personalul necesar în funcție de obiectivele, rezultatele și activitățile / livrabilele solicitate în prezentul document, garantând că personalul are calificarea și experiența profesională descrisă mai jos.

Ofertantul va prezenta componența echipei, instrumentele/metodele de coordonare a activității acesteia și va detalia rolurile, atribuțiile și responsabilitățile experților și modalitatea concretă în care echipa prezentată interacționează cu personalul de suport/back-stopping pentru îndeplinirea contractului.

Personalul cheie minim solicitat de către Autoritatea Contractantă și care va fi alocat de Prestator pentru a realiza efectiv activitățile care fac obiectul contractului este prezentat în secțiunea 11.2 a prezentului caiet de sarcini.

Prestatorul are obligația de a asigura desfășurarea activităților stipulate în contract prin alocarea și disponibilitatea personalului de specialitate pe toată durata contractului.

Pe parcursul derulării contractului, Prestatorul nu va efectua schimbări în cadrul Personalului stabilit, fără aprobarea prealabilă scrisă a Autorității contractante. Înlocuirea personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează numai în condițiile prevăzute de legislația aplicabilă achizițiilor publice.

Noul personal de specialitate nominalizat pentru îndeplinirea contractului trebuie să îndeplinească cel puțin cerințele minime prevăzute în cadrul documentației de atribuire și trebuie să obțină cel puțin același punctaj ca personalul propus la momentul aplicării factorilor de evaluare. Prestatorul are obligația de a transmite pentru noul personal documentele solicitate prin documentația de atribuire în vederea demonstrării îndeplinirii cerințelor minime, respectiv a calculării punctajului aferent factorilor de evaluare, după caz.

În situația în care Prestatorul sau Autoritatea contractantă solicită înlocuirea Personalului, Prestatorul va transmite Autorității contractante, pentru verificare și aprobare, documente justificative privind calificarea educațională și/sau profesională, abilitățile, experiența profesională generală și specifică a Personalului propus. În cazul în care Personalul înlocuit a generat Prestatorului un avantaj pe perioada derulării achiziției, la momentul aplicării criteriului de atribuire, Autoritatea contractantă are dreptul de a aproba înlocuirea Personalului cu un Personal cu caracteristici ce sunt inferioare celor ale Personalului înlocuit numai în situația în care noul Personal nominalizat pentru îndeplinirea Contractului obține cel puțin același punctaj ca Personalul propus la momentul aplicării factorilor de evaluare, chiar și în cazul în care caracteristicile Personalului propus sunt inferioare celor ale Personalului înlocuit.

În cazul respingerii Personalului propus, Autoritatea contractantă va notifica, în scris, motivele respingerii și termenul de prezentare a unei noi propuneri. În cazul în care Prestatorul nu este în măsură să furnizeze un înlocuitor în condițiile stabilite mai sus, care să nu diminueze avantajul obținut de Prestator ca urmare a aplicării criteriului de atribuire din prezentul Contract, Autoritatea contractantă poate să decidă rezilierea Contractului.

Autoritatea contractantă va transmite aprobarea/ respingerea schimbărilor de Personal în termen de maximum 5 zile lucrătoare, calculat de la primirea documentelor justificative în formă completă și corectă. Aprobarea înlocuirii personalului produce efecte de la data emiterii acesteia de către Autoritatea contractantă.

Cheltuielile suplimentare generate de înlocuirea personalului incumbă Prestatorului.

Prestatorul trebuie să se asigure că personalul de specialitate alocat fiecărei activități va fi implicat efectiv în activitățile contractului și va îndeplini obligațiile stabilite în sarcina sa.

AC are dreptul să efectueze verificări periodice ale activității echipei Prestatorului, inclusiv prin acces la repo-uri și cod sursă, analiza rapoartelor și timesheet-urilor etc.

Echipa este obligată să participe la ședințele de lucru, prezentările intermediare și demonstrațiile de progres, conform calendarului stabilit de AC.

Neimplicarea efectivă a personalului, lipsa participării la ședințe sau neîndeplinirea obligațiilor de raportare constituie abatere contractuală/ situație de neexecutare a obligațiilor contractuale și poate atrage aplicarea de penalități, în condițiile stabilite prin contract.

Nu se acceptă îndeplinirea cerințelor minime aferente unui expert prin cumul de către mai multe persoane și nici nominalizarea unei persoane pentru mai multe poziții.

	Experți cheie	Nr
1	Manager de proiect	1
2	Arhitect de sistem și technical lead (arhitectură / dezvoltatori / infrastructură / versiuni/baze de date) enterprise architect	1
3	Expert baze de date	1
4	Expert securitate informatică	1
5	Expert AI	1
6	Expert GIS	1
7	Expert infrastructură și livrare (DevOps)	1

8-9	Expert dezvoltare software senior	2
	Experți non-cheie	
10	Expert User Experience / User Interface (UX/UI) - Expert dezvoltare software (1 persoană)	1
11-13	Experți dezvoltare software	3
14	Manager de analiză	1
15	Analist de business	1
16-17	Expert testare software	2

11.2 Profilul experților cheie

Expert/ poziție	Activități din contractul ce urmează să fie atribuit	Cerințe minime
--------------------	---	----------------

Manager de proiect (1 persoană)	- Asigură coordonarea echipei Prestatorului desemnată pentru implementarea contractului; - Organizează și asigură bunul mers al activităților desfășurate de către echipa Prestatorului în cadrul contractului; - Este punct principal de contact în comunicarea cu echipa desemnată de Autoritatea Contractantă și reprezintă Prestatorul în relație cu AC; - Răspunde de managementul contractului conform metodologiei de implementare, respectiv de activitățile de planificare, organizare a execuției, monitorizare, control și încheiere a contractului; - Alocă resursele în cadrul contractului astfel încât Prestatorul să aibă capacitatea de a răspunde în mod optim necesităților, constrângerilor și obiectivelor Autorității Contractante; - Se asigură de faptul că livrabilele și documentele contractului corespund cerințelor Autorității Contractante; - Se asigură că toate condițiile contractuale sunt respectate, în special respectarea termenelor; - Identifică riscurile și problemele ce pot să apară și ia măsuri imediate pentru soluționarea acestora;	Deținerea de competențe aferente poziției pentru care este propus, dovedite prin: - prezentarea unei diplome/ a unui certificat de absolvire în domeniul managementului de proiect, eliberat(ă) de un organism de formare, sau - prin prezentarea de diplome de studii superioare care au inclus în curriculumul educațional cursuri de management de proiect sau - prin experiență specifică constând în implicarea în cel puțin două contracte în care să fi realizat activități similare cu cele din contractul ce urmează să fie atribuit
--	--	--

	- Asigură elaborarea și validarea tuturor documente prevăzute la capitolul 9.1, a celor de raportare a progresului și a celor de plată.	
Arhitect de sistem și technical lead (1 persoană)	- În calitate de Technical lead asigură coordonarea echipei de dezvoltare și cadrul tehnic necesar dezvoltării și implementării sistemului (controlul versiunilor, al configurațiilor, al mediilor tehnice etc);	Competențe în dezvoltarea arhitecturilor de tip enterprise prin utilizarea unei metodologii cadru de realizare a acestora, dovedite prin cel puțin o certificare în domeniu, recunoscută la nivel național sau internațional

	- Proiectarea și documentarea arhitecturii la nivel hardware, software și funcțional a sistemului și a specificațiilor de integrare în conformitate cu cerințele Autorității Contractante și cu standardele în vigoare; - Modificarea arhitecturii sistemului pe parcursul implementării, dacă este cazul. - Elaborarea documentației și păstrarea informațiilor și/ sau modelelor ale arhitecturii de sistem și ale structurilor de date. Se va ocupa de actualizarea și modificarea acestor informații pe parcursul derulării activităților; - Definirea arhitecturii sistemului, inclusiv a modelelor de date, structurilor de aplicație și fluxurilor de date între module - Identifică soluția tehnică optimă pentru a asigura realizarea funcționalităților sistemului informatic, astfel încât să asigure disponibilitatea și performanța sistemului informatic și să răspundă cerințelor Autorității Contractante - Coordonează integrarea componentelor sistemului astfel încât să se țină seama și de interconectările/ influențele directe/ indirecte ale modificărilor efectuate asupra tuturor componentelor; - Asigurarea îndeplinirii cerințelor funcționale, non-funcționale și de	și Competențe tehnice privind tehnologiile și limbajele de programare pe care le va utiliza în dezvoltarea sistemului, dovedite prin cel puțin o certificare recunoscută la nivel național / internațional care să demonstreze specializarea în tehnologia / limbajul de programare de bază utilizat în realizarea sistemului informatic sau prin studii superioare, absolvite cu diplomă de licență sau echivalent în specializările aferente domeniilor de licență Informatică, Cibernetică, statistică și informatică economică, Calculatoare și tehnologia informației sau Automatică, Informatică aplicată și sisteme inteligente sau în specializările Matematică-Informatică, Inginerie electrică și calculatoare, Rețele și software de telecomunicații, Securitate cibernetică, Informatică industrială, Matematică și informatică aplicată în inginerie. și Experiență specifică constând în implicarea în cel puțin un <i>contract comparabil</i>* în care să fi realizat activități similare cu cele din contractul ce urmează să fie atribuit.
--	--	---

	integrare, proiectare model de date și procese; - Avizarea documentelor de natură tehnică elaborate de către echipa prestatorului pe durata derulării contractului; - Urmărirea și asigurarea respectării caracteristicilor proiectate pe parcursul implementării sistemului; - Coordonează activitatea de punere în producție a sistemului informatic - Coordonează echipa și se va implica activ în activitatea de mentenanță, analizând solicitările și asigurând implementarea promptă a acestora - Participa la implementarea cerințelor de securitate pentru sistemul informatic conform cerințelor solicitate în Caietul de sarcini	
Expert baze de date (1 persoană)	- Definește specificațiile pentru realizarea unui model de date adecvat în funcție de cerințele contractului și de analiza cerințelor și specificațiilor tehnico-funcționale ale Autorității contractante; - Proiectează structura bazei de date prin transpunerea fluxurilor informaționale și a schemelor logice specifice sistemului, și realizează modelarea bazelor de date relaționale; - Realizează și răspunde de interconectarea bazelor de date, de rezolvarea problemelor legate de replicarea datelor (dacă este cazul)	Studii superioare, absolvite cu diplomă de licență sau echivalent și Competențe de specialitate în domeniul bazelor de date (proiectare conceptuală, modelare, utilizare și administrare SGBD) dovedite prin cel puțin o certificare în domeniu (ex. PostgreSQL Associate / Professional Certification, Oracle Database SQL Certified Associate, MySQL Database Developer etc.), recunoscută la nivel național sau internațional și

	și asigură legătura cu bazele de date existente; - Realizează și răspunde de configurarea bazelor de date pentru a obține performanțe maxime în raport cu cerințele componentelor software și stabilește resursele hardware necesare; - Colaborează cu echipa de dezvoltare pentru a înțelege cerințele de date ale sistemului; - Realizează operații de back-up / restore pentru bazele de date; - Elaborează și actualizează documentații tehnice detaliate privind structura bazei de date, pentru utilizare și pentru administrare; - Realizează managementul performanțelor bazelor de date, diagnosticarea potențialelor blocaje de performanță din cadrul bazelor de date, la nivelul fluxurilor/proceselor de lucru și inițiază metode/soluții de optimizare a acestora; - Are responsabilitatea menținerii integrității și acurateței bazei de date; - Împreună cu echipa de dezvoltare, stabilește și creează funcții de monitorizare (alerte generate automat), planul de acțiune și procedura de intervenție; - Identifica și rezolva erorile și bug-urile la nivelul bazei de date a	Experiență specifică constând în implicarea în cel puțin un <i>contract comparabil</i>* în care să fi realizat activități similare cu cele din contractul ce urmează să fie atribuit
--	---	---

	sistemului, coerent cu dezvoltările efectuate. Propune echipei de proiectare structuri de fișiere log și asigură disponibilitatea bazei de date aferente sistemului pentru toate celelalte baze de date cu care se interconectează; - Participă la activitatea de testare.	
Expert securitate informatică (1 persoană)	- Asigură identificarea și analiza riscurilor de securitate ale soluției, precum și implementarea, pe întregul lanț de dezvoltare software (SDLC), a controalelor și măsurilor adecvate pentru minimizarea sau eliminarea riscului de compromitere a sistemului sau a datelor acestuia; - Definește specificațiile de securitate ale sistemului digital în integralitatea lui; - Asigură suportul de specialitate în activitățile de analiză, dezvoltare, testare, implementare, cartografiere a datelor, precum și în alegerea măsurilor de protecție a datelor cu caracter personal; - Asigură conformitatea soluției cu legislația națională și europeană aplicabilă privind cerințele de securitate informațională (ex. NIS2, GDPR); - Verifică conformitatea sistemului implementat cu cerințele și arhitectura de securitate; - Definește scenarii - pentru testele de securitate interne pe întreg	Studii superioare, absolvite cu diplomă de licență sau echivalent și Competențe de nivel profesional în domeniul securității informatice și informaționale, privind gestionarea, implementarea și evaluarea politicilor și măsurilor de securitate, dovedite prin cel puțin o certificare recunoscută la nivel național sau internațional în domeniul securității informației și securității cibernetice (ex. CISSP – ISC², CISM – ISACA, CEH – EC-Council, CompTIA Security+, CompTIA CySA+ sau echivalent) sau prin diplomă de master în specializarea Securitate informatică și știința datelor sau domenii conexe (Tehnologii multimedia în aplicații de biometrie și securitatea informației, Managementul securității echipamentelor și sistemelor informaționale și de comunicație, Securitatea rețelelor informatice complexe, Sisteme avansate de securitate, Securitate și logică aplicată, Securitatea informatică, Securitate cibernetică, Securitatea informațiilor și sistemelor de calcul, Securitate

	lanțul de aprovizionare inclusiv pentru cele de penetrare; - Definește aria de acoperire a testelor și a excluziunilor; - Realizează teste de securitate, interpretează rezultatele obținute în urma procesului de testare de securitate, realizează rapoarte de testare a securității sistemului și propune soluții de remediere; - Efectuează testări de securitate SAST și DAST pe întreg ciclul de viață al dezvoltării, asigurând identificarea și remedierea timpurie și continuă a vulnerabilităților de cod, configurare, runtime etc.; - Evaluează și asigură securitatea întregului lanț de aprovizionare software, incluzând dependențe third-party, pipeline-uri CI/CD, containere etc.; - Are responsabilitatea proiectării/adaptării tuturor aspectelor securității de sistem de la început la sfârșit (“end-to-end”), inclusiv autentificarea, autorizarea, controlul accesului, setările de securitate pentru sistemele operaționale, portaluri, baze de date și servere de aplicații, logarea de siguranță, securitatea serviciilor web, manevrarea în siguranță a datelor etc.; - Are responsabilitatea definirii, implementării, documentării și testării periodice a componentei de recuperare (backup) pentru sistemul digital și datele acestuia	cibernetică și învățare automată, Securitate cibernetică și managementul riscurilor, Securitate cibernetică și tehnologii cuantice, Securitatea spațiului cibernetic, Securitatea informației, Inteligență artificială pentru apărare și securitate, Securitatea tehnologiei informației, Securitatea cibernetică a sistemelor și tehnologiilor operaționale) și Competențe de nivel profesional privind efectuarea testelor de penetrare asupra sistemelor informatice complexe și identificării riscurilor de securitate informatica, dovedite prin cel puțin o certificare recunoscută la nivel național sau internațional și Experiență specifică constând în implicarea în cel puțin un <i>contract comparabil*</i> în care să fi realizat activități similare cu cele din contractul ce urmează să fie atribuit (de evaluare a securității sistemelor informatice).
--	--	--

	- Este responsabil de înțelegerea, conștientizarea și respectarea normelor de confidențialitate și securitate, la nivelul echipelor Prestatorului și Autorității Contractante, impuse de legislația în vigoare (ex. prelucrarea datelor cu caracter personal în conformitate cu Regulamentul 679/2016 și legislația subsecventă, măsuri de securitate pentru entități esențiale conform OUG 155/2024 și a legislația subsecventă etc.)	
Expert AI (1 persoană)	- Implementează, integrează, testează și validează funcționalitățile AI în sistemul digital; - Asigură conformitatea modelelor AI cu specificațiile din caietul de sarcini / documentul de analiză și cu reglementările în vigoare din domeniu; - Realizează și documentează procesul de dezvoltare și antrenare a modelelor AI, inclusiv metodologia, sursele de date, parametri tehnici, rezultatele evaluării performanței și mecanismele de revizuire; - Asigură transfer de cunoștințe către echipa Autorității Contractante pentru utilizarea și administrarea modului AI; - Colaborează cu echipa de dezvoltare software și ceilalți experți pentru integrarea coerentă a funcționalităților AI;	Studii superioare, absolvite cu diplomă de licență sau echivalent în domeniul IT (studii superioare, absolvite cu diplomă de licență sau echivalent în specializările aferente domeniilor de licență Informatică, Cibernetică, statistică și informatică economică, Calculatoare și tehnologia informației sau Automatică, Informatică aplicată și sisteme inteligente sau în specializările Matematică-Informatică, Inginerie electrică și calculatoare, Rețele și software de telecomunicații, Securitate cibernetică, Informatică industrială, Matematică și informatică aplicată în inginerie.) sau diplomă de master în una dintre specializările Inteligență artificială, Analiza inteligentă a datelor, Inteligență artificială și prelucrări de semnale în electronică și telecomunicații, Inteligență și viziune artificială, Inteligență artificială în producția industrială, Inteligență artificială pentru industrii conectate,

	- Monitorizează performanța și asigurarea funcționării robuste a funcționalităților AI în cadrul platformei digitale.	Inteligență computațională aplicată, Metode și modele în inteligență artificială, Inteligență artificială și calcul aplicat, Inteligență artificială în mecatronică și robotică, Inteligență artificială și optimizare, Inteligență artificială pentru apărare și securitate, Data Science, Procesarea limbajului natural, Știința datelor și inteligență artificială, Securitate cibernetică și învățare automată, Învățare automată, robotică și control, Învățare automată). și Experiență specifică constând în implicarea într-un contract care a presupus și dezvoltarea, implementarea sau integrarea de soluții bazate pe inteligență artificială, în care să fi realizat activități similare cu cele din contractul ce urmează să fie atribuit.
--	--	---

Expert GIS (1 persoană)	- Instalează, configurează, dezvoltă infrastructura GIS și întreține componentele acestui sistem pentru a îndeplini cerințele Autorității Contractante; - Administrarea și configurarea serverelor GIS; - Gestionarea datelor geospațiale; - Colaborează cu administratorul baze de date și proiectează structura de date GIS; - Colaborează cu Autoritatea Contractantă pentru a identifica cerințele specifice privind datele spațiale și lucrează cu echipa de dezvoltatori pentru a configura soluția.	Competențe de specialitate în utilizarea platformelor GIS desktop și WebGIS, în gestionarea și analiza datelor spațiale în baze de date geospațiale (ex: PostgreSQL/PostGIS), precum și în integrarea datelor spațiale în aplicații web, dovedite prin cel puțin o certificare recunoscută la nivel național sau internațional (exemple: Esri Technical Certification, ArcGIS Desktop Entry Certification, ArcGIS Desktop Associate Certification, ArcGIS Desktop Professional Certification, ArcGIS Enterprise Administration Associate, ArcGIS Enterprise Administration Professional, ArcGIS Developer Associate). și Experiență specifică constând în implicarea în cel puțin un <i>contract comparabil*</i> în care să fi realizat activități similare cu cele din contractul ce urmează să fie atribuit.
Expert infrastructură și livrare (DevOps) (1 persoană)	- Stabilește standarde și linii directoare pentru dezvoltare și livrare, inclusiv gestionarea codului sursă, versionarea, pipeline-urile CI/CD și controlul schimbărilor în medii de testare și producție - Configurează, administrează și optimizează medii de dezvoltare, testare și producție;	Studii superioare, absolvite cu diplomă de licență sau echivalent în specializările aferente domeniilor de licență Informatică, Cibernetică, statistică și informatică economică, Calculatoare și tehnologia informației sau Automatică, Informatică aplicată și sisteme inteligente sau în specializările Matematică-Informatică, Inginerie electrică și calculatoare, Rețele și software de telecomunicații,

	- Implementează și întreține pipeline-urilor CI/CD pentru aplicațiile contractului (build, test, deploy); - Automatizează procesele de livrare și monitorizare a componentelor software și infrastructurii; - Administrează și optimizează servere, containere și clustere (ex. Docker, Kubernetes, OpenShift); - Gestionează configurațiile sistemelor, managementul versiunilor și controlul schimbărilor; - Supraveghează performanța sistemelor și rezolvarea incidentelor tehnice legate de infrastructură și componentele software; - Implementează și monitorizează politicile de backup, restaurare și continuitate a serviciilor, în colaborare directă cu Expertul baze de date; - Colaborează cu echipele de dezvoltare și arhitectură pentru integrarea optimă a componentelor software cu infrastructura; - Asigură securitatea infrastructurii și respectarea standardelor și reglementărilor aplicabile; - Documentează configurațiile, procedurile și politicile DevOps; - Asigură transferul de cunoștințe către echipa Autorității Contractante privind procesele DevOps și bunele practici.	Securitate cibernetică, Informatică industrială, Matematică și informatică aplicată în inginerie. și Competențe profesionale dovedite prin certificări recunoscute la nivel național și/sau internațional în domeniul DevOps și administrării infrastructurii, dovedite prin cel puțin o certificare recunoscută la nivel național sau internațional care să demonstreze specializarea în domeniul DevOps și administrării infrastructurii (ex. AWS Certified DevOps Engineer, Microsoft Azure DevOps Engineer, Kubernetes Administrator, Red Hat Certified Engineer sau echivalent). și Experiență în monitorizarea aplicațiilor și infrastructurii folosind instrumente precum Prometheus, Grafana, ELK Stack, Zabbix etc. dovedită prin CV și Experiență specifică constând în implicarea în cel puțin un <i>contract comparabil</i>* în care să fi realizat activități similare cu cele din contractul ce urmează să fie atribuit.
--	---	---

Expert dezvoltare software senior (2 persoane)	- Transpune cerințele documentate în funcționalități ale sistemului; - Participă la activitățile de proiectare și dezvoltare a componentelor și modulelor sistemului digital; - Participă la proiectarea modelului logic al datelor din cadrul sistemului digital în conformitate cu cerințele funcționale și arhitectura generală a sistemului; - Proiectează și implementează proceduri de integrare și interoperabilitate a datelor prin API-uri standardizate (REST/JSON, XML, CSV); - Stabilește și implementează politici de backup, restaurare și continuitate operațională; - Contribuie la definirea modelelor de date în corelare cu ontologiile și vocabularele controlate utilizate de sistem; - Colaborează strâns cu arhitectul de sistem și cu echipa de dezvoltare pentru asigurarea coerenței arhitecturale și funcționale; - Coordonează echipa de dezvoltare și asigură cadrul tehnic necesar implementării versiunilor (controlul versiunilor, etc); - Documentează codul sursă și configurările efectuate și asigură transfer de cunoștințe către echipa de Autorității Contractante - Testează și coordonează activitatea de testare privind funcționarea sistemului digital cu setul de date de test agreat cu Autoritatea Contractantă astfel	Studii superioare, absolvite cu diplomă de licență sau echivalent în specializările aferente domeniilor de licență Informatică, Cibernetică, statistică și informatică economică, Calculatoare și tehnologia informației sau Automatică, Informatică aplicată și sisteme inteligente sau în specializările Matematică-Informatică, Inginerie electrică și calculatoare, Rețele și software de telecomunicații, Securitate cibernetică, Informatică industrială, Matematică și informatică aplicată în inginerie. sau cel puțin o certificare recunoscută la nivel național sau internațional care să demonstreze competențe în dezvoltare de software în limbajul de programare de bază / tehnologia în care va fi realizată soluția oferată. și Peste 5 ani experiență în limbajele și frameworkurile aferente propunerii tehnice și peste 3 ani experiență în dezvoltare UI (ex. REACT, jQuery, JavaScript, HTML5, CSS) și cunoștințe de baze de date relaționale și non-relaționale. și Experiență specifică constând în implicarea în cel puțin un <i>contract comparabil*</i> în care să fi realizat activități similare cu cele din contractul ce urmează să fie atribuit.
---	--	---

	încât să fie acoperite cerințele solicitate.	
--	--	--

***Prin *contract comparabil* se înțelege un contract de dezvoltare și implementarea a unui sistem informatic, încheiat cu un beneficiar public sau privat.** Autoritatea contractantă va lua în considerare experiența dobândită în contracte finalizate sau aflate în desfășurare, dacă activitățile similare prestate integral au fost confirmate și recepționate de beneficiar.

Nu se ia în calcul experiența acumulată în derularea proiectelor interne ale angajatorului expertului (proiectele de dezvoltare software realizate intern).

Din documentele suport trebuie să reiasă clar și fără echivoc participarea efectivă a expertului în respectivul contract, poziția acestuia, perioada și durata implicării, activitățile similare pe care le-a avut expertul cu cele pe care le va avea în contractul ce urmează să fie atribuit și îndeplinirea condițiilor privind contractul comparabil.

11.3 Alte condiții referitoare la calificarea experților

Pentru fiecare expert cheie propus se vor prezenta următoarele documente:

- a. Curriculum Vitae, datat și semnat olograf sau electronic, personalizat pentru poziția din contract, din care să reiasă clar studiile, experiența și principalele contracte în care și-a desfășurat activitatea - trebuie să conțină explicit experiența profesională relevantă aferentă cerințelor;
- b. Diplome, certificate de absolvire, certificări (recunoscute la nivel național sau internațional în specializarea solicitată sau, după caz, în tehnologiile solicitate), autorizații, atestate profesionale sau orice alte documente similare prin care să se demonstreze pregătirea/calificarea solicitată (aflate, acolo unde este cazul, în termen de valabilitate la termenul limita stabilit pentru depunerea ofertelor);
- c. Documente suport privind experiența similară:
 - recomandări, contracte sau documente similare emise/contrasemnate de beneficiarii contractelor comparabile, din care să reiasă îndeplinirea cerințelor privind experiența similară, respectiv participarea efectivă a expertului în respectivul contract, poziția acestuia, perioada și durata implicării, activitățile similare pe care le-a avut expertul cu cele pe care

le va avea în contractul ce urmează să fie atribuit și îndeplinirea condițiilor privind contractul comparabil

- alte tipuri de documente relevante, precum fișă de post, contract de muncă, contracte, recomandări sau documente similare emise de angajatori, cu mențiunea că acestea trebuie să fie susținute de documente justificative/ suport de la beneficiarii contractelor comparabile (de exemplu documente constatatoare, certificări de bună-execuție, documente de recepție fără obiecții etc), astfel încât să se poată face dovada îndeplinirii cerințelor privind experiența similară, respectiv participarea efectivă a expertului în respectivul contract, poziția acestuia, perioada și durata implicării, activitățile similare pe care le-a avut expertul cu cele pe care le va avea în contractul ce urmează să fie atribuit și îndeplinirea condițiilor privind contractul comparabil

- d. Declarație de disponibilitate pentru perioada aferentă activităților pe care și le asumă din prezentul contract (se prezintă în cazul în care se propun persoane care nu sunt angajați ai ofertantului), datat și semnat olograf sau electronic, personalizată pentru poziția din contract sau extras Revisal dacă persoana este angajat al ofertantului;

Eventualele diplome/certificări/autorizații/atestate prezentate trebuie să fie emise de o autoritate publică competentă sau de către un organism de drept public/privat care respectă standardele europene de certificare - ISO IEC 17024 (înțelegând prin aceasta organisme al căror obiect de activitate este formarea/perfecționarea profesională, indiferent de forma de organizare a respectivelor entități publice/private ca ONG-uri, universități/academii/companii de profil ce emit astfel de certificări).

Se accepta prezentarea de documente echivalente în conformitate cu prevederile art. 202 alin. (4) din Legea nr. 98/2016, prin intermediul cărora se probează în mod concludent, îndeplinirea respectivelor cerințe.

În conformitate cu principiul recunoașterii reciproce, Autoritatea Contractantă acceptă documente echivalente celor solicitate la nivelul documentației de atribuire, emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/ autorizațiilor în cauză.

Operatorul economic străin trebuie să întreprindă, acolo unde legislația națională impune, demersurile necesare pentru a putea prezenta pe parcursul derulării Contractului autorizațiile recunoscute de autoritățile române.

Sarcina probei incumbă ofertantului, autoritatea contractantă rezervându-și dreptul de a solicita, dacă se consideră necesar, clarificări privind documentele prezentate.

În cazul în care experții prezentați din cadrul echipei nu sunt vorbitori de limba română, ofertantul va asigura pe costul său servicii de traducere și interpretariat de specialitate în limba română, pe toata durata contractului. Ofertantul va lua toate măsurile pentru asigurarea unor traduceri de calitate.

Fiecare dintre persoanele propuse trebuie să îndeplinească integral toate cerințele minime aferente expertului (profilului de persoană) pentru care au fost nominalizate.

Autoritatea contractantă își rezervă dreptul de a:

- verifica exactitatea informațiilor și a dovezilor furnizate de ofertanți și de a solicita și alte documente/ informații care să clarifice experiența echipei de experți propusa;
- contacta beneficiarii contractelor prezentate ca experiență profesională, în vedere confirmării celor prezentate de către ofertanți.

11.4 Alți experți non-cheie

Pe lângă experții cheie, vor fi necesari și alți experți, denumiți în continuare **experți non-cheie**. Complexitatea contractului necesită o echipă cu o diversitate de aptitudini și competențe care să poată fi alocată dinamic, în funcție de necesitățile apărute.

În acest context, pot fi implicați și alți experți, precum cei enumerați mai jos (cu titlu exemplificativ, fără ca enumerarea să fie limitativă), care pot fi mobilizați în calitate de experți non-cheie, în funcție de necesitățile specifice implementării contractului, după cum urmează:

- **Expert User Experience / User Interface (UX/UI) - Expert dezvoltare software (1 persoană)**
 - Proiectează interfața utilizator astfel încât să fie intuitivă, ușor de utilizat și să corespundă nevoilor utilizatorilor
 - Elaborează prototipuri și machete de interfață pentru aplicațiile web și mobile ale sistemului;
 - Proiectează arhitectura vizuală și comportamentală a interfețelor, conform principiilor de design centrat pe utilizator;
 - Asigură coerența vizuală și funcțională a interfețelor pentru toate modulele platformei;
 - Colaborează cu echipele de dezvoltare pentru implementarea designului UI/UX și validarea comportamentului interactiv;
 - Testează utilizabilitatea interfețelor și să propună ajustări pentru îmbunătățirea experienței utilizatorilor;
 - Asigură conformitatea cu standardele de accesibilitate web (WCAG 2.2) și cu cerințele de design multilingv și responsive;
 - Participă la elaborarea ghidurilor de design, a regulilor de interfață și a manualelor de utilizare;

- Se asigură că interfețele oferă o experiență intuitivă și uniformă pentru toate categoriile de utilizatori (funcționari, experți, administratori, public larg);
- Colaborează cu experții funcționali, arhitecții de soluție și echipa tehnică pentru armonizarea aspectelor vizuale, funcționale și tehnice ale sistemului.

- Experți dezvoltare software (3 persoane)

- Participarea la implementarea, configurarea și personalizarea sistemului digital;
- Activități specifice de implementare și configurare a soluției software;
- Dezvoltarea de software și integrare, inclusiv programarea și testarea API-urilor pentru asigurarea comunicării între componentele sistemului.
- Colaborarea cu ceilalți membri ai echipei pentru a asigura implementarea corectă a cerințelor;
- Participarea la definirea bunelor practici în dezvoltare, standardelor de cod și procedurilor de mentenanță;
- Propunerea și implementarea de soluții de îmbunătățire a performanței și eficienței sistemului;
- Documentarea configurărilor efectuate și transfer de cunoștințe către echipa de administrare IT din partea Autorității Contractante.
- Colaborarea cu echipa de securitate IT și alte echipe tehnice pentru a asigura respectarea standardelor și politicilor de securitate;

- Manager de analiză (1 persoană)

- Coordonarea activităților echipei de analiști de business;
- Planificarea și monitorizarea activităților de analiză și colectare de date;
- Validarea cerințelor funcționale și tehnico-funcționale transmise de analiști;
- Supravegherea elaborării fluxurilor de informație, a specificațiilor de interconectare și a documentației de analiză;
- Asigurarea coerenței între cerințele Autorității Contractante și soluțiile propuse de echipele tehnice;
- Identificarea și gestionarea riscurilor asociate activităților de analiză;
- Coordonarea și revizuirea documentației elaborate de analiști (manuale de utilizare, specificații funcționale);
- Facilitarea comunicării între beneficiari, analiști și echipele tehnice;

- Supravegherea activităților de testare a sistemului din perspectiva cerințelor;
- Raportarea progresului activităților de analiză către managerul de proiect sau echipa de conducere a contractului;
- Asigurarea respectării metodologiilor de management al cerințelor și a standardelor de bune practici în analiză.

- Analist de business (1 persoană)

- Analiza cerințelor și specificațiilor tehnico-funcționale ale Autorității Contractante;
- Participare la modelarea datelor și la definirea funcțională a aplicațiilor;
- Identificarea proceselor interne ale Autorității Contractante;
- Colectarea și validarea datelor documentate de la beneficiar;
- Identificare riscuri asociate implementării sistemului;
- Furnizarea informațiilor, restricțiilor precum și recomandărilor privind implementarea platformei;
- Elaborarea fluxurilor de informație și a specificațiilor de interconectare;
- Participă la elaborarea manualelor de utilizare;
- Acordă suport utilizatorilor cheie pentru testarea de acceptanță a sistemului;
- Colaborarea cu echipele tehnice (Realizarea de interviuri cu persoanele implicate)

- Experți testare software (2 persoane)

- Implementarea planurilor, scenariilor și cazurilor de test;
- Testarea aplicațiilor software din punct de vedere tehnic, funcțional, performanță și identificarea posibilelor erori;
- Testarea tuturor cerințelor din caietul de sarcini, și a celor identificate/detaliat în urma desfășurării fazei de analiză și proiectare;
- Analiza problemelor și recomandarea de soluții;
- Testarea funcționalităților sistemelor conform unei metodologii de testare recunoscută;
- Activități de testare componente și testare funcțională;
- Identificarea, specificarea și implementarea îmbunătățirilor în ceea ce privește funcționarea soluțiilor software;
- Crearea de scenarii de utilizare și scripturi de testare;
- Întocmirea și livrarea rapoartelor de testare și implementare.

- Vor conlucra îndeaproape cu ceilalți experți și cu echipa de implementare, pentru a asigura că toate modulele și funcționalitățile sistemului sunt testate riguros, atât individual, cât și în ansamblul lor integrat, conform specificațiilor tehnice și de business;
- Elaborează documentația de testare.

În cazul în care ofertantul considera necesară suplimentarea echipei și cu alți experți față de experții de mai sus, pe care îi consideră necesari pentru îndeplinirea optimă a activităților care fac obiectul acordului-cadru, ofertantul va include în ofertă următoarele informații:

- tipul și numărul acestor experți suplimentari considerați necesari pentru îndeplinirea contractului;
- descrierea atribuțiilor acestora în cadrul contractului (profilul profesional al acestora)
- angajamentul ferm al ofertantului privind asigurarea disponibilității acestor experți non-cheie pe parcursul implementării contractului.

Aceștia vor fi considerați experți non-cheie.

Pentru experții non-cheie nu este necesară prezentarea identității exacte a acestora în cadrul propunerii tehnice și a documentelor suport la momentul ofertării.

Pentru experții non-cheie propuși, în cadrul ofertei tehnice se vor prezenta numai informații privind modul de implicare a acestora în activitățile contractului, responsabilitățile, momentul implicării precum și metodologia care va fi utilizată pentru identificarea/ recrutarea acestora și includerea în echipa în momentele necesare. Spre deosebire de experții cheie, pentru care se solicită documentele justificative la termenul limită de depunere a ofertelor, pentru experții non-cheie documentele justificative se prezintă și se evaluează la momentul implicării acestora în activitățile viitorului Contract.

Experții non-cheie vor fi implicați în derularea contractului doar cu notificarea prealabilă a Autorității Contractante cu minimum 10 zile înainte de data propusă pentru implicarea în contract. Notificarea va fi în mod obligatoriu însoțită de documentele justificative.

Prestatorul va prezenta, pe parcursul implementării contractului, pentru fiecare expert non cheie propus, următoarele informații/documente:

- numele persoanei propuse pentru fiecare poziție;
- curriculum Vitae (CV), semnat de către titular și datat;
- declarația privind disponibilitatea, semnată în original;

- copii ale documentelor justificative relevante care demonstrează îndeplinirea cerințelor referitoare la studiile, expertiza și experiența specifică relevantă solicitată și prezentată în CV, cum ar fi:
 - o diplome de studii, certificări, alte diplome relevante;
 - o recomandări sau alte documente edificatoare din care să reiasă activitățile desfășurate și care să evidențieze experiența profesională specifică relevantă.

Evaluarea de către beneficiar a îndeplinirii cerințelor privind calificările și experiența similară, stabilite în prezentul caiet de sarcini pentru experții non-cheie, se va realiza în baza documentelor transmise de prestator înainte de implicarea acestora în activitățile contractului.

Beneficiarul are dreptul de a respinge motivat expertul non-cheie, în situația în care constată că acesta nu prezintă documente justificative conforme cu rolul pentru care este propus sau constată existența unui conflict de interese.

Toate costurile aferente personalului Prestatorului (experți cheie, experți non-cheie, personal administrativ) vor fi suportate de Prestator și vor fi incluse în propunerea sa financiară.