NR_16/IICG_PNRR/29.01.2026

Aprob,

Președinte

Dragoș-Cristian VLAD

Vlad Dragos-Cristian
2026.01.29 17:09:51 +02'00'

Propun aprobarea,

Secretar General

Dragoș-Cosmin NICULESCU

Niculescu Dragos-Cosmin
Digitally signed by Niculescu Dragos-Cosmin
Date: 2026.01.29 16:57:25 +02'00'

CAIET DE SARCINI

pentru achiziția publică având ca obiect:

FURNIZARE PLATFORMĂ DE JURNALIZARE SI NOTIFICARE CPG

în cadrul proiectului **„Implementarea infrastructurii de cloud guvernamental”**

72265000-0 Servicii de configurare de software

72200000-7 Servicii de programe și de consultanță software

48000000-8 Pachete software și sisteme informatice

Cuprins

1. INTRODUCERE

Caietul de sarcini face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor pe baza cărora fiecare ofertant va elabora Oferta (Propunerea Tehnică și Propunerea Financiară) pentru realizarea serviciilor care fac obiectul Contractului ce rezultă din această procedură.

În cadrul acestei proceduri, Autoritatea pentru Digitalizarea României - ADR îndeplinește rolul de autoritate contractantă.

Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

Ofertele care nu îndeplinesc toate cerințele minimale vor fi declarate neconforme. Nu se acceptă depunerea de oferte alternative. Nu se admit ofertele parțiale din punct de vedere cantitativ și calitativ, ci numai ofertele integrale, care corespund tuturor cerințelor stabilite prin prezentul Caiet de sarcini. Orice ofertă care se abate de la cerințele minimale va fi considerată admisibilă numai în condițiile în care aceasta asigură un nivel calitativ superior cerințelor minimale.

În conformitate cu regulile de elaborare a documentației de atribuire din Legea nr. 98/2016, privind achizițiile publice, cu modificările și completările ulterioare (denumită în continuarea Legea nr. 98/2016) art. 156 alin (2) și (3) specificațiile tehnice din prezentul Caiet de sarcini care precizează un anumit producător, o anumită origine sau un anumit procedeu care caracterizează produsele sau serviciile furnizate 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.

2. CONTEXTUL REALIZĂRII ACESTEI ACHIZIȚII DE SERVICII

Autoritatea pentru Digitalizarea României, denumită în continuare ADR, are rolul de a realiza și coordona implementarea strategiilor și a politicilor publice în domeniul transformării digitale și societății informaționale.

ADR funcționează în baza prevederilor HG nr. 89/2020, cu modificările și completările ulterioare. În contextul importanței tot mai mari a tehnologiilor și a infrastructurilor digitale în viața noastră, misiunea ADR este esențială.

Transformarea digitală vizează optimizarea modului de lucru și a procedurilor pentru o productivitate mai ridicată într-o organizație. Acest lucru se realizează prin adoptarea, cu celeritate și la toate nivelurile, a noilor tehnologii digitale.

Transformarea digitală a economiei este condiționată de o transformare a competențelor forței de muncă, inclusiv o generalizare a programelor de formare pe parcursul vieții. În acest sens, instruirea în dezvoltarea competențelor digitale este esențială.

2.1. Informații despre Autoritatea Contractantă

Potrivit HG. nr.89/2020 privind organizarea și funcționarea Autorității pentru Digitalizarea României, cu modificările și completările ulterioare,, ADR se organizează și funcționează ca structură cu personalitate juridică în subordinea Ministerului Economiei, Digitalizării, Antreprenoriatului și Turismului, având rolul de a realiza strategiile și politicile publice în domeniul transformării digitale și societății informaționale și de a coordona implementarea acestora, precum și rolul de a asigura monitorizarea și controlul asupra respectării reglementărilor interne și internaționale în domeniul transformării digitale și societății informaționale.

În acord cu art.3 la HG.nr.89/2020, Autoritatea pentru Digitalizarea României are următoarele obiective:
a) contribuie la transformarea digitală a economiei și societății românești;
b) realizează guvernarea electronică la nivelul administrației publice din România;
c) contribuie la îndeplinirea obiectivelor pentru România ale programelor de asistență financiară ale Uniunii Europene în domeniul său de competență.

AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI (ADR)
Sediul principal: Bd. Libertății nr 14, sector 5, București, România, cod poștal 050706
Sediul secundar: Strada Italiană, nr. 22, sector 2, București, cod poștal 020976
Cod fiscal: R042283735
Telefon: 021 3052710
Fax: 021 3032899
Programul de lucru normal: L-J – 8.30-17.00, V - 8.30-14.30

2.2. Informații despre contextul care a determinat achiziționarea serviciilor

La data de 28 octombrie 2021, Consiliul Uniunii Europene a aprobat Planul Național de Redresare și Reziliență al României (PNRR) conform art. 20 din Regulamentul nr.

241/2021 al Parlamentului European și al Consiliului de instituire a Mecanismului de redresare și reziliență, în acest sens fiind emisă Decizia de punere în aplicare a Consiliului din 29 octombrie 2021 de aprobare a evaluării planului de redresare și reziliență al României.

Potrivit cadrului legal național, respectiv OUG nr. 155/2020 privind unele măsuri pentru elaborarea Planului național de redresare și reziliență necesar României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de redresare și reziliență, cu modificările și completările ulterioare (OUG nr. 124/2021 privind stabilirea cadrului instituțional și financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare și reziliență, precum și pentru modificarea și completarea OUG nr. 155/2020 privind unele măsuri pentru elaborarea Planului național de redresare și reziliență necesar României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de redresare și reziliență), Ministerul Investițiilor și Proiectelor Europene (MIPE) este coordonatorul național pentru elaborarea, negocierea, aprobarea și implementarea PNRR.

Potrivit:

- prevederilor Regulamentului (UE) 2021/241,
- prevederilor Deciziei de punere în aplicare a Consiliului din 3 noiembrie 2021 de aprobare a evaluării Planului de Redresare și Reziliență al României,
- prevederilor O.U.G. nr. 155/2020, cu modificările și completările ulterioare,
- prevederilor O.U.G. nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice,
- prevederilor HG nr. 112/2023 privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental,
- prevederilor O.U.G. nr. 153/2024, privind stabilirea unor măsuri la nivelul administrației publice centrale,
- prevederilor HG nr. 504/2023 pentru aprobarea Notei de fundamentare referitoare la necesitatea şi oportunitatea efectuării cheltuielilor aferente proiectului de investiții "Implementarea infrastructurii de cloud guvernamental", prevederilor Legii nr. 92/1996 privind organizarea și funcționarea Serviciului de Telecomunicații Speciale, cu modificările și completările ulterioare,
- Acordului de parteneriat nr. 2279/27.06.2022 - 355947/27.06.2022 - 154824/28.06.2022 încheiat între Autoritatea pentru Digitalizarea României (ADR), în calitate de Lider de parteneriat-Partener 1, Serviciul de Telecomunicații Speciale (STS) în calitate de Partener 2 și Serviciul Român de Informații prin U.M. 0929 București (SRI) în calitate de Partener 3,
- Contractului de finanțare încheiat între Ministerul Cercetării, Inovării și Digitalizării (MCID), în calitate de coordonator de reforme și investiții pentru PNRR, Componenta C7. Transformare digitală și ADR, prin Organismul Intermediar pentru Promovarea Societății Informaționale (OIPSI), în calitate de agenție de implementare pe de o parte și ADR, în calitate de lider de parteneriat și beneficiar, STS în calitate de partener și beneficiar și SRI în calitate de partener și beneficiar,

ADR participă, în parteneriat cu STS și SRI, la implementarea investiției (proiectului) *IMPLEMENTAREA INFRASTRUCTURII DE CLOUD GUVERNAMENTAL,* finanțată prin PNRR, Componenta C7. Transformare digitală.

ADR a încheiat contractul de finanțare nr. 3131 / 2022 pentru implementarea proiectului **„Implementarea Infrastructurii de Cloud Guvernamental”**, finanțat din PNRR, aferent Investiției 1 - „Implementarea Infrastructurii de Cloud Guvernamental”, Componenta C7 - Transformare digitală.

Obiectivul general al proiectului este: realizarea infrastructurii cloudului guvernamental, folosind tehnologii de ultimă generație, cu un înalt grad de securitate cibernetică, eficiente din punct de vedere energetic, necesare asigurării găzduirii de sisteme informatice publice centrale și interoperabilității acestora, într-un mod unitar și standardizat.

Conform OUG nr. 89/2022 *privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice*, Cloud-ul Guvernamental al României este referențiat ca Platforma de Cloud Guvernamental și are o componentă de Cloud Privat, denumită în continuare Cloudul Privat Guvernamental (CPG).

Conform Componentei 7 - Transformare digitală din PNRR, CPG este organizat pe două niveluri, fapt ce conduce la necesitatea a două componente separate și complementare: Cloud-ul Intern (CI) care *„capitalizează soluțiile existente în prezent cu niveluri scăzute de virtualizare prin transformarea lor în soluții informatice cloudificate IaaS și PaaS accesibile instituțiilor din administrația publică„* și Cloud-ul Dedicat (CD) care *„se bazează pe soluțiile de Cloud disponibile în sectorul industrial/comercial”*.

Strategia de cloud a Comisiei Europene descrie modul în care cloud computing modelează viitorul IT în cadrul instituției și este un factor favorizant pentru strategia digitală globală a Comisiei Europene.
În centrul strategiei cloud se află o abordare bazată pe cloud, cu o ofertă de servicii hibride multi-cloud sigure.
Strategia Digitală a Comisiei Europene (ECDS) -
https://commission.europa.eu/publications/european-commission-cloud-strategy_en
stabilește o viziune pentru o administrare transformată digital, axată pe utilizator și bazată pe date. Acest obiectiv ambițios necesită schimbări de transformare într-un număr de domenii cheie, transformarea IT sprijinind transformarea afacerii.
Unul dintre facilitatorii acestei transformări a IT este cloud computing.

Această nouă paradigmă a furnizării de servicii IT a adus două schimbări cheie în peisajul IT:

- Prima este o piață globală de servicii IT care permite consumul la cerere de resurse IT, blocuri IT avansate și chiar aplicații complexe de afaceri fără a investi în infrastructura IT;
- A doua este un nou mod de dezvoltare a sistemelor informaționale (cloud-native) bazate pe aceste servicii IT bazate pe cloud. Acest lucru permite o complexitate redusă a sistemului informațional și, în schimb, o concentrare sporită pe valoarea afacerii. Împreună, aceste două schimbări permit schimbarea transformațională a IT pentru a sprijini transformarea afacerii.

Comisia Europeană a promovat cloud computing în rândul companiilor și administrațiilor publice deopotrivă de la adoptarea primei strategii europene de cloud computing [1]în 2012. În conformitate cu politicile europene de cloud față de autoritățile guvernamentale, DIGIT a fost pionier în experimentarea cloud computing de către instituțiile și agențiile UE și a rafinat experiența într-o listă cuprinzătoare de lecții învățate.

Experiența a confirmat potențialul de transformare al cloud computing, dar arată și că guvernanța corporativă și managementul securității necesită o atenție specială pentru a evita expunerea nedorită la riscuri în domeniul costurilor și securității informațiilor.
Pe baza acestor lecții învățate, Comisia Europeană definește o viziune pentru cloud computing:
Cloud-first înseamnă că sistemele ar trebui mai degrabă concepute în așa fel încât să poată beneficia de avantajele modelelor de livrare bazate pe cloud, care există atât on-premise, cât și în cloud-ul public. Alegerea arhitecturii, în special a cloud-ului on premise și/sau public, va depinde de avantajele, constrângerile și riscurile pentru un anumit sistem. Deci nu înseamnă că toate sistemele ar trebui să meargă în cloud public.

Abordarea **cloud-first** implică faptul că orice nouă dezvoltare ar trebui să fie, de preferință, nativă din cloud, iar sistemele de informații existente ar trebui reevaluate pentru transformare, rescriere sau înlocuire în contextul planurilor de modernizare prevăzute de strategia digitală a Comisiei Europene, valorificând oportunitățile apărute în ciclul de viață al afacerii și al aplicațiilor.

Oferta de servicii Cloud disponibilă Comisiei Europene trebuie să fie:
- **Securizat** prin identificarea și gestionarea riscurilor de securitate informatică și gestionarea datelor în conformitate cu clasificarea acesteia, precum și în conformitate cu obligațiile **de protecție a datelor** ale Comisiei Europene;
- **Hibrid** prin utilizarea serviciilor atât de la furnizorii de cloud public, cât și de la un cloud privat administrat de Comisia Europeană;
- **Multi-cloud** prin nelegarea Comisiei Europene de un singur furnizor public de cloud și sursă de la furnizorul de cloud cel mai potrivit pentru a furniza serviciul solicitat;
- **Eficient energetic** în linie cu prioritatea generală a UE de reducere a amprentei de carbon și cu politica de achiziții publice ecologice.

Pentru a implementa această viziune, sunt necesare schimbări în mai multe domenii cheie:
În domeniul **guvernanței IT**, Comisia Europeană va revizui, în contextul pachetului de guvernanță adoptat în noiembrie 2018, procesele de guvernanță pentru ciclul de viață al sistemelor informatice și se va asigura că acestea sunt adecvate scopului pentru a gestiona toate aspectele cloud computing. În plus, va pune în aplicare mecanismele necesare pentru a se asigura că foile de parcurs de modernizare necesare în contextul Strategiei digitale a Comisiei Europene sunt aliniate la principiile cloud-first.

Guvernarea riscurilor specifice cloud va fi susținută de un nou instrument, GovSec, care oferă suport pentru gestionarea riscurilor hands-on pentru sistemele bazate pe cloud. Instrumentul va permite o abordare practică și comună în ceea ce privește gestionarea peisajului de risc din cloud, economisind timp prețios în timpul fazei obligatorii de

[1]COM(2012) 529 Dezlănțuirea potențialului cloud computing în Europa

evaluare a riscurilor a proiectelor, asigurând în același timp o bază comună în cadrul Comisiei Europene, instituțiilor și agențiilor.

DIGIT va continua să funcționeze ca broker de cloud interinstituțional, pentru a permite Comisiei Europene și instituțiilor și agențiilor europene interesate să achiziționeze în mod eficient și în siguranță servicii cloud de la o gamă largă de furnizori de servicii cloud, atenuând riscul blocării furnizorilor, să faciliteze monitorizarea costurilor și previziunile și să ofere îndrumări. Pentru Comisia Europeană, Cloud Broker va oferi, de asemenea, servicii cloud de bază și va impune o bază comună de securitate și protecție a datelor în toate utilizările cloud.

În domeniul **Soluțiilor Digitale**, Comisia Europeană va favoriza aprovizionarea cu soluții generice sau standard de pe piața aplicațiilor de afaceri bazate pe cloud (Software as a Service). Pentru soluții specifice politicilor, Comisia Europeană ar trebui să promoveze o trecere la metodologii de dezvoltare native în cloud, o schimbare care necesită o transformare a mentalității, proceselor, arhitecturii și tehnologiei.

În zona **Platformei de soluții reutilizabile**, Comisia Europeană va transforma serviciile, cadrele, blocurile de construcție și platformele tehnice existente în servicii native din cloud în cadrul unei platforme cuprinzătoare de soluții reutilizabile.

În domeniul Ecosistemului de **Date**, Comisia Europeană se va transforma într-o organizație bazată pe date prin înființarea unui ecosistem de date pentru captarea, conservarea, stocarea, protejarea, elaborarea, accesarea, utilizarea, reutilizarea, consumarea, analizarea, diseminarea și partajarea datelor.

În zona **Digital Workplace**, DIGIT va folosi o platformă hibrid cloud SaaS pentru a oferi Comisiei Europene un mediu digital la locul de muncă care le permite utilizatorilor să lucreze și să colaboreze oriunde și oricând de pe orice dispozitiv corporativ.

În domeniul **infrastructurilor digitale**, DIGIT va furniza servicii Hibrid Cloud Comisiei Europene și instituțiilor și agențiilor interesate. Pentru a atinge acest obiectiv, va crea un serviciu de arhitectură a soluției Hibrid Cloud și va transforma serviciile Data Center în servicii Hibrid Cloud, construite atât pe infrastructurile Cloud publice, cât și pe cele private.

În domeniul **Cloud Security Services**, DIGIT va furniza Comisiei Europene servicii de securitate activate în cloud pentru toate fazele ciclului de viață a tuturor tipurilor de consum de servicii Cloud.

In acest context European implementarea componentei de cloud dedicat a Cloudului Privat Guvernamental va facilita sporirea calității si securității serviciilor informatice si de comunicații la nivel național si european, precum si creșterea disponibilității si a nivelului de securitate a serviciilor oferite instituțiilor si entităților din administrația publica centrala si locala - ecosistemul digital guvernamental.

2.3. Obiectivul general la care contribuie realizarea serviciilor

Obiectivul general al Investiției 1 „Implementarea infrastructurii de CLOUD GUVERNAMENTAL” constă în realizarea infrastructurii Cloud-ului Guvernamental, folosind tehnologii de ultimă generație, cu un înalt grad de securitate cibernetică, eficiente din punct de vedere energetic, necesare asigurării găzduirii de sisteme informatice aparținând administrației publice centrale și interoperabilității acestora, într-un mod unitar și standardizat.

Dezvoltarea cloudului guvernamental se va realiza într-un model hibrid ce va permite autorităților centrale si locale din Romania sa beneficieze de o platforma tehnologică modernă care facilitează implementarea unor sisteme informatice interoperabile, uniforme, scalabile,si cu costuri si timpi de implementare reduse.

Se va folosi un model hibrid de cloud, special conceput pentru a construi o infrastructură de cloud privat guvernamental. Acesta va facilita migrarea și dezvoltarea sistemelor informatice ale instituțiilor publice centrale și locale către o arhitectură de tip cloud. Modelul acesta va oferi o gamă completă de servicii, incluzând atât Infrastructura ca Serviciu (IaaS), Platforma ca Serviciu (PaaS), cât și Software ca Serviciu (SaaS). În plus, modelul va gestiona aplicații orizontale, orientate atât către cetățeni, cât și către angajații autorităților centrale.

Obiectivul proiectului este verificarea legalității prelucrării datelor cu caracter personal, monitorizării și asigurării integrității și securității corespunzătoare datelor cu caracter personal vehiculate prin sistemele informatrice gazduite in cloudul guvernamental.

2.4. Informații despre beneficiile anticipate de către Autoritatea Contractantă

Societatea informațională se caracterizează prin accesul extins la informații și tehnologii, promovând o lume conectată și bazată pe cunoștințe. Transformarea digitală reprezintă o paradigmă globală care vizează utilizarea tehnologiilor digitale pentru a revoluționa aspectele economice, sociale și culturale ale societății.
Autoritatea pentru Digitalizarea României (ADR) este o instituție înființată prin HG nr. 89/2020, având rolul de a realiza și coordona implementarea strategiilor și a politicilor publice în domeniul transformării digitale și societății informaționale. Conform art. 3 lit. a) din HG nr. 89/2020, ADR contribuie la a transformarea digitală a economiei și societății românești.

Reziliența economică este asigurată de faptul că dezvoltarea Cloud-ului Guvernamental va duce la o creștere a gradului de digitalizare a serviciilor oferite de autoritățile / instituțiile publice din România.
Acest lucru va asigura următoarele beneficii din perspectiva serviciilor de e-guvernare:

- eficientizarea furnizării acestora;
- reducerea costurilor necesare asigurarii acestora;
- reducerea timpului in care cetățenii / operatorii economici beneficiază de aceste servicii;
- îmbunătățirea interacțiunii dintre cetățeni / mediul de afaceri cu autoritatile / institutiile publice;
- asigurarea continuitatii serviciilor IT chiar si in cazul evenimentelor neasteptate cu impact major asupra dezvoltarii normale a activitatilor din societate (de exemplu pandemia COVID-19, cutremure, inundatii);

- protejarea confidentialitatii, integritatii si disponibilitatii informatiilor in cadrul CPG (cloud privat guvernamental);
- protejarea impotriva atacurilor avansate de tip APT, realizate de catre actori cibernetici ce utilizeaza mecanisme de compromitere sofisticate, prin intermediul carora pot urmari, printre altele, identificarea si exfiltrarea de date sensibile din cadrul infrastructurilor afectate;
- securizarea serviciilor utilizate de institutiile beneficiare, din punctul de vedere al securitatii cibernetice, prin folosirea unor solutii specializate pentru asigurarea securitatii sistemelor, aplicatiilor si serviciilor accesibile din internet si analiza comportamentala, folosind tehnologii bazate pe IA.

Totodată, cel puțin 30 de instituții publice vor fi conectate la Cloud-ul Guvernamental și îl vor utiliza până la finele anului 2025.

Toate aceste beneficii obtinute prin dezvoltarea infrastructurii guvernamentale de Cloud vor contribui la rezilienta economiei prin asigurarea eficientei si continuitatii serviciilor publice furnizate de autoritatile / institutiile publice cetatenilor si mediului de afaceri. Totodata, va fi asigurata compatibilitatea functionala (cloud native, cloud ready) a Centrelor de Date din cadrul Cloud-ului pentru a asigura un grad ridicat de reziliență si scalabilitate in cazul unei situații de criza de lunga durata, de tipul pandemic.

2.5. Alte inițiative/proiecte/programe asociate cu această achiziție de servicii

Nu este cazul.

2.6. Cadrul general al sectorului în care Autoritatea Contractantă își desfășoară activitatea

Societatea informațională se caracterizează prin accesul extins la informații și tehnologii, promovând o lume conectată și bazată pe cunoștințe.

Autoritatea pentru Digitalizarea României, denumită în continuare ADR, are rolul de a realiza strategiile și politicile publice în domeniul transformării digitale și societății informaționale și de a coordona implementarea acestora, precum și rolul de a asigura monitorizarea și controlul asupra respectării reglementărilor interne și internaționale în domeniul transformării digitale și societății informaționale.

ADR exercită, în domeniul său de competență, următoarele funcții:
- de reglementare, prin care reglementează participarea la elaborarea cadrului normativ și instituțional în domeniul transformării digitale și societății informaționale, inclusiv cu privire la interoperabilitatea sistemelor informatice ale instituțiilor publice;
- de autoritate de stat, prin care se asigură urmărirea și controlul respectării reglementărilor în domeniul său de competență;
- de promovare, coordonare, monitorizare, control și evaluare a realizării politicilor în domeniul său de competență, precum și a cadrului național de interoperabilitate;
- de comunicare, prin care se asigură comunicarea atât cu celelalte structuri ale sectorului public, cât și cu sectorul privat și societatea civilă;

- de implementare și îndeplinește atribuțiile aferente acesteia, pentru componentele de investiții din PNRR, respectiv Componenta 7 - Transformare digitală, în condițiile acordului de implementare încheiat cu coordonatorul de reforme și investiții pentru Planul național de redresare și reziliență, responsabil pentru componenta C7 - Transformare digitală, conform art. 3 din Ordonanța de urgență a Guvernului nr. 124/2021 privind stabilirea cadrului instituțional și financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare și reziliență, precum și pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului național de redresare și reziliență necesar României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de redresare și reziliență, aprobată cu modificări și completări prin Legea nr. 178/2022, cu modificările și completările ulterioare;
- de monitorizare, control și evaluare a implementării politicilor în domeniul interoperabilității.

În ceea ce privește atribuțiile pe care ADR le are, relevante pentru prezenta procedură, în aria de afaceri europene, menționăm:
- asigură îndeplinirea, în domeniul de competență, a obligațiilor decurgând din calitatea României de stat membru al Uniunii Europene și al Organizației Tratatului Atlanticului de Nord, precum și de stat candidat la Organizația pentru Cooperare și Dezvoltare Economică, inclusiv în ceea ce privește transpunerea și/sau crearea cadrului juridic de aplicare directă a actelor juridice obligatorii ale Uniunii Europene, implementarea și monitorizarea aplicării acestora;
- propune ministrului cercetării, inovării și digitalizării elaborarea cadrului normativ-metodologic, necesar implementării politicilor, inclusiv prin transpunerea normelor europene în domeniul societății informaționale, tehnologiei informației, al interoperabilității sistemelor informatice și al transformării digitale, în procesul de armonizare a legislației naționale cu cea a Uniunii Europene;
- stabilește standardele și reglementările tehnice în domeniul guvernării electronice, societății informaționale și interoperabilității, prin decizie a președintelui ADR, care devin obligatorii la nivelul întregii administrații publice odată cu publicarea acestora în Monitorul Oficial al României, Partea I, și verifică implementarea acestora, dispunând, prin decizie a președintelui ADR, remedierea deficiențelor constatate;
- exercită rolul de coordonare pentru punerea în aplicare în România a Regulamentului (UE) 2018/1.724 al Parlamentului European și al Consiliului din 2 octombrie 2018 privind înființarea unui portal digital unic (gateway) pentru a oferi acces la informații, la proceduri și la servicii de asistență și de soluționare a problemelor și de modificare a Regulamentului (UE) nr. 1.024/2012;
- exercită rolul de coordonare pentru punerea în aplicare în România a Regulamentului (UE) 2017/1.128 al Parlamentului European și al Consiliului din 14 iunie 2017 privind portabilitatea transfrontalieră a serviciilor de conținut online în cadrul pieței interne;
- îndeplinește atribuțiile de autoritate responsabilă pentru realizarea, operaționalizarea și administrarea Punctului de contact unic electronic, potrivit Ordonanței de urgență a Guvernului nr. 49/2009 privind libertatea de stabilire a prestatorilor de servicii și libertatea de a furniza servicii în România,

aprobată cu modificări și completări prin Legea nr. 68/2010, cu modificările ulterioare;
- exercită calitatea de autoritate competentă pentru implementarea Regulamentului (UE) 2018/1.807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană;
- exercită calitatea de autoritate competentă la nivel național pentru serviciile de intermediere de date și de autoritate competentă în materie de reutilizare a datelor protejate, precum și calitatea de autoritate responsabilă de registrul public național al organizațiilor recunoscute de promovare a altruismului în materie de date, în conformitate cu Regulamentul (UE) 2022/868 al Parlamentului European și al Consiliului din 30 mai 2022 privind guvernanța datelor la nivel european și de modificare a Regulamentului (UE) 2018/1.724 (Regulamentul privind guvernanța datelor);
- în calitate de unitate centralizată de achiziții pentru aplicații software și serviciit, inclusiv în tehnologie de cloud2, încheie acorduri-cadru/sisteme dinamice de achiziție, în numele și pentru autoritățile și instituțiile publice, cu excepția acelor entități publice care sunt desemnate ca unități centralizate de achiziții, în conformitate cu prevederile art. 1 alin. (5) coroborate cu ale art. 4 alin. (3) din Ordonanța de urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice;
- dezvoltă și operează următoarele sisteme informatice, aprobate prin decizie a președintelui ADR, asigurând din punct de vedere tehnic și procedural funcționarea:
- (...)
    - sistemului „Punctul de contact unic electronic“ - PCUe;
    - platformei de cloud guvernamental;
    - platformei naționale de interoperabilitate;
    - În calitatea pe care ADR o are în cadrul Componentei 7 din PNRR, are în curs de derulare Investiția I1 referitoare la implementarea și operaționalizarea Cloudului Privat Guvernamental.

Potrivit următoarelor acte normative:
- Ordonanța de Urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice, cu modificările și completările ulterioare (Ordonanța de Urgență a Guvernului nr. 130/2023);
- Hotărârea Guvernului nr. 112/2023 privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental, cu modificările și completările ulterioare

ADR îndeplinește o serie de responsabilități ca Furnizor de Servicii de Cloud (FSC), potrivit Art. 6, Art. 20, Art. 21 alin (2) din HG nr. 112/2023.

Strategia **europeană de date** se străduiește să creeze o piață unificată a datelor în cadrul UE. Această viziune facilitează fluxul nerestricționat de date peste granițe și sectoare industriale, stimulând inovația și prosperitatea economică. Ea acordă prioritate atât controlului, cât și echității, permițând în același timp întreprinderilor să prospere

[2] HG nr. 89/2020, cu modificările și completările ulterioare, art. 5, lit. h), pct. 4^1, pct. 7

în economia bazată pe date. Această strategie deschide calea pentru crearea de **Spații europene comune de date ,** o piață unică pentru datele care asigură utilizarea conformă din punct de vedere legal a datelor atât din UE, cât și din țări terțe, indiferent de locația lor de stocare.

Legea privind guvernarea datelor (DGA)
Actul de guvernare a datelor (DGA) este primul pilon al Strategiei europene de date.
Este un regulament cuprinzător conceput pentru a guverna reutilizarea datelor deținute în mod public, promovând schimbul de date prin noi intermediari și încurajând partajarea altruistă a datelor. Acesta acoperă atât datele cu caracter personal, cât și cele nepersonale, Regulamentul general privind protecția datelor (GDPR) aplicându-se datelor cu caracter personal. DGA include garanții încorporate pentru a spori încrederea în partajarea și reutilizarea datelor, ceea ce este esențial pentru creșterea disponibilității datelor pe piață.

Regulamentul privind datele
Actul de date este al doilea pilon al Strategiei europene de date, completând Actul de guvernanță a datelor.
Acesta își propune să îmbunătățească economia de date a UE și să încurajeze o piață competitivă a datelor. Se concentrează pe a face datele industriale mai accesibile și mai utilizabile, încurajând inovația bazată pe date și sporind disponibilitatea datelor.
Legea asigură corectitudinea în alocarea valorii datelor și clarifică condițiile de utilizare a datelor. Odată cu creșterea rapidă a produselor conectate în UE, legea oferă utilizatorilor un control mai mare asupra datelor generate și stabilește condiții generale pentru obligațiile de partajare a datelor.
Include, de asemenea, măsuri pentru a promova corectitudinea și concurența pe piața europeană a cloud-ului, pentru a proteja companiile de abuzuri
termenii contractuali și să stabilească un mecanism pentru solicitările de date din sectorul public.
În plus, introduce garanții pentru a împiedica organismele guvernamentale din țări terțe să acceseze date nepersonale, cu încălcarea legislației UE sau naționale. Data Act, care completează Data Governance Act, urmărește să creeze o piață unică a UE pentru date, poziționând Europa ca lider în economia datelor în beneficiul economiei și societății.

3. DESCRIEREA SERVICIILOR SOLICITATE

3.1. Obiectivul general la care contribuie prestarea serviciilor

Obiectivul proiectului este de a pune la dispoziția cetățeanului istoricul privind acțiunile asupra datelor cu caracter personal proprii prelucrate de către USC prin intermediul sistemelor informatice găzduite în CPG.

3.2. Obiectivul specific la care contribuie prestarea serviciilor

Obiectivul specific este implementarea unei soluții informatice de jurnalizare si notificare în cloudul privat guvernamental care să furnizeze utilizatorilor finali o interfață prin care aceștia pot interacționa cu datele personale proprii prelucrate prin intermediul sistemelor informatice găzuite în CPG.

3.3. Descrierea serviciilor solicitate

3.3.1. Descrierea serviciilor

Platforma de Jurnalizare si Notificare are ca scop trasabilitatea prelucrării datelor cu caracter personal. Solutia trebuie sa asigure stocarea sub forma unor jurnale ce sunt prezentate în mod transparent și nemijlocit persoanei vizate , la cererea acesteuia sau prin intermediul aplicației de notificare a prelucrărilor de date cu caracter personal, după caz.

Implementarea sistemului de jurnalizare cuprinde dezvoltarea unei soluții tehnice astfel încât să asigure prelucrarea datelor și nerepudierea acțiunilor produse în sistemele și aplicațiile cloud de către factorul uman sau de aplicații, servicii sau interfețe de conectare. **Utilizatorul de servicii de cloud (USC)** este responsabil pentru colectarea, stocarea, gestionarea și protejarea datelor personale ale utilizatorilor în conformitate cu legislația aplicabilă. În calitate de operator, USC trebuie să asigure respectarea principiilor și cerințelor GDPR, precum: legalitatea, echitatea și transparența prelucrării, limitarea scopurilor prelucrării, minimizarea datelor, acuratețea, limitarea perioadei de stocare și integritatea și confidențialitatea datelor cu caracter personal.

ADR impreuna cu USC trebuie să identifice acțiunile relevante de prelucrare a datelor cu caracter personal care trebuie jurnalizate, cum ar fi accesul, modificarea, ștergerea sau transmiterea datelor.

Se vor dezvolta și implementa soluții tehnice care să asigure atât prelucrarea datelor într-un mod sigur și eficient, cât și nerepudierea acțiunilor realizate în sistemele și aplicațiile cloud.

Jurnalizarea accesului la datele cetățeanului se referă la procesul de a crea și a stoca o înregistrare criptata a datelor de identificare a solicitantului, precum și a datelor accesate (citite, scrise, modificate) pentru a fi ulterior procesată și accesată în platforma de notificare.

Utilizatorii asigură generarea, identificarea și înregistrarea jurnalului astfel încât evenimentele să fie transmise și stocate în platforma de jurnalizare a evenimentelor.

Soluția trebuie să asigure toate demersurile pentru prevenirea, modificarea, și distrugerea, fără drept, a înregistrărilor din jurnal, respectiv pentru protejarea

autenticității și a continuității procesului de înregistrare al evenimentelor, cu excepțiile stabilite doar prin cadrul legislativ.

Sistemul de jurnalizare și notificare este compus din:

- nomenclatorul utilizatorilor (administratorii datelor - USC)
- nomenclatorul tipurilor de date cu caracter personal
- serviciul de generare și transmitere a evenimentelor care conțin date cu caracter personal asigurat de utilizatorii datelor
- serviciul de colectare/centralizare a evenimentelor, asigurat de furnizorul de servicii cloud, care preia de la administratorii datelor evenimentele generate de operațiunile de prelucrare a datelor cu caracter personal
- serviciul de notificare a evenimentelor asigurat de furnizorul de servicii cloud. Acest serviciu de notificare va include notificări de tip e-mail și va fi pregătit pentru notificări de tip push pe aplicații mobile care vor fi dezvoltate de statul roman.

ADR împreună cu furnizorii și consumatorii de date actualizează, de câte ori este nevoie, tipurile de date ce se vor jurnaliza și notifica.

1) **Nomenclatorul utilizatorilor**

Soluția trebuie sa conțină un nomenclator al utilizatorilor care folosesc servicii din platforma cloud privat guvernamental și care prelucrează date cu caracter personal conform Regulamentului (UE) nr. 679/2016.

Nomenclatorul trebuie să conțină date precum, fără a se limita la :

- numele autorității sau a instituției publice;
- identificatorul entității ce are dreptul sa acceseze informații conform legislației în vigoare;
- aplicația care conține datele cu caracter personal;
- status: activ, inactiv;
- informații de timp pentru fiecare intervenție pe datele din nomenclator.

2) **Nomenclatorul tipurilor de date cu caracter personal**

Datele cu caracter personal cuprinse în Regulamentul (UE) nr. 679/2016 trebuie să fie stabilite și încadrate în nomenclatorul tipurilor de date. Utilizatorul poate genera și alte valori în nomenclator dacă consideră că prelucrează alte date cu caracter personal diferite de cele din Regulamentul (UE) nr. 679/2016.

Nomenclatorul trebuie să cuprindă informații precum, fără a se limita la:

- denumire informație, data cu caracter personal accesată;
- furnizorul informației;
- cod numeric informație, identificator unic;
- acțiune CRUD: creare, citire, actualizare, ștergere;
- status: activ, inactiv;

- informații de timp pentru fiecare intervenție pe datele din nomenclator.

3) Serviciul de generare și inregistrare a evenimentelor

Deoarece datele cu caracter personal sunt prelucrate de către utilizator, aceștia vor înregistra orice acțiune (eveniment) asupra acestor date astfel încât oricând se va cere o informație având ca referință date din sistemul de jurnalizare, această informație logată de către autoritatea și/sau instituția publică (utilizator) să poată fi pusă la dispoziția cetățeanului căreia i-au fost accesate datele personale la cererea acestuia. Aceste informații sunt puse la dispoziția cetățeanului prin platforma unica de notificare din cloudul privat guvernamental.

Serviciul de generare și înregistrare a evenimentelor trebuie să aibă cel puțin următoarele funcționalități:

- să fie compatibilă cu aplicația care gestionează date cu caracter personal;
- să capteze toate acțiunile asupra datelor cetățenilor, cu precădere cele care conțin date cu caracter personal stabilite în nomenclatorul tipurilor de date;
- evenimentele salvate trebuie să conțină metadate, ce vor fi stocate criptat, fără a se limita la, precum:
    - identificator unic pentru utilizatorul definit în nomenclatorul utilizatorilor;
    - CNP sau alta informație care sa identifice unic cetățeanul(NIF de exemplu);
    - identificator unic al informației accesate, din nomenclator;
    - aplicația, sistemul care a generat evenimentul;
    - acțiune;
    - timestamp.
- să capteze toate cererile din alte sisteme/aplicații informatice prin interfețele de tip API , care conțin date cu caracter personal stabilite în nomenclatorul tipurilor de date
- să asigure, confidențialitatea, integritatea evenimentelor și disponibilitatea prin implementarea unei soluții de tipul message broker sau o tehnologie asemănătoare în vederea transmiterii evenimentelor către un serviciu de colectare intern prin interfața de conectare

În momentul în care un utilizator accesează date cu caracter personal pentru un cetățean din alt sistem informatic, sistemul de jurnalizare va înregistra un eveniment, exemplu în figura 1.

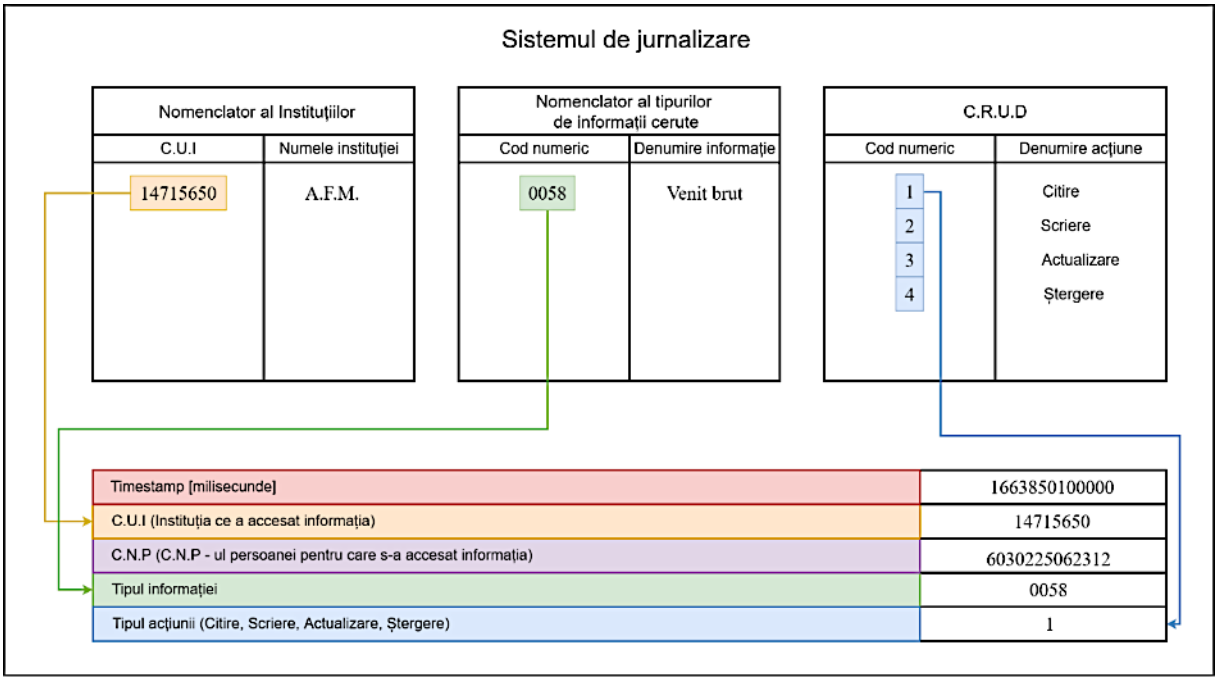


Figura 1 Eveniment jurnalizat

4) Serviciu de colectare/centralizare a evenimentelor

Serviciul este conceput pentru a oferi suport complet și necondiționat în colectarea solicitărilor din sistemele integrate și conectate.

Funcționalitățile sale trebuie sa cuprindă, dar fără a se limita:

- Colectarea/centralizarea evenimentelor din aplicațiile integrate;
- Asigurarea confidențialității, integrității și disponibilității datelor colectate;
- Capacitatea de interceptare a tuturor cererilor, indiferent de tipul informațiilor transmise;
- Protecția jurnalului împotriva modificării sau ștergerii datelor și a succesiunii lor cronologice;
- Posibilitatea de identificare a evenimentelor după data, persoana pentru care s-a accesat informația și codul de identificare al sistemului sursă;
- O interfață/dashboard user-friendly pentru monitorizare și administrare a sistemului de colectare/jurnalizare a evenimentelor;
- Sistem de jurnalizare internă pentru evenimentele platformei centralizate;
- Managementul accesului utilizatorilor, inclusiv definirea permisiunilor, rolurilor și nomenclatoarelor;
- Instrumente pentru vizualizare, raportare, căutare și descărcare, adecvate auditării;
- Nivel înalt de securitate și confidențialitate a datelor și platformei;
- Sistem de alerte pentru evenimente importante;
- Module pentru raportarea detaliată a evenimentelor.

Pentru stocarea datelor, se va folosi o bază de date multimodel, utilă atât pentru sistemul de notificare, cât și pentru cel de jurnalizare. Nomenclatoarele suport vor fi criptate, beneficiind de protecția oferită de tehnologia bazei de date. Logurile vor fi, de asemenea, securizate și criptate at the rest si in tranzit.

5) Serviciu de notificare a evenimentelor

Interfața de Notificări poate fi accesată de orice cetățean care este deja identificat prin sistemul de identificare pus la dispoziție de statul roman.

Serviciul de notificare a evenimentelor asigurat de furnizorul de servicii cloud. Interfața aplicației de Notificări este împărțită în mai multe zone de informații:

- Notificările vor conține date precum, fără a se limita la,:
    - Dată eveniment
    - Instituția care a generat evenimentul
    - Tipul de informație accesată
    - Acțiunea pentru informația accesată

Serviciu de notificare va cuprinde următoarele funcționalități, fără a se limita la:

Autentificare și Autorizare

- Un sistem de autentificare sigur pentru ca utilizatorii să se poată loga în aplicație - ROeID.
- Autorizarea utilizatorilor astfel încât aceștia să aibă acces doar la propriile lor date.
- Aplicația trebuie să permită utilizatorului autentificat să adauge la contul său unul sau mai mulți utilizatori suplimentari, care îndeplinesc criteriile de validare stabilite. Utilizatorul principal va avea drepturi de administrare asupra acestor utilizatori suplimentari, incluzând crearea, consultarea și revocarea accesului acestora.

Notificări

- Funcționalitate pentru ca utilizatorii să poată seta preferințele de notificare. Ei pot decide ce tipuri de notificări doresc să primească legate de accesul la datele lor cu caracter personal.

Interfață Prietenoasă

- O interfață simplă și ușor de folosit pentru ca cetățenii să poată configura preferințele lor de notificare și să vizualizeze informațiile legate de acces la date.

Managementul Datelor Personale

- Un sistem eficient de gestionare a datelor personale ale utilizatorilor, astfel încât aceștia să poată actualiza informațiile lor sau să le revizuiască în orice moment.

Notificări în Timp Real

- Capacitatea de a trimite notificări în timp real atunci când se efectuează accesuri la datele personale ale utilizatorilor conform preferințelor acestora.

Filtre și Preferințe

- O secțiune în aplicație care permite utilizatorilor să configureze filtre și preferințe specifice pentru notificările lor. Acestea includ setarea de filtre pentru tipul de acces (citire, actualizare, ștergere), perioada de timp, tipul de date accesate etc.
- Utilizatorii pot seta filtre specifice pentru tipurile de acces la date cu caracter personal:
    - Tipul de acțiune (citire, actualizare, ștergere).
    - Tipurile de date accesate (informații medicale, date financiare, date de identificare, etc.).
    - Intervalul de timp (notificări în timp real sau sumare zilnice/săptămânale).
- Aplicația conține canale de notificare prin care utilizatorii pot alege prin ce canale doresc să primească notificări, cum ar fi e-mail, notificări pe aplicație sau alte metode de comunicare preferate.
- Aplicația include funcționalitatea de configurare a detaliilor de contact, care constă într-o funcționalitate ce permite utilizatorilor să actualizeze și să gestioneze detaliile lor de contact electronic, astfel încât notificările să fie trimise la adresele corecte.
- Utilizatorii au opțiunea de a stabili care tipuri de acces la date doresc să fie notificați în mod prioritar sau pentru care doresc să primească o notificare mai detaliată.
- Aplicația permite utilizatorilor să solicite din platforma de notificare oprirea temporară sau anularea notificărilor pentru perioade specificate sau pentru tipurile de acces care nu sunt relevante.

Jurnalizare și Raportare

- Funcționalitatea de jurnalizare înregistrează toate evenimentele de acces la date și notificările generate.
- Utilizatorii pot genera rapoarte sau istoricuri ale accesului la date pentru a verifica cine, când și cum a accesat datele lor.
- Aplicația permite utilizatorilor să:
    - genereze rapoarte personalizate care prezintă istoricul accesului la datele lor. Aceste rapoarte pot include detalii despre cine a accesat datele, când s-a întâmplat acest lucru, tipul de acțiune efectuat și alte informații relevante.
    - vizualizeze rapoartele generate direct în aplicație, pentru a avea o imagine completă și actualizată asupra accesului la datele lor.
    - seteze diferite alerte pentru evenimente semnificative, cum ar fi accesări neautorizate sau modificări majore ale datelor lor cu caracter personal.
    - să aibă opțiunea de a exporta rapoartele în formate uzuale, precum PDF sau CSV, pentru a le stoca sau a le trimite altor părți interesate.

Ștergere Notificări

- utilizatorii pot șterge notificările individuale direct din lista de notificări. Fiecare notificare are un buton sau o opțiune pentru ștergere.

- aplicația va conține o funcționalitate de ștergere multiplă permite utilizatorilor să selecteze mai multe notificări și să le șteargă într-o singură acțiune. Aceasta este utilă atunci când utilizatorii doresc să șteargă mai multe notificări în același timp.
- utilizatorii pot aplica filtre pentru a afișa doar anumite categorii de notificări, apoi pot șterge notificările în funcție de aceste filtre. De exemplu, pot filtra notificările pe baza tipului de acces sau perioadei de timp și apoi le pot șterge pe baza acestor criterii.
- utilizatorii pot șterge notificările pentru anumite tipuri de evenimente sau accesuri la date. Aceasta înseamnă că pot alege să nu mai primească notificări pentru anumite acțiuni sau categorii de date.
- aplicația va conține o funcționalitate de gestionare a preferințelor include opțiunea de a dezactiva notificările pentru anumite tipuri de acces sau pentru anumite date cu caracter personal. Astfel, utilizatorii pot personaliza ce informații doresc să primească sau sa se șteargă automat.
- aplicația va solicita o confirmare de la utilizatori pentru a evita ștergerile accidentale.

6) Reținerea evenimentelor din jurnalizare

Platforma de jurnalizare trebuie să asigure disponibilitatea și confidențialitatea jurnalelor pentru cel puțin o perioada de 36 luni.Volumul de stocare trebuie să fie suficient și să aibă un mecanism de alertă dacă spațiul ocupat depășește 75% din capacitatea totală.

3.3.2. Arhitectura funcțională a sistemului

Pentru asigurarea obiectivelor în cadrul sistemului vor fi incluse mai multe componente si submodule împărțite pe următoarele categorii:

- *Nivel de prezentare* – site web de prezentare și portalul pentru accesul la serviciile administrative;
- *Nivel de aplicații* – componentele necesare funcționării platformei;
- *Nivelul de date* – componentele de stocare si prelucrare a datelor gestionate în cadrul platformei;
- *Nivel de suport* – componentele de administrare ale sistemului;
- *Securitate* – componentele de securizare a datelor la nivelul sistemului și la nivelul datelor.

Principalele componente funcționale, de securitate și de suport ale platformei sunt:

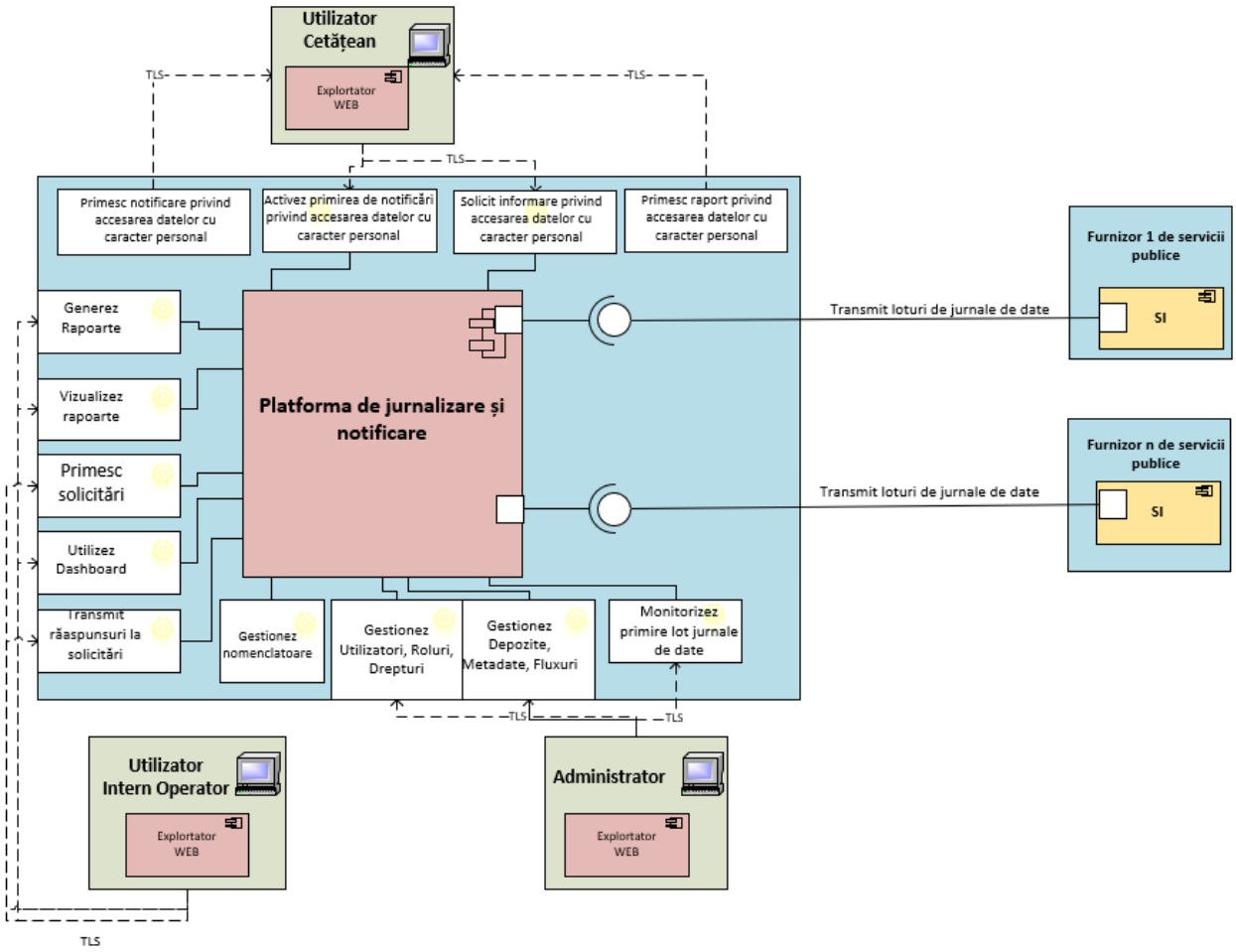
- Componenta de **portal** prin intermediul căreia se expun informațiile și procesele administrative necesare;
- Sistem de **gestiune a bazelor de date** în cadrul căruia se vor stoca toate instanțele bazelor de date aferente modulelor funcționale și portalului;
- O componenta de **analiză și raportare**;
- Componenta de **interoperabilitate** ce va permite schimbul de informații intre diferite sisteme existente bazata pe tehnologie de tip API management;

- O soluție de **securizare a accesului privilegiat** care are rolul de a proteja, gestiona și monitoriza accesul privilegiat la resursele sistemului.

PJN se va implementa în cadrul cloud-ului privat guvernamental care este bazat pe tehnologie Azure stack hub și care va pune la dispoziție infrastructura de mașini virtuale sau containerele Docker necesare implementării și soluția de disaster recovery.

Soluția trebuie să se bazeze pe licențe perpetue/subscripții de tip COTS pentru toate produsele software incluse în soluție sau sub formă de subscripție valabilă pentru toate funcționalitățile pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție.

Furnizorul va pune la dispoziție și va folosi pentru toate componentele sistemului informatic sisteme de operare recomandate de producătorii produselor software ofertate.



Platforma de jurnalizare și notificare (PJN) va asigura:

- autentificarea cetățenilor prin platforma RoeID;

- preluarea electronică a solicitărilor cetățenilor privind accesarea datelor cu caracter personal din sistemele informatice ale furnizorilor de servicii publice;
- transmiterea răspunsurilor la solicitările cetățenilor privind accesarea datelor cu caracter personal din sistemele informatice ale furnizorilor de servicii publice;
- posibilitatea cetățenilor autentificați de a activa primirea automată a notificărilor privind accesarea datelor cu caracter personal din sistemele informatice ale furnizorilor de servicii publice;
- transmiterea automată a notificărilor către cetățeni (pentru cei care au activat această opțiune) privind accesarea datelor cu caracter personal din sistemele informatice ale furnizorilor de servicii publice;

PJN va fi compusă din două componente principale: Componenta Portal Web și Componenta de Jurnalizare.

Componenta Portal web va asigura interacțiunea cu cetățenii, funcționând în regim de proxy și va aplica regulile de securitate ce se impun la nivel de sursă a conexiunilor. De asemenea conexiunile cu serverul proxy vor fi executate doar prin protocol securizat HTTPS (SSL).

Componenta de jurnalizare va asigura ingestia, stocarea și procesarea jurnalelor de date, transmise în loturi (batch) de către sistemele informatice ale furnizorilor de servicii publice, în scopul generării minim a următoarelor rapoarte:

- Vizualizare listă cetățeni care au accesat serviciile publice ale unui furnizor de servicii publice pe o perioadă de timp;
- Vizualizează listă funcționari care au accesat datele cu caracter personal ale unui cetățean stocate într-un sistem informatic al unui furnizor de servicii publice pe o perioadă de timp;
- Vizualizează listă funcționari care au accesat datele cu caracter personal ale unui cetățean stocate în toate sistemele informatic ale furnizorilor de servicii publice pe o perioadă de timp;
- Vizualizează listă notificări transmise unui cetățean privind accesarea datelor sale cu caracter personal din sistemele informatice ale furnizorilor de servicii publice

Portalul web se va integra prin servicii web de tip RestAPI cu Componenta de Jurnalizare.

Pe baza configurării unor alerte specifice, Componenta de jurnalizare (prin intermediul integrării cu Portalul web) va putea transmite automat informații privind accesarea datelor cu caracter personal pentru cetățenii care au activat această opțiune pe măsură ce se primesc jurnale de date relevante de la furnizorii de servicii publice.

Notificările vor fi transmise în contul cetățeanului din Portal de fiecare dată ce sunt accesate datele sale caracter personal stocate în sistemele informatice ale furnizorilor de servicii publice.

La definirea arhitecturii soluției se va lua în considerare necesitatea configurării următoarelor medii:

a. Mediul de producție: asigură funcționarea în producție a soluției informatice și reprezintă mediul care va fi utilizat efectiv de întreg personalul;

b. Mediul de preproducție
    - copie a mediului de producție la o scară cât mai apropiată
    - folosit pentru validarea modificărilor, integrărilor înaintea promovării acestora în producție
    - folosit pentru testarea de performanță a sistemului înainte de a promova modifcările în producție
    - validarea integrării cu diverse sisteme informatice ale furnizorilor de servicii publice;
    -
c. Mediul de testare – dezvoltare, va fi utilizat pentru:
    - Validarea funcțională inițială a dezvoltărilor, testarea automată și manuală, precum și identificarea defectelordezvoltarea de funcționalități noi;
d. Mediul de Disaster Recovery – asigurat de cloudul guvernamental

Componenta de jurnalizare a Platformei de jurnalizare și notificare va fi implementată pe baza unei arhitecturi orientate pe microservicii, în care componentele individuale sunt proiectate, dezvoltate și gestionate independent, comunicând prin API-uri bine definite. Fiecare microserviciu va fi containerizat folosind tehnologii precum Docker, iar orchestrarea containerelor va fi realizată cu Kubernetes pentru a asigura scalabilitate, reziliență și gestionare eficientă a resurselor.

Componenta de jurnalizare va implementa un model de multitenancy, permițând gestionarea simultană a mai multor tenanți (furnizori de servicii publice) într-un mod izolat și securizat, cu separarea logică a datelor, configurațiilor și fluxurilor de lucru specifice fiecărui tenant, utilizând baze de date dedicate sau scheme separate per tenant.

Platforma de jurnalizare și notificare va fi instalată în CPG, respectând cerințele de securitate, control și conformitate specifice.

Componente software

1) **Componenta de portal**

PJN va asigura preluarea electronică a solicitărilor cetățenilor și transmiterea notificărilor către aceștia privind accesarea datelor cu caracter personal din sistemele informatice ale furnizorilor de servicii publice, prin intermediul componentei Portal web.

Portalul web va fi conceput pentru a fi responsive, accesibil atât de pe computere personale, cât și de pe dispozitive mobile inteligente, adaptându-se optim la diferite dimensiuni de ecran și tipuri de dispozitive. Browser-ele web prin care se va realiza accesarea vor fi Chrome, Edge, Firefox, Safari compatibile cu standardele HTML5, CSS și JavaScript.

Solicitările cetățenilor se vor elabora în Portal prin formularele web care vor include pentru unele câmpuri controale de culegere a informației, după caz de tip text simplu, text multilinie, lista de selecție valori dintr-un nomenclator sau bifă (checkbox).

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

În procesul de completare a formularelor web, sistemul va inițializa formularul (sau câmpuri ale acestuia) cu unele dintre informațiile structurate salvate în cadrul profilului utilizatorului.

Utilizatorii autentificați vor putea accesa și vizualiza în mod organizat istoricul solicitărilor/notificărilor trimise către PJN și stadiul procesării acestora.

La finalizarea procesului aferent depunerii solicitării, Portalul 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 toate 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 şi paragrafe formatate de text predefinit.

Ulterior transmiterii unei solicitări, utilizatorul este notificat automat de către Portal prin email despre stadiul procesării şi poate vizualiza online stadiul acesteia, utilizând un link inclus în mesajul email primit.

Portalul va asigura preluarea solicitărilor de informații privind accesarea datelor cu caracter personal și direcționarea automată către utilizatorii interni autorizați.

Se va implementa un set de reguli clare și auditabile privind identificarea persoanelor fizice care solicită serviciile PJN, astfel:

a. Depunerea solicitărilor de către persoanele fizice nu se poate realiza decât după autentificarea acestora în contul propriu, creat și activat în Portal;
b. Crearea și activarea contului de către persoana fizică se va realiza în mod automat prin utilizarea ROeID din cadrul Platformei Software Centralizate pentru Identificare Digitală (PSCID) implementată de către Autoritatea pentru Digitalizarea României (https://www.adr.gov.ro/proiecte-in-implementare/platforma-software-centralizata-pentru-identificare-digitala-pscid/)
c. Autentificarea persoanei fizice în contul activat se realizează, de fiecare dată, prin utilizarea mecanismului de autentificare delegată, pus la dispoziție de către ROeID implementat de către Autoritatea pentru Digitalizarea României

Documentele de răspuns pentru solicitările primite în formă electronică vor fi transmise către solicitant în contul acestuia din Portal.

Portalul web va permite cetățenilor autentificați să opteze pentru activarea notificărilor privind accesarea datelor cu caracter personal stocate în sistemele informatice ale furnizorilor de servicii publice. În acest sens, Portalul web se va integra prin servicii web de tip RestAPI cu Componenta de Jurnalizare. Notificările vor fi transmise în contul cetățeanului din Portal de fiecare dată ce sunt accesate datele sale caracter personal stocate în sistemele informatice ale furnizorilor de servicii publice.

Paginile web ale Portalului trebuie să îndeplinească cerințele de compatibilitate şi accesibilitate pentru persoane cu dizabilități, în concordanță cu specificațiile W3C (World Wide Web Consortium, 5 Mai 1999) şi recomandările WAI (Web Accessibility Initiative), acceptate la nivel mondial drept standarde internaționale în domeniul accesibilității web: Web Content Accessibility Guidelines (WCAG) 2.0 – minimum nivel AA.

Interfața Portalului web va fi proiectată astfel încât să respecte prevederile OUG 112/2018 privind transpunerea Directivei 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.

Componenta Portal web va fi bazată pe o soluție software matură, introdusă deja în circuitul comercial. Maturitatea soluției presupune îndeplinirea tuturor următoarelor condiții:

a. existența referințelor publice pe website-ul producătorului din care să rezulte trecerea prin mai multe iterații/versiuni prin care s-au îmbunătățit funcționalitățile și performanța în cel puțin ultimii 3 ani;
b. existența unui roadmap publicat de producător privind dezvoltarea produsului;
c. recomandări din partea a cel puțin 5 beneficiari finali din care să rezulte furnizarea produsului;
d. existența unui portal ce include documentație tehnică de produs și exemple de bună practică privind implementarea;

Produsul software trebuie să pună la dispoziție un mediu unificat integrat de dezvoltare (Integrated Development Environment), asigurând o experiență fără întreruperi pentru dezvoltare și administrare. Acest mediu trebuie să permită colaborarea în timp real și în cadrul său să ofere o interfață de tip drag-and-drop pentru dezvoltare și administrare, dispunând în acest sens de următoarele categorii de funcționalități:

a. Managementul rolurilor
b. Managementul permisiunilor
c. Managementul utilizatorilor
d. Interfațare API și administrare
e. Automatizare
f. Fluxuri de lucru
g. Funcții predefinite
h. Managementul entităților
i. Managementul meniurilor
j. Managementul paginilor
k. Managementul formularelor

l. Managementul listelor

Funcționalitățile de managementul rolurilor trebuie să includă:

a. Adăugarea, editarea sau ștergerea rolurilor;
b. Configurarea rolurilor pentru restricționarea accesului la nivel de pagină, componentă, acțiune, flux de lucru sau entitate;

Funcționalitățile de managementul permisiunilor trebuie să asigure definirea schemei de permisiuni astfel:

a. Configurarea permisiunilor la nivel de pagină (de acces sau de editare) în funcție de rol;
b. Configurarea permisiunilor la nivel de entitate, determinând astfel operațiunile disponibile utilizatorului prin interfață, cum ar fi Creare, Citire, Actualizare sau Ștergere;
c. Configurarea permisiunilor la nivel de modul pentru a restricționa accesul sau pentru a acorda opțiuni de editare rolurilor;
d. Configurarea permisiunilor la nivel de acțiuni și butoane, astfel încât acestea să fie disponibile doar pentru anumite roluri;
e. Configurarea permisiunilor la nivel de căutare prin stabilirea de reguli care să restricționeze afișarea rezultatelor în funcție de roluri;
f. Configurarea permisiunilor de utilizare a resurselor API.

Funcționalitățile de managementul utilizatorilor trebuie să includă:

a. Crearea utilizatorilor și asocierea acestora la cel puțin un rol;
b. Modificarea utilizatorilor, acordarea sau revocarea rolurilor;
c. Ștergerea utilizatorilor.

Funcționalitățile de interfațare API trebuie să includă:

a. Crearea de interfețe REST API;
b. Crearea metodelor API (GET, POST, PUT, DELETE) pentru execuția logicii (acțiunilor) la nivel de server sau pentru preluarea datelor;
c. Securizarea API-urilor prin chei API și token web JSON;
d. Implementarea mecanismelor de partajare a resurselor restricționate ale unei pagini web dintr-un alt domeniu aplicativ (CORS - Cross-Origin Resource Sharing)..
e. Funcționalitățile de automatizare trebuie să includă:
f. Posibilitatea programării execuției automate de joburi/acțiuni, periodic la anumite momente/intervale (declanșatoare de timp, declanșatoare de interval) sau când are loc un eveniment (la lansarea/închiderea aplicației, la începutul/sfârșitul fiecărei solicitări);
g. Programarea execuției automate a următoarelor job-uri/acțiuni:
    i. rulare interogări SQL;
    ii. rulare executabile;
    iii. rulare scripturi;
    iv. postarea de date;
    v. transmiterea de e-mailuri;

Funcționalitățile asociate fluxurilor de lucru trebuie să includă:

a. Posibilitatea definirii unei liste de acțiuni, ce trebuie efectuate într-o anumită succesiune, care poate include o logică condiționată;
b. Posibilitatea definirii fluxurilor de lucru prin utilizarea a cel puțin următoarelor elemente BPMN: eveniment de start, eveniment de stop, activități, poartă de decizie (XOR);
c. Posibilitatea testării fluxurilor de lucru prin rularea acestora și indicarea erorilor prin mesaje de eroare;
d. Posibilitatea clonării fluxurilor de lucru cu logică similară și editarea acestora în scopul creării unui flux nou;
e. Posibilitatea adăugării activităților în fluxul de lucru prin intermediul funcțiilor predefinite (secvențe de cod) cu variabile/parametrii de intrare și de ieșire.

Soluția va dispune de următoarele funcții predefinite:

- Adăugarea unei casete de verificare (checkbox) prin care să se afișeze/ascundă un câmp dinamic în urma verificării condiției adevărat/fals;
- Adăugarea unui selector de dată și oră;
- Adăugarea unui câmp derulant (dropdown);
- Adăugarea unui câmp de tip text;
- Adăugarea de elemente de tip opțiuni multiple (multiple choice) cu casete de verificare (checkboxes);
- Adăugarea de elemente de tip opțiuni multiple (multiple choice) cu câmpuri derulante (dropdown);
- Adăugarea de elemente de tip opțiuni multiple (multiple choice) cu butoane de opțiune (radio button);
- Adăugarea unei casete de text pentru introducerea unui număr;
- Adăugarea unui element de tip glisor (slider);
- Adăugarea de text static;
- Încărcarea unui câmp dinamic dintr-un JSON;
- Transmitere email către unul sau mai mulți recipienți;
- Transmitere email cu fișier atașat
- Crearea unei entități noi;
- Crearea unui obiect JSON;
- Crearea unei pagini noi;
- Crearea unui rol;
- Crearea unui thumbnail;
- Adăugarea, ștergerea, vizualizarea sursei de date;
- Afișare mesaje (de eroare, de confirmare, etc.);
- Descărcare fișier;
- Executare cod Javascript;
- Adăugare modul la o pagină;
- Criptare/decriptare date AES și RSA;
- Modificarea permisiunilor pentru foldere;
- Autorizarea utilizatorilor;
- Închidere formulare pop-up;
- Închidere ferestre pop-up;

- Copiere fișier într-un alt folder;
- Ștergere entitate, fișier, folder, modul, pagină, rol, utilizator;
- Executare listă de acțiuni;
- Generare PDF din șablon HTML;
- Generare credențiale;
- Interogare date în sursa de date;
- Creare folder nou;
- Încărcare conținut dintr-un modul HTML;
- Încărcare pagină în contextul de execuție;
- Creare arhivă de fișiere specificate;
- Dezarhivare fișiere dintr-o arhivă;
- Parsare valori multiple din aceeași sursă;
- Parsare JSON pentru extragerea valorilor parametrilor;
- Parsare XML pentru extragerea valorilor parametrilor;
- Redirecționarea utilizatorului către o altă pagină din portal sau către un URL, după transmiterea unui formular;
- Rulare SQL Query
- Actualizare modul, pagina, rol, profil utilizator, nume utilizator;
- Validare utilizator/parolă;
- Înregistrare utilizator;

Funcționalitățile de managementul entităților trebuie să includă:

a. Adăugarea, editarea, ștergerea și vizualizarea entităților;
b. La crearea unei entități trebuie:
    i. să se genereze automat tabelele în baza de date, cu chei index pe baza relațiilor definite cu alte entități;
    ii. să se genereze o pagină ce va apare în meniul principal al aplicației, existând totuși posibilitatea dezactivării afișării paginii entității în meniul principal (fiind accesată de exemplu la completarea unui formular); Pagina trebuie să poată fi definită ca o pagină de nivel superior sau ca un copil al unei pagini existente;
    iii. să se genereze un formular pentru introducerea datelor cu câmpuri bazate pe proprietățile definite la crearea entității;
    iv. să se poată genera o listă de valori pentru a afișa înregistrările asociate entității;
    v. să se poată defini o sursă de date pentru entitate;
    vi. să se genereze automat butoane în interfață prin care să se ofere posibilitatea de a crea, edita, șterge și vizualiza înregistrările;
    vii. să se poată defini funcții predefinite care să fie utilizate pentru operațiuni de creare, ștergere, actualizare parțială, actualizare și citire;
    viii. să se poată defini/utiliza API-uri pentru crearea, preluarea, actualizarea și ștergerea înregistrărilor;
    ix. să se poată genera un tablou de bord vizual în care să se definească KPI-uri pe baza datelor din entitate;
c. Reprezentarea vizuală a relației dintre entități;

d. Posibilitatea definirii relațiilor dintre entități;
e. Configurarea permisiunilor pentru restricționarea accesului la nivel de entitate: vizualizare, adăugare, editare, ștergere;

Funcționalitățile de managementul meniurilor trebuie să includă:

a. Posibilitate grupării paginilor pentru crearea de sub-meniuri;
b. Posibilitatea organizării meniului prin funcții de tip drag-and-drop a paginilor definite;
c. Posibilitatea organizării meniului pentru diferite profiluri de utilizator;

Funcționalitățile de managementul paginilor trebuie să includă:

a. Posibilitatea restricționării accesului la nivel de pagină în funcție de rol: vizualizare, adăugare pagină, editare proprietăți pagină, mutare pagină și ștergere pagină ;
b. Posibilitatea definirii ca pagină copil a unei pagini părinte;
c. Posibilitate definirii de cuvinte cheie pentru o pagină;
d. Posibilitatea publicării programate (sau scoaterii din publicare) la o anumită dată și oră;
e. Afișarea paginii în meniul principal, existând totuși posibilitatea dezactivării afișării (fiind accesată de exemplu la completarea unui formular).
f. Posibilitatea așezării conținutului, în fiecare pagină, prin componente de tip HTML (text), formulare, liste și tab-uri;

Funcționalitățile de managementul formularelor trebuie să includă:

a. Posibilitatea definirii unui formular pe oricare pagină în vederea colectării de date;
b. Definirea de formulare cu următoarele tipuri de câmpuri:
c. Casetă de text – permite introducerea de conținut de tip text pe o singură linie sau pe mai multe, permițând condiționarea numărului de caractere sau introducerea unei validări personalizate;
d. Număr întreg;
e. Email – permite introducerea de conținut de tip text. Validează conținutul pentru a fi o adresa de email validă.
f. Telefon - permite introducerea de conținut de tip text sub forma de număr de telefon în formatul definit de standardul internațional E.164. Permite realizarea automată a preselecției prefixului în funcție de țară;
g. Casetă de text cu editor WYSIWYG - permite introducerea de conținut de tip text și formatarea acestuia prin următoarele opțiuni:
    i. Alegerea stilului caracterelor: bold, italic, subliniat, superscript, subscript;
    ii. Alegerea dimensiunii caracterelor;
    iii. Alegerea de liste numerotate automat sau cu bullet-uri;
    iv. Alegerea spațierii între rânduri;
    v. Alegerea alinierii textului la stânga, la centru, la dreapta;
h. Text static – permite afișarea de informații ce nu pot modificate de către utilizator, cum ar fi mesaje de informare sau mesaje de ajutor. Permite formatarea/stilizarea textului;

i. Dropdown - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică;
j. Dropdown cu autocompletare - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică, permițând filtrarea listei de opțiuni pe măsură de textul este introdus;
k. Dropdown cu casete de verificare - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică, prin bifarea acesteia;
l. Alegere multiplă cu casete de verificare - permite alegerea uneia sau mai multor opțiuni dintr-o listă predefinită sau dinamică.
m. Casete cu butoane de opțiune (radio button) - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică de tip radio button;
n. Caseta de dată și oră – permite alegerea unei date și ore sau a unui interval de date sau date și ore. Formatul afișat trebuie să se poată configura, putându-se dezactiva date din viitor sau din trecut, precum și personalizarea în funcție de criterii dinamice;
o. Caseta de Încărcare a unui singur fișier - Permite încărcarea unui fișier, cu o extensie ce se validează printr-o listă de extensii valide (sigure), configurabile. Permite limitarea dimensiunii unui document care poate fi încărcat. Asigură gestionarea fișierelor duplicate prin suprascriere sau redenumire;
p. Caseta de Încărcare fișiere multiple - Permite încărcarea mai multor fișiere, cu extensii ce se validează printr-o listă de extensii valide (sigure), configurabile. Permite limitarea dimensiunii unui document care poate fi încărcat. Asigură gestionarea fișierelor duplicate prin suprascriere sau redenumire;
q. Parolă/Confirmare parolă - permite introducerea parolelor. Parolele nu sunt vizibile la tastare și sunt criptate.
r. Posibilitatea definirii direcției etichetelor pentru fiecare câmp (sus, stânga, dreapta);
s. Posibilitatea adăugării de instrucțiuni de completare pentru fiecare câmp;
t. Posibilitatea definirii de validatori personalizați pentru orice câmp. Aplicația va dispune de următorii validatori predefiniți:
    i. Număr întreg;
    ii. Număr întreg pozitiv;
    iii. Email;
    iv. Dată;
    v. Obligatoriu;
u. Posibilitatea condiționării validatorilor în funcție de alte câmpuri pentru a putea permite crearea logicii afișării sau validării câmpurilor unui formular;
v. Generarea listei de opțiuni pentru câmpurile cu alegere multiplă de tip dropdown sau cu casete de verificare, trebuie să se poată realiza prin:
    i. Listă statică de formă cheie/valoare;
    ii. Interogări ale bazei de date prin care se aduc datele;
    iii. API ce returnează format JSON;
w. Posibilitatea de a construi formulare dinamice prin utilizarea de expresii de legătură, care pot controla afișarea sau activarea câmpurilor.

Funcționalitățile de managementul listelor trebuie să includă:

i. Posibilitatea definirii afișării listelor de date, sub formă tabelară, din următoarele surse de date: formulare, tabele din baza de date, interogări SQL și solicitări JSON de la un API;
ii. Posibilitatea adăugării de noi surse de date;
iii. Permite definirea pentru fiecare coloană a funcționalităților de filtrare, ordonare, sortare și căutare;

Licențierea Portalului web va asigura un drept de utilizare perpetuu pentru beneficiar și nu va impune limite privind numărul de utilizatori ce-l vor accesa în mod autentificat sau neautentificat.

Produsul va beneficia de suport tehnic pe o perioadă de 36 luni, acoperind dreptul beneficiarului de a face update–uri precum și access direct la site-ul producătorului pentru a deschide direct cazuri de suport cu acesta.

2) Componenta de jurnalizare

Platforma de jurnalizare și notificare (PJN) va include o componentă de jurnalizare ce se va implementa pe baza unei soluții software mature, introduse în circuitul comercial.

Maturitatea soluției presupune îndeplinirea tuturor următoarelor condiții:

a. existența referințelor publice pe website-ul producătorului din care să rezulte trecerea prin mai multe iterații/versiuni prin care s-au îmbunătățit funcționalitățile și performanța în cel puțin ultimii 3 ani;
b. existența unui roadmap publicat de producător privind dezvoltarea produsului;
c. recomandări din partea a cel puțin 5 beneficiari finali din care să rezulte furnizarea produsului;
b. existența unui portal ce include documentație tehnică de produs și exemple de bună practică;

Soluția trebuie să pună la dispoziție un mediu unificat integrat, asigurând o experiență fără întreruperi pentru configurare și administrare, asigurând ingestia, indexarea, stocarea, analizarea și corelarea jurnalelor de date (jurnalelor de date) din sistemele informatice ale furnizorilor de servicii publice (autorități și instituții publice centrale, cu scopul de a audita accesarea datelor cu caracter personal ale cetățenilor.

Soluția va fi instalată în Platforma de Cloud Guvernamental (CPG) și va permite implementarea într-o arhitectură distribuită, prin utilizarea unui model de tip multitenancy. Astfel, pentru fiecare furnizor de servicii publice va fi creat un tenant distinct, asigurând separarea seturilor de date specifice fiecărui furnizor în parte, în scopul garantării protecției și securității acestora.

Soluția trebuie să includă următoarele module funcționale:

- Modul afișare – asigură afișarea în format tabelar a tuturor jurnalelor de date ingerate. Interfața va putea fi configurabilă din punctul de vedere al câmpurilor ce pot fi vizualizate și va permite filtrări avansate precum și ordonări ale jurnalelor de date;

- Modul panouri de bord – asigură vizualizări grafice pentru jurnalele de date ingerate, sub formă de tablouri de bord. Acestea vor putea fi configurabile în funcție de nevoile de business;
- Modul Raportare – va asigura intrinsec rularea și vizualizarea de rapoarte. De asemenea, permite crearea de noi rapoarte, editarea rapoartelor existente, va conține funcții de planificare a rulării și transmiterii rapoartelor și funcții de export a rezultatelor rapoartelor.
- Modul Alertare - include implicit afișarea de alerte. Alertele vor fi definite/editate într-o interfață grafică, intuitivă.
- Managementul incidentelor – permite personalului să desfășoare în mod colaborativ activități de investigare a incidentelor.
- Depozite de date - Soluția va stoca datele cel puțin în două depozite:
    - Online – datele sunt stocate indexat cu accesare rapidă pentru nevoi de raportare
    - Arhiva – datele sunt depozitate pentru păstrare pe termen lung, comprimate
        - Rata compresie – minim 20 la 1
        - Va asigura mecanisme anti-repudiere: criptare și semnare digitală a datelor

Nu se acceptă tehnologii proprietare pentru depozitele de date, accesarea/utilizarea datelor nu trebuie să fie dependente de soluția ofertată.

Soluția nu trebuie să limiteze capacitatea de stocare a jurnalelor de date ingerate.

Depozitul on-line trebuie să poată fi scalat în funcție de nevoi, oricând pe durata de utilizare a soluției, fără a implica niciun cost de licențiere pentru baza de date.

Depozitul de arhivă trebuie să poate fi scalat în funcție de nevoie, oricând pe durata de utilizare a soluției, fără a implica niciun cost de licențiere pentru baza de date.

Soluția trebuie să asigure ingestia jurnalelor de date, transmise în loturi (batch) de către sistemele informatice ale furnizorilor de servicii publice, prin intermediul protocolului TLS, utilizând HTTPS și autentificare cu token.

Soluția trebuie să identifice sistemul informatic de la care au fost transmise jurnalele de date asigurând analiza acestora în funcție de furnizorul de servicii publice /aplicație.

Soluția trebuie să permită configurarea de alerte inclusiv pentru praguri de ingestie jurnale de date/număr de jurnale de date care așteaptă să fie ingestate/procesate de soluție.

Soluția va dispune de funcții de tip self-audit. Astfel, vor fi auditate toate operațiunile efectuate de utilizatorii și de serviciile componente ale soluției.

Soluția trebuie să pună la dispoziția utilizatorului un API de integrare pentru sistemele informatice ale furnizorilor de servicii publice. În acest sens, în cadrul proiectului se va stabili o Structură Standard de Audit (format de jurnale de date) ce va fi utilizată de către furnizorii de servicii publice pentru transmiterea loturilor de jurnale de date.

Soluția trebuie să fie scalabilă astfel încât să ofere posibilitatea de a mări performanța de corelare/procesare/stocare prin adăugarea unor resurse de procesare suplimentare.

Soluția trebuie să asigure o consolă de management de tip web-based care nu necesită instalarea de software adițional și prin care sunt accesate toate funcționalitățile acesteia. Astfel, interfața de operare și administrare a aplicației trebuie să fie de tip WEB, asigurând totodată compatibilitate cu orice browser modern (Chrome, Microsoft Edge, Opera, Firefox etc.)

Soluția trebuie să asigure facilități de indexare a jurnalelor de date,

Soluția trebuie să poată asigura stocarea jurnalelor de date ingestate și în format brut (raw).

Soluția trebuie să asigure un mecanism integrat de compresie a datelor, iar după expirarea perioadei configurate de retenție a jurnalelor de date din depozitul online, stocarea jurnalelor de date 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.

Soluția trebuie să asigure vizualizarea/analiza/interpretarea jurnalelor de date printr-o consolă/interfață unică.

Soluția trebuie să asigure mecanisme de protecție a integrității datelor stocate prin intermediul algoritmilor de tip hash.

Soluția trebuie să asigure exportarea jurnalelor de date ingestate în format CSV, JSON.

Soluția 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

Soluția trebuie să asigure investigarea accesului la datele cu caracter personal ale cetățenilor pornind de la log-ul corelat până la identificarea jurnalelor de date primare ce au generat alerta.

Soluția trebuie să asigure utilizarea expresiilor regulate si operatori logici de tip Boolean (AND, OR, NOT) în aplicația de căutare.

Soluția trebuie să asigure generarea de rapoarte pe baza unor interogări cât și exportul acestora in format CSV, PDF, XLS etc.

Soluția trebuie să asigure salvarea rapoartelor în format PDF.

Soluția trebuie să asigure opțiunea de personalizare a dashboard-urilor.

Soluția trebuie să asigure geolocalizarea adreselor IP identificate în cadrul jurnalelor de date ingestate.

Autentificarea utilizatorilor pentru acces la administrarea soluției trebuie să se poată realiza pe baza de conturi de utilizatori definiți local, integrare cu sisteme terțe precum Microsoft Active Directory, RADIUS sau LDAP.

Soluția trebuie să asigure salvarea configurației din interfața grafică, configurație ce include cel puțin următoarele resurse:

- reguli,
- rapoarte

Soluția trebuie să asigure crearea unor spații de lucru diferite utilizatorilor, în funcție de rolul de business al acestora, precum utilizator intern operator, administrator, etc.

Soluția trebuie să poată să fie integrată cu componenta Portal web via metode specifice de API.

Soluția trebuie să ofere un panou central pentru filtrarea și corelarea în timp real a evenimentelor generate de jurnalele de date.

Soluția trebuie sa ofere suport pentru IPv4 și IPv6 atât pentru administrare, cât și pentru inspectarea protocoalelor de rețea.

Soluția va oferi vizualizări grafice pentru evenimentele ingestate, sub forma de tablouri de bord (dashboards). Acestea vor putea fi configurabile pentru fiecare utilizator, în funcție de nevoile de business. Astfel, se va crea un tablou de bord pentru fiecare furnizor de servicii publice, dar de asemenea se va permite căutarea în toate tablourile relativ la un criteriu sau set de criterii comune.

Soluția va oferi un modul de rapoarte avansat ce asigură:

1. Rapoarte preconfigurate : Soluția se va livra cu cel puțin următoarele rapoarte preconfigurate:
   Vizualizare listă cetățeni care au accesat serviciile publice ale unui furnizor de servicii publice pe o perioadă de timp;
   Vizualizează listă funcționari care au accesat datele cu caracter personal ale unui cetățean stocate într-un sistem informatic al unui furnizor de servicii publice pe o perioadă de timp;
   Vizualizează listă funcționari care au accesat datele cu caracter personal ale unui cetățean stocate în toate sistemele informatic ale furnizorilor de servicii publice pe o perioadă de timp;
   Vizualizează listă notificări transmise unui cetățean privind accesarea datelor sale cu caracter personal din sistemele informatice ale furnizorilor de servicii publice
2. Personalizare și creare: Utilizatorii pot crea noi rapoarte, edita cele existentele și planifica rularea/transmiterea acestora.
3. Funcționalități avansate: soluția trebuie sa ofere opțiuni de exportare a rezultatelor rapoartelor pentru analize ulterioare.

Soluția va furniza un modul de tip UEBA pentru identificarea si alertarea asupra acelor acțiuni care ies dintr-un șablon de comportament considerat normal.

Soluția va avea un modul de tip incident management. Prin intermediul acestui modul, personalul de audit poate desfășura în mod colaborativ activități de investigare a incidentelor privind accesarea datelor cu caracter personal ale cetățenilor.

Nu va exista nicio limitare de licență privind numărul de jurnale de date ingestate, procesate și/sau stocate (capacitatea depozitelor de date online sau arhivă), iar acesta va putea fi scalat, pe parcursul sau după încheierea proiectului, în funcție de nevoile

beneficiarului, fără niciun cost suplimentar de licențiere pentru dimensiunea depozitelor de date. Astfel, soluția se va licenția pentru cel puțin 48 de nuclee de procesare, în mod perpetuu și suport inclus pentru 36 de luni și va fi instalata în CPG.

Sistemele informatice ale furnizorilor de servicii publice sunt sistemele pe care cetățenii le accesează pentru servicii publice electronice. Fiecare dintre aceste servicii necesită autentificarea utilizatorilor și identificarea acestora.

În plus, furnizorii de servicii publice sunt obligați conform prevederilor legale să implementeze controale de audit prin care să răspundă la următoarele întrebări legate de datele cu caracter personal ale cetățenilor ce sunt prelucrate în cadrul propriului sistem:

- Ce activitate a fost efectuată?
- Cine sau ce a efectuat activitatea?
- Pe ce sistem sau resursă a fost efectuată activitatea?
- Din ce locație sau pe ce sistem a fost efectuată activitatea?
- Când a fost efectuată activitatea?
- Cu ce instrument(e) a fost efectuată activitatea?
- Care a fost starea, rezultatul sau consecința activității?

În vederea implementării uniformizate pentru toate sistemele informatice ale furnizorilor de servicii publice ce vor transmite către PJN jurnale de date referitoare la serviciile publice și a datelor cu caracter personal ale cetățenilor sunt necesare următoarele:

- stabilirea unei Structuri Standard de Audit (format de jurnale de date) ce va fi utilizată de către furnizorii de servicii publice pentru transmiterea loturilor de jurnale de date.
- dezvoltarea interfețelor și a conectorilor în cadrul PJN pentru comunicație cu sistemele informatice ale furnizorilor de servicii publice
- elaborarea unui set de specificații de integrare pe baza căruia furnizorii de servicii publice să poată realiza comunicația cu PJN.

Structura standard de audit (SSA) trebuie să răspundă la următoarele întrebări legate de datele cu caracter personal ale cetățenilor:

- Ce activitate a fost efectuată?
- Cine sau ce a efectuat activitatea?
- Pe ce sistem sau resursă a fost efectuată activitatea?
- Din ce locație sau pe ce sistem a fost efectuată activitatea?
- Când a fost efectuată activitatea?
- Cu ce instrument(e) a fost efectuată activitatea?
- Care a fost starea, rezultatul sau consecința activității?

Jurnalele de date din cadrul SSA trebuie create ori de câte ori oricare dintre următoarele activități în legătură cu accesarea serviciilor publice și a datelor cu caracter personal sunt efectuate în cadrul sistemului informatic al unui furnizor de servicii publice:

- Transmiterea de către cetățean a unei solicitări referitoare la un serviciu public;
- Crearea, citirea, actualizarea sau ștergerea datelor cu caracter personal de către cetățean

- Crearea, citirea, actualizarea sau ștergerea datelor cu caracter personal de către funcționar

Soluția propusa va include realizarea unor interfețe de furnizor de servicii publice de tip DEMO al căror scop este a testa funcționarea corecta a transmite către PJN jurnale de date referitoare la serviciile publice și a datelor cu caracter personal ale cetățenilor.

Aceste instanțe DEMO vor trebui să includă mecanismele de autentificare ce vor fi suportate de către PJN în comunicația cu furnizorii de servicii publice bazate pe token.

Pentru asigurarea interconectării și prezentarea modului de funcționare a PJN se va implementa o pagină web dedicată în cadrul Portalului web, care va fi utilizată și pentru accesul la secțiunea DEMO. Tot în această pagină se va publica documentația și specificațiile de interconectare.

În etapa de analiză, modelarea proceselor și a activităților trebuie să se realizeze în conformitate cu standardele de modelare recunoscute (UML sau echivalent).

În cadrul etapei de analiză se va identifica setul de date necesar pentru proiectarea Structurii Standard de Audit (format de jurnale de date) ce va fi utilizată de către furnizorii de servicii publice pentru transmiterea loturilor de jurnale de date

Va rezulta ca livrabil un set de specificații general valabil pentru furnizorii de servicii publice în ceea ce privește setul de date necesar prelucrării jurnalelor de date din sistemele proprii în vederea transmiterii către PJN.

Tot în cadrul acestei etape vor fi identificate soluțiile tehnice și procedurale ce pot fi adoptate.

Se va efectua o analiza a cerințelor tehnice, elaborarea cerințelor și specificațiilor și dezvoltarea componentelor software de tip API și interfețe de comunicații cu sistemele informatice ale furnizorilor de servicii publice.

Livrabilul acestei etape constă într-un un set de specificații de integrare pe baza căruia un furnizor de servicii publice să poată prelucra și transmite jurnalele de date conform SSA pentru a le transmite în PJN.

Procesul de interconectare a sistemelor informatice ale furnizorilor de servicii publice cu PJN se va realiza pe baza specificațiilor de integrare.

În cadrul proiectului pentru demonstrarea fezabilității soluției propuse, furnizorul va asigura interconectarea a cel puțin 3 furnizori de servicii publice cărora le va fi acordată asistența tehnică privind implementarea soluțiilor necesare în sistemele informatice proprii astfel încât să se conecteze și să transmită cu succes loturi de jurnale de audit în PJN.

În acest scop vor fi contactați prioritate furnizorii de servicii publice electronice care au implementat soluții de jurnalizare în propriile sisteme informatice.

Furnizorilor selectați li se va acorda asistență tehnică pentru analiza cerințelor tehnice, elaborarea specificațiilor privind procesarea jurnalelor de date în formatul de SSA și dezvoltarea interfețelor de comunicații pentru interconectarea cu PJN.

După implementarea soluției în cadrul sistemului informatic al furnizorului de servicii publice electronice, se vor realiza testele de interconectare cu PJN.

3) **Componenta de Stocare, Indexare și Raportare**

Pentru această componentă se va utiliza stiva ELK (Elasticsearch, Logstash, Kibana) pusă la dispoziție de Cloud-ul Privat Guvernamental, precum și o platformă de streaming de evenimente(Ex. Kafka, Azure Event Hubs), care va permite rularea în mod asincron a componentei . Platforma de streaming de evenimente va implementa protocolul kafka.

Arhitectura soluției:

- Elasticsearch: Motor de căutare și analiză distribuită pentru indexarea și stocarea datelor
- Logstash: Pipeline de procesare a datelor pentru colectare, transformare și încărcare
- Kibana: Interfață de vizualizare și explorare a datelor, pusă la dispoziția administratorilor platformei
- Platformă de streaming de evenimente: Stocare de scurtă durată.

Rapoarte și Dashboard-uri pentru administratori. Se va utiliza kibana, pusă la dispoziție de CPG:
Vor fi dezvoltate minimum 10 dashboard-uri/vizualizări structurate după cum urmează:

a) Rapoarte simple (5 bucăți) - Complexitate mică
- Dezvoltate pe baza unui singur index/tip de document
- Vizualizări de tip: grafice simple, tabele, metrici agregate
- Exemple: totaluri, medii, numărări pe o singură dimensiune

b) Rapoarte medii (3 bucăți) - Complexitate medie
- Dezvoltate pe baza a 2-3 indici/tipuri de documente
- Utilizează agregări pe multiple niveluri
- Vizualizări combinate: grafice multi-serie, pie charts etc.
- Filtrare pe 2-3 criterii simultane

c) Rapoarte complexe (2 bucăți) - Complexitate mare
- Dezvoltate pe baza a mai mult de 3 indici/tipuri de documente
- Agregări complexe, calcule derivate, transformări de date
- Dashboard-uri interactive cu filtre dinamice
- Multiple criterii de selecție/filtrare (>3)
- Vizualizări avansate: time series, capabilității drilldown etc.

Rapoarte și Dashboard-uri pentru utilizatori finali:
Pentru utilizatorii finali va fi dezvoltată o interfață, independentă de soluția Kibana.
Vor fi dezvoltate minimum 10 dashboard-uri/vizualizări structurate după cum urmează:

a) Rapoarte simple (5 bucăți) - Complexitate mică
- Dezvoltate pe baza unui singur index/tip de document
- Vizualizări de tip: grafice simple, tabele, metrici agregate
- Exemple: totaluri, medii, numărări pe o singură dimensiune

b) Rapoarte medii (3 bucăți) - Complexitate medie
- Dezvoltate pe baza a 2-3 indici/tipuri de documente
- Utilizează agregări pe multiple niveluri
- Vizualizări combinate: grafice multi-serie, pie charts etc.
- Filtrare pe 2-3 criterii simultane

c) Rapoarte complexe (2 bucăți) - Complexitate mare
- Dezvoltate pe baza a mai mult de 3 indici/tipuri de documente

- Agregări complexe, calcule derivate, transformări de date
- Dashboard-uri interactive cu filtre dinamice
- Multiple criterii de selecție/filtrare (>3)
- Vizualizări avansate: time series, capabilități drilldown etc.

Specificații tehnice:
- Rapoartele și dashboard-urile vor fi definite pe parcursul fazei de analiză/colectare a cerințelor
- Vor fi implementate query-uri Elasticsearch optimizate pentru performanță
- Se vor configura refresh rate-uri adecvate pentru fiecare tip de raport

4) Componenta de securizare a accesului privilegiat

Aceasta componenta are rolul de a proteja, gestiona și monitoriza accesul privilegiat la resursele critice ale sistemului. Accesul privilegiat se referă la permisiunile și drepturile speciale care sunt acordate utilizatorilor, conturilor sau aplicațiilor pentru a accesa, administra și controla sisteme, rețele și informații sensibile.

Tipuri de soluții acceptate:
Platforma poate fi:
- Aplicație software disponibilă comercial (COTS) cu licențiere perpetuă sau sub formă de subscripție validă pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție

  Sau

- Soluție open source cu contract de suport tehnic profesional garantat pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție, furnizat de către producătorul soluției sau de un partener autorizat

Cerințe funcționale de bază:
Gestionarea accesului și autorizărilor:
- Soluția trebuie să aibă posibilitatea de a oferi acces pe baza de roluri definite (RBAC - Role-Based Access Control) pentru a evita accesul neautorizat sau al unui utilizator cu rol diferit la serverele critice
- Soluția trebuie să permită integrarea cu un server LDAP extern unde sunt ținuți utilizatorii. Soluția LDAP va fi un Active Directory care va fi pus la dispoziție ca licență de Beneficiar. Furnizorul va trebui să îl instaleze și să îl integreze în sistem
- Soluția trebuie să ofere posibilitatea de a oferi accesul la resurse pe baza unui program de timp care să poată fi definit
- Soluția trebuie să permită definirea de politici de acces la resurse pe baza criteriilor multiple: interval orar, metodă de acces, metodă de logare, etc.
- Soluția trebuie să permită definirea de politici de acces individualizate pentru sisteme, în funcție de rolul acestora

Reducerea privilegiilor și segregarea sarcinilor:

- Soluția trebuie să ofere posibilitatea de a reduce controlat și granular privilegiile conturilor de tip "superuser" pentru administratorii de aplicații Microsoft și "root" pentru UNIX/Linux
- Soluția trebuie să ofere posibilitatea eliminării conturilor administrative comune prin implementarea funcționalităților de delegare a sarcinilor administrative, administratorii având drepturi doar la componentele necesare îndeplinirii sarcinilor
- Soluția trebuie să suporte definirea de roluri, astfel încât pe baza grupurilor din care face parte utilizatorul, să i se permită accesul la diferite funcționalități

Monitorizare și audit:
- Soluția trebuie să monitorizeze integritatea fișierelor și a programelor utilizând cel puțin următoarele criterii: informații aferente HDD (dimensiune fișier, proprietar fișier etc.), precum și algoritmi de digital hashing (MD5, SHA-256 sau superior)
- În cazul în care un fișier monitorizat se dovedește a fi diferit de parametrii inițiali, soluția trebuie să genereze un eveniment înregistrat în fișierul de log și/sau o alertă e-mail
- În cazul în care fișierul care a fost modificat reprezintă un program executabil, soluția trebuie să poată fi configurată pentru a bloca executarea programului până la momentul în care fișierul este considerat din nou de încredere
- Soluția trebuie să înregistreze integral sesiunile utilizatorilor privilegiați pentru audit și conformitate

Controlul accesului la fișiere și directoare:
- Soluția trebuie să asigure suplimentarea controalelor native furnizate de sistemul de operare pentru Fișiere și Directoare (atât pentru sisteme Windows cât și Linux/Unix)
- Trebuie asigurat cel puțin controlul operațiilor de: read, write, execute, create, delete, rename, chown și chmod asupra fișierelor și directoarelor

Securitate și conformitate:
- Soluția trebuie să dețină o certificare de securitate emisă de o instituție independentă recunoscută internațional – Common Criteria (minimum EAL3+) sau echivalent, SAU să fie auditată și certificată conform standardelor internaționale de securitate (ISO 27001, SOC 2 Type II sau echivalent)
- Soluția trebuie să ofere politici predefinite care să fie în conformitate cu bunele practici de securitate (CIS Benchmarks, NIST, PCI-DSS)
- Soluția trebuie să suporte criptarea datelor transmise prin rețea (TLS 1.2 sau superior) și a datelor aplicației (AES-256 sau superior)

Funcționalități firewall și rețea:
- Soluția trebuie să permită definirea de politici pentru implementarea unei funcționalități de tip firewall în funcție de porturi, adresă sursă, tipul conectării precum și timp
- Această funcționalitate trebuie oferită atât pentru conexiunile egress cât și pentru cele ingress
- Soluția trebuie să permită definirea de politici de securitate ce pot fi distribuite pe grupuri de servere, indiferent de domeniul din care acestea fac parte

Administrare centralizată:

- Soluția trebuie să ofere posibilitatea administrării și definirii de politici într-un mod centralizat, indiferent de sistemul de operare care rulează pe sisteme
- Soluția trebuie să suporte administrarea multi-tenant și segregarea completă între medii (dezvoltare, test, producție)

Gestionarea parolelor și credențialelor:

- Soluția trebuie să ofere funcționalități de administrare a parolelor conturilor partajate și privilegiate
- Soluția trebuie să permită accesul utilizatorilor la parolele conturilor privilegiate pe baza de reguli de acces. Regulile de acces trebuie să poată fi create și modificate de către administratorul soluției
- Soluția trebuie să ofere posibilitatea integrării cu aplicații dezvoltate in-house în vederea schimbării parolelor
- Soluția trebuie să ofere suport pentru a putea extrage parolele din sistem, folosind linia de comandă și API (REST API sau echivalent)
- Soluția trebuie să asigure funcționalități pentru a permite aplicațiilor care necesită acces la conturi privilegiate să primească datele de conectare în mod programatic, eliminând necesitatea de a transcrie ("hardcode") credențialele de acces în script-uri sau în aplicații
- Soluția trebuie să implementeze rotația automată a parolelor conform politicilor definite

Acces transparent (SSO/Login automat):

- Soluția trebuie să permită utilizatorilor folosirea conturilor înregistrate în sistem, fără ca aceștia să poată vedea parola prin folosirea unei metode de tip login automat
- Soluția trebuie să suporte cel puțin protocoalele RDP, SSH și Telnet pentru loginul automat
- Soluția trebuie să suporte protocoale suplimentare: HTTPS, VNC, Kubernetes API, Database protocols (PostgreSQL, MySQL, MSSQL)

Înregistrare și redare sesiuni:

- Soluția trebuie să ofere posibilitatea autentificării utilizatorului în mod automat pentru sesiunile SSH, Telnet, RDP prin folosirea interfeței web, întreaga sesiune fiind înregistrată și stocată
- Soluția trebuie să pună la dispoziție opțiunea de a vizualiza din interfața web sesiunile înregistrate cu funcționalități de căutare și filtrare
- Soluția trebuie să extragă comenzile rulate în cadrul sesiunilor SSH și Telnet și să le atașeze înregistrării sesiunii
- Pentru fiecare sesiune, înregistrarea cât și lista comenzilor executate trebuie să poată fi vizualizate în interfața web
- Soluția trebuie să permită export-ul înregistrărilor în formate standard pentru arhivare și analiză

Workflow de aprobare:

- Pentru conturile cu un grad mare de risc, soluția trebuie să ofere posibilitatea definirii unui proces de aprobare (multi-level approval workflow)

- Astfel, înaintea folosirii contului, utilizatorul să ceară aprobarea unei alte persoane sau a mai multor persoane (în funcție de politica definită)
- Accesul la cont să se permită numai după obținerea aprobării, cu notificări automate către solicitant și aprobatori
- Soluția trebuie să permită definirea de termene limită pentru aprobări și escaladare automată

Integrare și API:
- Soluția trebuie să ofere API-uri REST documentate complet pentru integrare cu alte sisteme
- Soluția trebuie să permită integrarea cu sisteme SIEM pentru corelarea evenimentelor de securitate
- Soluția trebuie să suporte notificări prin multiple canale (email, SMS, webhook, Slack, etc.)

5) Componenta de API management

Soluția de Management API va oferi o interfață vizuală pentru a configura politici complexe de securitate pentru protecția API-urilor și serviciilor web. De asemenea, va pune la dispoziție instrumente integrate de testare și monitorizare care să asigure un management continuu al întregului ciclu de viață a serviciilor API.

Tipuri de soluții acceptate:
Soluția poate fi:
- Aplicație software disponibilă comercial (COTS) cu licențiere perpetuă sau sub formă de subscripție validă pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție

sau
- Soluție open source cu contract de suport tehnic profesional garantat pentru perioada de implementare a contractului și pentru întreaga perioadă de garanție, furnizat de către producătorul soluției sau de un partener autorizat

Obiective generale:
Soluția propusă va oferi un mediu API securizat - unul care protejează toate etapele ciclului de viață API, inclusiv partea de furnizare (construcția, implementarea și gestionarea traficului API), cât și partea de consum - descoperirea, achiziția și consumul de către dezvoltatorii de aplicații și alte API consumatori.
Va facilita schimbul de date cu acuratețe, în mod eficient și în condiții de siguranță între diferite sisteme informatice (atât din cadrul autorității contractante cât și din cadrul altor instituții cu care există sau vor exista protocoale de colaborare) conform proceselor de lucru operaționale specifice instituțiilor implicate.

Cerințe de implementare:

Moduri de deployment:
- Soluția trebuie să permită implementare ca software de sine stătător
- Implementare ca appliance software

- Implementare în mediu cloud IaaS (Redhat OpenStack sau Azure Stack Hub) sau implementare în containere (Docker, Kubernetes)
- Suport pentru arhitecturi cloud-native și microservicii

Management și administrare:
- Posibilitatea de a aplica versiuni noi/patch-uri de la distanță
- Management centralizat al tuturor nodurilor din cluster într-o singură pagină de administrare
- Scripting în linie de comandă pentru politici (CLI și/sau IaC - Infrastructure as Code)
- Suport pentru disaster recovery out-of-the-box
- Monitorizare și alertare centralizată
- Suport pentru configurare declarativă (YAML, JSON sau echivalent)

Arhitectură și stocare:
Portalul API va trebui să utilizeze o arhitectură containerizată pentru a ușura implementarea, migrarea și upgrade-ul în viitor. Componentele portalului să fie implementate în containerele Docker, facilitând schimbarea/înlocuirea containerelor pe măsură ce se lansează noi funcționalități ale acestei componente.
Soluția trebuie să suporte integrare cu multiple tipuri de baze de date și sisteme de stocare:
- Baze de date relaționale: PostgreSQL, MySQL, Microsoft SQL Server. etc
- Stiva ELK (Elasticsearch, Logstash, Kibana) pentru:
    - Indexarea și stocarea metadatelor API
    - Logs și evenimente de audit
    - Metrici de performanță și utilizare
    - Analytics și raportare în timp real
- Baze de date NoSQL: MongoDB, Redis, Cassandra (opțional)
- Posibilitatea de a utiliza multiple surse de date simultan pentru diferite componente

Funcționalități de bază:

Server de email integrat:
- Componenta va trebui să pună la dispoziție nativ un server de email propriu (SMTP) care să poată fi configurat independent față de serverul de email al beneficiarului
- Suport pentru template-uri de email personalizabile
- Suport pentru multiple canale de notificare (email, webhook, SMS)

Gestionarea utilizatorilor și organizațiilor:
- Permită crearea de utilizatori, conturi, organizații
- Permită configurarea de abonamente la nivel de API sau de conturi de dezvoltator
- Permită crearea de mai mulți utilizatori pentru un singur cont de dezvoltator
- Pună la dispoziție un flux de lucru pentru înregistrarea unui dezvoltator software nou pentru accesul la serviciile API oferite
- Permită crearea de utilizatori de tipul publisher care permite organizațiilor terțe să publice și să administreze propriile servicii API expuse
- Suporte adăugarea de câmpuri custom cerute la înregistrarea unui utilizator nou
- Integrare cu sisteme de identitate externe (LDAP, Active Directory, OAuth2, SAML)

Portal dezvoltatori:

Portalul API trebuie să simplifice descoperirea API pentru dezvoltatori și să le ofere acces la datele terțelor instituții care vor publica servicii API pentru a crea aplicații rapid. Relațiile cu dezvoltatorii, partenerii și terții să fie ușor de gestionat prin oferirea de funcționalități de:

- Publicare documentații de folosire a API-urilor (OpenAPI/Swagger, AsyncAPI)
- Configurare drepturi de acces granulare
- Posibilitatea de a publica instrumente educaționale, inclusiv aplicații demo
- API Explorer interactiv pentru testare în timp real
- Generarea automată de cod pentru serviciile API publicate în portal
- Pună la dispoziție o zonă de forum de discuții între dezvoltatorii de software înregistrați în sistem
- Sistem de rating și review pentru API-uri

Generare cod și testare:

- Permită generarea de cod automat client-side în cel puțin următoarele limbaje: JavaScript, Node.js, Python, Ruby, PHP, Objective-C, Java, Go, C#
- Ofere un API Explorer cu funcționalități de:
    - Testare interactivă a endpoint-urilor
    - Vizualizare răspunsuri în multiple formate
    - Salvare și partajare cereri de test
    - Mock servers pentru dezvoltare

Expunere date prin API:

- Permită expunerea unei baze de date prin REST API
- Suport pentru GraphQL
- Suport pentru gRPC și Protocol Buffers
- Suport pentru WebSocket și evenimente în timp real
- Transformare automată date între formate (JSON, XML, CSV)

Gestionarea cheilor și autentificare:

Pună la dispoziție o zonă de administrare a cheilor API care să permită:

- Generare automată de chei API
- Suspendarea/revocarea cheilor API
- Crearea unui certificat sau token (în plus față de cheia API generată)
- Suport pentru multiple metode de autentificare:
    - API Keys
    - OAuth 2.0 / OpenID Connect
    - JWT (JSON Web Tokens)
    - mTLS (Mutual TLS)
    - Basic Authentication
- Rotație automată a secretelor și cheilor
- Rate limiting și throttling configurabil per cheie/utilizator

Control acces și securitate:

- Ofere controale RBAC (Role-Based Access Control) pentru utilizatori de tipul autor, editor și publisher

- Suport pentru politici de securitate granulare la nivel de:
    - Endpoint
    - Metodă HTTP
    - Parametru
    - Header
    - Payload
- Validare automată a cererii și răspunsului conform schemelor definite
- Protecție împotriva atacurilor comune (SQL Injection, XSS, CSRF, DDoS)
- Rate limiting avansat cu algoritmi configurabili (token bucket, leaky bucket, fixed window)

Raportare și Analytics:

- Integrare cu Elasticsearch/Kibana: Soluția va utiliza stiva ELK pentru colectarea, indexarea și vizualizarea datelor de utilizare și performanță. Rapoartele vor fi generate prin dashboard-uri Kibana configurabile și vor include cel puțin următoarele informații:

a) Metrici de utilizare:

- Utilizarea API-ului de către dezvoltator individual
- Utilizarea API-ului de către grupul de dezvoltatori
- Utilizarea API-ului de către anumiți clienți dezvoltatori
- Utilizarea API în raport cu cota alocată
- Top API-uri după număr de apeluri
- Distribuția geografică a utilizatorilor

b) Metrici de performanță:

- Timpii de răspuns API (min, max, average, percentile 95/99)
- Latență API backend
- Throughput (cereri pe secundă/minut/oră)
- Dimensiunea payload-urilor (request/response)

c) Metrici de disponibilitate și erori:

- Erori de rutare API
- Rate de eroare per API/endpoint
- Depășire limite de utilizare API (rate limiting violations)
- Disponibilitate API (uptime/downtime)
- Status code distribution (2xx, 4xx, 5xx)

- Capabilități de raportare:
- Dashboard-uri în timp real cu refresh automat
- Alerting bazat pe praguri configurabile
- Rapoarte programate (zilnice, săptămânale, lunare)
- Export rapoarte în multiple formate: **CSV, PDF, HTML, JSON, Excel**
- Vizualizări personalizabile: grafice, tabele, heat maps, time series
- Agregări complexe și calcule derivate

- Istoricizare date pentru analiză trend

- Capacități de căutare și filtrare:
- Căutare full-text în logs și evenimente
- Filtrare multi-dimensională (timp, utilizator, API, status, etc.)
- Queries salvate și partajabile
- Drilldown în detalii pentru investigații

Integrări și extensibilitate:

- Integrări standard:
- Sisteme SIEM pentru securitate
- Platforme de monitorizare (Prometheus, Grafana, New Relic, Datadog)
- Sisteme de ticketing (Jira, ServiceNow)
- Sisteme CI/CD (Jenkins, GitLab CI, GitHub Actions, Gitlab, Bitbucket, Bamboo)
- Message brokers (RabbitMQ, Apache Kafka)
- Service mesh (Istio, Linkerd)

- Extensibilitate:
- Plugin system pentru funcționalități custom
- Webhook-uri pentru evenimente
- API complet documentat pentru automatizare
- Suport pentru middleware/interceptor custom
- Transformări date programabile (Lua, JavaScript, Python)

Securizare Acces

Următoarele cerințe tehnice trebuie acoperite de soluția propusa:

- Soluția trebuie să realizeze conversia XML-JSON direct fără a fi nevoie de scheme separate pentru XML și JSON. Transformarea XML-JSON trebuie să fie bidirecțională, XML-JSON și JSON-XML.
- Sa ofere control asupra performantelor apelurilor API:
    - configurare „throttling” si „rate limit”
    - prioritizare de trafic
    - limitare acces API pe utilizator, orar si adresa IP
    - rutare trafic in funcție de regiune geografica, adresa IP si timp de răspuns
- Să ofere funcționalități de cluster păstrând funcționalitățile de securitate precum si politicile de performanță definite la nivelul tuturor nodurilor prin replicare automată (limite interogări, protecție la atacuri, firewall xml)
- Sa ofere suport pentru diverși algoritmi de criptare: 3DES , AES, SHA, RSA
- Sa suporte algoritm de criptare curba eliptica
- Soluția trebuie să detecteze automat atașamentele SOAP;
- Soluția trebuie să permită definirea și detectarea de atașamente neașteptate sau incompatibile cu cerințele definite;
- Soluția trebuie să detecteze cererile XML cu un număr foarte mare de atribute ceea ce indică un atac la nivel de conținut.
- Să ofere mecanisme SSO end-to-end pe toate dispozitivele precum si integrare nativa cu solutia de SSO web/browser-based ofertata.

- Sa asigure suport pentru menținerea corespondentei intre sesiunea de front-end si cea de backend.
- Să asigure capabilități de WS/API firewall și funcții de control acces pe baza de politici de acces de tip RBAC;
- Să poată inspecta conținutul apelurilor folosind XML Schemas, XPath JSON Schemas, JSON Path, expresii regulate si comparații de stringuri
- Să permită următoarele metode de autentificare:
    - HTTP Basic;
    - WS-Security
    - Security Assertion Markup Language (SAML);
    - ticket Kerberos;
    - token OAuth.
- Să ofere mecanisme de securitate pentru echipamente Mobile și IoT prin OAuth (client și server side) și OpenID Connect.
- Să ofere suport pentru notificări către end-user prin Email, Apple Push Notification Service si Android alerts.
- Să permită un management complex a serviciilor API oferite prin:
    - Versionare si rollback
    - Orchestrare
    - Suport pentru creare de politici ramificate si politici globale
    - Validarea politicilor create in real-time
    - Aplicarea oricăror modificări de politici real-time fără necesitatea repornire vreunei componente
    - Automatizarea migrărilor serviciilor API pe toate nodurile clusterului

De asemenea, soluția trebuie:

- să limiteze mărimea documentului XML incluzând sau nu dimensiunea atașamentului;
- să detecteze vulnerabilități de genul SQL-injection sau XPATH-injections;
- să poată limita numărul de mesaje pe o perioadă de timp: pe secundă, pe minut, pe oră și pe zi;
- să poată limita numărul de conexiuni concurente către un anumit serviciu web expus;
- să poată preveni atacuri de tip “replay”: mesaj autentic cu credențiale valide repetat de foarte multe ori;
- să aibă posibilitatea ștergerii, înlocuirii, criptării sau mascării de date confidențiale;
- soluția trebuie să monitorizeze tranzacțiile în timp real și să permită vizualizarea statisticilor pe perioade de timp.;
- să poată cripta și decripta mesaje XML;
- să suporte WS-Security și XML Encryption;
- să valideze semnătura pentru a determina daca un mesaj este de încredere;
- să valideze certificatele pe baza unei liste de certificate revocate;
- să poată bloca accesul de la o lista de IP-uri sau subnet-uri;
- să poată permite accesul pe baza unei liste de adrese IP sau subnet;
- să poată monitoriza și alerta în cazul în care unul sau mai multe servicii API expuse nu sunt disponibile;

- să poată monitoriza și alerta în cazul în care unul sau mai multe servicii API expuse au o performanta deteriorate, sub nivelul unei limite pentru: timp de răspuns și număr de reîncercări;
- să permită logarea evenimentelor la nivel de servicii, client și tranzacții;
- să ofere următoarele opțiuni de logging:
  - fișier log local;
  - server Syslog;
  - bază de date;
  - trap SNMP;
- să permită posibilitatea separării evenimentelor de securitate de cele care privesc tranzacțiile.

Trebuie sa ofere capabilități suplimentare pentru a proteja amenințările aplicațiilor web conform cerințelor de mai jos descrise de OWASP:

- Trebuie să ofere acces deplin la toate cererile web și conținutul de răspuns și context pentru a permite inspecția și protecția în timpul execuției.
- Să poată cere autentificare puternică sau multifactorială prin protocoale securizate pentru a proteja împotriva atacurilor de forță brută folosind politici simple sau sofisticate de limitare a ratei de interogări sau politici de throughput.
- Să poată detecta și proteja împotriva atacurilor bazate pe sesiune, controlând atributele de securitate ale cookie-urilor, folosind semnături digitale și criptare sau urmărirea și maparea, și politici de impunere a identificatorilor de sesiune sticky trimiși.
- Să poate impune prin politici criptare în repaus sau în tranzit și sa poată fi configurat conform PCI-DSS - îndeplinind nevoile industriilor reglementate, cum ar fi sectorul financiar, asistența medicală și sectorul public.
- Să protejeze împotriva execuției de cod de la distanță și a atacurilor de denial of services (DoS).
- Să ofere mecanisme de control al accesului proprietare și conform standardelor din industrie, pentru a se asigura că resursele protejate pot fi accesate numai de utilizatori și aplicații autentificați și autorizați, folosind politici de securitate centralizate.
- Trebuie să permită o implementare ușoară și sigură în DMZ și să fie conformă cu certificarea Common Criteria pentru profilurile Enterprise Security Management, Policy Management și Enterprise Security Management, Access Control.
- Să ofere protecție maximă împotriva atacurilor pentru servicii, API-uri și aplicații și să le permite clienților să detecteze, să răspundă și să blocheze atacurile folosind politici de securitate centralizate ca firewall la nivel de aplicație.
- Să ofere niveluri de monitorizare definibile, permițând un nivel adecvat de raportare pe baza cerințelor beneficiarului.
- Trebuie să permită integrarea cu scanere de viruși și să protejeze împotriva amenințărilor la nivel de mesaj prin validarea traficului împotriva metadatelor la nivel de aplicație, cum ar fi schemele XML și schemele JSON .
- Să ofere capabilități de reverse proxy web:
  - Memorare în cache
  - Throttling/shaping
  - Comprimare
  - Terminare SSL

- Rutare dinamică/echilibrare de încărcare inteligentă
- Rescrierea adreselor URL
- Manipulare antet
- Manipulare parametri
- Manipulare cookie.

Etapele de implementare a sistemului informatic

Activitățile de analiză, proiectare, instalare și configurare, testare și implementare a soluției trebuie să fie realizate în conformitate cu prevederile de mai jos și vor fi prezentate în cadrul Ofertei într-un plan de proiect detaliat care, pe lângă detalierea activităților din cadrul fiecărei faze va cuprinde și menționarea duratei, a efortului, a resurselor cheie și non-cheie implicate și va conține și o detaliere a dependențelor și prerechizitelor.

1) Analiza și proiectarea

Rolul principal al fazei de analiză este de a înțelege corect nevoile utilizatorilor înainte de proiectarea și implementarea unui sistem care să le îndeplinească.

În vederea implementării sistemului, Furnizorul va trebui să execute activități de analiză care să asigure premizele unei implementări eficiente.

Analiza se va efectua de către Furnizor la sediul Beneficiarului și va avea ca finalitate un pachet de specificații funcționale agreat de comun acord cu Beneficiarul.

Serviciile de analiză vor acoperi cel puțin aspectele prevazute în etapele 1-4 si care fac obiectul realizării sistemului informatic.

Se vor considera cel puțin următoarele livrabile **(Pachet Livrabile Analiză):**
- Documentul de analiză a cerințelor de business la nivel de fiecare componentă a soluției;
- Arhitectură sistem informatic (necesarul infrastructurii de cloud, software, componentele logice și straturile de organizare a datelor la nivel de componente).

Rolul principal al fazei de proiectare este de a descrie la un nivel suficient de detaliu sistemul care urmează a fi implementat.

În vederea implementării sistemului, Furnizorul va trebui să execute activități de proiectare care să asigure premizele unei implementări eficiente.

Proiectarea sistemului dorit, care va conține detalierea la nivel tehnic a cerințelor și specificațiilor rezultate din activitatea de analiză pentru toate nivelurile și componentele sistemului care va fi realizat:
- Arhitectura de sistem – va prezenta cel puțin următoarele niveluri: componente software instalate, arhitectura logică cuprinzând descrierea componentelor de sistem, a celor dezvoltate sau personalizate și caracteristicile funcționale și non-funcționale ale acestora;

- Scenarii (cazuri) de utilizare – din care să reiasă modul de utilizare a sistemului informatic din perspectiva utilizatorului, modul în care utilizatorii interacționează cu sistemul, în corespondență directă cu activitățile menționate în cadrul proceselor operaționale ale acestor utilizatori. De asemenea, scenariile de utilizare vor fi însoțite de o listă a actorilor sistemului și maparea acestora cu actorii de business. Pentru prezentarea cazurilor de utilizare se vor folosi instrumente în conformitate cu standarde de modelare și reprezentare recunoscute (UML sau echivalent);
- Scenarii (cazuri) de testare și plan de testare – din care să reiasă modul în care se va face testarea implementării corecte a tuturor cerințelor din prezentul Caiet de Sarcini care au fost detaliate pe parcursul fazei de analiză, inclusiv teste de penetrare și managementul continuității;
- Modelul de securitate – la nivel logic (organizarea pe roluri, grupuri, drepturi, poziția în structura organizatorică etc.) și la nivel fizic (aplicații etc.);
- Integrările la nivel de componentă software – pentru fiecare interacțiune se va specifica sistemul sursă/destinație, modalitatea de implementare, canalul de comunicare, setul și structura de date transferate, reguli specifice de validare etc;
- Proiectarea şi realizarea structurii bazei de date nominale la nivel central;
- Modelul interfețelor utilizatorilor, pentru fiecare componentă în parte;
- Planul de instruire.

Proiectarea sistemului trebuie să ofere o soluție optimă, urmărindu-se ușurința și eficiența realizării și implementării soluției, în cadrul restricțiilor de ordin tehnic, organizatoric sau financiar.

Documentul/documentele de specificații, rezultate în urma activităților de analiză și proiectare, vor descrie soluția în detaliu, vor conține informații privind toate funcționalitățile necesare și vor sta la baza stabilirii și realizării testelor de acceptanță.

Din punct de vedere al livrabilelor, se vor considera cel puțin următoarele documente **(Pachet Livrabile Proiectare):**

- Designul logic al fluxurilor de date;
- Documentul de design al interfețelor utilizator;
- Plan și strategie testare (final), inclusiv scenarii testare;
- Plan Instruire utilizatori;
- Plan Asigurare Calitate (actualizat);
- Plan de proiect (actualizat);
- Tabel corespondență prin care se va detalia modul prin care fiecare cerință din caietul de sarcini va fi implementată.

În urma activităților de analiză și proiectare, pentru a se obține un sistem final operațional se vor desfășura activități de configurare, testare și implementare (trecere în producție).

La finalizarea activităților de analiză și proiectare și după finalizarea documentelor livrabile Furnizorul va organiza sesiuni de prezentare a documentelor livrabile cu echipa de proiect a Beneficiarului.

Faza de analiză și proiectare se va considera finalizată după predarea de către Furnizor și verificarea, validarea și acceptarea de către Beneficiar a tuturor livrabilelor prevăzute la această fază și semnarea Proceselor Verbale de Recepție și a Proceselor Verbale de Acceptanță Cantitativă și Calitativă.

Ofertanții vor descrie, în mod detaliat atât în cadrul Ofertei document dar și **în Planul de proiect anexă a Ofertei**, modul în care vor considera abordarea activităților cuprinse în cadrul acestei faze, menționând și riscurile, dependențele, livrabilele, resursele implicate (roluri) și durata de derulare.

2) **Instalare, configurare și dezvoltarea platformei**

În cadrul acestei faze se vor derula activități de instalare, configurare, customizare și dezvoltare a componentelor sistemului informatice (definire fluxuri, dezvoltare module/componente, dezvoltare interfețe, dezvoltare proceduri/procese arhivare/back-up/restaturare soluție și date, etc) astfel încât la finalul fazei de dezvoltare va rezulta o soluție informatică completă, dezvoltată în conformitate cu cerințele menționate în Caietul de Sarcini, și detaliate în cadrul fazei de analiză și proiectare.

Ofertanții vor lua în calcul că activitățile de dezvoltare se vor desfășura pe date cu caracter protejat de intrare puse la dispozitie de Beneficiar.

Vor fi considerate următoarele livrabile **(Pachet Livrabile Dezvoltare):**

- Scripturile pentru crearea bazelor de date și a componentelor funcționale, interfețe utilizatori, configurări utilizatori și drepturi de acces;
- Plan de Asigurare a Calității actualizat;
- Plan de Testare actualizat (inclusiv scenarii și cazuri de testare);
- Rezultatele Testelor Interne;
- Tabel corespondență actualizat (matricea de trasabilitate);

Faza de Dezvoltare se va considera finalizată după predarea de către Furnizor și verificarea, validarea și acceptarea de către Beneficiar a tuturor livrabilelor prevăzute la această fază și semnarea Proceselor Verbale de Recepție și a Proceselor Verbale de Acceptanță Cantitativă și Calitativă.

Ofertanții vor descrie, în mod detaliat atât în cadrul Ofertei document dar și în Planul de proiect anexă a Ofertei, modul în care vor considera abordarea activităților cuprinse în cadrul acestei faze, menționând și riscurile, dependențele, livrabilele, resursele implicate (roluri) și durata de derulare.

3) **Instruirea**

Faza de instruire va cuprinde sesiuni de instruire pentru administrarea sistemului (toate componentele sale) și pentru operarea sistemului.

Programul de instruire se realizează sub forma de cursuri ținute de experți (cheie și non-cheie).

Scopul activităților de instruire este de a instrui personalul Beneficiarului în vederea asigurării operării sistemului informatic și în administrarea componentelor sale (software de bază, baze de date și a aplicației). De asemenea, prin participarea la cursurile de instruire cursanții vor avea un nivel de cunoștințe referitoare la funcționalitățile soluției dezvoltate care le va permite să desfășoare în cele mai bune condiții atât activitățile de testare de acceptanță a soluției cât și activitățile curente ce presupun utilizarea soluției.

Toate cursurile vor conține activități practice, documentații și manuale. Manualele de curs referitoare la sistemul ce urmează a fi instalat se pun la dispoziția cursanților cu cel puțin 10 zile înainte de data de desfășurare a cursurilor. Manualele de curs vor fi livrate atât în format fizic cât și electronic, în limba româna pentru materialele de instruire pentru utilizatori și administrare a sistemului.

Instruirea va fi coordonată și prestată de către personalul furnizorului soluției pentru cel puțin următoarele grupuri de utilizatori:

- 5 administratori de sistem - curs general de administrare sistem informatic (inclusiv componentă de securitate, gestiune a utilizatorilor și a drepturilor de acces);
- 5 administratori de aplicație - curs general de administrare a aplicației (portal si site web).

Instruirea administratorilor are în vedere dobândirea cunoștințelor necesare:

- administrării utilizatorilor și permisiunilor asociate acestora în cadrul aplicației;
- design-ului interfețelor;
- administrării și particularizării sistemului;
- consultării jurnalelor de auditare a accesului și operațiunilor desfășurate în cadrul sistemului;
- întreținerea aplicației.

Instruirea utilizatorilor va avea în vedere dobândirea de cunoștințe privind:

- utilizarea generală a sistemului;
- adăugarea/modificarea/ștergerea datelor în cadrul sistemului;
- definirea/generarea de rapoarte în funcție de rol (definire rapoarte/generare rapoarte).

Instruirea administratorilor și a utilizatorilor se va face în bază unei proceduri/metodologii, parte integrantă a ofertei tehnice a furnizorului soluției informatice. Procedura va conține cel puțin următoarele informații:

- Descrierea cursurilor și a rezultatelor așteptate;
- Modalitatea de evaluare a cursurilor;
- Formulare utilizate.

Totodată, instruirea va avea la bază un plan de instruire al utilizatorilor care va conține toate serviciile solicitate pentru numărul specificat de utilizatori, precum și curricula cursurilor de instruire. Atât planul de instruire cât și curricula cursurilor vor fi parte integrantă a ofertei tehnice a furnizorului soluției informatice.

Instruirea va începe înainte de derularea activităților de Testare de Acceptanță, atunci când soluția este complet dezvoltată și este stabilă din punct de vedere al funcționării.

Vor fi considerate cel puțin următoarele livrabile pe care Furnizorul va trebui să le prezinte spre validare/aprobare către Beneficiar la terminarea activităților de instruire **(Pachet Livrabil Instruire):**

- Materiale de curs (pentru fiecare tip de instruire);
- Manuale operaționale/de utilizare pentru Administratori de sistem, Administratori de aplicație
- Foaie de prezență nominală zilnică, semnată de către toți participanții Beneficiarului la sesiunile de instruire
- Chestionare referitoare la nivelul de cunoștințe al utilizatorilor în legatura cu soluția/functionalitățile implementate, la inceputul și la sfarsitul cursului, pentru a putea determina nivelul de cunoștințe acumulate de către participanți pe durata derulării cursului
- Chestionare referitoare la calitatea și conținutul cursurilor, semnate de către fiecare participant la sesiunile de instruire
- Raport de Instruire, care va detalia activitățile desfășurate pe parcursul sesiunilor de instruire.

Sesiunile de instruire se vor derula în limba română.

Materialele de curs vor fi redactate în limba română și se vor referi la soluția/functionalitățile implementate.

Faza de Instruire se va considera finalizată după predarea de către Furnizor și verificarea, validarea și acceptarea de către Beneficiar a tuturor livrabilelor prevăzute la această fază și semnarea Proceselor Verbale de Recepție și a Proceselor Verbale de Acceptanță Cantitativă și Calitativă.

4) Testarea de acceptanță și asigurarea calității

Testele de acceptanță se vor derula în conformitate cu Planul de Testare realizat de Furnizor și agreat de Beneficiar, plan ce va fi în concordanță cu întregul ciclu de realizare al contractului: etape de testare distribuite pe iterații, seturi de funcționalități sau alte tipuri de teste.

Planul de testare pentru acceptanță va cuprinde toate testele necesare pentru a demonstra acoperirea în întregime a cerințelor din prezentul caiet de sarcini. Astfel, se va avea în vedere faptul că sistemul funcționează corect din punct de vedere al respectării cerințelor, al consistenței datelor, al constrângerilor de timp, al validărilor de date și al gestiunii erorilor, inclusiv pentru funcționalitățile existente care au fost extinse sau modificate. Criteriul de succes – sistemul trece toate testele definite în planul de testare agreat împreună cu Beneficiarul și toate cerințele (funcționale și non-funcționale) au fost implementate și toate componentele funcționează la parametrii solicitați. Pentru fiecare caz de testare (test-case) și scenariu de testare Beneficiarul va redacta un raport de testare care va descrie testul/testele efectuate, condițiile în care testul a fost efectuat, rezultatele așteptate, rezultatele obținute și rezultatul final al testării: Test Trecut / Test Picat.

Testele de acceptanță se vor rula pe fiecare componentă în parte și pentru întreaga soluție.

Se vor rula:
- Teste de sistem (system testing);
- Teste funcționale (funcțional testing);
- Teste non-funcționale: teste de securitate, teste de folosire (usability testing).

În cazul în care există teste care sunt în status „Failed", Beneficiarul va transmite lista lor către Furnizor pentru remediere/rezolvare. Furnizorul va dezvolta o nouă versiune a componentei pe care o va instala pe mediul de test pentru retestare. Testele vor fi reluate până la finalizarea cu succes a tuturor scenariilor/cazurilor de testare.

O primă variantă a planului de testare va fi prezentată odată cu oferta. Planul detaliat de testare, însoțit de scenariile și cazurile de testare, va fi realizat de către Furnizor și aprobat de Beneficiar înainte de fiecare etapă de testare agreată prin planul de proiect.

Testele de acceptanță (un set relevant) vor fi rulate și pe mediul de producție după finalizarea fazei de Implementare.

Se vor considera cel puțin următoarele livrabile (Pachet Livrabile Testare):
- Rezultatele testelor (consolidat și detaliat) și uneltele folosite pentru testare (dacă este cazul)
- Versiunea finală a codului sursă și a executabilelor
- Scripturile de instalare
- Setările pentru configurare
- Setările pentru conectivitate cu alte sisteme
- Documentația de proiect (livrată în cadrul fazelor anterioare) actualizată (dacă este cazul)
- Tabel corespondență actualizat; se va considera Tabelul de corespondență prezentat la ofertare, completată la fiecare cerință, cu demonstrarea modului în care cerința a fost îndeplinită/implementată.

Faza de Testare de Acceptanță se va considera finalizată după predarea de către Furnizor și verificarea, validarea și acceptarea de către Beneficiar a tuturor livrabilelor prevăzute la această fază și semnarea Proceselor Verbale de Recepție și a Proceselor Verbale de Acceptanță Cantitativă și Calitativă.

Ofertanții vor descrie, în mod detaliat atât în cadrul Ofertei document dar și în Planul de proiect anexă a Ofertei, modul în care vor considera abordarea activităților cuprinse în cadrul acestei faze, menționând și riscurile, dependențele, livrabilele, resursele implicate (roluri) și durata de derulare.

5) Punerea în producție

Planul de trecere în producție trebuie să țină cont de legăturile logice între subsisteme/componente ale sistemului astfel încât să se asigure o trecere în producție coerentă și cu impact minim asupra activităților zilnice a angajaților Beneficiarului.

În faza de Punere în Producție sistemul (complet, cu toate componentele sale) va fi utilizat de către utilizatori în mod normal și Furnizorul va realiza ajustarea proceselor și fluxurilor implementate având ca obiectiv optimizarea funcționării și exploatării sistemului. De asemenea, pe parcursul derulării activităților de trecere în producție mai pot fi identificate eventuale erori/bug-uri care nu au fost identificate pe parcursul fazelor de testare; acestea vor fi semnalate Furnizorului pentru remediere și, după remedierea lor acestea vor intra în procedura de testare de acceptanță/implementare și punere în producție.

Pe perioada de punere în producție a sistemului Furnizorul va oferi, atunci când este solicitat de către Beneficiar (telefonic sau prin e-mail), îndrumare în utilizarea soluției și va asigura, dacă este cazul, sesiuni suplimentare de instruire fie la sediul Beneficiarului fie prin video-conferință.

Furnizorul va transmite următoarele livrabile **(Pachet Livrabile Punere Productie):**

- va fi livrat sistemul informatic funcțional conform cerintelor prezentului caiet de sarcini – matrice de conformitate
- se vor livra certificatul de garanție, declarație de conformitate pentru întreg sistemul informatic
- matricea de trasabilitate actualizată
- manuale de utilizare și de operare actualizate
- codul sursă pentru soluție și pentru toate aplicațiile dezvoltate și utilizate în implementarea proiectului. Codul sursă va fi comentat și va trebui predat pe suport electronic.

Faza se va considera finalizată dacă livrabilele de mai sus au fost livrate și verificate/validate/aprobate de către Beneficiar și au fost semnate Procele Verbale de Acceptanță Cantitativă și Calitativă Finale.

Ofertanții vor descrie, în mod detaliat atât în cadrul Ofertei document dar și în Planul de proiect anexă a Ofertei, modul în care vor considera abordarea activităților cuprinse în cadrul acestei faze, menționând și riscurile, dependențele, livrabilele, resursele implicate (roluri) și durata de derulare.

6) Garanție

Pentru întregul sistem integrat se va acorda o **garanție minimă de 3 ani**.

Prin garanție în acest context se înțelege asigurarea funcționalităților existente la data finalizării implementării sistemului informatic.

Pentru toate componentele se va asigura suport tehnic pe perioada garanției de 3 ani, începând cu data livrării sistemului informatic final, adica semnarea fara obiectiuni a Proceselor Verbale de Acceptanță Cantitativă și Calitativă Finale.

Intervențiile vor fi realizate cu tehnicieni autorizați de producator.

Pe întreaga perioadă de garanție furnizorul soluției informatice va asigura obligativitatea funcționării sistemului în perioada de post-implementare, va presta servicii de suport

pentru toate sistemele software furnizate, iar această activitate va fi monitorizată de către Responsabilul de proiect.

Prestatorul va pune la dispoziția Autoritatii Contractante un „Serviciu de suport tehnic" care va avea scopul de a oferi utilizatorilor finali un Punct Unic de Contact pentru toate solicitările de intervenţii asupra componentelor software, pentru suport operativ şi pentru semnalările unor funcţionari defectuoase a soluţiei furnizate.

Remedierea defecţiunilor pe perioada garanţiei se va face la sediul beneficiarului proiectului sau prin intervenţie de la distanţă (remote maintenance), iar în cazul unor defecte mai grave, echipamentele se vor transporta la sediul furnizorului de către acesta.

Fiecare intervenţie în perioada de garanţie va fi documentată cu ajutorul unei fişe de intervenţie care va conţine următoarele detalii: data intervenţiei, descrierea intervenţiei, modalitatea de rezolvare a intervenţiei (reparaţie/înlocuire), durata de intervenţie şi confirmarea recepţiei prin semnăturile furnizorului şi beneficiarului.

Controlul intervenţiilor

Pentru înregistrarea tuturor tipurilor de intervenţii în perioada de garantie și pentru asigurarea bunei funcţionări a produselor ofertate, se va propune daca este cazul, un model de registru pentru controlul intervenţiilor, care va fi validat de comun acord în urma workshop-urilor comune avute cu beneficiarul. Beneficiarul va actualiza acest registru cu toate informaţiile care descriu intervenţiile respective.

Prin garanţie se va asigura faptul că produsele sunt conforme cu specificaţiile tehnice, fără costuri suplimentare, pe toată durata garanției.

Timpii de rezolvare sunt definiți mai jos în funcție de gravitatea incidentului apărut:

Nivel Criticitate	**Timp de răspuns**	**Timp soluționare temporară**	**Timp soluționare finală**
Critic	1 oră	6 ore	12 ore
Mediu	6 ore	12 ore	36 ore
Minor	12 ore	36	72 ore

Tipurile incidentelor:

1. **Critic**: una sau mai multe resurse din mediul productiv sunt nefuncționale sau profund degradate, iar impactul acestui incident duce la imposibilitatea utilizării sistemului.
2. **Mediu**: impactul produs de degradarea uneia sau mai multor resurse duce la scăderea performanței sau afectarea parțială a unor funcționalități ale sistemului. Sistemul este funcțional pentru cea mai mare parte a scenariilor de utilizare.
3. **Minor**: impactul produs de degradarea uneia sau mai multor resurse este redus sau există soluție temporară.

Sistemul, o dată finalizat, va deveni proprietatea Beneficiarului fără nici o restricție. Vor fi puse la dispoziția Beneficiarului atât codurile sursă (editabile) ale

componentelor dezvoltate cât și toată documentația aferentă, inclusiv manualele operaționale și documentația/manualele de instruire.

Beneficiarul nu va putea revinde componente ale soluției dar va putea opera modificări asupra lor (nu în perioada de garanție) și/sau le va putea pune la dispoziția unui alt Furnizor în cazul unor contracte de mentenanță corectiva sau evolutivă (sub condiția unor clauze de confidențialitate).

Sistemul informatic va asigura standardele de securitate și confidențialitate a informațiilor, de prelucrare a datelor cu caracter personal conform Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare și conform Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare.

Toate componentele și subcomponentele vor trebui să se regăsească în cadrul ofertei tehnice propuse pentru a asigura rularea aplicației în bune condiții (ținând cont și de infrastructura existentă a Beneficiarului), fără a fi necesară achiziția de către Beneficiar de produse suplimentare atât pe perioada de derulare a contractului, cât și în perioada de garanție. Sistemul livrat nu va genera costuri suplimentare pentru Beneficiar la instalare, ulterior sau în perioada de garanție.

4. ATRIBUȚIILE ȘI RESPONSABILITĂȚILE PĂRȚILOR

Atribuțiile și responsabilitățile Părților vor fi guvernate de prevederile prezentului Caiet de Sarcini și ale contractului care va fi semnat între ADR și operatorul economic desemnat câștigător, în conformitate cu prevederile documentației de atribuire.

În raport cu serviciile solicitate și cu cerințele stipulate în prezentul Caiet de Sarcini, responsabilitățile și atribuțiile părților sunt:

4.1. Autoritatea contractantă are următoarele obligații principale:

- punerea la dispoziție a tuturor informațiilor de care dispune pentru obținerea rezultatelor așteptate în limita competențelor pe care le deține;
- desemnarea echipei implicate și responsabile cu interacțiunea și suportul oferit contractantului;
- asigurarea accesului în spațiile în care urmează a se realiza prestarea serviciilor;
- mobilizarea tuturor resurselor care sunt în sarcina sa, pentru buna derulare a contractului;
- colaborarea cu Contractantul pentru a identifica în timp util orice eventuale probleme care ar putea apărea pe parcursul derulării contractului;
- asigurarea acurateței oricăror informații puse la dispoziția Contractantului pe durata derulării contractului;
- monitorizarea îndeplinirii tuturor cerințelor din Caietul de Sarcini și a oricăror elemente ale Propunerii Tehnice și Financiare pe durata derulării contractului, efectuarea și păstrarea unei arhive cu înregistrări pentru documentarea nivelului de performanță a Contractantului;
- notificarea Contractantului prin canalele de comunicare puse la dispoziție de acesta privind orice incidente sau disfuncționalități care intervin pe perioada de derulare a contractului;
- verificarea tuturor documentelor asociate recepției serviciilor care fac obiectul contractului, respectiv care confirmă prestarea serviciilor potrivit condițiilor de calitate stabilite în Caietul de sarcini.

4.2. Ofertantul devenit Contractant are următoarele obligații

4.2.1. Obligații generale ale Ofertantului devenit Contractant:

a) mobilizarea de resurse suficiente și cu expertiză adecvată pentru a asigura gestionarea contractului, astfel cum este solicitat la nivelul Caietului de Sarcini;
b) îndeplinirea obligațiilor contractuale, cu respectarea bunelor practici din domeniu, a prevederilor legale și contractuale relevante, astfel încât să se asigure că obligațiile sunt îndeplinite la parametrii solicitați;
c) asigurarea unui grad de flexibilitate în planificarea modalității de gestionare a contractului, pe toată durata de derulare a contractului;
d) transmiterea datelor de identificare și de contact ale personalului alocat pentru executarea contractului;
e) colaborarea cu personalul autorității contractante alocat pentru verificarea produselor livrate și realizarea recepțiilor;

f) reducerea, în măsura posibilă, la minim, a situațiilor de întârzieri în efectuarea livrărilor, minimizând astfel impactul negativ asupra activității autorității/entității contractante;
g) asigurarea că orice documente, documentații și/sau instrucțiuni furnizate către personalul autorității contractante sunt exacte și elaborate în conformitate cu bunele practici specifice în domeniu;
h) prezentarea rapoartelor solicitate de personalul autorității contractante, potrivit cerințelor de raportare stablite prin Contract;
i) colaborarea cu personalul autorității contractante alocat pentru furnizarea produselor care fac obiectul contractului și pentru asigurarea serviciilor accesorii;
j) completarea unei Declarații de imparțialitate, confidențialitate și privind conflictul de interese de către Personalul desemnat de Contractant, înainte de implicarea în implementarea contractului;
k) la livrarea produselor și soluțiilor, Contractantul trebuie să asigure respectarea practicilor de securitate în muncă și de protecție a mediului înconjurător;
l) livrările, instalările, configurările, punerile în funcțiune, operaționalizările și integrarea produselor și soluțiilor trebuie să fie în concordanță cu termenele de livrare, instalare, configurare, punere în funcțiune, testare, operaționalizare și integrare prezentate de Contractant în propunerea tehnică;
m) contractantul este responsabil să se asigure că pentru toate activitățile cuprinse în propunerea tehnică dispune de toate resursele necesare pentru îndeplinirea contractului.

Obligațiile principale ale Ofertantului devenit Contractant se completează cu obligațiile prevăzute în Contract.

4.2.2. Obligații principale ale Ofertantului devenit Contractant:

a) respectarea și implementarea cerințelor GDPR:
   - asigurarea conformității activităților desfășurate în cadrul contractului cu toate cerințele GDPR, inclusiv protejarea datelor cu caracter personal colectate, prelucrate sau stocate;
   - implementarea măsurilor tehnice și organizatorice adecvate pentru a asigura securitatea și confidențialitatea datelor;
   - furnizarea de suport și consultanță pentru îndeplinirea cerințelor GDPR de către organizație, inclusiv politici și proceduri de protecție a datelor, evaluări de impact și acorduri de prelucrare a datelor;
b) colaborarea pentru implementarea unui cadru de guvernanță digitală (DGA):
   - dezvoltarea și implementarea unui cadru de guvernanță digitală adaptat la nevoile organizației, asigurând o structură clară și un set de politici pentru gestionarea datelor;
   - oferirea de consultanță pentru identificarea și gestionarea riscurilor asociate guvernanței datelor și protecției acestora;
   - asistența în stabilirea și documentarea unui flux de lucru pentru colectarea, stocarea, accesarea și arhivarea datelor, inclusiv reguli pentru păstrarea și distrugerea acestora;
c) asigurarea confidențialității și a protecției datelor pe durata contractului:
   - respectarea clauzelor de confidențialitate impuse de contract și implementarea măsurilor necesare pentru a preveni accesul neautorizat la datele organizației;

- raportarea promptă a oricăror breșe de securitate sau incidente care ar putea compromite integritatea datelor;

d) evaluarea și consultanța în procesarea datelor personale:
   - efectuarea de evaluări de impact privind protecția datelor (DPIA) pentru activitățile de procesare cu un risc ridicat pentru drepturile și libertățile persoanelor fizice;
   - recomandarea celor mai bune practici și măsuri de protecție pentru a diminua riscurile asociate cu procesarea datelor personale;
e) suport pentru comunicarea de criză în cazul încălcării securității datelor:
   - pregătirea unei proceduri de răspuns în caz de incidente de securitate și oferirea de suport pentru comunicarea eficientă în caz de breșe de date, în conformitate cu cerințele GDPR;
   - asigurarea că orice incident de securitate este documentat, evaluat și raportat către autoritatea de supraveghere, dacă este necesar, în termenul prevăzut de GDPR (72 de ore);
f) formarea și instruirea personalului în privința conformității GDPR și DGA:
   - organizarea de sesiuni de instruire pentru angajații organizației pentru a se asigura că aceștia înțeleg și respectă cerințele GDPR și DGA;
   - crearea unor materiale informative sau ghiduri care să susțină personalul în activitățile de procesare și protecție a datelor;
g) documentarea și raportarea activităților de consultanță:
   - furnizarea de rapoarte periodice către client privind stadiul implementării cerințelor DGA și GDPR, dificultățile întâlnite și soluțiile propuse;
   - păstrarea unei evidențe complete a activităților și a măsurilor implementate în vederea conformității, pentru a putea fi prezentate autorităților de supraveghere, la cerere;
h) consultanță continuă și actualizare la schimbările legislative:
   - monitorizarea oricăror modificări legislative și recomandarea de ajustări ale politicilor și practicilor de conformitate GDPR și DGA;
   - informarea organizației cu privire la noi reglementări, interpretări sau bune practici în domeniul guvernanței digitale și al protecției datelor personale.

4. IPOTEZE ȘI RISCURI

La elaborarea ofertei, ofertanții trebuie să aibă în vedere cel puțin ipotezele și riscurile descrise în continuare, să estimeze posibilele efecte ale acestora precum și modalitatea de reducere/remediere a riscului. În acest sens, la elaborarea ofertei, ofertantul trebuie să ia în considerare resursele necesare (financiare, de timp, umane și de orice altă natură), pentru implementarea strategiilor de risc propuse.

4.3. Ipoteze

Ipotezele avute în vedere sunt:

- buna cooperare între contractant și autoritate contractantă, în special între persoanele desemnate în derularea contractului;
- contractantul va furniza servicii la un înalt nivel de calitate, cel puțin egal cu cel solicitat în prezentul caietul de sarcini;
- conținutul serviciilor solicitate este descris în mod explicit în Caietul de Sarcini;
- nu se prevăd schimbări ale cadrului instituțional și legal care să afecteze major executarea și desfășurarea în bune condiții a acordului cadru, respectiv a contractelor subsecvente;
- corelarea dintre resursele necesare și rezultatele așteptate este realistă;
- toate informațiile relevante și disponibile la nivelul Autorității Contractante pentru realizarea serviciilor vor fi puse la dispoziția Contractantului.

4.4. Riscuri

Pentru a identifica și combate efectele adverse pe care contractul ar putea să le întâmpine, au fost identificate o serie de riscuri și măsuri de atenuare a acestora.
Autoritatea contractantă își asumă responsabilitatea pentru urmărirea și aplicarea strategiei de răspuns pentru fiecare dintre riscurile identificate pentru implementarea contractului, în sfera sa de responsabilitate.
Contractantul își asumă responsabilitatea pentru urmărirea și aplicarea strategiei de răspuns pentru fiecare dintre riscurile aferente implementării contractului ce cad în sfera sa de responsabilitate.

Riscurile și măsurile de combatere a acestora care vor fi luate în considerare pe durata implementării serviciilor, sunt:

Nr. crt.	**Risc identificat**	**Măsuri de răspuns / atenuare ale riscului**
1	Prelungirea termenelor procedurilor de achiziție publică	- realizarea și actualizarea permanentă a unui plan de achiziții; - analiza permanentă a legislației referitoare la achizițiile publice; - un membru al echipei de proiect are rolul de a coordona și realiza derularea achizițiilor publice.

2	Începerea activităților cu întârziere	- realizarea și actualizarea permanentă a unui plan de management; - monitorizarea permanentă a respectării termenelor.
3	Adăugarea de activități/ solicitări de informații noi, în funcție de progresul activităților	- contractantul va avea o abordare caracterizată de agilitate; - autoritatea contractantă va avea în vedere o abordare pro-activă ce vizează identificarea potențialelor schimbări / modificări cât mai curând posibil și informarea adecvată a Contractantului.
4	Din cauza capacității tehnice / financiare/ profesionale reduse a Contractantului este posibil ca obiectul contractului / obligațiile contractuale să fie neîndeplinite / îndeplinite necorespunzător, ori cu întârziere	- autoritatea contractantă introduce în caietul de sarcini cerințe minime privind personalul responsabil de implementarea Contractului, extinse la nivelul factorilor tehnici de evaluare; - stabilirea unor indicatori de performanță ce vor fi avuți în vedere la etapa de recepție și în etapa de întocmire a certificatului constatator; - autoritatea contractantă va solicita constituirea de către Contractant a unei garanții de bună execuție, în cuantum de 10% din valoarea contractului ce va putea fi reținută în condițiile descrise în Contract; - autoritatea contractantă a prevăzut în Contract sancțiunile și penalitățile aplicabile.
5	Fluctuații de personal la nivelul autorității contractante	- selectarea atentă a persoanelor din echipa de proiect; - selectarea unei echipe de formate din persoane, care vor fi angajate pe toata durata proiectului.
6	Solicitări de modificare a Personalului desemnat de Contractant pentru implementarea contractului sau modificări în structura organizatorică a Contractantului	- asigurarea flexibilității în planificarea și utilizarea resurselor umane incluse în implementarea contractului și posibilitatea suplimentării resurselor alocate în cazul în care riscul se materializează; - la nivel contractual sunt introduse reguli clare referitoare la modalitățile de înlocuire a personalului Contractantului.
7	Depunerea unui număr mare de solicitări de sprijin într-o perioadă scurtă de timp	- contractantul va asigura o suplimentare a personalului, astfel încât să acopere eventuale „vârfuri de sarcină”.
8	Din cauza unei organizări deficitare, regulile privind evitarea conflictului de interese sunt încălcate	- sunt prevăzute reguli clare și precise pentru prevenția conflictului de interese, atât în etapa de ofertare, cât și în etapa de implementare a Contractului; - sunt prevăzute sancțiuni pentru încălcarea

		regulilor referitoare la conflictul de interese.
9	Dificultăți de colaborare și comunicare între factorii interesați implicați (inclusiv personal insuficient sau diferențe de înțelegere ale noțiunilor din caietul de sarcini)	- se va urmări în mod continuu fluxul de comunicare între personalul Autorității Contractante și al Prestatorului; - atât Autoritatea Contractantă cât și Prestatorul vor avea permanent în vedere o listă de rezervă a personalului responsabil cu implementarea proiectului.
10	Datele și informațiile necesare în vederea desfășurării serviciilor comunicate de către autoritatea contractantă nu sunt suficiente pentru îndeplinirea cerințelor solicitate prin caietul de sarcini	- atât Autoritatea Contractantă cât și Prestatorul vor monitoriza continu fluxul de lucru, cu scopul de a remedia deficientele, iar, după caz autoritatea contractanta va pune la dispoziție toate informațiile disponibile pentru îndeplinirea cerințelor solicitate la nivelul de calitate așteptat, conform graficului de prestare a activităților asumat de Prestator.

Ofertantul va prezenta în cadrul Propunerii tehnice un **Plan de management al riscurilor**. Această secțiune va conține cel puțin următoarele:
a) descrierea unor riscuri suplimentare relevante, identificate de Ofertant, care pot afecta execuția contractului, precum și măsurile asociate de răspuns/atenuare a riscurilor astfel identificate;
b) recomandări suplimentare de reducere/atenuare/eliminare pentru riscurile identificate de autoritatea contractantă, fără afectarea cerințelor caietului de sarcini.

Referitor la riscurile de natură contractuală, identificate la nivelul ambelor părți contractante, Autoritatea contractantă a inclus în modelul de contract clauze de natură să minimizeze aceste riscuri.

5. METODOLOGIE ȘI PLAN DE LUCRU ÎN CADRUL CONTRACTULUI

În această secțiune se va prezenta modul în care Ofertantul înțelege contextul, scopul, obiectivele contractului și sarcinile stabilite de autoritatea contractantă.

Astfel, vor fi descrise soluțiile pe care le propune autorității contractante pentru atingerea obiectivelor contractului și modul de abordare ce va fi urmat pentru atingerea rezultatului.

Se vor avea în vederea respectarea cerințelor funcționale minimale prevăzute în prezentul caiet de sarcini al achiziției.

În cazul în care, oferta este depusă de o asociere, se va descrie implicarea fiecărui asociat în prestarea serviciilor solicitate, a modului de colaborare între asociați în vederea executării contractului, inclusiv prin delimitarea sarcinilor și responsabilităților individuale în prestarea serviciilor, descrierea oricăror aranjamente de subcontractare a unei părți a serviciilor solicitate, a interacțiunii dintre ofertant și subcontractor/i, precum și o descriere detaliată a serviciilor ce vor fi subcontractate.

Ofertanții vor detalia într-o anexă distinctă ***metodologia*** și ***planul de lucru*** ținând cont de informațiile detaliate în prezentul caiet de sarcini și de instrucțiunile pentru ofertanți detaliate în secțiunea ***Modul de prezentare a Propunerii tehnice***.

Metodologia propusă va detalia cel puțin modul de organizare a resurselor propuse de Ofertant pentru obținerea rezultatelor la nivelul cantitativ și calitativ așteptat.

Ofertantul are libertatea de a alege metodologia de planificare și realizare a activităților din Contract fără să se înregistreze abateri de la cerințele minime sau condiționări de orice fel.

Metodologia și planul de lucru sunt componente-cheie și obligatorii ale ofertei tehnice. Oferta tehnică trebuie conțină si următoarele:

a) metodologia pentru realizarea serviciilor;
b) planul de lucru pentru realizarea serviciilor;
c) personalul utilizat pentru realizarea serviciilor și organizarea acestuia.

6.1. Metodologia

În această secțiune trebuie prezentate:

- obiectivele contractului și sarcinile stabilite prin caietul de sarcini;
- modul de abordare ce va fi urmat în prestarea serviciilor, inclusiv descrierea conceptului utilizat pentru atingerea obiectivelor contractului;
- metodologia de realizare a activităților în scopul obținerii rezultatelor așteptate.

Cel puțin următoarele informații trebuie prezentate:

- prevederile legale în domeniul de activitate aferent obiectului contractului ce urmează a fi atribuit, ce pot avea incidență asupra derulării/implementării acestuia;
- identificarea și explicitarea aspectelor-cheie privind îndeplinirea obiectivelor contractului și atingerea rezultatelor așteptate;
- modalitatea de abordare a activităților ce corespund rezultatului final al contractului și a rezultatelor intermediare aferente, în raport cu serviciile și responsabilitățile stabilite prin caietul de sarcini.

Activitățile descrise la acest capitol trebuie reprezentate ca durată, la capitolul aferent din planul de lucru.

6.2. Planul de lucru

Cel puțin următoarele informații trebuie prezentate:
- denumirea și durata activităților și pachetelor de activități din cadrul contractului, așa cum sunt acestea prezentate la capitolul "Metodologie";
- succesiunea și inter relaționarea acestor activități;
- punctele-cheie de control - "jaloanele" proiectului.

Planul de lucru propus trebuie să fie:
1. conform cu abordarea și metodologia propusă;
2. să demonstreze:
   - înțelegerea prevederilor din caietul de sarcini;
   - abilitatea de a transpune prevederile într-un plan de lucru fezabil;
   - încadrarea activităților în timp de așa manieră încât să se asigure finalizarea serviciilor în termenul specificat în caietul de sarcini;
3. realizat utilizând un software de planificare a timpului.

Planul de lucru care va fi prezentat împreună cu oferta trebuie să acopere cel puțin toate tipurile de activități menționate mai sus.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice modalitatea în care se va realiza raportarea progresului pentru activitățile din cadrul proiectului.

Ofertantul trebuie să prezinte în cadrul proiectului modalitatea prin care se va realiza comunicarea între participanții la proiect.

Ofertantul va prezenta în cadrul propunerii tehnice modul în care se va gestiona rezolvarea problemelor care pot să apară pe parcursul proiectului. Se va descrie procesul de management al problemelor și formularele care vor fi utilizate pentru managementul problemelor, escaladarea și rezolvarea acestora.

Ofertantul va prezenta în cadrul propunerii tehnice planul de acceptanță care va fi utilizat în cadrul proiectului pentru recepțiile/acceptanțele parțiale (provizorii) și recepția / acceptanța finală. Se va prezenta planul împărțit pe etape, precum și formularele aferente recepțiilor / acceptanțelor parțiale (provizorii) și recepției/acceptanței finale.

Ofertantul va prezenta în cadrul propunerii tehnice și modalitatea de tratare a schimbărilor în cadrul proiectului. Se va prezenta procedura de management al schimbărilor precum și formularele care vor fi utilizate în cadrul acestui proces pe durata proiectului.

6.3. Personalul utilizat pentru realizarea serviciilor și organizarea acestuia

Cel puțin următoarele informații trebuie prezentate:

- structura echipei propuse pentru managementul contractului;
- modul de abordare a activității de raportare cu privire la progresul serviciilor, inclusiv documentele finale în raport cu prevederile caietului de sarcini;
- descrierea infrastructurii pe care contractorul o utilizează pentru realizarea activităților propuse pentru îndeplinirea obiectului contractului. Această infrastructură trebuie să fie corespunzătoare scopului contractului și să îndeplinească toate cerințele solicitate de legislația în vigoare;
- modul de abordare a activității de identificare a riscurilor ce pot apărea pe parcursul derulării contractului și măsuri de diminuare a riscurilor în raport cu prevederile caietului de sarcini;
- modul de abordare a activităților corespunzătoare îndeplinirii cerințelor privind sănătatea și securitatea în muncă, inclusiv modul în care ofertantul devenit contractor se va asigura că pe parcursul executării contractului obligațiile legale referitoare la condițiile de muncă și protecția muncii sunt respectate (dacă este cazul);
- modul de abordare și gestionare a relației cu subcontractorii, în raport cu activitățile subcontractate (dacă este cazul).

Pentru a demonstra o foarte bună înțelegere a caietului de sarcini metodologia și planul de lucru trebuie să fie adaptate cerințelor specifice ale contractului, fiind descurajate abordările de tip copy-paste.

7. GRAFIC DE PRESTARE PENTRU ACTIVITĂȚILE / SERVICIILE SOLICITATE

Ofertanții vor detalia în propunerea tehnică într-o anexă distinctă ***Graficul de prestare*** ținând cont de informațiile din prezentul caiet de sarcini și de instrucțiunile pentru ofertanți detaliate în *secțiunea Modul de prezentare a Propunerii tehnice*.

Graficul de prestare va fi realizat utilizând un software de planificare a timpului și va cuprinde informații privind:

- denumirea și durata activităților și sub activităților/pachetelor de lucru din cadrul contractului, livrabilele aferente fiecărei activități;
- succesiunea și inter-relaționarea acestor activități;
- punctele-cheie de control - "jaloanele" contractului.

8. LOCUL ȘI DURATA DESFĂȘURĂRII ACTIVITĂȚILOR

8.1. Locul desfășurării activităților

Activitățile necesare în vederea prestării serviciilor de se pot desfășura la sediul Prestatorului sau în alte locații.

Având în vedere natura activităților, activitățile ce fac obiectul contractului se vor desfășura în principal în regim de telemuncă, dar Autoritatea Contractantă își rezervă dreptul de a solicita prezența experților Contractantului la sediul ei, atunci când consideră că este necesar.

8.2. Durata prestării serviciilor

Activitățile din cadrul contractelor subsecvente vor fi demarate începând cu data semnării acestora de ambele parți.

Durata contractului este de 3 luni de la semnarea acestuia de către ambele parți.
Autoritatea contractantă își rezervă opțiunea de a prelungi contractul cu maximum 3 luni. Pentru a exercita această opțiune, Autoritatea contractantă va notifica Contractantului intenția cu 30 de zile înainte de finalizarea contractului sau până la sfârșitul oricărei prelungiri.

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

Ofertanții vor nominaliza specialiștii proprii care vor asigura pe parcursul contractului serviciile prevăzute.

Ofertanții trebuie să aibă capacitatea de a oferi servicii de calitate, sens în care trebuie să dispună de personal calificat pentru prestarea serviciilor raportat la sarcinile fiecărui specialist solicitat, experții fiind un factor important în execuția și finalizarea cu succes a contractului. Este important ca experții propuși să aibă competențe și experiență dovedite, capabil să ducă la bun sfârșit cu succes sarcinile definite prin prezentul caiet de sarcini, astfel ca, în final, să contribuire la îndeplinirea obiectivului general și a obiectivelor specifice ale contractului, în condițiile respectării cerințelor de calitate și a termenelor stabilite și încadrarea în bugetul prevăzut.

În vederea prestării cu succes a serviciilor prevăzute în caietul de sarcini al achiziției, Prestatorul va organiza și va pune la dispoziția Beneficiarului o echipă de experți care, prin atribuțiile și pregătirea lor, vor realiza toate activitățile prevăzute în cadrul contractelor subsecvente aferente acordului cadru.

Prestatorul este responsabil în exclusivitate și integral pentru stabilirea componenței echipei, pentru organizarea tuturor experților propuși, precum și pentru depunerea efortului necesar desfășurării în bune condiții a tuturor activităților solicitate prin prezentul caiet de sarcină.

În cazul necesității de implicare a unor asemenea experți, este în răspunderea Prestatorului:

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

Pentru prestarea serviciilor solicitate prin Caietul de sarcini, Contractantul trebuie să pună la dispoziția autorității contractante o echipă de experți principali (cheie) și secundari (non-cheie), care să dețină competențele necesare fiecărui tip de serviciu solicitat, în calitatea și la momentele de timp relevante.

Funcționarii publici pot fi recrutați ca experți cu respectarea prevederilor art. 96 alin.(1) din Legea nr.161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, cu modificările și completările ulterioare.

Selecția experților trebuie să fie făcută de către Contractant în baza principiilor privind nediscriminarea, tratamentul egal și lipsa unui posibil conflict de interese.

Contractantul este obligat să asigure traducători pe toată durata activităților desfășurate în cadrul contractului, pentru experții care nu sunt vorbitori nativi de limba română sau care nu au cunoștințe avansate de limba română. Costurile aferente traducătorilor sunt incluse în tariful tuturor experților.

În conformitate cu principiul recunoașterii reciproce, beneficiarul 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.

Autoritatea Contractantă are posibilitatea să solicite înlocuirea experților pe perioada derulării contractului, pe baza unei cereri scrise motivate, dacă consideră că un membru al personalului este ineficient sau nu își îndeplinește sarcinile la nivelul cerințelor stabilite.

Nu se acceptă îndeplinirea cerințelor minime aferente unui expert-cheie prin cumul de către mai multe persoane.

Prin aceste cerințe se urmărește obținerea unor servicii de calitate și a unei garanții minime că obiectivul general și obiectivele specifice ale achiziției vor fi îndeplinite.

9.1. Numărul de experți pe categorie de expertiză

Cerințe minime pentru personalul de specialitate / Experți

Ofertantul trebuie să demonstreze accesul la personalul de specialitate de care dispune sau al cărui angajament a fost obținut de către ofertant pentru îndeplinirea corespunzătoare a contractului care urmează a fi atribuit. În acest sens, ofertantul va face dovada că dispune de cel puțin următorii experți care au obligația de a îndeplini următoarele cerințe minime și obligatorii:

Nr.	TIP EXPERT CHEIE	Număr experți
1	Manager de proiect	1
2	Expert analist de business	1
3	Expert arhitect de sistem	1
4	Expert guvernanță și managementul datelor	1
5	Expert administrare și prelucrare date	1
6	Expert securitate cibernetică	1
7	Expert legislație	1
8	Expert protecția datelor	1
9	Expert politici publice	1
10	Expert comunicare	1

Experții cheie au fost solicitați cu respectarea art. 3 din Instrucțiunea președintelui ANAP nr. 1/2017, deoarece activitatea acestora va fi reflectată direct în rezultatul contractului.

9.2. Experți principali (experți cheie)

Ofertanții vor prezenta la nivelul ofertei tehnice, lista cu experții propuși care vor realiza efectiv serviciile din cadrul contractului, în care va enumera persoanele nominalizate și în care va descrie modalitatea prin care experții propuși îndeplinesc cerințele.
Fiecare dintre persoanele propuse pentru rolurile de expert-cheie detaliate mai jos trebuie să îndeplinească integral toate cerințele minime aferente rolului pentru care au fost nominalizate.

Pentru demonstrarea îndeplinirii cerințelor minime și, după caz, pentru obținerea punctajului tehnic, ofertanții trebuie să prezinte, pentru fiecare expert-cheie solicitat din Caietul de sarcini, următoarele informații/documente:

(a) în Propunerea tehnică se va indica numele persoanei propuse pentru fiecare poziție și indicații clare privind paginile unde pot fi regăsite documentele suport anexate aferente fiecărui expert;
(b) anexate la Formularul de Propunere tehnică, pentru fiecare expert cheie se vor prezenta:
   (i) **Curriculum Vitae (CV)**, semnat de către fiecare titular în parte și datat;
   (ii) Documente referitoare la disponibilitatea expertului cheie - Pentru persoanele propuse care au calitatea de salariați ai ofertantului, se va prezenta în mod obligatoriu orice document prin care să se demonstreze relația contractuală dintre expertul-cheie nominalizat și Ofertant (extras Revisal/Contract de muncă etc.). În cazul în care se propune personal care nu este salariat al Ofertantului, pentru îndeplinirea cerinței de disponibilitate se va anexa **o Declarație de disponibilitate semnată de titular**, cu referire strictă la obiectul contractului ce face obiectul prezentei proceduri;
   (iii) Copii documente justificative relevante care demonstrează îndeplinirea cerințelor referitoare la studiile prezentate în CV**: Diplome de studii, certificări, alte diplome relevante**;
   (iv) Copii documente justificative relevante care demonstrează îndeplinirea cerințelor referitoare la expertiza și experiența specifică relevantă solicitată și prezentate în CV**:** Contracte de muncă / Contracte de colaborare / Fișe de post / Adeverințe sau alte documente edificatoare de la beneficiari sau de la angajatori, din care să reiasă în mod clar **denumirea, beneficiarul și perioada de realizare a proiectelor / contractelor** (în care produsele / serviciile / livrabilele au fost recepționate fără obiecții de către beneficiar) **în care expertul propus a acumulat experiența solicitată și activitățile prestate** de către persoana propusă precum și **rolul deținut în proiect**, care să evidențieze **experiența profesională specifică similară**;
   (v) **Recomandări / Declarații** pe proprie răspundere în ceea ce privește experiența expertului. Implicarea și rolul experților în contracte / proiecte care sunt de interes pentru evaluare, poate fi demonstrată și prin recomandări / declarații pe propria răspundere emise de însuși ofertant, dacă și numai dacă acestea sunt însoțite de documente care să demonstreze

relația contractuală dintre expertul propus și emitentul recomandării, la data derulării proiectului referit și orice documente relevante care să demonstreze participarea expertului propus în implementarea contractului/proiectului prezentat drept experiență specifică. În cazul în care se prezintă declarație pe proprie răspundere/recomandare emisă de ofertant, aceasta va cuprinde în mod obligatoriu, pe lângă celelalte informații necesare, următoarea mențiune: *„Cunosc prevederile art. 57 din Regulamentul financiar UE nr.966/2012 și legislația națională în vigoare cu privire la conflictul de interese, precum și prevederile art.292 „Falsul în declarații" din Codul penal potrivit căruia „Declararea necorespunzătoare a adevărului, făcută unui organ sau instituții de stat ori unei alte unități în vederea producerii unei consecințe juridice, pentru sine sau pentru altul, atunci când, potrivit legii ori împrejurărilor, declarația făcută servește pentru producerea acelei consecințe, se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă."*

Prin depunerea ofertei, Ofertantul își asumă răspunderea cu privire la conformitatea cu originalul a oricăror documente depuse în copie.
Certificatele/diplomele/documentele justificative emise în altă limbă decât limba română vor fi prezentate în limba de origine, însoțite de traducerea autorizată în limba română.

În urma verificării exactității informațiilor și a dovezilor furnizate de către ofertanți, autoritatea contractantă poate solicita și alte documente/informații care să clarifice experiența profesională solicitată. De asemenea, autoritatea contractantă își rezervă dreptul de a contacta beneficiarii finali ai proiectelor prezentate la experiența profesională, în vederea confirmării celor prezentate de către ofertanți.
Autoritatea contractantă are dreptul de a verifica exactitatea informațiilor și a dovezilor furnizate de ofertanți și de a solicita și alte documente/ informații care să clarifice experiența profesională respectivă

Ofertanții vor transmite documentele solicitate în caietul de sarcini care certifică îndeplinirea cerințelor minime de calificare, pentru experții cheie.

Înlocuirea experților cheie

Pe parcursul derulării Contractului, modalitatea de înlocuire a personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează conform prevederilor art. 162 din HG nr. 395/2016 și în condițiile clauzelor prevăzute în Contract.

Un membru al echipei de proiect poate fi înlocuit pe parcursul derulării contractului doar cu notificarea prealabilă a beneficiarului cu minim 15 zile înainte de data propusă pentru înlocuire. Notificarea va fi în mod obligatoriu însoțită de documentele justificative asociate noului expert, așa cum au fost acestea solicitate prin documentația de atribuire a contractului. Contractantul are obligația de a se asigura că expertul nou propus îndeplinește toate cerințele minime solicitate de beneficiar pentru expertul înlocuit (precum și toate calificările sau experiența suplimentară care a făcut obiectul evaluării ofertelor), inclusiv condițiile și cerințele cu privire la inexistența unui conflict de interese.

Astfel, înlocuirea experților nominalizați se realizează numai cu acceptul Autorității contractante, această modificare nereprezentând o modificare substanțială, așa cum este aceasta definită în art. 221 din Legea nr. 98/2016, decât în situația în care noul expert nominalizat pentru îndeplinirea contractului nu îndeplinește cel puțin criteriile de calificare solicitate pentru expertul care este înlocuit, așa cum au fost prevăzute în cadrul documentației de atribuire.

În situațiile prezentate anterior, Contractantul are obligația de a transmite pentru noul personal, documentele solicitate prin caietul de sarcini, în vederea demonstrării îndeplinirii cerințelor stabilite prin prezentul caiet de sarcini.

Autoritatea contractantă are dreptul de a respinge motivat noul expert propus, în situația în care constată că acesta nu îndeplinește cerințele minime prevăzute în documentația de atribuire sau constată existența unui conflict de interese.

În cazul în care un membru al personalului Contractantului implicat în implementarea contractului (inclusiv experți cheie și non cheie) trebuie înlocuit, înlocuirea se va face prin raportare la cerințele solicitate prin prezentul caiet de sarcini și oferta depusă, iar dacă experiența/calificarea expertului înlocuit au făcut obiectul aplicării vreunui factor de evaluare și a fost acordat un anumit punctaj, înlocuitorul acestuia trebuie să dețină cel puțin experiența și calificarea corespunzătoare astfel încât după aplicarea algoritmului de calcul al punctajului, expertul înlocuitor să obțină minim punctajul obținut de expertul înlocuit la faza de atribuire a contractului.
Îndeplinirea acestui criteriu (obținerea cel puțin a aceluiași punctaj) este suficientă pentru considerarea ca acceptabil a expertului înlocuitor, din punct de vedere al experienței/calificării. Autoritatea contractantă va putea respinge experții propuși pentru înlocuire sau solicita argumentat înlocuirea experților în situația în care aceștia nu îndeplinesc cerințele/sarcinile precizate în prezentul caiet de sarcini și în ofertă.
Costurile suplimentare generate de înlocuirea personalului incumbă Contractantului. În cazul în care expertul nu este înlocuit imediat şi funcțiile acestuia urmează să fie preluate după o anumită perioadă de timp de către noul expert, Autoritatea contractantă poate solicita Contractantului să desemneze un expert temporar pentru Proiect, până la sosirea noului expert, sau să ia alte măsuri pentru a compensa absența temporară a expertului absent.

Experiența specifică a experților, necesară pentru a îndeplini sarcinile din cadrul contractului de achiziție publică poate fi demonstrată prin îndeplinirea unor activități/servicii similare cu cele pe care urmează să le îndeplinească în prezentul contract.

Profilul, cerințele minime și obligatorii ale experților pe fiecare categorie în parte, se regăsește mai jos:

9.1.1. Manager de Proiect

Condiții:

- ✓ Studii universitare de licență absolvite cu diploma de licență (sau echivalent);

- ✓ Deținerea de cunoștințe în domeniul managementului de proiect dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel național sau internațional;
- ✓ Deținerea de cunoștințe în domeniul managementului de risc (risk management) dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel național sau internațional;
- ✓ Deținerea de cunoștințe în domeniul managementului schimbărilor (change management) dovedite prin prezentarea unei diplome/ certificări recunoscute la nivel național sau internațional;

Atribuții:

- este punctul unic de contact în relația cu Autoritatea contractantă și va avea între atribuțiile sale conducerea unică a echipei de proiect;
- planifică activitatea echipei de proiect;
- stabilește cerințele de management al proiectului;
- monitorizează implementarea proiectului;
- elaborează planul revizuit de activități și urmărește respectarea termenelor proiectului;
- elaborează rapoartele de progres ce vor fi înaintate spre aprobare Autorității contractante;
- supraveghează îndeplinirea de către furnizor a obligațiilor asumate în conformitate cu contractul semnat.

9.1.2. Expert analist de business

Condiții:

- ✓ Studii universitare de licență absolvite cu diploma de licență (sau echivalent);
- ✓ Certificare profesionala in domeniul managementului serviciilor IT dovedite prin certificate recunoscute la nivel național sau internațional;
- ✓ Certificare in domeniul analizei de business software recunoscuta la nivel național sau internațional;
- ✓ Deținerea de competente in domeniul managementului îmbunătățirilor de procese, dovedite prin certificate recunoscute la nivel național sau internațional;

Atribuții:

- activități specifice de analiză și implementare procese de business în cadrul sistemului informatic;
- activități specifice de optimizare a proceselor de business în perioada de analiză a specificațiilor funcționale;
- definirea și implementarea corectă a fluxurilor de business;
- instructaj pentru administratorii sistemului informatic și pentru utilizatorii sistemului informatic din punct de vedere al definirii de noi fluxuri de business sau pentru modificarea celor existente.

9.1.3. Expert arhitect de sistem

Condiții:

- ✓ Studii universitare de licență absolvite cu diploma de licență (sau echivalent);

- ✓ Deținerea de competente avansate in cel puțin un framework de realizare de arhitecturi de tip Enterprise, dovedite prin certificate recunoscute la nivel național sau internațional;
- ✓ Certificare profesionala in domeniul managementului serviciilor IT dovedite prin certificate recunoscute la nivel național sau internațional;
- ✓ Certificare in domeniul analizei de business software recunoscuta la nivel național sau internațional;

Atribuții:

- coordonează echipa tehnica formata din experții tehnici;
- asigura suport managerului de proiect pentru urmărirea respectării termenelor din punct de vedere tehnic;
- definirea soluțiilor detaliate pentru noile subsisteme;
- definirea arhitecturii de integrare a componentelor sistemului;
- activități de implementare, asistență și suport tehnic;
- identificarea riscurilor și problemelor tehnice și a soluțiilor de rezolvare.

9.1.4. Expert guvernanță și managementul datelor

Condiții:

- ✓ Studii universitare de licență absolvite cu diploma de licență (sau echivalent);
- ✓ Certificare profesionala in domeniul managementului serviciilor IT dovedite prin certificate recunoscute la nivel național sau internațional;
- ✓ Certificare in domeniul analizei de business recunoscuta la nivel național sau internațional;
- ✓ Deținerea de competente in domeniul managementului îmbunătățirilor de procese, dovedite prin certificate recunoscute la nivel național sau internațional;

Atribuții:

- dezvoltarea politicilor și standardelor de guvernanță a datelor:
  - crearea și implementarea politicilor de guvernanță a datelor pentru a asigura conformitatea cu reglementările și cerințele organizaționale;
  - stabilirea standardelor și procedurilor pentru colectarea, stocarea, prelucrarea și partajarea datelor;
- managementul calității datelor:
  - dezvoltarea și implementarea unor procese de verificare a calității datelor pentru a asigura acuratețea, consistența și integritatea acestora;
  - colaborarea cu echipele de IT și alte departamente pentru a identifica și corecta erorile de date;
- asigurarea conformității cu reglementările privind protecția datelor:
  - monitorizarea reglementărilor de protecție a datelor, cum ar fi GDPR, și asigurarea că organizația le respectă;
  - colaborarea cu echipele juridice pentru a evalua riscurile și pentru a implementa măsuri de protecție a datelor;
- Implementarea și gestionarea unui cadru de guvernanță a datelor:
  - definirea unui cadru clar pentru guvernanța datelor, inclusiv rolurile și responsabilitățile în ceea ce privește gestionarea datelor;

- implementarea unui sistem de management al datelor care să permită monitorizarea și controlul continuu al acestora;
- analizarea și îmbunătățirea proceselor de management al datelor:
  - evaluarea continuă a proceselor de colectare, stocare și utilizare a datelor pentru a identifica oportunități de îmbunătățire;
  - Crearea de rapoarte și analize periodice privind performanța și conformitatea proceselor de guvernanță a datelor;
- asistență pentru alte departamente:
  - colaborarea cu alte departamente pentru a le ajuta să înțeleagă și să implementeze cerințele de guvernanță a datelor;
  - oferirea de training și suport pentru angajați, ajutându-i să adopte bune practici de gestionare a datelor;
- managementul riscurilor asociate cu datele:
  - identificarea riscurilor potențiale în ceea ce privește securitatea, accesibilitatea și integritatea datelor;
  - implementarea unor măsuri preventive și de răspuns pentru a reduce riscurile de securitate și pierderi de date;
- crearea de raportări și metrici de guvernanță a datelor:
  - dezvoltarea unor indicatori de performanță pentru a măsura succesul guvernanței și managementului datelor;
  - raportarea către conducere cu privire la starea guvernanței datelor și recomandarea unor măsuri de îmbunătățire.

9.1.5. Expert testare

Condiții:

- ✓ Studii universitare de licență absolvite cu diploma de licență (sau echivalent);
- ✓ Certificare profesionala in domeniul testării software recunoscuta la nivel național sau internațional;
- ✓ Certificare in domeniul dezvoltării software într-un limbaj de programare recunoscuta la nivel național sau internațional

Atribuții:

- colectarea și stocarea datelor:
  - colectarea și organizarea datelor din surse variate, asigurându-se că acestea sunt corecte și complete;
  - implementarea procedurilor de stocare a datelor într-o manieră eficientă și sigură, utilizând baze de date și alte soluții de stocare;
- administrarea bazelor de date:
  - gestionarea bazei de date, inclusiv configurarea, optimizarea și monitorizarea performanței acesteia;
  - asigurarea securității datelor și controlul accesului utilizatorilor pentru a preveni accesul neautorizat;
- prelucrarea și transformarea datelor:
  - transformarea datelor brute în informații structurate, curățarea datelor de erori și inconsecvențe;
  - aplicarea de procese ETL (Extract, Transform, Load) pentru a integra datele din diverse surse în sisteme centralizate;
- asigurarea calității datelor:

    - implementarea și monitorizarea unor proceduri de control al calității datelor pentru a garanta acuratețea, completitudinea și consistența acestora;
    - identificarea și corectarea erorilor sau lacunelor din date, colaborând cu alte echipe pentru a menține standardele de calitate;
- optimizarea și securitatea datelor:
    - optimizarea bazelor de date pentru performanță maximă și reducerea timpilor de răspuns;
    - implementarea măsurilor de securitate pentru a proteja datele împotriva pierderii, accesului neautorizat sau atacurilor cibernetice;
- automatizarea și îmbunătățirea proceselor de prelucrare a datelor:
    - dezvoltarea și implementarea unor scripturi și procese automate pentru colectarea și prelucrarea datelor;
    - îmbunătățirea continuă a proceselor de lucru pentru a reduce erorile manuale și a spori eficiența;
- analizarea și raportarea datelor:
    - analizarea datelor și crearea de rapoarte sau vizualizări care să ofere informații relevante pentru luarea deciziilor;
    - colaborarea cu departamentele de business pentru a le ajuta să înțeleagă datele și să extragă informații valoroase;
- colaborarea cu echipele de dezvoltare și analiză:
    - colaborarea cu echipele de IT și de analiză pentru a asigura integrarea și prelucrarea corespunzătoare a datelor în sistemele de business;
    - sprijinirea echipelor de analiză prin furnizarea datelor necesare și optimizarea accesului la acestea;
- documentarea și întreținerea proceselor de prelucrare a datelor:
    - documentarea tuturor proceselor și procedurilor legate de administrarea și prelucrarea datelor;
    - menținerea documentației la zi și asigurarea că toți utilizatorii cunosc procedurile corecte de accesare și utilizare a datelor;
- învățare și adaptare continuă la noi tehnologii și instrumente de date:
    - menținerea la curent cu tendințele și tehnologiile noi în domeniul gestionării și prelucrării datelor;
    - participarea la cursuri de formare și adaptarea la noi tehnologii pentru a asigura eficiența și securitatea proceselor.

9.1.6. Expert securitate cibernetică

Condiții:

- Studii superioare finalizate cu diplomă de licență (sau echivalent);
- Experiență specifică demonstrată prin participarea în cel puțin un proiect cu componentă IT, în care a avut responsabilități specifice rolului de EXPERT SECURITATE CIBERNETICĂ;
- Deținerea de cunoștințe dovedite în domeniul gestiunii securității informațiilor, evaluării riscului, securității rețelei, testarea și respectarea normelor legale și de reglementare în securitate cibernetică**, prin prezentarea unei diplome/certificări recunoscute la nivel național (DNSC)/internațional**;
- Deținerea de cunoștințe dovedite în testarea vulnerabilităților, dovedite prin prezentarea unei diplome / certificări recunoscute la nivel național / internațional.

Atribuții:

- analiza cerințelor de business;
- realizarea documentelor de specificații funcționale și a scenariilor de testare;
- activități de implementare, asistenta și suport tehnic;
- activități pentru monitorizarea performanței funcționării infrastructurii HW și SW (servere, baze de date, servere aplicații) utilizate pentru rularea platformei pentru prevenirea breșelor de securitate cauzate de blocarea / indisponibilitatea funcționării infrastructurii HW și SW care deservesc platforma de gestiune a accesului utilizatorilor și a securității sistemului;
- suport acordat utilizatorilor cheie pentru testarea de acceptanță a sistemului

9.1.7. Expert protecția datelor

Condiții:

- Studii universitare absolvite cu diplomă de licență (sau echivalent);
- Experiență specifică demonstrată prin participarea în cel puțin un proiect/contract în care a realizat activități similare;
- Deținerea de cunoștințe probată prin prezentarea unei certificări recunoscută la nivel național/internațional, care atestă competențele și cunoștințele profesionale ale unui specialist în soluții de protecție a datelor, respectiv abilități de proiectare, implementare și gestionare soluții eficiente de protecție a datelor, respectând standardele și reglementările relevante în domeniul protecției datelor.

Atribuții:

- implementarea politicilor și procedurilor de protecție a datelor:
  - dezvoltarea, implementarea și monitorizarea politicilor de protecție a datelor pentru a se asigura conformitatea cu legislațiile relevante, cum ar fi GDPR;
  - crearea și actualizarea procedurilor interne privind colectarea, stocarea și procesarea datelor cu caracter personal;
- asigurarea conformității cu reglementările de protecție a datelor:
  - monitorizarea respectării legislației și reglementărilor privind protecția datelor în toate operațiunile și activitățile organizației;
  - evaluarea conformității organizației cu cerințele de protecție a datelor și recomandarea măsurilor necesare pentru a remedia eventualele deficiențe;
- gestionarea riscurilor legate de datele cu caracter personal:
  - efectuarea evaluărilor de impact asupra protecției datelor (DPIA) pentru a identifica și evalua riscurile asociate procesării datelor personale;
  - implementarea de măsuri preventive și corective pentru a reduce riscurile de breșe de securitate și pierderi de date;
- formarea și informarea personalului privind protecția datelor:
  - oferirea de training-uri periodice pentru angajați pe teme de protecție a datelor și securitatea informațiilor personale;
  - informarea echipelor despre importanța protejării datelor și despre bunele practici de gestionare a acestora;
- asistență în gestionarea cererilor de acces și rectificare a datelor:
  - gestionarea cererilor din partea persoanelor vizate pentru accesul, rectificarea, ștergerea sau portabilitatea datelor lor;
  - asigurarea că toate cererile sunt tratate în termenul prevăzut de lege și în conformitate cu cerințele legale;

- monitorizarea și raportarea breșelor de securitate:
  - monitorizarea și documentarea tuturor incidentelor de securitate care pot afecta datele personale;
  - raportarea breșelor de securitate relevante către autoritățile de reglementare și către persoanele afectate, conform cerințelor legale;
- asigurarea confidențialității și securității datelor:
  - colaborarea cu echipele de securitate IT pentru a implementa măsuri de securitate cibernetică și de confidențialitate a datelor;
  - evaluarea și îmbunătățirea continuă a măsurilor de securitate, cum ar fi criptarea, autentificarea și controlul accesului;
- realizarea auditului de protecție a datelor:
  - efectuarea de audituri interne periodice pentru a evalua conformitatea cu politicile de protecție a datelor și cerințele legale;
  - documentarea și corectarea eventualelor deficiențe identificate în urma auditului;
- documentarea proceselor de prelucrare a datelor:
  - crearea și menținerea documentației privind activitățile de prelucrare a datelor, inclusiv registrele de evidență a activităților de prelucrare;
  - asigurarea că documentația este actualizată și ușor accesibilă pentru controale sau inspecții;
- gestionarea relației cu autoritățile de reglementare:
  - menținerea unei relații constructive cu autoritățile de protecție a datelor și răspunderea la solicitările acestora;
  - furnizarea de informații și rapoarte către autorități în cazul investigațiilor legate de protecția datelor.

9.2. Experți secundari (experți non-cheie)

Ofertanții au dreptul de a include în oferte și alți experți în afara celor indicați în caietul de sarcini al achiziției, în cazul în care consideră că aceștia sunt necesari în vederea bunei derulări a contractelor subsecvente și a atingerii obiectivelor acestora.

Ofertantul poate propune experți și personal suport în afara celor solicitați, fără a-i nominaliza, însă cuprinzând în Propunerea tehnică activitățile lor, făcând dovada unei planificări realiste menite să asigure realizarea livrabilelor contractului.

Experții non-cheie vor lucra în permanență sub coordonarea experților cheie nominalizați.

Pentru experții non-cheie, Ofertantul va prezenta numai informații privind modul de implicare a acestora în activitățile proiectului, responsabilitățile și momentul implicării, precum și metodologia care va fi utilizată pentru identificarea/recrutarea acestora și includerea în echipa de proiect în momentele necesare.

Pentru experții non-cheie NU este necesară prezentarea în cadrul Propunerii Tehnice nici a identității exacte a acestora și nici a vreunui document suport.

9.3. Personalul administrativ și personalul suport / backstopping pentru activitatea experților principali în cadrul Contractului

Contractantul va asigura personalul administrativ/suport care este necesar pentru desfășurarea activității echipei sale.

De asemenea, dacă Ofertantul consideră că pe lângă experții solicitați de autoritatea contractantă, sunt necesari și alți experți pentru îndeplinirea corespunzătoare și la timp a activităților prevăzute în Caietul de sarcini, acesta are obligația să prevadă aceste resurse și să includă în propunerea financiară costurile aferente.

În plus, Contractantul va asigura pentru serviciile din contract, personal de backstopping pentru prestarea serviciilor.

Prin personal de backstopping se înțelege personal de înaltă calificare al Contractantului care acordă sprijin echipei de experți implicați în derularea activităților în Contract. Sprijin înseamnă orice activitate care contribuie la îndeplinirea serviciilor conform Contractului.

9.4. Infrastructura Contractantului, necesară pentru desfășurarea activităților Contractului

Ofertantul devenit Contractant trebuie să se asigure că personalul care își desfășoară activitatea în cadrul Contractului dispune de sprijinul material și de infrastructura necesară pentru a permite acestuia să se concentreze asupra realizării activităților din cadrul Contractului, respectiv dispune de computer cu licențe și acces la internet, produse de birotică, utilități etc. Toate costurile vor fi incluse în costurile unitare ofertate, nefiind decontate separat.

Ofertantul va prezenta în propunerea tehnică o listă cu dotările existente sau a aranjamentelor întreprinse pentru a avea acces la dotările necesare pentru o bună implementare a contractului.

9.5. Infrastructura și resursele disponibile la nivel de Autoritate Contractantă pentru îndeplinirea Contractului

Autoritatea contractantă va desemna o persoană de contact ce va fi interlocutorul privilegiat în raport cu Contractantul.

Totodată, autoritatea contractantă va aloca personal implicat în procesele de recepție calitativă și cantitativă a serviciilor prestate.

10. MANAGEMENTUL CONTRACTULUI ȘI ACTIVITĂȚI DE RAPORTARE

Managementul contractului include o componentă de management și o componentă administrativă (de administrare efectivă a contractului) și presupune coordonarea continuă, monitorizarea și controlul tuturor activităților și rezultatelor realizate de Contractant.

Contractantul este pe deplin responsabil de managementul contractului din punct de vedere administrativ, financiar, orientat spre obținerea rezultatelor. Acesta trebuie să respecte toate condițiile formulate în prezentul caiet de sarcini.

Pe parcursul derulării Contractului, Autoritatea contractantă verifică la intervale stabilite și comunicate prin Caietul de sarcini dacă toate activitățile planificate au fost realizate conform cerințelor.

10.1. Gestionarea relației dintre Contractant și Autoritatea Contractantă

Contractantul va adopta o atitudine constructivă (pro-activă), caracterizată de agilitate, în îndeplinirea obiectivelor contractului, demonstrând capacitatea de a se adapta modificărilor din proiectul în care este implicat. Contractantul trebuie să consulte Autoritatea contractantă cu privire la orice aspect/ problemă care apare în procesul de implementare, evitând implicarea acesteia în aspecte de micro management al Contractului.

10.1.1. Ședințe / întâlniri

Un instrument în derularea activității de monitorizare vor fi ședințele/întâlnirile dintre echipa Contractantului și echipa Autorității contractante, ședințe care au drept scop și urmărirea progresului Contractului.

Pentru buna desfășurare a activităților și atingerea rezultatelor proiectului, Contractantul va colabora permanent cu echipa de implementare a proiectului.

În termen de 3 zile lucrătoare de la data începerii contractului, va fi organizată o întâlnire de lucru la care vor participa reprezentanți ai Autorității contractante (membrii echipei de implementare a proiectului), pentru obținerea asigurării că Autoritatea Contractantă și Contractantul au aceeași perspectivă asupra activităților și rezultatelor din Contract.
Autoritatea contractantă va organiza prima întâlnire de lucru la care vor participa reprezentanți ai Autorității contractante și ai Contractantului (cel puțin expertul cheie desemnat ca responsabil de contract). În cadrul acestei întâlniri se va pune la dispoziția contractantului datele de care dispune Autoritatea contractantă necesare prestării serviciilor.
Responsabilă de organizarea întâlnirii este Autoritatea contractantă.
În cadrul acestei întâlniri vor fi stabilite următoarele:
(a) principiile de comunicare reciprocă;
(b) planul de lucru;

(c) detaliile privind colaborarea;
(d) frecvența reuniunilor;
(e) modelele de procese-verbale;
(f) modelele de rapoarte privind progresele înregistrate;
(g) planurile de acțiune în cazul apariției unor probleme;
(h) alte detalii logistice și organizaționale.

Alte întâlniri / ședințe care ar putea fi desfășurate pe parcursul derulării contractului:
(a) ședințe periodice de monitorizare și control al progresului în cadrul contractului și evaluarea stadiului contractului, la un interval de o lună, pe perioada desfășurării contractului. Frecvența acestora poate fi modificată în funcție de situațiile specifice ce ar putea apărea;
(b) întâlniri ad-hoc de rezolvare a unor probleme specifice care pot fi stabilite/planificare într-un termen scurt, ceea ce înseamnă că trebuie să existe disponibilitatea contractantului în termen de 1 zi lucrătoare de la solicitare pentru întâlnirile online și 3 (trei) zile lucrătoare de la solicitare pentru întâlnirile în format fizic.

Rezultatele ședințelor vor fi documentate în minute de ședință întocmite de Contractant și validate de autoritatea contractantă. Ședințele se vor desfășura, în funcție de context, fie virtual (teleconferințe/videoconferințe) atunci când nu este necesară prezența fizică a Contractantului la fiecare întâlnire/ședință, fie fizic, prin prezența Contractantului la sediul autorității contractante.
Participarea reprezentanților Contractantului la ședințe / reuniuni / întâlniri nu va genera costuri suplimentare pentru Autoritatea contractantă, față de cele indicate în propunerea financiară.

10.1.2. Modalitatea de abordare a eventualelor cereri de schimbare / modificări nesubstanțiale

Contractantul are obligația de a informa Autoritatea contractantă permanent și în mod corect despre evoluția contractului. Pe baza informațiilor furnizate de Contractant și în baza analizei actorilor implicați în gestionarea proiectului, autoritatea contractantă poate decide modificarea/completarea anumitor detalii legate de implementarea Contractului, în situația în care acest lucru se impune.

Părțile contractante au dreptul, pe durata valabilității Contractului, de a conveni modificarea și/sau completarea clauzelor acestuia, fără organizarea unei noi proceduri de atribuire, cu acordul părților, fără a afecta caracterul general al contractului, în limitele dispozițiilor prevăzute de art. 221 și art. 222 din Legea nr. 98/2016.

Modificările nesubstanțiale sunt singurele modificări ale Contractului care pot fi făcute fără organizarea unei noi proceduri de atribuire.

Modificările contractuale nu trebuie să afecteze, în niciun caz și în niciun fel, rezultatul procedurii de atribuire, prin anularea sau diminuarea avantajului competitiv pe baza căruia Ofertantul a fost declarat câștigător în cadrul procedurii de atribuire.

Ofertantul va prezenta în cadrul propunerii tehnice modalitatea de tratare a schimbărilor în cadrul Contractului.

10.2. Raportare

Contractantul este responsabil de elaborarea și transmiterea rapoartelor către Autoritatea Contractantă.
Rapoartele /documentele solicitate sunt prevăzute în tabelul de mai jos și acestea pot fi semnate cu semnătură olografă sau cu semnătură electronică.

Identificare Raport solicitat	**Conținut Raport solicitat**	**Momentul transmiterii Raportului** (varianta de lucru, sau varianta finală, după caz)
Raport la începerea activității prestării serviciilor	Analizarea situației existente prin raportare la data efectivă de începere a activității în cadrul Contractului	În termen de **cel mult 10 zile** de la începerea realizării activităților
Raport de progres al activităților în cadrul Contractului	Se vor elabora rapoarte lunare conform perioadei de prestare a serviciilor	**Rapoarte lunare**
Raport final	Raportul final va cuprinde o analiză a situației la finalul Contractului prin raportare la conținutul Raportului inițial, al evoluției înregistrate prin prestarea serviciilor	La finalizarea contractului

Anterior convocării oricărei recepții și, implicit anterior emiterii oricărei facturi, **Contractantul** va elabora raportul de progres, în care va preciza cel puțin:

a) detalii tehnice cu privire la activități derulate și rezultate obținute în termeni cantitativi și calitativi;
b) detalii financiare referitoare la toate cheltuielile efectuate, cu respectarea categoriilor de cheltuieli și a prețurilor unitare conform propunerii financiare;
c) detalii referitoare la măsurile întreprinse pentru prevenirea/evitarea conflictului de interese;
d) dificultățile întâmpinate în cursul implementării activităților și soluțiile propuse pentru a depăși respectivele dificultăți, dacă este cazul;
e) întârzieri înregistrate, dacă este cazul;
f) recomandări/propuneri de planificare a activităților pentru perioada următoare,

dacă este cazul;
g) alte informații solicitate de către autoritatea contractantă/organismul intermediar.

10.2.1. Transmiterea și aprobarea rapoartelor

Rapoartele trebuie transmise la datele de contact din Contract în atenția Managerului de Contract desemnat din partea Autorității contractante.

Variantele intermediare, de lucru, vor fi transmise Autorității Contractante în format electronic editabil.

Variantele finale vor fi transmise atât în format editabil, cât și în format .pdf semnate cu semnătură electronică.

Aprobarea rapoartelor se face de către Comisia de recepție desemnată de Autoritatea Contractantă.

10.3. Recepția serviciilor / Acceptarea rezultatelor în cadrul Contractului

Recepția serviciilor se face în baza Certificatului de acceptanță și a Procesului verbal de recepție întocmit Beneficiar, în urma transmiterii de către Prestator a rapoartelor lunare.

Recepția livrabilelor trimise de către Prestator va consta în:
- identificarea serviciilor prestate;
- verificarea respectării condițiilor de prestare conform specificațiilor din caietul de sarcini;
- constatarea eventualelor neconcordante;

Acceptarea rezultatelor/livrabilelor obținute din derularea Contractului se finalizează prin semnarea, după caz, a proceselor-verbale de recepție parțială / finală.

Dreptul achizitorului de a verifica, dacă este necesar, de a respinge serviciile, nu va fi limitat sau amânat din cauza faptului că serviciile au fost verificate de Contractant.

Recepția serviciilor se va efectua pe baza de proces verbal semnat de contractant și reprezentanții autorității contractante. Reprezentantul Contractantului va semna procesele verbale pentru luare la cunoștință și posibilitatea de a prezenta eventuale explicații și/sau observații.

Procesul verbal de recepție parțială atestă îndeplinirea parțială de către Contractor a obligațiilor prevăzute în Caietul de sarcini, respectiv faptul că serviciile au fost prestate corespunzător. Documentul „proces verbal de recepție parțială” nu va fi emis dacă un serviciu a fost respins de către Autoritatea Contractantă și ulterior nu a mai fost acceptat/aprobat printr-un nou proces verbal de recepție.

Procesul verbal de recepție finală se emite de regulă în baza proceselor verbale de recepție parțială și reprezintă acordul final al Autorității contractante cu privire la întregul Contract.

Procesul verbal de recepție calitativă și cantitativă va include unul din următoarele rezultate:

- **admiterea recepției** cu sau fără obiecții;
- **suspendarea recepției**;
- **respingerea recepției** (dacă se constată vicii care nu pot fi remediate și care, prin natura lor, împiedică realizarea uneia sau a mai multor exigențe esențiale).

Autoritatea Contractantă, în urma recepției, va aproba rapoartele/livrabilele sau va prezenta observațiile sale în termen de maximum 10 zile lucrătoare de la primirea lor.

În cazul unor modificări, Contractantul are obligația de a răspunde pozitiv solicitărilor Autorității Contractante de modificare/completare a rapoartelor/livrabilelor, corespunzător cu observațiile Autorității Contractante, în termen de maximum **5 zile lucrătoare** de la data primirii acestora. Autoritatea Contractantă, prin recepție, va proceda la aprobarea sau respingerea rapoartelor, după caz, în termen de **15 zile lucrătoare** de la data primirii acestora în forma revizuită, termen care poate fi prelungit în funcție de situațiile specifice.

Comisia de recepție recomandă **suspendarea recepției** când:

(a) se constată existența unor neconformități, neconcordanțe ori deficiențe care sunt de natură să afecteze calitatea serviciului conform scopului, dar care pot fi remediate;
(b) se constată existența unor servicii realizate necorespunzător sau nefinalizate, care pot afecta cerințele fundamentale aplicabile, dar care pot fi remediate/finalizate;
(c) se constată existența, în mod justificat, a unor suspiciuni rezonabile cu privire la calitatea serviciilor și este necesară realizarea unor verificări aprofundate pentru a le clarifica;
(d) contractantul nu pune la dispoziția comisiei de recepție documentele prevăzute în contract și caietul de sarcini.

În cazul în care comisia de recepție decide suspendarea procesului de recepție, aceasta încheie un proces-verbal de suspendare a procesului de recepție în care consemnează decizia de suspendare, măsurile recomandate în scopul remedierii aspectelor constatate, precum și termenul de remediere, iar autoritatea contractantă comunică Contractantului decizia comisiei în maximum 3 zile lucrătoare de la luarea la cunoștință a procesului-verbal de suspendare a procesului de recepție, împreună cu un exemplar al acestuia.

Termenul de remediere acordat de comisia de recepție va fi stabilit în funcție de neconformitatea constatată, fiind cuprins între min. 1 (una) și max. 15 zile lucrătoare, calculate de la momentul aducerii la cunoștință a procesului-verbal de suspendare a procesului de recepție. În cazul în care Contractantul nu remediază aspectele constatate și nu adoptă măsurile recomandate în cadrul procesului-verbal de suspendare a procesului de recepție în termenul stabilit, comisia de recepție va decide respingerea recepției.

Pentru evaluarea livrabilelor/rezultatelor intermediare/finale Autoritatea Contractantă utilizează ca date de intrare informații din:

(a) cerințele din Caietul de Sarcini;
(b) informațiile furnizate în Propunerea tehnică pentru a demonstra îndeplinirea cerințelor, pentru aplicarea criteriului de atribuire și orice alte beneficii oferite de Contractant pentru obținerea avantajului competitiv pe perioada evaluării;
(c) contract;
(d) documentele /rapoartele/ puse la dispoziție de Contractant;
(e) orice alte evidențe considerate relevante pentru analiza livrabilelor/ rezultatelor intermediare/finale.

În cazul în care calificativul obținut se încadrează în categoria nesatisfăcător sau foarte nesatisfăcător, autoritatea contractantă **respinge recepția**, Contractantul nefiind în drept să primească plată pentru serviciile prestate.

10.4. LIVRABILE pentru serviciile prestate

În maxim 5 zile lucrătoare de la sfârșitul perioadei de prestare lunară, Prestatorul transmite responsabilului de contract al Beneficiarului raportul de activitate în care va consemna atât detaliat cât și sintetic activitățile și serviciile prestate.

Forma și structura acestor liste și rapoarte va fi stabilită și adoptată de reprezentanții celor două părți, imediat după semnarea contractului.

Raportul, împreuna cu anexele sale, va fi transmis comisiei de acceptanță de către responsabilul de contract al Beneficiarului, după ce acesta va fi verificat și adoptat de echipa de suport tehnic a Beneficiarului. În cazul unor neconformități de formă, responsabilul de contract al Beneficiarului poate solicita Prestatorului printr-o notificare scrisă, remedierea acestora.

Prestatorul va remedia neconformitățile semnalate și va transmite o nouă versiune a raportului în maximum 5 zile lucrătoare, de la data notificării.

Principalele activități și livrabile ce trebuie avute în vedere de Prestator în cadrul acestui contract, dar fără a se limita la acestea, sunt cele prevazute la cap 3.3.2. Etapele de implementare a sistemului informatic

Pentru administrarea, configurarea și utilizarea Componentelor descrise in capitolele anterioare, următoarele livrabile vor fi furnizate în cadrul proiectului:
1. Cod Sursă (dacă este cazul)
    - Codul sursă al modulului va fi livrat la finalul proiectului, împreună cu drepturile de proprietate intelectuală transferate beneficiarului.
    - Codul sursă va fi complet comentat, iar limba utilizată pentru comentarii va fi romana sau engleza, asigurând claritatea și ușurința de înțelegere.
    - Beneficiarul va avea dreptul de a modifica și extinde codul sursă după finalizarea prestării tuturor serviciilor aferente contractului.
2. CI/CD Configurat (dacă este cazul)
    - Sistemul de integrare și livrare continuă (CI/CD) va fi configurat pentru gestionarea și asamblarea noilor versiuni ale aplicației.
    - Include scripturi de build, testare automată și implementare.
3. Ghidul Utilizatorului

Document destinat operatorilor modulelor.

- Include instrucțiuni despre cum să utilizeze modulul livrat in cadrul proiectului

4. Ghidul Administratorului

Ghid detaliat adresat administratorului tehnic, incluzând:

- Proceduri pentru configurarea, reantrenarea, îmbunătățirea și întreținerea modulului.
- Gestionarea utilizatorilor și permisiunilor.
- Monitorizarea performanței și depanarea problemelor.

5. Procedura de Instalare

Ghid cuprinzător pentru instalarea și configurarea sistemului, incluzând:

- Cerințe preliminare (prerequisites).
- Pașii de instalare și configurare.
- Set minimal de teste pentru validarea funcționării corecte.

6. Document de Arhitectură și Design

Include o descriere completă a arhitecturii sistemului, cu detalii despre:

- Tehnologiile utilizate.
- Componentele logice și fizice ale soluției.
- Mod de conectare și comunicare între componente.
- Protocoale de comunicație utilizate.
- Componente terțe folosite și pattern-uri aplicate, dacă este cazul.

7. Documentația Bazei de Date

Document cuprinzător despre structura bazei de date, incluzând:

- Diagrama bazei de date.
- Descrierea tabelelor și semnificația câmpurilor.
- Relațiile dintre tabele și denormalizări (dacă există).
- Strategii de securizare, autentificare și autorizare.
- Strategii de indexare și constrângeri.
- Elemente de programabilitate (proceduri stocate, funcții, view-uri).

8. Documentație API

Document care descrie toate punctele finale ale API-ului modulului, incluzând:

- Metodele suportate (de exemplu: GET, POST, PUT, DELETE).
- Structura cererilor și răspunsurilor.
- Parametrii necesari și codurile de eroare.
- Exemple de utilizare.

9. Rapoarte de Testare și Validare

- Include rezultatele testelor de funcționalitate, performanță, securitate și integrare.
- Ghid pentru replicarea testelor și validarea funcționalităților modulului.

10. Manual de Configurare CI/CD (dacă este cazul)

Include pașii detaliați pentru configurarea și ajustarea procesului CI/CD, oferind suport pentru personalizarea viitoare.

11. Set de Date pentru Testare

Set de date și cazuri de test relevante pentru validarea funcționalității modulului în condiții simulate.

Modulul va fi instalat în cadrul platformei, configurat și testat și va fi predat către achizitor o dată cu punerea în funcțiune a întregii platforme.

10.5. Finalizarea serviciilor în cadrul Contractului

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

(a) toate cerințele cuprinse în Caietul de Sarcini au fost îndeplinite;
(b) rezultatele/rapoartele au fost aprobate de Autoritatea Contractantă, pe baza cerințelor incluse în Contract;
(c) procesul verbal de recepție finală a fost aprobat fără obiecțiuni de către Autoritatea Contractantă.

În cazul în care calificativul final obținut se încadrează în categoria nesatisfăcător sau foarte nesatisfăcător, autoritatea contractantă emite documentul constatator cu selectarea opțiunii de neîndeplinire a obligațiilor contractuale.

10.6. Monitorizarea realizării activităților și a rezultatelor pe perioada derulării Contractului

În sensul prezentului caiet de sarcini următorii termeni au sensul definit mai jos:

- **monitorizarea** este activitatea de colectare de date și informații cu privire la modul de implementare a activităților contractului, vizând atât aspecte cantitative, cât și calitative;
- **controlul** implică identificarea acțiunilor preventive și corective pentru abordarea abaterilor de la condițiile contractuale.

Ofertantul va include în Propunerea tehnică detalii referitoare la modul concret prin care acesta va asigura monitorizarea și controlul activităților și rezultatelor prevăzute de Contract.

Pentru monitorizarea activității Contractantului, autoritatea contractantă va avea în vedere următoarele aspecte:

(a) Contractantul și-a îndeplinit atribuțiile, așa cum reies acestea din cadrul prezentului caiet de sarcini, iar rezultatele contractului au fost atinse;
(b) Contractantul a respectat termenele de realizare a activităților contractului și a predat la timp livrabile;
(c) Contractantul a respectat cerințele minime ale caietului de sarcini și asumate prin propunerea tehnică cu privire la forma și calitatea livrabilelor contractului;
(d) Contractantul a respectat obligațiile contractuale prin raportare la termenii contractului de finanțare.

Monitorizarea se va realiza pe tot parcursul proiectului, iar controlul se va realiza cel puțin trimestrial.
Contractantul are obligația de a furniza date și informații corecte, complete și la timp pentru a facilita activitatea de monitorizare și control.

10.7. Asigurarea calității

Ofertantul trebuie să prezinte în cadrul propunerii tehnice o descriere a modului concret de asigurare și control al calității proceselor pe care le derulează în cadrul Contractului.

Ofertantul trebuie să aloce în planul detaliat de implementare timpi suficienți de verificare și validare din punct de vedere calitativ pentru serviciile prestate și pentru revizuirea livrabilelor/documentelor rezultate.

Contractantul va presta serviciile descrise în prezentul caiet de sarcini, asigurând un standard de calitate ridicat și va gestiona toate aspectele administrative și de organizare în vederea realizării serviciilor descrise în prezentul caiet de sarcini.

10.8. Evaluarea performanței Contractantului

Pentru activitățile și rezultatele relevante pentru îndeplinirea obiectului contractului autoritatea contractantă definește nivelurile de performanță prezentate în continuare.

Este important ca performanța să fie monitorizată în mod regulat atât de către Contractant, cât și de către Autoritatea contractantă, iar acțiunile corective să fie implementate în cazul în care rezultatele nu ating nivelul așteptat. În acest sens, Contractantul va ține evidența valorilor asociate indicatorilor de performanță și va include informații referitoare la nivelul de performanță înregistrat în toate rapoartele și documentele întocmite pentru realizarea întâlnirilor de pe durata derulării contractului, așa cum sunt acestea descrise în caietul de sarcini.
Autoritatea Contractantă utilizează indicatorii de performanță de mai jos:

10.8.1. Termenele de prestare

Indicator	Descrierea indicatorului
Categorie indicator	Tehnic - nivel de calitate
Denumire indicator de performanță	Termenele de predare a rezultatelor / livrabilelor contractului
Nivelul de performanță așteptat	Livrabil/rezultat final predat în termenul agreat
Formula de calcul	Se compară termenul efectiv de prestare cu termenul/termenele convenite în graficul de prestare aprobat
Modalitatea de evaluare	**Calificativele vor fi acordate** după cum urmează: **Foarte satisfăcător (5 PUNCTE)** - Livrabil/rezultat predat în termenele convenite **Satisfăcător (4 PUNCTE)** - Livrabil/rezultat predat imediat după încheierea termenelor convenite însă fără întârzierea activităților din calendarul general al proiectului. **Acceptabil (3 PUNCTE** - Livrabil/rezultat predat după încheierea termenelor convenite conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate.

	Nesatisfăcător (2 PUNCTE) –Livrabil/rezultat predat cu mult după încheierea termenelor convenite conducând la întârzieri ale activităților din calendarul general al proiectului pentru mai mult de *30 de zile*. **Foarte nesatisfăcător (1 PUNCT)** –Livrabil/rezultat predat cu mult după încheierea termenelor convenite conducând la întârzieri majore ale activităților din calendarul general al proiectului pentru mai mult de *60 de zile*.

În cazul în care calificativul obținut se încadrează în categoria nesatisfăcător sau foarte nesatisfăcător, autoritatea contractantă respinge recepția, Contractantul nefiind în drept să primească plată pentru serviciile prestate.

11. BUGETUL CONTRACTULUI ȘI EFECTUAREA PLĂȚILOR ÎN CADRUL CONTRACTULUI

Valoarea estimată a serviciilor este:

Nr. crt.	SERVICII	VALOARE ESTIMATĂ
1	Servicii de dezvoltare soluție Platforma de Jurnalizare si Notificare	**5.000.000,00lei fără TVA**

Se estimează realizarea de plăți în baza rapoartelor întocmite de Contractant conform prevederilor caietului de sarcini.
Contractantul va emite facturile în sistemul Ro-eFactura, potrivit prevederilor OUG nr. 120/2021, aprobată cu modificări prin Legea nr. 139/2022, pentru produsele livrate și acceptate.
Plățile în favoarea contractantului se vor efectua în lei în termen de 30 de zile de la data înregistrării facturilor fiscale de către autoritatea contractantă, însoțite de toate documentele justificative.
Fiecare factură va avea menționat numărul contractului, datele de emitere și de scadență ale facturii respective.
Factura va fi emisă după admiterea recepției cantitative și calitative și semnarea de către autoritatea contractantă a procesului verbal de recepție cantitativă și calitativă fără obiecții. Procesul verbal/Procesele verbale de recepție calitativă și cantitativă va/vor însoți factura și reprezintă elementul necesar realizării plății.

12. METODOLOGIA DE EVALUARE A OFERTELOR PREZENTATE

Criteriul de atribuire: **cel mai bun raport calitate preț**.
Având în vedere criteriul de atribuire stabilit, oferta câștigătoare se va determina după cum urmează:

12.1. Componenta financiară

Componenta financiară = maximum 40 Puncte

Pf - Punctaj financiar = $Preț_{minim}$ / $Preț_{ofertă}$ x40, unde:

$Preț_{minim}$ este prețul cel mai scăzut dintre ofertele considerate admisibile și conforme din punct de vedere tehnic și i se va acorda maximul de puncte, respectiv **40** de puncte.

$Preț_{ofertă}$ este prețul ofertei evaluate.

12.2. Componenta tehnică

Componenta tehnică = maximum 60 Puncte

Punctajul tehnic (Pt) se obține prin însumarea punctajelor obținute pentru componenta tehnică după cum urmează:

Pt=∑(Pt1: Ptn)=60 puncte, unde
Pt1 = Punctaj factor tehnic 1
Pt2 = Punctaj factor tehnic 2
Ptn = Punctaj factor tehnic n

12.3. Punctaj maxim total

Punctaj maxim total = 100 Puncte

Punctajul final al ofertei (PT) va fi stabilit prin calcularea sumei punctajelor aferente componentei financiare și componentei tehnice.

PT = Pf + Pt

unde:

- PT – este punctajul total;
- Pf – punctajul obținut pentru propunerea financiară;
- Pt – punctajul obținut pentru factorii de evaluare tehnici.

Oferta cu punctajul cel mai mare va fi considerată oferta câștigătoare.

Conform prevederilor art.139 alin. (3) din HG nr. 395/2016, „*În cazul în care două sau mai multe oferte sunt clasate pe primul loc, cu punctaje egale, departajarea se va face având în vedere punctajul obținut la factorii de evaluare în ordinea descrescătoare a ponderilor acestora. În situația în care egalitatea se menține, autoritatea contractantă are dreptul să solicite noi propuneri financiare, și oferta câștigătoare va fi desemnată cea cu propunerea financiară cea mai mică.*”

12.4. Stabilirea factorilor de evaluare, a ponderii acordate fiecărui factor și algoritmul de calcul pentru acordarea punctajului

Factorii de evaluare a ofertelor şi punctajele alocate sunt prezentați în tabelul de mai jos:

Nr. crt.	FACTOR DE EVALUARE	PUNCTAJ MAXIM ALOCAT
Componenta financiară		
1	PREȚUL OFERTEI (Pf)	40
Componenta tehnică		
1	Pt1 – Experiență Manager de proiect	5
2	Pt2 - Experiență Expert analist de business	5
3	Pt3 - Experiență Expert arhitect de sistem	5
4	Pt4 - Experiență Expert guvernanță și managementul datelor	5
5	Pt5 - Experiență Expert testare	5
6	Pt6 - Experiență Expert securitate cibernetică	5
7	Pt7 - Experiență Expert protecția datelor	5
8	Pt8 – Calitate propunere tehnică - metodologia de implementare	25
	TOTAL	**100**

12.4.1. Componenta financiară

DENUMIRE FACTOR EVALUARE	DESCRIERE	PONDERE
Prețul ofertei (Pf)	Componenta financiară	40%

Algoritm de calcul:
Punctajul se acorda astfel:
a) Pentru cel mai scăzut dintre preturi se acorda punctajul maxim alocat;
b) Pentru celelalte preturi ofertate punctajul P(n) se calculează proporțional, astfel:
P(n) = (Preț minim ofertat / Preț n) x punctaj maxim alocat.

Prețurile unitare şi valorile totale sunt franco - destinația finală, fără TVA.
S-a acordat factorului ”Prețul ofertei” o pondere de 40% deoarece reprezintă un element important pentru încheierea acestui contract, creându-se astfel premisele respectării principiului utilizării cu eficiență, eficacitate și economicitate, în condiții de legalitate și regularitate, a creditelor bugetare aprobate Autorității contractante prin buget, principiu prevăzut de Legea nr. 500/2002 privind finanțele publice, cu modificările și completările ulterioare.

12.4.2. Componenta tehnică

Factorii tehnici de evaluare vizează aspecte calitative și sunt în strictă legătură cu obiectul contractului de achiziție publică ce urmează a fi atribuit prin prezenta procedură, vizând extinderea unor cerințe minime stabilite în caietul de sarcini, în conformitate cu prevederile art. 188 alin. (1) din Lege.

S-a acordat factorilor privind experiența profesională specifică pentru personalul desemnat pentru implementarea contractului o pondere de 5% pentru fiecare expert cheie deoarece reprezintă un avantaj cert pentru Autoritatea contractantă în vederea asigurării unei implementări cu succes a contractului.

Punctajul acordat factorilor privind experiența profesională specifică pentru personalul desemnat pentru implementarea contractului (maxim 35% din punctajul total), se justifică pe deplin de necesitatea asigurării unei experiențe extinse a personalului care va realiza activitățile specifice incluse în contract și pentru a demonstra potențialul tehnic al operatorului economic participant la procedură de a-și îndeplini contractul în cazul în care oferta sa va fi declarată câștigătoare.

O experiență extinsă a experților ce vor realiza activitățile specifice incluse în contractul asigură autoritatea contractantă că aceste activități în cadrul contractului vor fi realizate cu profesionalism în vederea atingerii obiectivelor stabilite la cele mai înalte standarde de calitate.

Autoritatea contractantă consideră că îndeplinirea contractului ce face obiectul acestei proceduri de achiziție publică în termeni de maximă eficiență și calitate poate fi realizată numai cu dovedirea unei experiențe profesionale de calitate relevantă.

12.4.2.1. ***Pt1 - Experiență Manager de proiect***

DENUMIRE FACTOR EVALUARE	DESCRIERE	PONDERE
Pt1 - Experiență Manager de proiect	Componenta tehnică	5%
Algoritm de calcul: Se punctează numărul de contracte/proiecte similare (*prin contract similar se înțelege contractul în care expertul a deținut POZIȚIA DE MANAGER DE PROIECT*), la nivelul cărora expertul a desfășurat activități similare celor pentru care este propus, astfel:		
1 contract/proiect (cerința minimă)		0 PUNCTE
2 contracte/proiecte		2,5 PUNCTE
3 contracte/proiecte sau mai mult		5 PUNCTE

12.4.2.2. ***Pt2 - Experiență Analist de business***

DENUMIRE FACTOR EVALUARE	DESCRIERE	PONDERE
Pt2 - Experiență Analist de business	Componenta tehnică	5%
Algoritm de calcul: Se punctează numărul de contracte/proiecte similare (*prin contract similar se înțelege contractul în care expertul a deținut o poziție similară și a desfășurat activități similare cu responsabilitățile din acest contract*), la nivelul cărora expertul a desfășurat activități similare celor pentru care este propus, astfel:		
1 contract/proiect (cerința minimă)		0 PUNCTE

2 contracte/proiecte	2,5 PUNCTE
3 contracte/proiecte sau mai mult	5 PUNCTE

12.4.2.3. ***Pt3 - Experiență Arhitect de sistem***

DENUMIRE FACTOR EVALUARE	DESCRIERE	PONDERE
Pt2 - Experiență Arhitect de sistem	Componenta tehnică	5%
Algoritm de calcul: Se punctează numărul de contracte/proiecte similare (*prin contract similar se înțelege contractul în care expertul a deținut o poziție similară și a desfășurat activități similare cu responsabilitățile din acest contract*), la nivelul cărora expertul a desfășurat activități similare celor pentru care este propus, astfel:		
1 contract/proiect (cerința minimă)		0 PUNCTE
2 contracte/proiecte		2,5 PUNCTE
3 contracte/proiecte sau mai mult		5 PUNCTE

12.4.2.4. ***Pt4 - Experiență guvernanță și managementul datelor***

DENUMIRE FACTOR EVALUARE	DESCRIERE	PONDERE
Pt2 - Experiență Expert guvernanță și managementul datelor	Componenta tehnică	5%
Algoritm de calcul: Se punctează numărul de contracte/proiecte similare (*prin contract similar se înțelege contractul în care expertul a deținut o poziție similară (GUVERNANȚĂ ȘI MANAGEMENT DATE) și a desfășurat activități similare cu responsabilitățile din acest contract*), la nivelul cărora expertul a desfășurat activități similare celor pentru care este propus, astfel:		
1 contract/proiect (cerința minimă)		0 PUNCTE
2 contracte/proiecte		2,5 PUNCTE
3 contracte/proiecte sau mai mult		5 PUNCTE

12.4.2.5. ***Pt5 - Experiență Expert testare***

DENUMIRE FACTOR EVALUARE	DESCRIERE	PONDERE
Pt2 - Experiență testare	Componenta tehnică	5%
Algoritm de calcul: Se punctează numărul de contracte/proiecte similare (*prin contract similar se înțelege contractul în care expertul a deținut o poziție similară și a desfășurat activități similare cu responsabilitățile din acest contract*), la nivelul cărora expertul a desfășurat activități similare celor pentru care este propus, astfel:		
1 contract/proiect (cerința minimă)		0 PUNCTE
2 contracte/proiecte		2,5 PUNCTE

3 contracte/proiecte sau mai mult	5 PUNCTE

12.4.2.6. ***Pt6 - Experiență Expert securitate cibernetică***

DENUMIRE FACTOR EVALUARE	DESCRIERE	PONDERE
Pt2 - Experiență Expert securitate cibernetică	Componenta tehnică	5%

Algoritm de calcul:
Se punctează numărul de contracte/proiecte similare (*prin contract similar se înțelege contractul cu componentă IT, în care expertul a deținut o poziție similară (EXPERT SECURITATE CIBERNETICĂ) și a desfășurat activități similare cu responsabilitățile din acest contract*), la nivelul cărora expertul a desfășurat activități similare celor pentru care este propus, astfel:

1 contract/proiect (cerința minimă)	0 PUNCTE
2 contracte/proiecte	2,5 PUNCTE
3 contracte/proiecte sau mai mult	5 PUNCTE

12.4.2.7. ***Pt7 - Experiență Expert protecția datelor***

DENUMIRE FACTOR EVALUARE	DESCRIERE	PONDERE
Pt2 - Experiență Expert protecția datelor	Componenta tehnică	5%

Algoritm de calcul:
Se punctează numărul de contracte/proiecte similare (*prin contract similar se înțelege contractul în care expertul a deținut o poziție similară și a desfășurat activități similare (elaborarea de propuneri de reglementare) cu responsabilitățile din acest contract*), la nivelul cărora expertul a desfășurat activități similare celor pentru care este propus, astfel:

1 contract/proiect (cerința minimă)	0 PUNCTE
2 contracte/proiecte	2,5 PUNCTE
3 contracte/proiecte sau mai mult	5 PUNCTE

12.4.2.8. ***Pt8 - Calitate propunere tehnică – metodologia de implementare***

DENUMIRE FACTOR EVALUARE	DESCRIERE	PONDERE
Pt8 - Calitate propunere tehnică - metodologia de implementare	Componenta tehnică	25%

Algoritm de calcul:
Se analizează propunerea tehnică propusă și anexele acesteia, inclusiv metodologia de implementare, din perspectiva relevanței, corectitudinii și a nivelului de detaliere prin raportare la obiectivele și cerințele stabilite în caietului de sarcini. Se va evalua atât conținutul, cât și prezentarea metodică și profesională a informațiilor.

Detaliile suplimentare vor contribui la obținerea unui punctaj mai mare, atâta timp cât acestea sunt relevante și susținute de o logică solidă. Fiecare membru al comisiei va acorda independent puncte pentru acest criteriu, ținând cont de descriptorii de performanță detaliați mai jos, după care se va realiza media aritmetică/criteriu pentru punctajele acordate de toți membrii comisiei.	
Propunerea tehnică conține Formularul de propunere tehnică precum și toate anexele indicate ca fiind obligatorii, inclusiv un capitol distinct cu Metodologia de implementare. Resursele alocate pentru implementarea contractului se limitează la cele minim solicitate prin caietul de sarcini (cerința minimă).	0 PUNCTE
Propunerea tehnică conține Formularul de propunere tehnică precum și toate anexele indicate ca fiind obligatorii, inclusiv un capitol distinct cu Metodologia de implementare. Metodologia de implementare este bine structurată, cu o organizare clară și logică a informațiilor. De fiecare dată când este relevant, conținutul anexelor este adaptat specificului contractului. Limbajul utilizat este clar și concis, ușor de înțeles, cu evitarea ambiguităților. Metodologia de implementare și planul de lucru reflectă o abordare coerentă în abordarea problemelor specifice și sunt aliniate cu obiectivele și cerințele caietului de sarcini. Resursele alocate depășesc cerințele minime, sunt corelate parțial cu duratele activităților și efortul estimat pentru acestea. Există unele propuneri ale Ofertantului de natură să conducă la o optimizare a serviciilor.	15 PUNCTE
Propunerea tehnică conține Formularul de propunere tehnică precum și toate anexele indicate ca fiind obligatorii, inclusiv un capitol distinct cu Metodologia de implementare. Propunerea tehnică este foarte bine structurată, cu o organizare foarte clară și logică a informațiilor. De fiecare dată când este relevant, conținutul anexelor este adaptat specificului contractului, prezentând abordări puternic particularizate. Limbajul utilizat este clar și concis, ușor de înțeles, cu evitarea ambiguităților și a exprimărilor neangajante. Metodologia și planul de lucru reflectă o abordare coerentă în abordarea problemelor specifice, sunt aliniate cu obiectivele și cerințele caietului de sarcini și prezintă un nivel foarte bun de detaliere. Resursele alocate depășesc atât din punct de vedere cantitativ, cât și calitativ cerințele minime sunt corelate cu duratele activităților și efortul estimat pentru acestea. Există propuneri inovatoare și creative de natură să conducă la o optimizare a serviciilor și a activităților suport.	25 PUNCTE

6. Cadrul legal care guvernează relația dintre Autoritatea Contractantă și Contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Contractantul trebuie să respecte toate prevederile legale, aplicabile la nivel național, dar și regulamentele aplicabile la nivelul Uniunii Europene (acolo unde se impune).

Pe perioada realizării tuturor activităților din cadrul Contractului, Contractantul este responsabil pentru implementarea celor mai bune practici, în conformitate cu legislația și regulamentele existente la nivel național și la nivelul Uniunii Europene. Contractantul va fi ținut deplin responsabil pentru subcontractanții săi în prestarea serviciilor prevăzute în Caietul de Sarcini, urmând să răspundă față de Autoritatea Contractantă, pentru orice nerespectare sau omisiune a respectării oricăror prevederi legale și normative aplicabile.

Autoritatea Contractantă nu va fi ținută responsabilă pentru nerespectarea sau omisiunea respectării de către Contractant sau de către subcontractanții acestuia a oricărei prevederi legale sau a oricărui act normativ aplicabil precum și atât pentru prestarea serviciilor cât și pentru rezultatele generate de prestarea serviciilor.

În cazul în care intervin schimbări legislative, Contractantul are obligația de a informa Autoritatea Contractantă cu privire la consecințele asupra activităților care fac obiectul Contractului și de a-și adapta activitatea în funcție de decizia Autorității Contractante în legătură cu schimbările legislative. În cazul în care o astfel de situație este aplicabilă trebuie precizat în Contract mecanismul de soluționare a unor astfel de situații.

Ofertantul devenit Contractant are obligația de a respecta în executarea Contractului, obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii enumerate în anexa X la Directiva 2014/24, respectiv:

- Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;
- Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectivă;
- Convenția nr. 29 a OIM privind munca forțată;
- Convenția nr. 105 a OIM privind abolirea muncii forțate;
- Convenția nr. 138 a OIM privind vârsta minimă de încadrare în muncă;
- Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de muncă și profesie);
- Convenția nr. 100 a OIM privind egalitatea remunerației;
- Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor.

Ofertantul va prezenta o declarație pe proprie răspundere, privind faptul ca la elaborarea ofertei a ținut cont de obligațiile relevante din domeniile mediului, social și al relațiilor de muncă pe toată durata de îndeplinire a contractului de servicii, în conformitate cu prevederile art. 51 din Legea nr.98/2016 privind achizițiile publice.
Actele normative și standardele indicate mai jos sunt considerate indicative și nelimitative; enumerarea actelor normative din acest capitol este oferită ca referință și nu trebuie considerată limitativă:

6.1. Legislație europeană

- Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 privind normele financiare aplicabile bugetului general al Uniunii, de modificare a Regulamentelor (UE) nr. 1296/2013, (UE) nr. 1301/2013, (UE) nr. 1303/2013, (UE) nr. 1304/2013, (UE) nr. 1309/2013, (UE) nr. 1316/2013, (UE) nr. 223/2014, (UE) nr. 283/2014 și a Deciziei nr. 541/2014/UE și de abrogare a Regulamentului (UE, Euratom) nr. 966/2012;
- Regulamentul (UE) nr. 241/2021 al Parlamentului European și al Consiliului din 12 februarie 2021 de instituire a Mecanismului de redresare și reziliență;
- Regulamentul Delegat (UE) 2021/2106 al Comisiei din 28 septembrie 2021 de completare a Regulamentului (UE) 2021/241 al Parlamentului European și al Consiliului de instituire a Mecanismului de redresare și reziliență prin stabilirea indicatorilor comuni și a elementelor detaliate ale tabloului de bord privind redresarea și reziliența;
- Decizia de punere în aplicare a Consiliului de aprobare a evaluării planului de redresare și reziliență al României din 29 octombrie 2021;
- Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană;
- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).
- Regulamentul (UE) 2022/576 al Consiliului din 8 aprilie 2022 de modificare a Regulamentului (UE) nr. 833/2014 privind măsuri restrictive având în vedere acțiunile Rusiei de destabilizare a situației în Ucraina;
- Directiva (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 (denumită în continuare Directiva (UE) 2015/849);

6.2. Legislație națională

- Legea nr. 98/2016 privind achizițiile publice, cu modificările și completările ulterioare;
- Normele metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziție publică /acordului-cadru din Legea nr. 98/2016 privind achizițiile publice, aprobate prin HG nr. 395/2016, cu modificările și completările ulterioare;
- Legea nr. 101/2016 privind remediile și căile de atac în materie de atribuire a contractelor de achiziție publică, a contractelor sectoriale și a contractelor de concesiune de lucrări și concesiune de servicii, precum și pentru organizarea și funcționarea Consiliului Național de Soluționare a Contestațiilor, cu modificările și completările ulterioare;
- Ordonanța de urgență a Guvernului nr. 155 / 2020 privind unele măsuri pentru elaborarea Planului național de relansare și reziliență necesar României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de redresare și reziliență (denumită în continuare OUG nr.155/2020);

- Ordonanța de urgență nr. 124/2021 privind stabilirea cadrului instituțional și financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare și reziliență, precum și pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului național de redresare și reziliență necesar României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de redresare și reziliență, respectiv normele metodologice de aplicare a prevederilor Ordonanței de urgenta a Guvernului nr. 124/2021, cu modificările ulterioare;
- Legea nr. 190/2018 privind masurile de aplicare a GDPR;
- 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 (denumită în continuare Legea nr. 129/2019);
- Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei;
- Ordinul Ministerului Cercetării, Inovării și Digitalizării nr. 20.279/2023 pentru aprobarea criteriilor de stabilire și a listei nominale privind produsele, serviciile și entitățile producătoare și/sau furnizoare interzise, provenind direct sau indirect din Federația Rusă.
- Instrucțiunea nr. 6 privind obținerea unor date și informații privind verificarea ex-ante a beneficiarului real al destinatarului fondurilor din cadrul PNRR (denumită în continuare Instrucțiunea 6 PNRR);
- ;
- Instrucțiunile MCID/ MIPE publicate, aplicabile pentru contractele finanțate din PNRR.

6.3. Conflict de interese

Se aplică prevederile art. 61 alin. (1) din Regulamentul (UE, Euratom) 2018/1046 al Parlamentului European și al Consiliului din 18 iulie 2018 și legislația națională în vigoare cu privire la conflictul de interese.

Pentru a se asigura independența Ofertantului, acesta va completa DUAE prin care certifică faptul că nu se află în conflict de interese în momentul depunerii ofertei și că va informa Autoritatea Contractantă în cazul în care se va afla la un moment dat în situația de conflict de interese, chiar potențial, în timpul îndeplinirii sarcinilor pentru care a fost contractat.

6.4. Confidențialitate

Atât contractantul, cât și personalul pus la dispoziție de acesta trebuie să păstreze confidențialitatea informațiilor și datelor la care au acces pe parcursul implementării contractului.
Obligațiile de confidențialitate care intră în sarcina părților sunt incluse în Acordul de Confidențialitate (anexă la contractul de achiziție publică)

6.5. Drepturi de proprietate intelectuală

Toate documentele ce vor fi elaborate în executarea Contractului (livrabile, rapoarte, clauze contractuale, etc.) vor face obiectul dreptului exclusiv de proprietate (inclusiv,

dar fără a se limita la drepturi de autor și/sau orice alte drepturi de proprietate intelectuală) al Autorității Contractante, care le poate utiliza, publica sau transfera după cum consideră necesar, fără nicio limitare geografică sau de alta natură.

7. INFORMAȚII SUPLIMENTARE / ADMINISTRATIVE

Limba de lucru: română.
Ofertantul își asumă răspunderea exclusivă pentru legalitatea și autenticitatea tuturor documentelor prezentate în original, copie și/sau copie „conformă cu originalul" în vederea participării la procedură. În acest scop, analizarea de către comisia de evaluare a documentelor prezentate de ofertanți nu angajează din partea acesteia nicio răspundere sau obligație fată de acceptarea respectivelor documente ca fiind autentice sau legale și nu înlătură răspunderea exclusivă a ofertantului sub acest aspect. În acest sens, operatorii economici care, fie nu prezintă sau prezintă informații parțiale cu privire la propria lor situație privind incidența motivelor de excludere sau îndeplinirea criteriilor de calificare sau care se fac vinovați de declarații false în conținutul informațiilor transmise la solicitarea autorității contractante vor fi respinși, cu aplicarea în mod corespunzător a dispozițiilor / consecințelor legale incidente.
Autoritatea contractantă nu este responsabilă pentru nici un fel de cheltuieli suplimentare față de serviciile incluse în contract. Toate cheltuielile generate de încălcările și/sau nerespectările prevederilor de mai sus vor fi suportate de către Contractant și nu vor fi decontate de autoritatea contractantă.
Ofertantul suportă toate cheltuielile datorate elaborării și prezentării ofertei sale.
Toate documentele / informațiile folosite / prelucrate pe parcursul derulării contractului vor fi puse la dispoziția autorității contractante, în format electronic și editabil.
Pentru a demonstra o foarte bună înțelegere a caietului de sarcini, propunerea tehnică, metodologia și planul de lucru trebuie să fie adaptate cerințelor specifice ale caietului de sarcini, trebuie să fie prezentate și dezvoltate într-o manieră proprie și originală, nefiind permise abordările de tip copy-paste. Fiecare cerință va fi prezentată detaliat, la modul cum urmează a fi implementată, nefiind permise abordările de răspuns doar cu "DA" sau "NU", sau prin copierea ad-litteram a cerinței impuse.
Nu se acceptă trimitere către link-uri, ci doar documente atașate ofertei, dacă este cazul.
Neregăsirea în propunerea tehnică a cerințelor minime din caietul de sarcini, va presupune declararea ofertei ca fiind neconformă. Propunerea tehnică va fi astfel prezentată încât să asigure posibilitatea verificării conformității acesteia cu cerințele minime obligatorii prevăzute în caietul de sarcini.
Documentele ofertei vor fi semnate electronic de o persoană sau de persoane autorizate de drept să semneze în numele Ofertantului. Pentru evaluarea cu celeritate, ofertanții se vor îngriji să anexeze și variantele editabile ale documentelor ce compun propunerea tehnică, acolo unde este specificat de autoritatea contractantă. O ofertă care va fi prezentată în orice alt format sau nu va fi transmisă conform cerințelor de mai sus, va fi respinsă ca fiind inadmisibilă.
Paginile Ofertei vor fi numerotate, **organizate** pe diferite secțiuni ținând cont de fiecare categorie de cerințe din caietul de sarcini; oferta va include un **OPIS** care să poată face trimitere la fiecare secțiune (**indicând pagina și/sau paragraful**), toate paginile fiind numerotate corespunzător, pentru a permite o identificare rapidă, conform cerințelor din caietul de sarcini.

Nume și prenume	Funcția	Semnătura
Anghel Lucian-Emanuel	Consilier președinte	ANGHEL LUCIAN-EMANUEL Digitally signed by ANGHEL LUCIAN-EMANUEL Date: 2026.01.29 16:45:34 +02'00'
Pădureanu Valeriu-Florian	Consilier președinte	Padureanu Valeriu-Florian 2026.01.29 16:02:38 +02'00'