Nr YA/7099/12.12.2025

Aprobat,
Director General
Ing. Cristian PISTOL

Semnatar: Caruna Viorica-Gabriela
Data si ora semnarii: 2025.12.19 13:43:37 +0200

# CAIET DE SARCINI

# *IMPLEMENTAREA SISTEMULUI e-SIGUR*

**Director General Adjunct,**
**Ion - Cosmin PETRESCU**

**Director - Direcția Întreținere, Siguranța Circulației Drumuri si Poduri**
**Ing. Cristian ANDREI**

**Director Adjunct Siguranța Circulației și ITS**
**Dr. Ing. Flavius PAVAL**

**Șef Serviciu ITS,**
**An. Lucian ILINA**

# Cuprins


**1 INTRODUCERE ..... 5**

1.1 INFORMAȚII GENERALE ..... 5
1.2 CADRUL LEGAL CARE GUVERNEAZĂ RELAȚIA DINTRE AUTORITATEA CONTRACTANTĂ ȘI CONTRACTANT ..... 6
1.3 TERMENI SI DEFINIȚII ..... 7
1.4 INFORMAȚII DESPRE AUTORITATEA CONTRACTANTĂ ..... 8
1.5 INFORMAȚII DESPRE CONTEXTUL CARE A DETERMINAT PREZENTA ACHIZIȚIE ..... 9
1.6 INFORMAȚII DESPRE BENEFICIILE ANTICIPATE DE CĂTRE AUTORITATEA CONTRACTANTĂ ..... 10
1.7 FACTORI INTERESAȚI ȘI ROLUL ACESTORA ..... 10
1.8 OBIECTIVELE SPECIFICE ALE PROIECTULUI ..... 10

**2 DESCRIEREA PRODUSELOR SI A ACTIVITATILOR DIN CADRUL PROIECTULUI „IMPLEMENTAREA SISTEMULUI E-SIGUR" ..... 14**

2.1 PRODUSELE CARE FAC OBIECTUL „SISTEMULUI E-SIGUR" ..... 14
*2.1.1 STRUCTURA TIP CONSOLĂ ..... 14*
*2.1.2 CABINET ..... 16*
*2.1.3 INFRASTRUCTURĂ NUCLEU CENTRAL (CMT) ..... 16*
*I. Specificații minimale servere – minim 9 buc ..... 18*
*II. Specificatii componenta WAF (Web Application Firewall) ..... 18*
*2.1.4 PRODUSE IN TEREN (ECHIPAMENTE) ..... 21*
***Specificațiile minimale pentru camerele de viteză: ..... 22***
***Specificațiile minimale pentru echipamentele de procesare locala ..... 25***
2.2 SERVICIILE CARE FAC OBIECTUL „SISTEMULUI E-SIGUR" ..... 26
*2.2.1 DESCRIERE FUNCȚIONALĂ ..... 26*
*2.2.2 SERVICII DE ANALIZA DETALIATĂ A CERINȚELOR PENTRU SISTEMUL E-SIGUR ..... 28*
*2.2.3 SERVICII DE PROIECTARE SOFTWARE - PROIECTAREA SOLUȚIEI INFORMATICE E-SIGUR 29*
*2.2.4 SERVICII DE DEZVOLTARE/CUSTOMIZARE, INSTALARE ȘI CONFIGURARE A SOLUȚIEI INFORMATICE E-SIGUR ..... 30*
*2.2.5 SCENARII DE UTILIZARE ȘI FLUXURI OPERAȚIONALE ..... 31*
*Transmitere notificări către IGPR sau CNAIR ..... 31*
*Furnizare informații la cerere ..... 32*
*A. Procesare date istorice pentru a determina poziționarea optimă a echipamentelor în teren ..... 33*
*B. Procesare date istorice pentru îmbunătățirea algoritmilor de filtrare și prioritizare a notificărilor ..... 33*
*C. Procesare date istorice pentru a determina indicele de sănătate a echipamentelor ..... 33*
*D. Diagramă arhitectură ..... 36*
2.3 SPECIFICATII COMPONENTA SOFTWARE ..... 36
***Componenta management de documente și lucru colaborativ ..... 43***
*2.3.1 CERINȚE PRIVIND FLUXURILE ELECTRONICE ..... 48*
*2.3.2 CERINȚE PRIVIND SEMNAREA ELECTRONICĂ A DOCUMENTELOR ..... 49*
*2.3.3 CERINȚE PRIVIND TRANSMITEREA ȘI EXPORTUL DOCUMENTELOR ..... 50*
*2.3.4 CERINȚE PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL ..... 50*
*2.3.5 CERINȚE PRIVIND ADMINISTRAREA ȘI CONFIGURAREA ..... 51*
*2.3.6 CERINȚE PRIVIND ARHITECTURA INTERNĂ ȘI PERFORMANȚA ..... 55*
*2.3.7 COMPONENTA BAZA DE DATE ..... 55*

*2.3.8 COMPONENTA GIS ȘI ANALYTICS* ... *57*
*2.3.9 COMPONENTA CHATBOT* ... *58*
*2.3.10 COMPONENTA BI ȘI MONITORIZARE FLUXURI* ... *58*
*2.3.11 COMPONENTA ESB & API MANAGEMENT* ... *60*
*2.3.12 CERINȚE SECURITATE* ... *61*

**3 LIVRARE, AMBALARE, ETICHETARE, TRANSPORT SI ASIGURARE PE DURATA TRANSPORTULUI ... 65**

3.1 LIVRAREA/RECEPTIE ... 65
3.2 AMBALAREA ȘI ETICHETAREA ... 66
3.3 TRANSPORTUL ... 66
3.4 RECEPȚIE - CERINȚE GENERALE ... 67

**4 SERVICI DE INSTRUIRE A UTILIZATORILOR ȘI ADMINISTRATORILOR SISTEMULUI ... 68**

**5 SERVICII DE TESTARE A SOLUȚIEI IMPLEMENTATE SI OPERAȚIONALIZAREA SISTEMULUI ... 69**

OPERAȚIONALIZAREA SISTEMULUI INFORMATIC INTEGRAT LA NIVELUL STRUCTURILOR IMPLICATE ... 70

**6 DURATA DE IMPLEMENTARE A CONTRACTULUI ... 71**

**7 ETAPELE DE IMPLEMENTARE ... 71**

**8 GARANTIE ... 73**

**9 SUPORT TEHNIC – SERVICII DE MENTENANTA CORECTIVA ... 75**

9.1 SLA (SERVICE LEVEL AGREEMENT) ... 76
9.2 SERVICII DE MENTENANTA PREVENTIVA ... 79

**10 ORGANIZARE ȘI METODOLOGIE DE PREZENTARE A OFERTEI ... 80**

**11 GESTIONAREA RELAȚIEI DINTRE CONTRACTANT ȘI AUTORITATEA CONTRACTANTĂ ... 80**

11.1 RESURSELE NECESARE/EXPERTIZA NECESARĂ PENTRU REALIZAREA ACTIVITĂȚILOR ÎN CONTRACT ȘI OBȚINEREA REZULTATELOR ... 82
11.2 NUMĂRUL DE EXPERȚI PE CATEGORIE DE EXPERTIZĂ NECESARĂ ... 83
11.3 PROFILUL EXPERȚILOR PRINCIPALI ... 84
11.4 ALTE CERINȚE LEGATE DE PERSONALUL DIRECT IMPLICAT ÎN PRESTAREA SERVICIILOR 84

*Experti – cerințe minime* ... *85*

**12 MODALITĂȚI ȘI CONDIȚII DE PLATĂ ... 83**

**13 CERINTE PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL ... 88**

13.1 CONTEXT ... 88
13.2 METODOLOGIE ... 89
13.3 IDENTIFICAREA DATELOR CU CARACTER PERSONAL ... 89
DATE IMPORTATE (PRELUATE DIN CMI) ... 90
DATE PRELUCRATE DE E-SIGUR ... 90

13.4 ANALIZA DE IMPACT ..... 92
*13.4.1 PRELUCRAREA DATELOR SENSIBILE* ..... *92*
SCOPUL PRELUCRĂRII DATELOR ..... 93
13.5 PERIOADA DE RETENȚIE A DATELOR ..... 93
13.6 DREPTURILE PERSOANEI VIZATE ..... 94
**14 IPOTEZE SI RISCURI ..... 95**
14.1 REGISTRU RISCURI ..... 95
14.2 MĂSURI TEHNICE ȘI ORGANIZATORICE (TOMS) GDPR ..... 97
14.3 IPOTEZELE ..... 95
**15 DREPTURI DE PROPRIETATE INTELECTUALĂ ..... 101**
**16 ALTE MENTIUNI ..... 102**

# 1 INTRODUCERE

## 1.1 INFORMAȚII GENERALE

Prezentul Caiet de Sarcini include ansamblul cerințelor pe baza cărora fiecare Ofertant va elabora Oferta (Propunerea Tehnică și Propunerea Financiară) pentru furnizarea sistemului e-Sigur, precum și a lucrărilor și serviciilor asociate, care fac obiectul Contractului „Implementarea sistemului e-Sigur" ce rezultă din această procedură.

Oferta prezentată va fi considerată conformă în măsura în care Propunerea tehnică va fi întocmită cu respectarea cerințelor din prezentul Caiet de Sarcini.

Caietul de sarcini face parte integrantă din Documentația de atribuire pentru achiziția de echipamente necesare, inclusiv analiza, proiectarea si dezvoltarea modulelor software specifice proiectului și constituie ansamblul cerințelor minime obligatorii pe baza cărora se elaborează Propunerea Tehnică de către fiecare Ofertant.

Cerințele impuse vor fi considerate ca fiind minime și obligatorii. În acest sens, orice Propunere Tehnică prezentată, care se abate de la prevederile Caietului de sarcini, va fi luată în considerare doar în măsura în care presupune asigurarea unui nivel calitativ corespunzător si daca e cazul superior cerințelor minime din prezentul Caiet de sarcini. Propunerea Tehnică ce conține caracteristici inferioare celor prevăzute în Caietul de sarcini poate fi considerată neconformă.

Prezentul caiet de sarcini cuprinde cerințele care trebuie respectate astfel încât potențialii ofertanți să elaboreze propunerea tehnică corespunzător cu necesitățile autorității contractante.

**Specificațiile tehnice care indică o anumită origine, sursă, producție, un produs special, o marcă de fabricație sau de comerț, un brevet de invenție, o licență de fabricație sunt menționate doar pentru identificarea cu ușurință a tipului de produs și nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau anumitor produse. Aceste specificații vor fi considerate ca având mențiunea "sau echivalent".**

Fără a aduce atingere altor prevederi legale sau dispozițiilor legale privind liberul acces la informațiile de interes public ori ale altor acte normative care reglementează activitatea autorității contractante, autoritatea contractantă are obligația de a nu dezvălui informațiile din propunerea tehnică, elementele din propunerea financiară și/sau fundamentări/justificări de preț/cost transmise de operatorii economici indicate și dovedite de aceștia ca fiind confidențiale întrucât sunt: date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală. Caracterul confidențial se aplică doar asupra datelor/informațiilor indicate și dovedite ca fiind date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală.

Operatorii economici vor indica și dovedi în cuprinsul ofertei care informații din propunerea tehnică, elemente din propunerea financiară și/sau fundamentări/justificări de preț/cost sunt confidențiale întrucât sunt: date cu caracter personal, secrete tehnice sau comerciale sau sunt protejate de un drept de proprietate intelectuală. Informațiile indicate de operatorii economici din propunerea tehnică, elemente din propunerea financiară și/sau fundamentări/justificări de preț/cost ca fiind confidențiale trebuie să fie însoțite de dovada care le conferă caracterul de confidențialitate.

Ofertantul suportă toate cheltuielile datorate elaborării și prezentării ofertei sale, indiferent de rezultatul obținut la adjudecarea ofertei.

Orice termen descris într-un anumit capitol din Caietul de Sarcini și nespecificat explicit în alt capitol, trebuie interpretat ca fiind menționat în toate capitolele unde se consideră de către Ofertant că acesta trebuia menționat pentru asigurarea îndeplinirii obiectului Contractului.

Oriunde, în prezentul document, termenii referitori la sisteme de transport inteligente sunt echivalenți cu cei referitori la sisteme inteligente de transport și cei cu sisteme ITS.

Echipamentele ofertate trebuie sa fie noi și nefolosite si sa beneficieze de suport din partea producătorului (nu se accepta echipamente uzate sau care nu se mai afla in linia de fabricație a producătorului).

## 1.2 CADRUL LEGAL CARE GUVERNEAZĂ RELAȚIA DINTRE AUTORITATEA CONTRACTANTĂ ȘI CONTRACTANT

(inclusiv în domeniile mediului, social și al relațiilor de muncă)

În cadrul procedurii de achiziție publica, Compania Națională de Administrare a Infrastructurii Rutiere SA (CNAIR SA) îndeplinește rolul de Autoritate contractantă.

Pe perioada derulării Contractului, Contractantul este responsabil pentru realizarea activităților în conformitate cu documentația tehnică și implementarea celor mai bune practici, in conformitate cu regulile si regulamentele existente la nivel național și la nivelul Uniunii Europene.

Prin depunerea unei Oferte ca răspuns la cerințele din prezentul Caiet de sarcini, se prezumă că, Contractantul are cunoștințe și are în vedere toate și orice reglementări aplicabile și că le-a luat în considerare la momentul depunerii Ofertei sale pentru atribuirea Contractului.

În cazul în care, pe parcursul derulării Contractului, apar schimbări legislative de natură să influențeze activitatea Contractantului în raport cu cerințele stabilite prin prezentul Caiet de sarcini, Contractantul are obligația de a informa Autoritatea Contractantă cu privire la consecințele asupra activităților sale ce fac obiectul Contractului și de a își adapta activitatea, de la data și în condițiile în care sunt aplicabile.

Contractantul va fi deplin responsabil pentru realizarea tuturor activităților în condiții de maximă securitate și în deplină conformitate cu legislația aplicabilă, precum și cu respectarea prevederilor referitoare la securitate și sănătate în muncă și controlul calității cuprinse în standarde/ instrucțiuni/ proceduri/ ghiduri, aplicabile în speță.

Contractantul va fi considerat deplin responsabil pentru subcontractanții acestuia, chiar și în situația în care au fost în prealabil agreați de Autoritatea Contractantă, 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 considerată responsabilă pentru nerespectarea sau omisiunea respectării de către Contractant sau de către subcontractanții acestuia a oricărei prevederi legale sau normative aplicabile.

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:

a. Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;
b. Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectivă;
c. Convenția nr. 29 a OIM privind munca forțată;
d. Convenția nr. 105 a OIM privind abolirea muncii forțate;
e. Convenția nr. 138 a OIM privind vârsta minimă de încadrare în muncă;
f. Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de muncă și profesie);
g. Convenția nr. 100 a OIM privind egalitatea remunerației;
h. Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor;
i. Convenția de la Viena privind protecția stratului de ozon și Protocolul său de la Montreal privind substanțele care epuizează stratul de ozon;
j. Convenția de la Basel privind controlul circulației transfrontaliere a deșeurilor periculoase și al eliminării acestora (Convenția de la Basel);
k. Convenția de la Stockholm privind poluanții organici persistenți (Convenția de la Stockholm privind POP);
l. Convenția de la Rotterdam privind procedura de consimțământ prealabil în cunoștință de cauză, aplicabilă anumitor produși chimici periculoși și pesticide care fac obiectul comerțului internațional (UNEP/FAO) (Convenția PIC), 10 septembrie 1998, și cele trei protocoale regionale ale sale.

Contractantul va livra produsele solicitate si va desfășura activitățile specifice Contractului având în vedere toate prevederile legale naționale, europene și internaționale relevante existente la momentul semnării Contractului, precum și cele emise ulterior, pe parcursul derulării Contractului, precum și ansamblul reglementărilor subsecvente, al recomandărilor și practicilor incidente, enumerarea următoare nefiind limitativă:

### 1.3 TERMENI SI DEFINIȚII

In prezentul caiet de sarcini următorii termeni vor fi interpretați astfel:

*e-SIGUR* - un ansamblu de sisteme informatice, infrastructură de comunicații, elemente de interconectare și interoperabilitate cu alte sisteme informatice, platforme hardware și software pentru stocare, procesare automată, procesare manuală, preluare, afișare și transmitere de date, mijloace tehnice certificate sau omologate și verificate metrologic și capabilități și/sau servicii de imprimare masivă și comunicare a documentelor;

*ITS* - sisteme in cadrul cărora se aplică tehnologii ale informației si comunicațiilor în domeniul transportului rutier, inclusiv infrastructura, vehicule si utilizatori, in gestionarea traficului si gestionarea mobilității, precum si pentru interfețe cu alte moduri de transport;

*Produse* - produsele aferente îndeplinirii obiectului contractului, care trebuie furnizate conform prevederilor caietului de sarcini;

*Centru de management al traficului (CMT)*- locație unde toate fluxurile informaționale de interes in ceea ce privește traficul rutier si condițiile de circulație ajung si se distribuie in vederea monitorizării rețelei rutiere, care poate fi si CNMT situat in CIC Nod A0-A3, Autostrada A0 Nord, km 32+300, in functie de decizia CNAIR SA in implementarea contractului;

*Subsistemul de detecție a vitezei* - un ansamblu format dintr-o telecamera cu capabilități OCR si un dispozitiv radar de detecție a vitezei autovehiculului, ce poate măsura simultan viteza autovehiculelor care se deplasează pe mai multe benzi de circulație;

*ANPR (Automatic Number Plate Recognition)* – un ansamblu care permite identificarea in mod automat a numerelor de înmatriculare;

*SIEGMCR* - sistem informatic de emitere, gestiune, monitorizare și control rovinietă;

*Arhitectura sistemului informatic* - structurile, mecanismele și interfețele utilizate, precum și comunicarea între părțile componente ale sistemului informatic care descriu viziunea fizică și logică a sistemului propus;

*Semnalări si date de monitorizare a traficului* - informații privind posibila încălcare a cel puțin uneia dintre normele de circulație pe drumurile publice;

*Platformă software a Poliției Române* - sistem informatic, parte integrantă a platformei „Hub de servicii la nivelul M.A.I.", denumit în continuare platformă software, destinat prelucrării semnalărilor transmise de sistemele automate de detectare;

*Mijloace tehnice pentru monitorizarea traficului rutier* — orice echipament sau ansamblu de echipamente instalate pe drumurile care permite colectarea imaginilor, a sunetului și a informațiilor privind viteza de deplasare a unui vehicul și recunoașterea numărului de înmatriculare ori de înregistrare al acestuia ori a altor informații relevante monitorizării;

### 1.4 INFORMAȚII DESPRE AUTORITATEA CONTRACTANTĂ

Compania Națională de Administrare a Infrastructurii Rutiere S.A. (CNAIR) este o unitate de interes strategic național la care statul este acționar majoritar, entitate care funcționează sub autoritatea Ministerului Transporturilor, pe bază de gestiune economică și autonomie financiară, potrivit art. 2 din *OUG nr. 84/2003 pentru înființarea Compania Națională de Administrare a Infrastructurii Rutiere S.A. prin reorganizarea Regiei Autonome Administrația Națională a Drumurilor din România*, aprobată prin *Legea nr. 47/2004*, completată prin *OUG nr. 55 din 14 septembrie 2016 privind reorganizarea Compania Națională de Administrare a Infrastructurii Rutiere S.A. și înființarea Companiei Naționale de Autostrăzi și Drumuri Naționale din România – S.A. și înființarea Companiei Naționale de Investiții Rutiere – S.A.*, precum și modificarea și completarea unor acte normative.

Compania Națională de Administrare a Infrastructurii Rutiere S.A., având sediul în B-dul Dinicu Golescu nr. 38, sector 1, București, România cod poștal 0101873, email: office@andnet.ro este Beneficiarul final al acestui proiect.

C.N.A.I.R. S.A. are ca obiect principal de activitate: construirea, întreținerea, repararea, administrarea și exploatarea autostrăzilor, drumurilor expres, drumurilor naționale, variantelor ocolitoare, precum și a altor elemente de infrastructură rutieră conform legii, în scopul desfășurării traficului rutier în condiții de siguranță a circulației.

### 1.5 INFORMAȚII DESPRE CONTEXTUL CARE A DETERMINAT PREZENTA ACHIZIȚIE

În momentul de față, CNAIR SA deține Centrele de Management Trafic și echipamentele ITS deja instalate pe rețeaua de autostrăzi, elemente necesare dezvoltării sistemului e-SIGUR în România.

De asemenea, potrivit direcției de acțiune trasate în cuprinsul *pct. 5.2. - Utilizarea drumurilor în condiții de siguranță* din *Strategia națională privind siguranța rutieră pentru perioada 2022 - 2030*, direcție ce reunește două mari priorități - factorul uman și sistemele automate, sistemele tehnice automate pentru detecția, procesarea și sancționarea abaterilor presupun existența unui cadru legal în strânsă legătură cu trei principii de bază, respectiv: alocarea finanțării pentru funcționarea sistemului, crearea unor standarde de date și stabilirea unui nivel de acceptanță pentru Contractanții datelor de detecție.

Sistemele automate de management al traficului îndeplinesc mai multe funcții, printre care și: monitorizarea video a traficului cu scopul de a permite intervențiile rapide ale echipajelor de urgență, analiza calitativă și cantitativă a traficului rutier, recunoașterea automată a plăcuțelor de înmatriculare, etc.

La nivel internațional o serie de state au adoptat metode de impunere bazate pe o abordare *oriunde, oricând* pentru a preveni încălcarea regulilor de circulație, mesajul fiind clar: nerespectarea acestora reprezintă un comportament ilegal, inacceptabil și în dezacord cu interesele comunității. Totodată, s-a avut în vedere și monitorizarea comportamentului la volan conform unor criterii predefinite.

În acest context, în Monitorul Oficial, Partea I nr. 1279 din 30 decembrie 2022 a fost publicată *Legea nr. 383/2022 privind unele măsuri de eficientizare a monitorizării traficului rutier*, care reglementează monitorizarea traficului rutier pe drumurile publice din România într-un sistem integrat (denumit e-SIGUR), precum și condițiile în care pot fi utilizate datele colectate cu ocazia monitorizării. În conformitate cu prevederile art. 4, alin. (3) din Legea 383/2022, CNAIR SA *„asigură în cadrul centrelor [n.b. de management al traficului pe drumurile de interes național, administrate de către CNAIR] dezvoltarea, funcționarea, mentenanța și orice alte activități legate de administrarea e-SIGUR, cu excepția capabilității și/sau a serviciilor de imprimare masivă și comunicare a documentelor”*.

În contextul necesității de a îndeplini obiectivul de monitorizare a încălcărilor legislației rutiere prin mijloace automate (camere video, senzori), CNAIR SA deține Centrele de Management Trafic și echipamentele ITS deja instalate pe rețeaua de autostrăzi, elemente necesare dezvoltării sistemului e-SIGUR în România. Astfel, realizarea prezentului proiect reprezintă îndeplinirea obligațiilor CNAIR SA, așa cum reies ele din prevederile Legii 383/2022.

## 1.6 INFORMAȚII DESPRE BENEFICIILE ANTICIPATE DE CĂTRE AUTORITATEA CONTRACTANTĂ

Realizarea proiectului „Implementarea sistemului e-Sigur" contribuie la îndeplinirea obiectivului principal al *Strategiei naționale privind siguranța rutieră pentru perioada 2022 – 2030*, care urmărește implementarea normelor și liniilor directoare ale Uniunii Europene așa cum sunt ele prezentate în documentul cadru de politici europene în domeniul siguranței rutiere „Viziunea Zero", și anume reducerea numărului de decedați în accidente rutiere până în 2050 până aproape de zero. Implementarea proiectului contribuie și la obiectivul intermediar prin care România își asumă obiectivul Uniunii Europene de reducere a numărului de victime (răniți sau decedați) cu 50% până în 2030.

Totodată, realizarea proiectului „Implementarea sistemului e-Sigur" contribuie la îndeplinirea obiectivului specific 7 (OS7) din Strategia națională privind sistemele de transport inteligente pentru perioada 2022-2030 aprobată prin Hotărârea de Guvern nr. 1086/2022, care are în vedere creșterea siguranței rutiere prin implementarea soluțiilor de sisteme de transport inteligente (ITS) cu obiectivul de a reducere numărul de accidente rutiere și de a dezvolta o rețea rutieră sigură.

## 1.7 FACTORI INTERESAȚI ȘI ROLUL ACESTORA

Principalii factori sunt Poliția Română și CNAIR, realizarea obiectului prezentului proiect permițându-le să-și îndeplinească cu succes obligațiile legislative și să contribuie din poziția de dezvoltator la progresul din domeniul sistemelor de transport inteligente, având si următoarele roluri:

- Rol în procesul de stabilire a poziției echipamentelor de pe rețeaua rutieră din administrarea CNAIR: Poliția Romana - emite avizul privind amplasarea de mijloace tehnice pentru colectarea datelor de monitorizare a traficului rutier;
- Poliția Română – procesează semnalările prevăzute la art. 10 alin. (1) lit. a) și alin. (2) din Legea 383/2022.

Alți factori interesați sunt deținătorii de sisteme cu care se interconectează e-SIGUR în conformitate cu prevederile art. 7, alin. (1) din Legea 383/2022.

## 1.8 OBIECTIVELE SPECIFICE ALE PROIECTULUI

În scopul îndeplinirii obiectului contractului, proiectul presupune minim achiziția următoarelor produse, însoțite de serviciile si lucrările aferente:

- Produse: Cameră video cu radar care include unitate de procesare locala (400 buc)/ Cameră video cu radar (400 buc) si unitate de procesare locala (400 buc), Sistem de tip UPS (400 buc), Router industrial (400 buc), Accesorii si montaj ( Cabinete, infrastructura de rețea si montaj) (400 buc), Console (400 buc), Server (inclusiv sisteme de operare – 9 buc), Componenta WAF (2 buc), Sisteme de stocare (2 buc);

- Servicii: Servicii de proiectare infrastructură, Servicii de analiză, Servicii de proiectare software, Servicii de Dezvoltare/customizare, instalare și configurare a soluției informatice, Servicii de testare, Servicii de instruire, Servicii privind operationalizarea sistemului sau punerea acestuia in functiune, Servicii de mentenanță si suport tehnic pe perioada de garanție, Servicii de instalare si montaj echipamente, Obținerea oricărui aviz, autorizație, etc, necesare implementării proiectului;
- Lucrări: Lucrări de amenajare a terenului si/sau fundatiilor, Lucrări de instalare și montaj console, Lucrări de conectare la rețeaua națională de distribuție energie electrica, Lucrări de conectare fibra optica.

Obiectul contractului ce se va încheia pentru investiția *„Implementarea sistemului e-Sigur”*, denumită și Proiect, în Caietul de sarcini, presupune realizarea următoarelor etape:

- realizarea analizei cu privire la sectoare optime pentru amplasarea echipamentelor în teren, pe baza datelor din accidente aferente anilor 2023, 2024, 2025. Conform metodologiei vor fi luate în considerare 400 de puncte în ordinea importanței conform listei orientative de sectoare anexa la prezentul Caiet de Sarcini;
- efectuarea de vizite în teren (site-survey) pe sectoarele stabilite anterior pentru identificarea amplasamentului exact și a condițiilor optime de instalare/montare și documentarea activității (măsurători, imagini, etc.);
- elaborarea planurilor de situație (câte un plan pentru fiecare locație) și a planului transversal pentru fundație;
- obținerea avizului Poliției rutiere pentru punctele de amplasare a mijloacelor tehnice din teren, în conformitate cu prevederile art. 5, alin. (2) din *Legea nr. 383/2022 privind unele măsuri de eficientizare a monitorizării traficului rutier;*
- întocmirea documentației tehnice de proiect în vederea obținerii avizelor și efectuarea tuturor diligențelor necesare în vederea obținerii acestora (daca este cazul);
- stabilirea soluției si proiectarea pentru sistemul informatic pentru nucleul central si pentru echipamentele din teren și obținerea avizului CNAIR;
- întocmirea Proiectului Tehnic de execuție pentru instalarea si montarea consolelor in teren și/sau infrastructurii de rețea si/sau a altor lucrări de conectare la rețele, precum și obținerea avizului CNAIR;
- dezvoltare/customizare a soluției informatice
- livrare console;
- realizarea lucrărilor de instalare si montare a consolelor si infrastructurii de rețea;
- livrarea componentelor hardware si software din teren (cele 400 de sectoare);
- montarea echipamentelor în teren și configurare software/hardware acestora;
- livrarea componentelor hardware și software pentru nucleul central (sistem informatic);
- instalarea, configurarea echipamentelor hardware și a soluțiilor software pentru nucleul central (echipamentele pentru procesare și stocare, sistemul de operare, soluția de virtualizare, backup-restore, securitate aplicații precum și alte componente hardware și software necesare, în funcție de soluția ofertată), astfel încât sistemul informatic integrat

implementat în cadrul proiectului să respecte cerințele tehnice, funcționale și de performanță din prezentul caiet de sarcini;

- livrarea documentației tehnice a infrastructurii software (documentație de instalare și configurare, licențe);
- integrarea și operaționalizarea componentelor/echipamentelor instalate (punerea in exploatare a sistemului);
- elaborarea documentației de testare și de recepție pentru infrastructura furnizată;
- testarea echipamentelor din teren, a infrastructurii furnizate și operaționalizate;
- instruiri pentru personalul beneficiarului;
- lansarea in producție a sistemului;
- recepția lucrărilor și echipamentelor furnizate si a sistemului informatic;
- punerea la dispoziție a unei aplicații de ticketing, gratuit pe perioada de implementare si garanție;
- servicii de mentenanță si suport tehnic pe perioada de garanție;
- recepția finală la expirarea perioadei de garanție.

Toate proiectele, soluțiile, specificațiile și caracteristicile vor trebui detaliate de către Contractant și furnizate Autorității Contractante, spre acceptare si validare. Nici o lucrare, specificație sau caracteristică tehnică nu va fi considerată acceptată dacă nu îndeplinește cerințele minime specificate în prezentul Caiet de sarcini și nu este validată în scris de către Autoritatea Contractantă.

Pentru mijloacele tehnice fixe destinate măsurării vitezei (atât pentru camere video cu radar care au incorporata unitate de procesare locala cat si pentru camere video cu radar care nu au incorporata unitatea de procesare locala precum si pentru unitatea de procesare locala care nu este incorporata in camera video cu radar), Ofertanții vor prezenta în cadrul Propunerii tehnice cel putin documente/dovezi privind inițierea demersurilor de introducere a acestor echipamente în lista de echipamente cu aprobare sau recunoaștere de model a Biroului Român de Metrologie Legală (BRML), daca la data depunerii ofertei mijloacele tehnice fixe destinate masurarii vitezei nu se afla in respectivele liste. Pentru implementarea contractului inclusiv perioada de garantie verificarile metrologice initiale si periodice vor fi realizate în conformitate cu cerințele Caietului de sarcini, în urmă procedurii de site-survey, și în baza aplicării unor metodologii relevante, bazate pe cele mai bune practici naționale si internaționale în domeniul sistemelor inteligente de transport, cu respectarea legislatiei in vigoare la momentul respectiv.

## 1.9 Stabilire locații amplasare sistem de monitorizare a vitezei

Sistemul e-SIGUR va primi semnalări de la multipli senzori instalați pe infrastructura rutieră:

- camere video;
- camere LPR;
- camere cu sistem de măsurare a vitezei;
- sisteme de măsurare a vitezei medii;
- sisteme de cântărire;
- sisteme de tip inductiv;

- echipamente mobile.

În vederea stabilirii locațiilor prioritare pentru instalarea sistemelor video cu capacități de monitorizare a vitezei s-a efectuat o analiză pe baza datelor din accidente rutiere aferente anilor 2021, 2022, 2023 , iar in implementare se va efectua o noua analiza de către contractant astfel încât să se stabilească locațiile finale pe baza datelor din accidentele rutiere aferente anilor 2023, 2024 și 2025 . Datele legate de toate accidentele rutiere aferente anilor 2023, 2024, 2025 vor fi transmise Contractantului de către CNAIR în termen de 10 zile lucrătoare de la data semnării a Contractului.
La nivel european, bunele practici pentru reducerea numărului de accidente includ cu prioritate:

- campanii de educare;
- îmbunătățirea infrastructurii rutiere;
- iluminatul sectoarelor de drum critice;
- monitorizarea vitezei;
- aplicarea de sancțiuni în vederea disciplinării participanților la trafic.

Dintre acestea, monitorizarea și reducerea vitezei, detectarea manevrelor periculoase, împreună cu facilitarea aplicării sancțiunilor impuse de legislația în vigoare sunt singurele măsuri pe care sistemul e-SIGUR le poate implementa.

Pentru a determina locațiile optime de amplasare a sistemelor de monitorizare a vitezei și comportamentului rutier (întoarceri interzise, depășiri interzise, nerespectarea distanței) au fost analizate datele despre accidentele având viteza drept cauză principală.

Astfel, pentru realizarea noii analize se va tine cont de următoarele aspecte:

- vor fi preluate într-un software GIS datele legate de toate accidentele rutiere care au viteza drept cauză principală;
- se va împărți rețeaua națională de drumuri în sectoare de câte 1 km și accidentele mapare pe acestea;
- se va acorda un scoring în funcție de numărul total de victime și va rezulta o primă clasificare a acestora, cele cu număr mare de accidente fiind marcate cu roșu. La capătul opus, sectoarele cu număr minim de accidente vor fi marcate cu verde. Sectoarele cu rezultate intermediare vor fi marcate cu galben.
- pentru prioritizarea acestora se va calcula media numărului de victime și abaterea standard, având o repartiție normală. Sectoarele cu abatere mai mare decât cea standard se vor considera prioritare, iar cele cu abaterea mai mică se vor elimina din analiză.
- Se vor aplica următoarele ajustări manuale:
    - Sectoarele adiacente vor fi comasate în sectoare cu camere în cascadă;
    - Sectoarele aflate la distante foarte mici, de ordinul zecilor sau sutelor de metri, se vor comasa;
    - Se vor elimina punctele de pe bretelele autostrăzilor;
    - Punctele aflate la mare distanță de drum vor fi aduse manual pe sectorul de drum cel mai apropiat prin corectarea datelor accidentului, așa cum au fost ele raportate.

Datele vor fi prezentate tabelar, după următorul model:

| Nr. crt. | Latitudine | Longitudine | Tip punct (roşu/ galben/ verde) | Total Accidente | Total Victime | Indicativ drum | Poz. km. |
|---|---|---|---|---|---|---|---|

Contractantul va transmite rezultatele obținute și în format shapefile (cu fișierele asociate).

Amplasarea efectivă în teren a produselor se va realiza conform proiectului si a avizelor/autorizațiilor necesare, obținute de către contractant.

In vederea întocmirii ofertei, CNAIR pune la dispoziție tabelul cu locațiile (anexa 2 - **Lista orientativa a sectoarelor care poate suporta modificări in implementarea contractului** a caietului de sarcini) rezultate în baza analizei CNAIR descrisa anterior si care au ca date de intrare numărul de accidente din anii 2021, 2022, 2023.

# 2 DESCRIEREA PRODUSELOR, ACTIVITATILOR SI A LUCRARILOR DIN CADRUL PROIECTULUI „IMPLEMENTAREA SISTEMULUI e-SIGUR"

## 2.1 Produsele care fac obiectul „Sistemului E-Sigur"

### 2.1.1 STRUCTURA TIP CONSOLĂ

Console metalice rutiere

Aceste sisteme sunt construcții metalice suple, ușoare care pot fi transportate și instalate în timp scurt și cu un minim de resurse pe orice amplasament ce oferă un acces adecvat.

Înălțimea minimă la care se amplasează brațul consolei, respectiv înălțimea stâlpului consolei trebuie să fie proiectat, astfel încât să se asigure gabaritul pe înălțime de 5,5 m, măsurat de la cota în axul drumului până la limita inferioară a brațului consolei.

Brațul consolei va fi prevăzut cu un canal tehnic încorporat (jgheab/canelură de cablare), dimensionat astfel încât să permită dispunerea și protecția tuturor circuitelor necesare. În interiorul acestui canal vor fi instalate conductoarele pentru alimentarea cu energie electrică a echipamentelor montate pe consolă, precum și cablurile de comunicații destinate conectării camerelor video la cabinet. Sistemul de cablare va include atât circuitele de joasă tensiune, cât și traseele de date pe fibră optică, amplasate conform normelor privind separația și compatibilitatea electromagnetică. Canalul tehnic va asigura protecție mecanică, accesibilitate pentru mentenanță și etanșeitate corespunzătoare mediului exterior.

Stâlpii și brațele consolelor trebuie executați dintr-o singură bucată fără înnădiri pe lungime. Secțiunea stâlpilor și brațelor consolelor trebuie să fie rectangulară.

Consola trebuie să aibă prevăzută la bază o flanșă cu care se fixează în ancorele fundației. Pe fiecare ancoră de fundație, sub flanșa de bază, trebuie să existe o piuliță cu care se poate regla verticalitatea stâlpului consolei. Carcasa cu ancore se va fixa în fundație de beton care va rezulta in urma dimensionarii ansamblului format din consola si fundatie.

Tabla de oțel utilizată la confecționarea consolelor trebuie să fie garantată de producător conform SR EN 10025-2. Pentru a fi corespunzătoare zincării termice (SR EN 1461) mărcile de oțel trebuie să fie clasa 1 (7.4.3 SR EN 10025-2)
Îndreptarea și îndoirea pieselor se va face la cald sau la rece cu respectarea condițiilor impuse prin STAS 767/0.
Abaterea după îndreptare trebuie să respecte prevederile pct. 2.3.1. Din STAS 767/0.
Se vor folosi numai proceduri de sudură omologate.
La sudarea materialelor se vor aplica următoarele reguli:

- Cordoanele vor fi continue pe toată lungimea de contact a pieselor din îmbinare;
- Sudurile de colț vor avea înălțimea egală cu 0,7 din grosimea minimă a pieselor din îmbinare.

Toate îmbinările sudate trebuie examinate nedistructiv prin metodele și procentajul precizat în normativul C150-99 pentru nivelul „C" (precum și SR EN 25817:1993) de acceptare a defectelor în îmbinările sudate.
Condițiile tehnice generale pentru asamblările cu șuruburi, sunt conform STAS 767/2-78.
Toate găurile pentru șuruburi vor fi obținute prin așchiere sau prin stanțare și așchiere.
Este admisă găurirea numai prin stanțare dacă executantul folosește tehnologii omologate ce produc sistematic rezultate satisfăcătoare, adică:
A) încadrarea în cerințele dimensionale și de toleranță;
B) obținerea de găuri lipsite de bavuri sau micro fisuri marginale.
Tolerantele la diametrul găurilor vor fi:
A) +0/-0,5mm pentru găuri până la 20 mm inclusiv;
B) ±0,5mm pentru găuri mai mari de 20 mm.
Toate piulițele vor fi astfel montate încât să fie ușor accesibile în vederea strângerii și verificării strângerii. Organele de asamblare standardizate vor fi zincate conform cerințelor STAS 2700/8.
Toate piesele și subansamblele, cu excepția organelor de asamblare standardizate, vor fi zincate termic.
Condițiile tehnice generale sunt conform EN ISO 1461. Ofertantul trebuie să facă dovadă că are capacitatea să zincheze termic structurile metalice, în conformitate cu standardul EN ISO 1461.
Înainte de operația de zincare suprafețele vor fi curățate mecanic, prin periere cu peria de sârmă, pentru îndepărtarea urmelor de rugină și tundre și apoi vor fi degresate.
Consolele vor fi marcate clar și durabil cu numele sau simbolul producătorului, anul producției și codul unic de produs.
Subansamblele și piesele vor fi marcate în corespondența, astfel încât la montarea pe șantier să fie asigurată asamblarea corectă a acestora. Marcarea se va face cu o etichetă prin poansonare sau folosind vopsea rezistenta la intemperii. Piesele mărunte vor fi identificate prin marcarea cu etichete atașate piesei cu sârmă galvanizată.
Abaterile limita admise la formă și dimensiunile pieselor ale căror desene nu conțin indicații de toleranță vor fi conform:
STAS 767/0: pentru elemente din categoria B.
STAS 11111: pentru piese clasa 2 (piese tăiate și îndoite din tabla).
SR EN 22768-1: tolerante generale.

SR EN 22768-2: tolerante generale
Abaterea de la verticalitate va fi de maxim 2mm la 1m înălțime. Pentru stâlpul consolei abaterea totală de la verticalitate va fi de maxim 10mm.
Termenul de garantie al consolelor va fi de minim 5 ani.
Producătorul stâlpilor în consola trebuie sa dețină și să prezinte următoarele certificări și avizări:

- avizarea proiectelor MLPTL privind verificarea de calitate conform Legii 10/1995 și HG 25/1996 a cerințelor A1, A2 (se va prezenta un model de proiect tehnic avizat MLPTL);
- certificarea producătorului pentru proceduri de sudare conform SR EN ISO 3834-2/2006, respectiv EN ISO 3834-2/2006;
- certificare operare zincare la cald conform SR EN ISO 1461;
- Buletin încercări consola emis de un organism abilitat.
- Proiectul vizat de un verificator de proiecte autorizat.

### 2.1.2 CABINET

Cabinetele vor fi alimentate cu energie electrica utilizând branșarea la rețeaua publica de distribuție a energiei electrice. Realizarea branșamentelor electrice va fi in responsabilitatea si pe cheltuiala Contractantului. Eventualele avize, autorizații, acorduri, etc, sunt in sarcina Contractantului.
Cabinetele trebuie sa fie confecționate dintr-un material metalic cu o rezistenta ridicata la intemperii, grad de protecție minim IP 55. Dulapul trebuie sa fie inscripționat cu semnul "pericol de moarte" și textul "echipamente sub tensiune".

Cabinetele trebuie să fie dotate cu deschizături care să permită trecerea cablurilor de alimentare și de comunicații.

Cabinetele trebuie să fie dotate cu dispozitive pentru fixarea echipamentelor si cu sisteme anti-efracție.

Cabinetele trebuie sa fie dotate cu sistem de închidere și asigurare a ușilor împotriva persoanelor neautorizate.

Cabinetele se vor dimensiona si livra complet echipate cu toate echipamentele necesare (router, UPS, etc) si cu sistemele de prindere si montaj pe stâlpul consolei. Cabinetul va fi montat pe stâlpul consolei la o distanta de sol de minim 4 m fara scara de acces.

### 2.1.3 INFRASTRUCTURĂ NUCLEU CENTRAL (CMT/CNMT)

**a.** Strategia adoptata in dimensionarea si proiectarea infrastructurii se va baza pe asigurarea unei topologii redundante de tip 1+1 pentru toate elementele sistemului, fără niciun SPoF (Single Point of Failure), si asigurarea unui nivel de performanta ridicat. Echipamentele vor fi proiectate pentru utilizare 24/7.

**b.** Tacticile adoptate pentru atingerea obiectivelor strategiei de proiectare infrastructura sunt:
   - Virtualizare

- Shared storage
- Utilizare mecanisme de clustering

**c.** Furnizorul va dimensiona platforma hardware astfel încât sa corespunda următorilor parametri:
- Sistemul va asigura spațiu pentru stocare informații video in format H.264 de la 500 de radare pentru minim 3 ani, dat nu mai puțin de 900TB pe medii magnetice de tip SAS sau NL-SAS. Au fost considerate exclusiv camerele care vor fi instalate pentru eSigur, camerele video de supraveghere de pe autostrăzi si alte sectoare de drum fiind integrate de alte sisteme.
- Sistemul va asigura cel puțin 60TB spațiu de stocare de tip SSD in regim RAID 10 pentru zonele de stocare date istorice si operaționale.
- Timpii de răspuns pentru interogări vor fi de sub 4 secunde pentru orice cerere de populare caz care utilizează date interne.
- Sistemul e-SIGUR va trebuie sa poată prelua cel puțin 4 milioane de semnalizări pe zi de la echipamentele amplasate in teren, sa proceseze si sa stocheze date in zona de Data Lake. O semnalizare ce include timestamp, categorie vehicul, viteza si număr de înmatriculare nu va depăși 8KB spațiu de stocare.
- Serverele care vor deservi mașinile virtuale pentru soluția de analytics vor fi echipate cu suficienta memorie RAM pentru a permite procesarea in memoria bazei de date de evenimente, dar nu mai puțin de 4TB per server
- Numărul de servere pentru infrastructura nucleului central este de minim 9
- Sistemul va conține si cel puțin 2 sisteme de stocare atașate prin rețea SAN ale căror caracteristici tehnice se vor regăsi la cap 2.1.3.III.

**d.** Toate echipamentele vor fi de tip „rackmount 19"

**e.** Toate echipamentele utilizate vor avea configurație interna redundanta din punct de vedere al alimentarilor cu energie electrica si a sistemelor de răcire. In plus, aceste elemente vor fi de tip hot-plug/hot-swap.

**f.** Toate conexiunile intre echipamente vor fi redundante de nivel 1+1 in regim activ-activ, utilizând mecanisme adecvate la nivel logice (e.g STP pentru networking Layer 2 si MPIO pentru storage)

**g.** Echipamentele ofertate trebuie sa fie noi și nefolosite si sa beneficieze de suport din partea producătorului (nu se accepta echipamente uzate sau care nu se mai afla in linia de fabricație a producătorului).

**h.** Echipamentele vor încorpora cele mai recente îmbunătățiri privind design-ul și materialul, ultima revizie software a producătorului și nu sunt anunțate de producător ca fiind de tipul End of Sale, End of Life, End of Support sau echivalent la momentul livrării.

**i.** Toate echipamentele se vor instala în CNMT situat in CIC Nod A0-A3, Autostrada A0 Nord, km 32+300 sau in CMT-uri, la decizia CNAIR SA, furnizarea si instalarea rack-ului sau rack-urilor necesare instalării echipamentelor fiind in sarcina furnizorului.

**j.** Furnizorul va include in propunerea tehnica toate switch-urile de rețea si SAN necesare, echipate cu module adecvate propunerii sale de infrastructura

k. Furnizorul va livra toate elementele de conectică (conectori, cabluri, dispozitive de adaptare mecanică și prindere, electrică etc.) necesare instalării si punerii în funcțiune a echipamentelor.

l. Pe infrastructura platformei vor fi configurate 3 medii: productiv, dezvoltare si testare. Acestea sunt identice din punct de vedere arhitectural (inclusiv ca mecanisme de failover), chiar daca resursele hardware alocate mediilor de dezvoltare si testare sunt mai reduse fata de mediul productiv.

m. Furnizorul trebuie sa se asigure ca in cadrul Propunerii Tehnice sunt incluse toate componentele active și pasive ale infrastructurii de rețea, necesare pentru operarea integrală și eficientă a sistemului informatic.

**I.Specificații minimale servere – minim 9 buc**

| Caracteristică | Cerință tehnică minimală |
|---|---|
| **Procesor** | 2 x procesoare instalate Intel Xeon, AMD Epyc sau echivalent, fiecare cu minim 16 nuclee fizice, frecventa de lucru nativa de min.2.9 GHz sau echivalent. |
| **Memorie** | 512 GB registered ECC DDR4-3200 SDRAM memorie instalată pentru 6 servere si 4TB registered ECC DDR4-3200 SDRAM pentru 3 servere dedicate platformei de analytics |
| | Minim 32 sloturi pentru memorie RAM cu suport disponibile pe echipament |
| **Hard disk drive** | Doar mediile necesare hypervisorului |
| **Interfața grafică** | Integrată |
| **Fabrics** | 4 x 10 Gbit/s Ethernet<br>Interfața specifica soluție SAN ofertate |
| **Interfața administrare** | Out of band Ethernet dedicat |
| **Carcasa** | Montabil în rack cu ocupare maxim 2U spațiu |
| **Sursa de alimentare** | 2 surse redundante |
| **Ventilatoare** | ventilatoare redundante, hot plug |
| **Sisteme de operare suportate** | Linux, VMware, Windows, licențiat corespunzător pentru numărul de nuclee aferent procesorului ofertat |
| **Garanție** | 5 ani la sediul beneficiarului, de la data semnării procesului verbal de recepție cantitativă și calitativă pentru Faza privind Livrarea, instalarea și punerea în funcțiune a echipamentelor |

**II.Specificații componenta WAF (Web Application Firewall)**

| Caracteristică | Cerință tehnică minimală |
|---|---|
| **Tehnologie** | Suport pentru tehnologia de virtualizare ofertată în cadrul acestui proiect;<br>Să nu impună limitări cu privire la numărul aplicațiilor web protejate |

| Caracteristică | Cerință tehnică minimală |
|---|---|
| | Să fie licențiată pentru minim 4 (recomandat 8) nuclee de procesare.<br>Soluția trebuie să fie licențiată pentru o capacitate de procesare a traficului HTTP de minim 500 Mbps. |
| **Modalitati configurare** | Reverse proxy<br>Inline transparent<br>Proxy in mod transparent<br>Offline sniffing |
| **Definire politici** | Definire în mod automat și dinamic a profilelor de securizare pentru aplicații in urma monitorizarii traficului acestora<br>Politici de securitate predefinite<br>Opțiuni de partajare al accesului administrativ pentru configurația profilelor și politicilor de securizare pentru aplicațiile web protejate, prin utilizarea de domenii administrative |
| **Disponibilitate** | Clustering Activ/Pasiv cu sincronizare de configurație |
| **Capabilități de protecție la nivel de aplicație** | Protectie impotriva atacurilor de tip:<br>- Browser Exploits<br>- Brute Force Login<br>- Buffer Overflows<br>- Command Injection<br>- Cookie Tampering/Poisoning<br>- Cross Site Request Forgery<br>- Cross Site Scripting<br>- Denial Of Service<br>- Directory Traversal<br>- Forms Tampering<br>- Hidden Field Manipulation<br>- HTTP Header overflow<br>- Outbound Data Leakage<br>- Local file Inclusion<br>- Man in the Middle attacks<br>- Remote File Inclusion<br>- Session Hijacking<br>- Site Reconnaissance<br>- SQL Injection<br>- XML Intrusion Prevention<br>Protectie DLP cu reguli predefinite și reguli configurabile cu suport pentru expresii de tip Regex<br>Posibilitatea de a defini manual semnături de atac noi<br>Protecție împotriva botnet, crawler, search engine |

| Caracteristică | Cerință tehnică minimală |
|---|---|
| | Posibilitatea de a monitoriza și bloca traficul provenit dintr-o anumită regiune geografică sau țara<br><br>Protectie DoS pentru atacuri la nivel rețea și aplicație:<br>- limitare pentru numărul de cereri HTTP /sec de la o singura sursa IP<br>- limitare a numărului de conexiuni TCP concurente per adresa IP sursă ce folosesc acelaăi cookie HTTP<br>- protectie pentru HTTP request flood făcut de o sursa IP pentru același URL<br>- protectie împotriva cererilor HTTP generate de posibile scripturi (prin validarea browserului client)<br>- blocare a atacurilor de tip TCP SYN flood<br>- limitare a numarului de conexiuni TCP concurente per adresă IP sursă<br>Suport pentru redirectarea cererilor HTTP și modificarea URL-ului și a headerelor, Host și Referer din cereri<br><br>Suport pentru modificarea răspunsurilor HTTP<br><br>Posibilitatea de a impune clienților accesul intr-o anumită ordine a paginilor aplicatiei HTTP protejate, cererile unui client ce nu respecta aceasta ordine trebuie sa poata fi blocate<br><br>Funcționalitate de scanare programabilă și raportare automată a vulnerabilităților aplicațiilor web protejate<br><br>Posibiliatea de a include header pentru HTTP Strict Transport Security (HSTS) în răspunsul serverului de aplicație web către client |
| **Procesare trafic** | Load balancing la nivel de aplicație prin algoritmii: round-robin, weighted round-robin, least connections, round-robin cu persistența sesiunii HTTP<br><br>Rutare dupa conținut HTTP, dupa combinatie intre cookie, URL accesat si headerul Host din cerere<br><br>SSL offloading pentru aplicațiile protejate ce folosesc protocolul HTTPS cu posibilitatea de configurare a nvelului de securitate SSL/TLS |

III. **Specificațiile minimale pentru Sisteme de stocare (2 buc)**

| Caracteristica | Cerința minimă |
|---|---|
| Spațiu de stocare informații video | Format H 264 de la 500 de radare pentru minim 3 ani<br>Nu mai puțin de 900TB |
| Medii Magnetice | Minim 900 TB |

| | |
|---|---|
| | De tip SAS sau NL-SAS |
| Spațiu stocare date istorice si operaționale | Minim 60 TB<br>Tip SSD in regim RAID 10 |
| Timp de răspuns pentru interogări | < 4 sec |
| Capacitate preluare semnalizari | Cel putin 4 milioane/zi |
| Spatiu stocare semnalizare | Max 8KB |
| Stocare | Prin retea SAN |
| IOPS 4K random read | ≥ 1.000.000 |

### 2.1.4 PRODUSE IN TEREN (ECHIPAMENTE)

Camerele de supraveghere a vitezei care sunt echipate cu sistem radar funcționează prin emiterea de unde radio și analizarea reflecțiilor pentru a detecta obiecte și a calcula viteza acestora. În contextul camerelor de viteză, acest lucru implică emiterea de semnale radar către vehiculele care se apropie sau se îndepărtează, captarea semnalelor reflectate și utilizarea schimbării frecvenței pentru a determina distanța exactă a acestora într-un anumit moment (efect Doppler). Prin urmărirea vehiculului și captarea locației sale precise în timp, putem calcula viteza acestuia. Deoarece radarul analizează semnalele reflectate, este important ca aceste semnale să fie cât mai clare posibil raportat la zgomotul de fundal. Este extrem de important ca semnalele radar reflectate de vehicule să nu fie reflectate de alte obiecte din teren (cum ar fi suprafețe mari de metal de-a lungul drumului), deoarece acestea pot induce un așa-numit efect fantomă, ducând la evenimente false pozitive și potențial la măsurători eronate ale vitezei. Atât radarul cât și camera încearcă activ să filtreze astfel de cazuri, dar poziționarea corectă a sistemului este singura soluție pentru rezultate sustenabile pe termen lung. Este important de menționat că producătorii radarelor includ aceste recomandări în fișele de produs, iar nerespectarea lor conduce la posibile contestații ale măsurătorilor.

O cameră de măsurare a vitezei trebuie sa acopere minim 6 m lățime parte carosabila compusa din minim 2 benzi, cu posibilitatea detectării de evenimente de tip circulație pe contrasens sau întoarcere.

Înălțimea de instalare recomandată pentru camerele radar:

- minim 4 metri la amplasare in lateralul drumului;
- minim 5,5 m la amplasare deasupra părții carosabile, respectând limitele de gabarit de libera trecere.

Suportul pe care sunt montate camerele trebuie să fie stabil și să nu oscileze sub acțiunea factorilor de mediu sau a traficului. Camerele vor fi prevăzute cu giroscoape care să semnalizeze aceste condiții pentru a preveni măsurători eronate.

Structurile de montaj vor fi console, în funcție de numărul de benzi si specificațiile tehnice ale echipamentelor instalate.

În fiecare punct de măsurare este necesara următoarea infrastructură:

- suprastructura suport camere și celelalte echipamente;
- branșament energie electrică;
- conectivitate fibra optica, 5G sau microunde;
- cabinet echipamente termostat;
- sistem de tip UPS;
- router industrial;
- echipament de procesare locala;
- cameră video cu radar.

**Specificații design:**

a) Echipamentele vor fi alimentate în curent continuu de la un sistem UPS ce poate asigura autonomia de funcționare pentru minim 2 ore.
b) Camera video cu radar și echipamentul de procesare locala vor fi conectate la un router industrial prin legături Ethernet pe suport cupru SFTP sau optic.
c) Routerul industrial va oferi conectivitate Ethernet sau 5G, cu posibilitate de fallback între acestea.
d) Routerul, echipamentul de procesare locala, UPS-ul și bateriile vor fi amplasate într-un cabinet dedicat, cu grad de protecție IP55.
e) Camera video cu radar trebuie sa fie dotata cu funcții de instalare si management al instalării:
   - Configurare si upgrade web-based si prin software dedicat

Echipamentele vor fi conforme cu normele UE referitoare la: marcaj, imunitate electromagnetica, emisii nominale, siguranța, etc. Conformitatea se va demonstra prin prezentarea de documente justificative.

**Specificațiile minimale pentru camerele video cu radar:**

| **Caracteristica** | **Cerința minimă** |
|---|---|
| Număr senzori CMOS | 2 senzori, 30 FPS la 3Mp cel primar și 120 FPS la 720p cel secundar |
| Lentile | Zoom și focus motorizat |
| Zoom optic | Optics 1: 3.3x |
| Iluminare | Comutare automata zi/noapte<br>Iluminare IR pe timp de noapte |
| Distanță focală | Variabilă, 15-50mm senzor 1 și 4 – 80 mm senzor 2 |
| Distanță LPR/ANPR | Min 20 m |

| | |
|---|---|
| Distanță LPR/ANPR la 0 Lux (iluminat de noapte pentru numere de înmatriculare reflectorizante) | Min 35 m |
| Viteză citita/intregistrata | Intre 0 km si cel putin 250 Km/h |
| Tip radar | Omologat si metrologizat / In curs de omologare si metrologizare pana la punerea in funcțiune |
| Interval măsurare | Cel puțin 0-250 Km/h cu precizie de +/- 3 km/h pentru viteze de pana la 100 km/h, +/- 3% la viteze de peste 100 km/h |
| Număr de obiecte urmărite simultan | Minim 48, cu detecție poziție, viteză, unghi și direcție deplasare |
| Număr de benzi de circulație deservite (3m lățime) | Minim 3 |
| Funcționalități procesare internă | ANPR/LPR, detecție categorie vehicule, semnalizări ADR |
| Stocare internă | 40000 evenimente, cel puțin 32GB |
| Protocoale comunicație suportate | Streaming video ONVIF, RTSP<br>Networking: TCP/IPv6, DHCP,<br>Nivel aplicație: NTP, FTP, HTTPs, SFTP, DNS, SNMP<br>Securitate: SSL/TLS<br>Standardizare: NTCIP |
| Interfețe comunicație | Gigabit Ethernet, port RJ45 sau SFP+<br>GPIO programabil<br>RS232<br>RS485 |
| Standarde mecanice și de protecție | IP 67, IK10, operare intre -30 și +60 grade Celsius în lumina solara directa, carcasa pentru medii acide |

**Specificațiile minimale pentru Sisteme de tip UPS (400 buc)**

| **Caracteristica** | **Cerința minimă** |
|---|---|
| Tensiune de iesire | 12V/ 24V/ 48V |
| Temperatura de funcționare | -30°C la +60°C |
| Port de comunicare pentru Management de la distanta | DA |
| Remote on-off | DA |
| Autonomie | Minim 2 ore calculat in functie de consumul echipamentelor |
| Putere | 500 VA |
| Management SNMP | Inclus |
| Stabilizator/Regulator de tensiune | Inclus |
| Parametrii echipament | Protecție: IP65 |

**Specificațiile minimale pentru Router industrial (400 buc)**

| **Caracteristica** | **Cerința minimă** |
|---|---|
| Specificații hardware | - 8 interfețe GE RJ45<br>- interfețe 2 Gbps SFP<br>- Minim un modul 5G, |
| Capabilități | - Layer 2; IEEE802.3at |
| Protocoale si standarde | - Suport PPPoE<br>- Rutare dinamica<br>- VLAN Tagging(802.1q)<br>- Rutare intre VLAN-uri<br>- Aplicatie dedicata de Management |
| Temperatura de funcționare | - -30°C la +60°C |
| Alimentare | - Sursa dubla |

| | |
|---|---|
| Format | - Montare pe sina DIN |
| Umiditate | - 5-95% fara condens |
| Conectivitate | - 5G NR + fallback 4G |
| Dual SIM | - Da |
| VPN IPSec throughput | - ≥ 500 Mbps |
| Parametrii echipament | Protecție: IP65 |

**Specificațiile minimale pentru echipamentele de procesare locala**

În fiecare locație va fi amplasat un echipament pentru procesarea locală a evenimentelor care poate fi atât incorporat in camera video cu radar cat si separat de aceasta. Acesta va putea transmite alertele în timp real către sistemul e-SIGUR, înainte ca datele video să fie sincronizate în sistem.

Funcționalitățile asigurate de către echipamentul local de procesare sunt:

- detectare nerespectare semnificație culoare semafor;
- detectare nerespectare semnificație semne de circulație;
- detectare folosire bandă de urgență;
- detectare deplasare în sens interzis;
- detectare intrare în zonă interzisă;
- detectare schimbare direcție de mers în zone în care aceasta este obligatorie;
- detectare oprire neregulamentară;
- detectare trecere linie continuă;
- detectare întoarcere nepermisă;
- detectare nerespectare limită de viteză în funcție de categorie de vehicul și condiții meteo;
- detectare lipsă rovinieta validă.

Aceste echipamente vor fi compatibile cu orice cameră video RTSP, făcând posibilă amplasarea în puncte în care acestea deja există și asigurând funcționalitățile necesare e-SIGUR, fără a modifica sistemele centrale existente sau a necesita interfațarea cu acestea (cazul camerelor IP exploatate de către CMT-uri). Echipamentele de procesare locala vor intercepta stream-ul de la camera video cu radar și îl vor retransmite fără re-encodare.

Echipamentele de procesare locala pot fi amplasate în cabinet.

| **Caracteristica** | **Cerința minimă** |
|---|---|
| Input video | RTSP, H.264/H.265 |
| Output video | Input copy |

| | |
|---|---|
| Transmitere semnalizări | WEB API, upload SFTP/HTTPS |
| Stocare internă | 50000 evenimente cu înregistrări video aferente |
| Procesare | GPU sau ASIC |
| Conectivitate | Gigabit Ethernet RJ45 sau SFP+ |
| Standarde mecanice și de protecție | IP40, temperatură operare -30 până la +60 grade Celsius. |
| Standarde electrice | Alimentare CC 12/24 sau 48V, consum maxim 60W. |

## 2.2 SERVICIILE CARE FAC OBIECTUL „SISTEMULUI E-SIGUR"

### 2.2.1 DESCRIERE FUNCȚIONALĂ

Conform Legii 383/2022, e-SIGUR trebuie să asigure următoarele funcționalități:

a) agregare date de la senzorii aflați pe infrastructura rutieră existenta: camere video, ANPR, bucle inductive, radare fixe și mobile;
b) colectare date în scopul analizelor ulterioare;
c) transmitere de notificări către IGPR în cazul constatării unor posibile abateri prevăzute de art. 10 din lege:
   - posibila încălcare a normelor de circulație pe drumurile publice sau posibila prezență în trafic a unor vehicule supuse confiscării, căutate potrivit legii, sau care pot fi utilizate ca probă într-o procedură judiciară;
d) transmitere de notificări către IGPR privind posibila încălcare a normelor de circulație pe drumurile publice vizează:
   - limita maximă admisă de viteză pentru categoria de vehicul pe un anumit sector de drum;
   - interdicția sau restricția de a conduce un vehicul pe o bandă a sensului de deplasare;
   - semnificația culorii roșii a semaforului;
   - interdicția de a conduce pe drumurile publice un vehicul a cărui înmatriculare este suspendată;
   - trecerea la nivel cu calea ferată;
   - interdicția de a adopta un comportament agresiv în conducerea vehiculelor pe drumurile publice.
e) transmitere de notificări către CNAIR pentru prezența în trafic a unor vehicule care circulă fără achitarea tarifului de utilizare și a tarifului de trecere pe rețeaua de drumuri.
f) procesarea notificărilor se realizează exclusiv manual de către lucrătorii polițiști rutieri în sistemele proprii IGPR si numai in cazul vehiculelor care circula fără achitarea tarifului de

utilizare si a tarifului de trecere pe rețeaua de drumuri de către lucrătorii CNAIR, după caz, conform tipurilor de notificări menționate anterior.

Cerințele enumerate mai sus sunt completate după cum urmează:

a) au fost identificate mai multe tipuri de semnalări / cazuri, respectiv: încălcări ale legislației în vigoare, autovehicule căutate, abateri legate de nerespectarea restricțiilor temporare (va fi interogată și baza de date de restricții temporare, cu oprirea alertelor, de exemplu, la circulația dirijată pe sensul opus de mers, dar datele se vor menține), degradarea elementelor de semnalizare rutieră a părții carosabile (de exemplu, vandalism, furt, deteriorare parapet, acestea fiind tipuri de caz care trebuie deschise manual de operatorul CNAIR și se vor gestiona prin sistemul e-SIGUR până la sesizare/plângere). Acestea vor fi considerate dezvoltări ulterioare ale sistemului, nefiind parte din scopul contractului sau al prezentului document de specificații tehnice.
b) sistemul va permite configurarea unui număr arbitrar de tipuri de cazuri cu diverse câmpuri și meta date, fără a necesita dezvoltări suplimentare în sistem;
c) va fi configurat un flux unificat pentru toate interacțiunile identificate între sistemul e-SIGUR și parteneri. Acesta va include și posibilitatea unor reveniri necesare soluționării cazurilor, acestea fiind automatizate pentru toate acțiunile care permit acest lucru (de exemplu, o dată validat cazul de către agent, sistemul va solicita automat date/imagini relevante);
d) va exista un mecanism de filtrare și prioritizare multicriterial al notificărilor transmise către IGPR și CNAIR. Acesta va avea rolul de a aplatiza curba încărcării operatorilor care preiau cazuri, dar și de a reprioritiza urgențele (de exemplu, apropiere termen prescriere);
e) sistemul e-SIGUR va utiliza formatul de date predefinit pus la dispoziție de către IGPR și CNAIR pentru tipurile de cazuri operate de fiecare entitate în parte;
f) datele care vor fi stocate în sistemul e-SIGUR: numere de identificare autovehicule, înregistrări video, înregistrări senzori (bucle, stații meteo, etc). Toate aceste date vor fi corelate spațial și temporal (de exemplu, sistemul va putea să arate întreg parcursul unui autovehicul, înregistrările video aferente, variația greutății acestuia etc). Sistemul nu va stoca nume persoane fizice, nume societăți comerciale, date de contact;
g) toate echipamentele și sistemele de la care e-SIGUR va colecta date vor fi sincronizate în domeniul timp cu servere NTP GPS locale în cadrul fiecărui CMT sau punct de agregare date;
h) echipamentele de procesare locala si camere video cu radar vor fi certificate sau omologate și verificate metrologic, conform prevederilor legale;
i) sistemul e-SIGUR va stoca toate datele colectate, nu doar cele aferente notificărilor transmise către IGPR, într-un mediu de tip Data Lake, pentru procesări statistice ulterioare. Perioada de retenție va fi de minim 3 ani, aceasta fiind configurabilă atât la nivel de sistem pentru Data Lake cât și la nivel de caz;
j) sistemul va putea genera orice analize și rapoarte prin instrumente vizuale, accesibile, fără a fi necesară dezvoltarea unor funcționalități în acest sens;

k) sistemul implementat va avea funcționalități GIS, fiind capabil să stocheze, proceseze și afișeze date georeferențiate;
l) datele vor fi stocate în două containere distincte; OLAP pentru analize de tip big data și OLTP pentru susținerea fluxului operațional. Datele nestructurate vor fi stocate într-o paradigmă de tip Data Lake;
m) având în vedere multitudinea de echipamente și sisteme cu care e-SIGUR se va interfața atât la momentul implementării, cât și în viitor, va fi utilizată o componentă de tip middleware (ESB & API Management) pentru implementarea tuturor integrărilor. Aceasta va facilita integrări ulterioare fără modificări în aplicație;
n) pentru componentele din flux care vor necesita intervenții și completări manuale (de exemplu, se solicită înregistrări mai vechi sau din sisteme ce nu pot fi interfațate cu e-SIGUR fiind prea vechi), operatorii din CMT vor lucra direct într-un modul al e-SIGUR în care vor adăuga elemente cazurilor și vor răspunde la solicitări, transmiterea pe email sau pe suport magnetic/optic a acestora fiind imposibilă sau cel puțin ineficientă. În scopul implementării controalelor de tip chain-of-custody pentru probele administrate, operatorii CMT vor dispune de semnături electronice calificate;
o) sistemul implementat va fi dimensionat pe baza datelor de trafic actuale și a recomandării de amplasare echipamente pe baza de scoring a unor sectoare de drum problematice;
p) amplasarea echipamentelor va fi realizată pe baza unei analize inițiale a datelor disponibile la nivelul anilor 2023, 2024, 2025, conform cap 1.9. După operaționalizarea sistemului e-SIGUR, componenta sa analitică va genera alte sugestii pentru amplasarea de noi echipamente;
q) utilizatorii platformei e-SIGUR vor putea interacționa cu platforma și utilizând limbaj natural, în limba română, prin intermediul unei componente de tip Chatbot. Aceasta va putea fi utilizată pentru a genera ad-hoc rapoarte și analize exclusiv pe baza unui dialog cu utilizatorul.

### 2.2.2 SERVICII DE ANALIZA DETALIATĂ A CERINȚELOR PENTRU SISTEMUL E-SIGUR

Etapa de analiză detaliată presupune identificarea, detalierea, optimizarea proceselor/fluxurilor de lucru și activităților corespunzătoare domeniului specific de aplicare a sistemului e-SIGUR; a rolurilor și responsabilităților; identificarea cerințelor funcționale corespunzătoare nevoilor părților implicate, plecând de la abordarea prezentată în Caietul de sarcini, precum și asigurarea corespondenței între cerințele funcționale și funcționalitățile sistemului.

În cadrul acestei activități se vor analiza fluxurile de lucru, categoriile de date și documente, rolurile stabilite pentru utilizatori, în funcție de poziția ierarhică în cadrul organizației și se va urmări optimizarea proceselor operaționale specifice, existente la nivelul entităților în care urmează să se implementeze sistemul e-SIGUR, potrivit obiectivelor stabilite la nivelul proiectului.

Prin derularea activităților din cadrul acestei etape se urmărește:

- analiza detaliată a cerințelor operaționale;
- stabilirea rolurilor utilizate în sistem și sursele de date;
- analiza sistemelor sau a altor alte aplicații informatice existente la nivelul structurilor implicate în proiect pentru identificarea soluțiilor de integrare și/sau de migrare date/documente;
- identificarea și definirea cazurilor de utilizare, inclusiv a entităților informaționale necesare;
- alinierea cerințelor operaționale cu specificațiile tehnice;
- analiza fluxurilor informaționale și modelarea lor în vederea implementării fluxurilor tehnice;
- optimizarea fluxurilor pentru creșterea performanței sistemului informațional și a procesului de management.

Livrabile:

Raport detaliat de analiză e-SIGUR (fluxuri de lucru/procese operaționale specifice managementului cazurilor, cazuri de utilizare, elemente funcționale, surse și categorii de date, nomenclatoare, cerințe de configurare, integrare etc.). Raportul de analiză va conține inclusiv matricea de trasabilitate a cerințelor raportat la cerințele Caietului de sarcini și specificațiile ofertate.

### 2.2.3 SERVICII DE PROIECTARE SOFTWARE - PROIECTAREA SOLUȚIEI INFORMATICE E-SIGUR

În cadrul acestei etape, pe baza cerințelor funcționale, tehnice și de performanță detaliate/identificate în etapa de analiză, se elaborează un set de specificații de proiectare care să stea la baza construcției soluției. Se stabilesc: arhitectura de detaliu a soluției informatice e-SIGUR, interfețele, modulele, regulile specifice de business care vor fi implementate pentru fluxuri de lucru, sistemul de roluri de utilizare, modelul structurilor personalizate de date (entități, atribute și relații), intrările/ ieșirile în/din sistem, noile procese de lucru pentru utilizarea platformei implementate, specificații tehnice de integrare și de securitate.

Livrabile:

Raport de proiectare a soluției informatice e-SIGUR (arhitectura de sistem și modul în care se propune configurarea componentelor de sistem astfel încât să se obțină funcționalitățile solicitate în caietul de sarcini și/sau identificate/detaliate în etapa de analiză – arhitectura hardware de rețea și securitate, software și funcțională; interfețe; module; funcționalități; specificații tehnice fluxuri; tipuri/categorii de formulare/template-uri care vor fi gestionate; model de date; specificații de securitate și de integrare, rapoarte, etc.). Raportul de proiectare va conține inclusiv matricea de trasabilitate a cerințelor raportat la specificațiile tehnice și funcționale identificate în etapa de analiză.

Sistemul e-SIGUR creează semnalări care trebuie să conțină cel puțin următoarele informații:
a) data, ora și locația exactă a semnalării sau a coordonatelor GPS, după caz;
b) elementele de identificare ale mijlocului tehnic care a generat semnalarea;

c) vehiculul implicat și numărul de înmatriculare ori de înregistrare al acestuia, după caz;
d) viteza de deplasare măsurată cu mijloace tehnice pentru monitorizarea traficului rutier omologate și verificate metrologic, informații privind respectarea cerințelor de omologare și verificare metrologică, precum și viteza maximă admisă pe sectorul de drum, respectiv pentru categoria din care face parte autovehiculul condus;
e) extrasul cadrului din filmarea video care surprinde semnalarea;
f) semnalizarea rutieră a sectorului de drum public relevantă pentru încadrarea juridică a posibilei încălcări a normelor de circulație pe drumurile publice.

Sistemul e-SIGUR trebuie sa fie capabil sa exporte metadatele aferente semnalarilor in format .XML, conform Anexei nr. 3 la Caietul de Sarcini, insotite de Extrasul cadrului din filmarea video care surprinde semnalarea.

Extrasul cadrului din filmarea video care surprinde semnalarea trebuie să conțină o înregistrare de minimum 10 secunde, incluzând 5 secunde anterioare și 5 secunde ulterioare momentului exact al posibilei încălcări a normelor de circulație. Acest interval trebuie să fie nedivizat și să mențină integritatea fluxului video.

### 2.2.4 SERVICII DE DEZVOLTARE/CUSTOMIZARE, INSTALARE ȘI CONFIGURARE A SOLUȚIEI INFORMATICE E-SIGUR

Dezvoltarea/customizarea soluției informatice e-SIGUR, astfel încât să se asigure suportul tehnic necesar pentru gestionarea cazurilor la nivelul structurilor implicate, așa cum au fost ele identificate în etapa de analiză, presupune customizare module/funcționalități deja existente în soluțiile/componentele ofertate, dezvoltare de funcționalități suplimentare, personalizare interfețe grafice astfel încât acestea să reflecte realitățile activității specifice și să fie în conformitate cu reprezentarea validată în etapa de proiectare.

Etapa de dezvoltare/customizare a sistemului are ca obiectiv respectarea cerințelor prevăzute în Caietul de sarcini, respectiv aplicarea rezultatelor obținute în etapele de analiză și proiectare, și vizează implementarea modulelor și funcționalităților soluției informatice ce urmează a fi livrată.

Se vor derula activitățile specifice de dezvoltare/customizare la nivelul componentelor, modelare date/formulare, creare/configurare fluxuri de lucru și interfețe, inclusiv pentru migrarea de date/ integrarea cu alte sisteme existente la nivelul structurilor implicate în proiect.

Ulterior se va realiza instalarea și configurarea platformei e-SIGUR pe infrastructura nucleului central. În această etapă de implementare se va instala soluția software rezultată din activitățile de dezvoltare/configurare și se va realiza o primă testare a soluției implementate (testare internă efectuată de Contractant).

Toate cablurile de alimentare și interconectare pentru funcționarea sistemului vor fi puse la dispoziție de către Contractant.

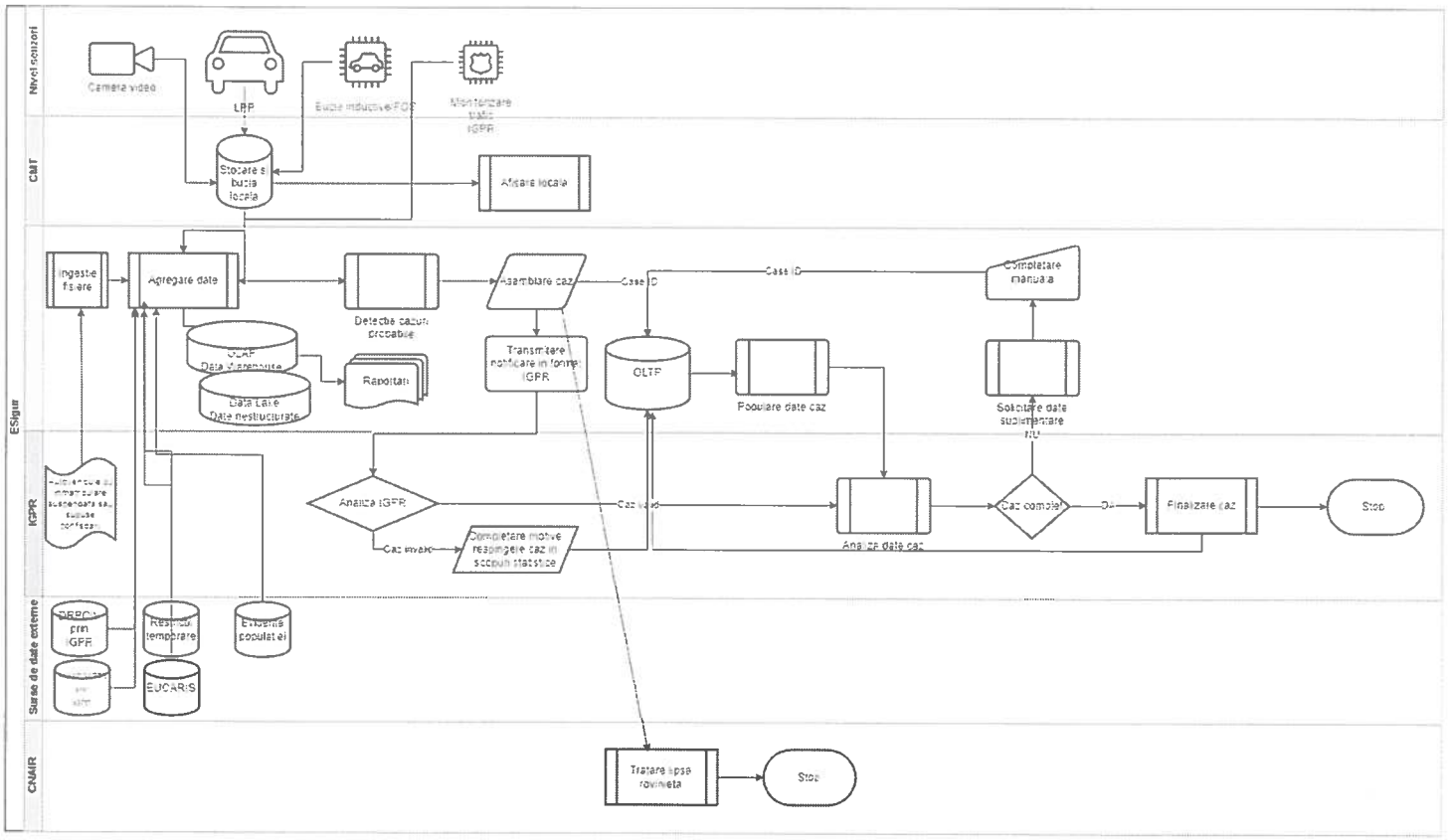
Activitățile de instalare și configurare a infrastructurii nucleu central se realizează la sediul/sediile Beneficiarului. În vederea pregătirii instalării, Contractantul va realiza inspecția locației / locațiilor și se va documenta cu privire la modalitatea de instalare.

Livrabile:

- Platforma software e-SIGUR dezvoltată/customizată, instalată, configurată și pusă în funcțiune pe infrastructura nucleului central;
- Documentația de instalare și configurare platformă e-SIGUR;
- Raport de testare internă.

### 2.2.5 SCENARII DE UTILIZARE ȘI FLUXURI OPERAȚIONALE

**Transmitere notificări către IGPR sau CNAIR**

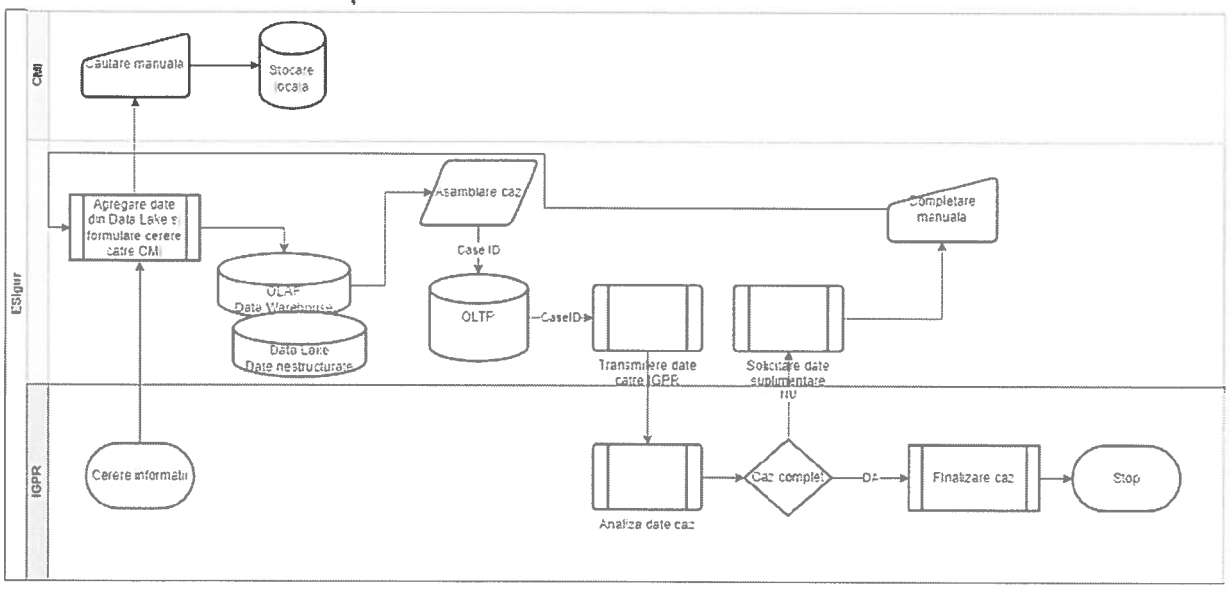



Descriere flux:

a) Datele de la camerele video, sisteme LPR, radare, bucle, senzori sunt colectate la nivelul CMT pentru afișare locală, dar și la nivelul e-SIGUR pentru procesare. Datele de la sistemele mobile sunt colectate direct în e-SIGUR.
b) Din partea IGPR / CNAIR se primesc listele cu vehicule fără drept de circulație, supuse confiscării sau urmărite.
c) Sistemele cu care e-SIGUR se interconectează transmit datele relevante și sunt interogate periodic sau la cerere.

d) Toate datele colectate sunt stocate în zona de Data Warehouse și de Data Lake pentru procesare analitică și raportare ulterioară.
e) Datele colectate parcurg simultan un modul de tip Rule Based Engine care realizează corelarea cu listele transmise și sincronizează datele în domeniile spațiu și timp. Suplimentar, modulul evaluează datele pentru a identifica, pe baza unui motor probabilistic, potențiale abateri ce trebuie semnalizate.
f) Daca este detectat un potențial caz, acesta este asamblat și o notificare este transmisă către platforma IGPR / CNAIR. În paralel cazul este pre populat cu toate elementele probatorii necesare: imagini, înregistrări, date referitoare la dinamica deplasării. Aceste informații vor fi automat copiate în zona de stocare operațională OLTP. Cazul creat are propriile reguli configurabile privind valabilitatea datelor și momentul la care acestea sunt șterse automat.
g) Dacă operatorul IGPR / CNAIR care preia cazul îl marchează spre închidere fără declanșarea unei proceduri de investigare sau sancționare, acesta este arhivat în scopuri statistice și datele aferente eliminate din zona OLTP.
h) Dacă operatorul IGPR / CNAIR marchează cazul spre investigare, acesta are opțiunea de a solicita direct din interfața sistemului date suplimentare sau să dicteze acțiuni cum ar fi urmărire continuă, istoric parcurs, etc. În cazul în care sistemul e-SIGUR nu are acces la aceste date (de exemplu, sunt necesare informații din sisteme vechi ce nu pot fi integrate), va fi generată automat o solicitare către CMT-ul care poate completa manual aceste date.
i) Când operatorul IGPR / CNAIR închide cazul ca urmare a emiterii unei sancțiuni sau a schimbării încadrării, sistemul e-SIGUR arhivează cazul împreună cu toate elementele constitutive, respectând procedurile de chain-of-custody pentru probatoriul administrat.

**Furnizare informații la cerere**




Descriere flux:

a) Operatorul IGPR transmite o cerere de informații către sistemul e-SIGUR, fie prin apelarea unui serviciu web fie prin email.
b) Sistemul identifică dacă există deja date stocate pentru vehiculul urmărit, locațiile și perioadele indicate în cerere. În cazul în care acestea nu există sau se regăsesc în sisteme

legacy cu care e-SIGUR nu posedă integrări, se transmite automat o cerere către CMT-ul responsabil.

c) Operatorii din CMT folosesc interfața web e-SIGUR dedicată pentru a încărca informațiile relevante găsite manual în sistemele CMT.
d) Datele sunt semnate cu semnătura calificată a operatorului CMT și asamblate într-un caz care va fi transmis ca notificare de update caz către operatorul IGPR.
e) Toate datele colectate sunt stocate în zona de Data Warehouse și de Data Lake pentru procesare analitică și raportare ulterioară.
f) Operatorul IGPR verifică dacă datele primite sunt suficiente și, în caz contrar, solicită noi informații printr-o cerere care parcurge întregul flux.
g) Când operatorul IGPR închide cazul ca urmare a emiterii unei sancțiuni sau a schimbării încadrării, sistemul e-SIGUR arhivează cazul împreună cu toate elementele constitutive, respectând procedurile de chain-of-custody pentru probatoriul administrat.

A. Procesare date istorice pentru a determina poziționarea optimă a echipamentelor în teren

Sistemul va permite analiza datelor de trafic și a raportărilor privind accidentele raportate și va face recomandări privind amplasarea de noi echipamente utilizând datele din zona de Data Lake și modulul GIS specializat.

B. Procesare date istorice pentru îmbunătățirea algoritmilor de filtrare și prioritizare a notificărilor

Pe baza deciziilor de urmărire sau nu a cazurilor de către operatorii IGPR, modulul de filtrare și prioritizare va parcurge un proces de învățare continuă pentru îmbunătățirea acurateței filtrării și a algoritmului de prioritizare (de exemplu, deprioritizarea abaterilor mici în perioade de încărcare mare a operatorilor pe baza timpului de soluționare și a numărului de semnalări).

C. Procesare date istorice pentru a determina indicele de sănătate a echipamentelor

Funcționalitățile de Machine Learning ale sistemului e-SIGUR vor fi utilizate pentru a analiza performanța echipamentelor amplasate pe rețeaua națională de drumuri. Setul minim de analize ce vor fi efectuate:

- Rate peste medie de erori în detectarea ANPR/LPR poate indica o amplasare defectuoasă a camerei sau o deteriorare a elementelor optice.
- Rate peste medie de erori în determinarea vitezei pot indica apariția în locația de instalare a unor elemente care generează semnale radar fantomă.
- Pierderea conectivității 5G poate indica necesitatea reconfigurării sau reorientării antenei echipamentului.
- Mentenanța predictivă prin urmărirea temperaturilor de funcționare, a curenților și tensiunilor.

**Arhitectură sistem**

Prin arhitectura sistemului informatic înțelegem structurile, mecanismele și interfețele utilizate, precum și comunicarea între părțile componente. Arhitectura de sistem descrie viziunea fizică și logică a sistemului propus, relevă modul în care sistemul va fi construit, definește modul în care vor fi utilizate diferite concepte, cât și aspecte vizând posibilitatea dezvoltării viitoare a sistemului.

La proiectarea, realizarea și implementarea sistemului informatic trebuie să se țină cont de respectarea întru totul a următoarelor principii generale:

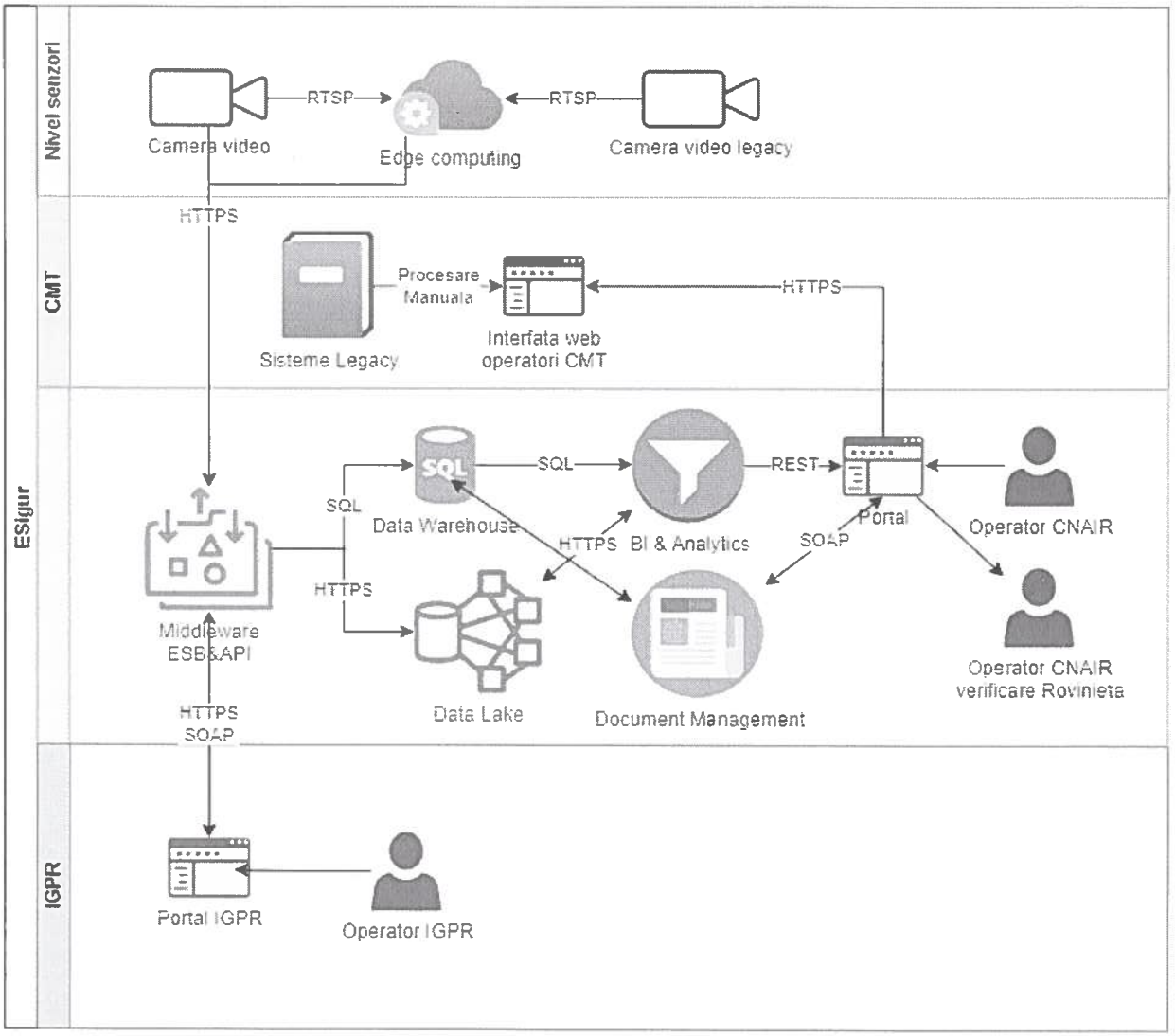
a) *principiul legalității:* presupune crearea și exploatarea sistemului în conformitate cu legislația națională în vigoare și a normelor și standardelor internaționale recunoscute în domeniu;
b) *principiul divizării arhitecturii pe nivele:* constă în proiectarea independentă a componentelor sistemului în conformitate cu standardele de interfață dintre nivele;
c) *principiul arhitecturii bazate pe servicii (SOA):* constă în distribuirea funcționalității aplicației în unități mai mici, distincte - numite servicii - care pot fi distribuite într-o rețea și pot fi utilizate împreună pentru a crea aplicații destinate implementării funcțiilor de business ale sistemului. Această arhitectură va putea să includă de asemenea micro servicii;
d) *principiul datelor sigure:* stipulează introducerea datelor în platformă doar prin canalele autorizate;
e) *principiul securității informaționale:* presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate și eficiență pentru protecția datelor de pierderi, alterări, deteriorări și de acces nesancționat;
f) *principiul transparenței:* presupune proiectarea și realizarea conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice și de telecomunicații. În acest sens este obligatorie evitarea utilizării standardelor proprietare în soluția propusă si este încurajată utilizarea soluțiilor OpenSource;
g) *principiul expansibilității:* stipulează posibilitatea extinderii și completării sistemului cu noi funcții sau îmbunătățirea celor existente;
h) *principiul scalabilității:* presupune asigurarea unei performanțe constante a soluției informatice la creșterea volumului de date și a solicitării sistemului;
i) *principiul simplității și comodității utilizării:* presupune proiectarea și realizarea tuturor aplicațiilor, mijloacelor tehnice și de program accesibile utilizatorilor sistemului, bazate pe principii exclusiv vizuale, ergonomice și logice de concepție;
j) *principiul integrității, plenitudinii și veridicității datelor:* presupune implementarea mecanismelor care permit păstrarea conținutului și interpretării univoce a datelor în condițiile unor influențe accidentale și eliminării fenomenelor de denaturare sau lichidare accidentală a acestora, furnizarea unui volum de date suficient executării funcțiilor de business ale sistemului și asigurarea unui grad înalt de corespundere a datelor cu starea reală a obiectelor pe care le reprezintă și care fac parte dintr-un sector concret al sistemului.

Arhitectura propusă pentru sistemul informatic va respecta următoarele principii:

a) implementarea unei soluții centralizate client-server WEB based cu acces autorizat la interfață și date, utilizând componente software mature;

b) vor fi utilizate containere și va fi implementată o soluție și logică de orchestrare pentru acestea. Soluția ofertată va permite configurarea atât declarativ, cât și prin automatizări sau pipelines CI/CD. Funcționalitățile oferite vor fi de load balancing, service discovery, self healing;
c) asigurarea unei securități adecvate a sistemului informatic pentru a proteja informația și subsistemele componente împotriva utilizării lor neautorizate sau a divulgării informației cu caracter personal sau a celei cu accesibilitate limitată;
d) recunoașterea informației ca patrimoniu și gestionarea ei adecvată;
e) dezvoltarea și implementarea sistemului informatic astfel încât să ofere posibilitatea reutilizării datelor pentru alte procese sau în perspectiva asigurării posibilității de dezvoltare de noi funcționalități;
f) asigurarea capacității de restabilire în urma dezastrelor (asigurarea securității fizice și logice) ca parte componentă a planului de implementare;
g) soluția va fi complet redundantă, evitând orice SPoF (Single Point of Failure); mecanismele de asigurare a redundanței (la nivel hardware și software) vor fi descrise la nivel de cea mai mică unitate funcțională indivizibilă a sistemului;
h) componenta hardware necesara funcționării sistemului va fi dimensionata ca putere de procesare și stocare astfel încât sa asigure funcționarea pentru o perioadă de minim 5 ani fără a necesita upgrade-uri.

D. Diagramă arhitectură




## 2.3 SPECIFICATII COMPONENTA SOFTWARE

Portalul se va implementa pe baza unei platforme de dezvoltare aplicații web din categoria Enterprise Low-Code Application Platform (LCAP). Platforma LCAP trebuie să fie o soluție matură și specializată, introdusă deja în circuitul comercial.

Pentru a asigura performanță, stabilitate și securitate soluția ofertată trebuie să permită implementarea într-o arhitectură de înaltă disponibilitate în configurații de tip activ-activ. Toate nodurile vor participa activ la deservirea cererilor utilizatorilor.

Pentru asigurarea neutralității tehnologice pe termen lung, Platforma de dezvoltare și administrare aplicații web (LCAP) va permite modificarea/ actualizarea/ extinderea aplicațiilor implementate dintr-o interfață grafică, fără a necesita scrierea de cod, dispunând în acest sens de următoarele categorii de funcționalități:

- Managementul rolurilor
- Managementul permisiunilor
- Managementul utilizatorilor
- Interfațare API și administrare
- Automatizare
- Fluxuri de lucru
- Funcții predefinite
- Managementul entităților
- Managementul meniurilor
- Managementul paginilor
- Managementul formularelor
- Managementul listelor
- Managementul funcțiilor de Chatbot

Funcționalitățile de managementul rolurilor trebuie să includă:

- Adăugarea, editarea sau ștergerea rolurilor;
- 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:

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

Funcționalitățile de managementul utilizatorilor trebuie să includă:

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

Funcționalitățile de interfațare API trebuie să includă:

- Crearea de interfețe REST API;
- Crearea metodelor API (GET, POST, PUT, DELETE) pentru execuția logicii (acțiunilor) la nivel de server sau pentru preluarea datelor;
- Securizarea API-urilor prin chei API și token web JSON;
- Mecanisme de partajare a resurselor restricționate ale unei pagini web dintr-un alt domeniu aplicativ.

Funcționalitățile de automatizare trebuie să includă:

- 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);
- Programarea execuției automate a următoarelor job-uri/acțiuni:
    - rulare interogări SQL;
    - rulare executabile;
    - rulare scripturi;
    - postarea de date;
    - transmiterea de e-mailuri;

Funcționalitățile asociate fluxurilor de lucru trebuie să includă:

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

Platforma 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 portal nou;
- 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;
- Conversia datelor HTML în Microsoft Word;
- Copiere fișier într-un alt folder;
- Ștergere entitate, fișier, folder, modul, pagină, portal, rol, utilizator;
- Executare listă de acțiuni;
- Generare cod de bare;
- Generare PDF din șablon HTML;
- Îmbinare (merge) fișiere PDF;
- Injectarea unei imagini în PDF;
- Generare credențiale;
- Interogare date în sursa de date;
- Creare folder nou;
- Conversia unei liste de entități în format CSV și/sau Excel;
- Conversia în format Excel a unei liste de rezultate obținute printr-o căutare (query) în baza de date;
- Încărcare listă de entități din conținutul unui fișier CSV, XLSX, JSON, precum și dintr-o interogare SQL;
- Încărcare conținut dintr-un modul HTML;
- Încărcare pagină în contextul de execuție;
- Încărcare portal 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, portal, rol, profil utilizator, nume utilizator;
- Încărcare fișier(e) pe un FTP;
- Validare utilizator/parolă;
- Înregistrare utilizator;

Funcționalitățile de managementul entităților trebuie să includă:

- Adăugarea, editarea, ștergerea și vizualizarea entităților;
- La crearea unei entități trebuie:
    - să se genereze automat tabelele în baza de date, cu chei index pe baza relațiilor definite cu alte entități;
    - 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;
    - să se genereze un formular pentru introducerea datelor cu câmpuri bazate pe proprietățile definite la crearea entității;
    - să se poată genera o listă de valori pentru a afișa înregistrările asociate entității;
    - să se poată defini o sursă de date pentru entitate;
    - să se genereze automat butoane în interfață prin care să se ofere posibilitatea de a crea, edita, șterge și vizualiza înregistrările;
    - să se poată defini funcții predefinite care să fie utilizate pentru operațiuni de creare, ștergere, actualizare parțială, actualizare și citire;
    - să se poată defini/utiliza API-uri pentru crearea, preluarea, actualizarea și ștergerea înregistrărilor;
    - să se poată genera un tablou de bord vizual în care să se definească KPI-uri pe baza datelor din entitate;
- Reprezentarea vizuală a relației dintre entități;
- Posibilitatea definirii relațiilor dintre entități;
- Configurarea permisiunilor pentru restricționarea accesului la nivel de entitate: vizualizare, adăugare, editare, ștergere;

Funcționalitățile de managementul meniurilor trebuie să includă:

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

Funcționalitățile de managementul paginilor trebuie să includă:

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

Funcționalitățile de managementul formularelor trebuie să includă:

- Posibilitatea definirii unui formular pe oricare pagină în vederea colectării de date;
- Definirea de formulare cu următoarele tipuri de câmpuri:

- 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;
- Număr întreg;
- Email – permite introducerea de conținut de tip text. Validează conținutul pentru a fi o adresa de email validă.
- 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;
- Casetă de text cu editor WYSIWYG - permite introducerea de conținut de tip text și formatarea acestuia prin următoarele opțiuni:
    - Alegerea stilului caracterelor: bold, italic, subliniat, superscript, subscript;
    - Alegerea dimensiunii caracterelor;
    - Alegerea de liste numerotate automat sau cu bullet-uri;
    - Alegerea spațierii între rânduri;
    - Alegerea alinierii textului la stânga, la centru, la dreapta;
- 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;
- Dropdown - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică;
- Dropdown cu autocompletare - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică, permițând filtrarea listei de opțiuni pe măsură de textul este introdus;
- Dropdown cu casete de verificare - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică, prin bifarea acesteia;
- Alegere multiplă cu casete de verificare - permite alegerea uneia sau mai multor opțiuni dintr-o listă predefinită sau dinamică.
- Casete cu butoane de opțiune (radio button) - permite alegerea unei opțiuni dintr-o listă predefinită sau dinamică de tip radio button;
- 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;
- 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;
- 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;
- Parolă/Confirmare parolă - permite introducerea parolelor. Parolele nu sunt vizibile la tastare și sunt criptate.
- Valută - Permite introducerea de sume de bani prin configurarea: monedei, definirea poziția însemnului distinctiv la monedei, definirea separatorului de zecimale, definirea separatorului de mii;
- Posibilitatea definirii direcției etichetelor pentru fiecare câmp (sus, stânga, dreapta);

- Posibilitatea adăugării de instrucțiuni de completare pentru fiecare câmp;
- Posibilitatea definirii de validatori personalizați pentru orice câmp. Aplicația va dispune de următorii validatori predefiniți:
    - Număr întreg;
    - Număr întreg pozitiv;
    - Email;
    - Dată;
    - Obligatoriu;
- Posibilitatea condiționării validatorilor în funcție de alte câmpuri pentru a putea permite crearea logicii afișării sau validării câmpurilor unui formular;
- Generarea listei de opțiuni pentru câmpurile cu alegere multiplă de tip dropdown sau cu casete de verificare, trebuie să se poată realiza prin:
    - Listă statică de formă cheie/valoare;
    - Interogări ale bazei de date prin care se aduc datele;
    - API ce returnează format JSON;
- 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:

- 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;
- Posibilitatea adăugării de noi surse de date;
- Permite definirea pentru fiecare coloană a funcționalităților de filtrare, ordonare, sortare și căutare;

Funcționalitățile de management al funcțiilor de chatbot trebuie să includă:

- mecanisme de inteligență artificială care să permită interacțiunea naturală a actorilor aplicațiilor web implementate;
- motor NLU multi-language care să identifice intențiile utilizatorului și entitățile de sistem;
- posibilitatea antrenării asistentului inteligent pentru a răspunde la întrebări simple sau complexe, atât cu fraze introduse manual, dar și prin integrarea cu surse de date din aplicațiile implementate;
- posibilitatea configurării trimiterii de notificări;
- generarea de rapoarte avansate în format PDF, MS Word sau Excel. Să asigure un generator PDF încorporat;
- asistarea utilizatorilor în completarea unor documente;
- detectarea intenției utilizatorului;
- extragerea automată a entităților;
- motor NLP cu suport pentru limba română;
- colectarea de date din informațiile introduse de utilizator, din acțiuni și din aplicații;
- utilizarea datelor colectate pentru a oferi răspunsuri contextuale;
- filtrarea conversațiilor.
- funcționalități built-in de OCR
- Suport nativ în limba română, cu diacritice
- Configurarea de fluxuri conversaționale ( fără scriere de cod)

- configurarea comportamentului chatbot-ului în cazul în care acesta nu înțelege cerința utilizatorului;
- monitorizarea calității modelului de antrenament;
- stocarea istoricului de conversații.

Conținutul aplicațiilor dezvoltate pe platforma portal va fi introdus și afișat în format Unicode (UTF-8) – lucru care va permite afișarea concomitentă a textelor în caractere latine (inclusiv diacriticele românești).

Din punctul de vedere al licențierii, Platforma de dezvoltare și administrare aplicații web (LCAP) trebuie să acopere un număr nelimitat de utilizatori, pentru toate instanțele de server web necesare respectării cerințelor de arhitectură a sistemului și cerințelor de performanță.

Licențierea platformei portal va asigura un drept de utilizare perpetuu pentru beneficiar și nu va impune limite privind numărul de utilizatori ce vor accesa aplicațiile web dezvoltate pe aceasta, în mod autentificat sau neautentificat.

**Componenta management de documente și lucru colaborativ**

Componenta trebuie să implementeze și să funcționeze ca un depozit central de documente, având totodată și funcționalitățile necesare de modelare și rulare procese de business ce au sau nu la bază documente electronice, ce produc sau nu documente electronice.

Aplicația software de management al documentelor va fi bazată pe o soluție „Low code/No code", introdusă în circuitul comercial de cel puțin 3 ani. Nu se accepta dezvoltări, ci doar configurări sau personalizări, pentru a se asigura implementarea soluției prin utilizarea unei metodologii de tip prototip evolutiv, oferind astfel utilizatorilor o imagine concretă asupra modului de gestionare a documentelor și a metadatelor asociate, a versiunilor acestora, precum și a fluxurilor de lucru cu documente.

Aplicația va asigura gestionarea documentelor și a metadatelor asociate, a versiunilor acestora, a tuturor fluxurilor de lucru și a obiectelor, facilitând astfel ținerea evidenței activității sistemului e-Sigur în sistem informatizat și circulația electronică a documentelor în cadrul acestuia.

Aplicația va asigura înregistrarea, scanarea și stocarea în forma electronica a oricărui document, alături atributele, metadatele și datele descriptive conexe, care să ajute la o rapidă organizare și regăsire ulterioară a informației;

Aplicația va asigura trasabilitatea circuitului documentelor în cadrul sistemului e-Sigur, punând la dispoziție instrumente prin care să asigure în orice moment vizualizarea traseului documentelor, utilizatorul la care se află documentul, starea asociată etc.

Aplicația va asigura automatizarea proceselor de lucru existente în cadrul sistemului e-Sigur prin implementarea de fluxuri de lucru electronice pentru circulația documentelor.

Aplicația software de management al documentelor trebuie să fie o soluție complet integrată, scalabilă, deschisă și extensibilă, pentru asigurarea interoperabilității cu alte aplicații/sisteme informatice, atât prin API cât și prin interfețe și/sau conectori dedicați.

Aplicația software de managementul documentelor va fi implementată astfel încât să asigure utilizarea de către următoarele categorii de utilizatori:

a) Utilizatori standard
b) Utilizatori avansați
c) Utilizatori de tip administrator

Utilizatorii avansați vor dispune de toate funcționalitățile oferite de aplicația software de managementul documentelor, accesibile la nivelul utilizatorului.

Utilizatorii standard vor dispune de toate funcționalitățile oferite de aplicația software de managementul documentelor, mai puțin cele referitoare la scanare.

Utilizatorii de tip administrator vor dispune de toate funcționalitățile oferite de aplicația software de managementul documentelor și, în plus, vor putea efectua următoarele acțiuni:

a) configurarea funcțiilor, a serviciilor și a meniurilor aplicației;
b) configurarea depozitelor de documente și a registrelor;
c) definirea fluxurilor;
d) configurarea integrării cu soluții de management a utilizatorilor și accesului;
e) gestionarea locațiilor de stocare a documentelor, a tipurilor de obiecte, cheilor de criptare, precum și definirea și gestionarea profilurilor de backup ale soluției, vizualizarea și editarea fișierelor de configurare, instalarea și managementul componentelor soluției;
f) configurarea directoarelor de rețea monitorizate pentru declanșarea automată a unor fluxuri de lucru ori de câte ori se importă un fișier;
g) configurarea interfațării cu server de email pentru transmiterea mesajelor generate de aplicație;
h) configurarea conturilor de email monitorizate pentru declanșarea automată a unor fluxuri de lucru ori de câte ori se importă un fișier;
i) configurarea interfațării prin servicii web de tip REST cu alte aplicații informatice, în vederea facilitării accesului la documentele stocate precum și pentru preluarea documentelor care trebuie stocate;
j) configurarea task-urilor pre-programate care trebuie declanșate la momente de timp pre-fixate;
k) monitorizarea conexiunii între diferitele componente ale soluției;
l) monitorizarea tuturor operațiilor și evenimentelor din soluție;
m) monitorizarea mesajelor legate erori survenite și/sau de blocarea unor fluxuri (de exemplu datorită unor erori de concepere a acestora în faza de proiectare);

Aplicația trebuie să asigure accesul utilizatorilor la funcționalități, în funcție de rol și locație, prin intermediul unor clienți web.

Accesarea aplicației de către utilizatorii standard ce utilizează client de tip web, se va realiza prin intermediul unui browser web, fără a fi necesară instalarea pe stația de lucru de utilitare sau plugin-uri. Browser-ele web prin care se va realiza accesarea vor fi Chrome, Edge, Firefox, Safari, compatibile cu standardele HTML5, CSS și JavaScript;

Pentru asigurarea unui acces centralizat și controlat, aplicația va asigura identificarea fiecărui utilizator în sistem prin utilizarea de conturi unice și personalizate de acces.

În funcție de autorizarea conferită utilizatorului, acesta va avea acces doar la documentele, fluxurile, registrele și funcționalitățile aplicației, în conformitate cu drepturile de acces stabilite, în raport cu rolul și locul din organizație;

Interfața aplicației prezentată utilizatorului va fi în limba română, inclusiv meniurile aplicației și mesajele de eroare;

Interfața aplicației trebuie să prezinte informațiile prin utilizarea de meniuri, sub-meniuri și meniuri contextuale.

Aplicația trebuie să permită utilizatorului modificarea și personalizarea modului de afișare, a schemelor de culoare, a casetelor de dialog, precum și configurarea accesului rapid la funcții sau ascunderea acestora.

Aplicația trebuie să permită utilizatorului configurarea afișării sarcinilor active după diverse criterii, precum ordonare ascendenta/descendenta, tipul sarcinii, termene limita, etc.

Aplicația trebuie să permită utilizatorului configurarea zonei de afișare a sarcinilor de lucru prin posibilitatea de definire a unor profile de vizualizare care să secționeze ecranul astfel încât utilizatorul să aibă acces la toate zonele necesare pentru desfășurarea activității în mod centralizat – în urma definirii acestor profile de vizualizare va avea acces minim la lista de sarcini active, formularul atașat fluxului de lucru și structura de directoare asociată sarcinii.

Interfața grafică a aplicației trebuie să fie dinamică, în sensul adăugării sau ascunderii automate a datelor și funcționalităților la care un utilizator/grup de utilizatori are/nu are acces;

Interfața grafică a aplicației trebuie să asigure utilizatorului facilități avansate de vizualizare a documentelor de tip imagine: scalarea imaginii, încadrare pe înălțime, încadrare pe lățime, full-screen, mărire imagine în funcție de procent, previzualizare document, rotire pagina etc.;

Câmpurile din interfața aplicației vor asigura introducerea și afișarea textului în format Unicode (UTF-8) – lucru care va permite afișarea textelor în caractere latine (inclusiv diacriticele românești).

Aplicația trebuie să permită definirea unei structuri arborescente pentru depozitele de documente electronice (arhive), organizată pe directoare și sub-directoare, pre-configurate sau generate dinamic în funcție de metadatele asociate documentelor.

Aplicația nu trebuie să limiteze tipul de format de fișier ce poate fi arhivat/stocat, fiind permise atât fișierele de tip text, imagine, cât și orice alt tip de fișier;

Aplicația trebuie să dispună de un motor de recunoaștere optică a caracterelor prin care se va realiza extragerea automată a textului din documentele electronice (inclusiv pentru fișiere de tip imagine), pentru a facilita căutarea avansată de tip full-text în toate documentele din depozit (pentru care exista drepturile de acces relevante).

Aplicația nu va limita posibilitatea de adăugare a metadatelor pe documente în funcție de tipul de document/fișier.

Aplicația trebuie să dispună de funcționalitatea de anulare (Undo) a următoarelor acțiuni efectuate în interfață asupra dosarelor și/sau documentelor: mutare dosar/document, ștergere dosar/document, utilizare ca referință dosar/document, editarea metadatelor la nivel de dosar/folder;

Aplicația trebuie să dispună de mecanisme de sincronizare a documentelor și metadatelor asociate din depozit cu un sistem extern de fișiere de date (file-system);

Aplicația trebuie să permită ordonarea elementelor din structura de organizare a depozitului în funcție de mai multe criterii: sortare manuală, alfabetică crescătoare sau descrescătoare, în funcție de data arhivării etc;

Aplicația trebuie să asigure trasabilitatea modificărilor efectuate pe documente prin jurnalizarea acțiunilor realizate de utilizator în acest sens.

Aplicația trebuie să permită afișarea unui document în mai multe locații din depozit prin crearea de referințe sau copii ale acestuia.

Aplicația trebuie să pună la dispoziție un mecanism de căutare complex care să permită identificarea rapidă și facilă a informației pe baza unor criterii multiple și a unor opțiuni de căutare avansata, în toate depozitele de documente electronice în care utilizatorul deține dreptul de a caută documente. Aplicația trebuie să permită realizarea căutărilor în funcție de metadate, comentarii, versiuni, adnotări asupra documentelor, precum și căutare în conținutul documentelor;

Aplicația trebuie să asigure facilitați avansate de căutare full-text în toate documentele din depozit (pentru care există drepturile de acces relevante) utilizând operatori logici, funcții de autocompletare în baza caracterelor deja introduse, auto-corecție a termenilor în cazul în care aceștia au fost introduși greșit, opțiunea de evidențiere a termenilor căutați, posibilitatea de excludere a unor termeni de căutare etc.

Aplicația trebuie să asigure limitarea apariției duplicatelor în cadrul depozitului verificând astfel, automat, la fiecare încărcare, nu doar denumirea noului fișier, ci și conținutul acestuia (CRC sau similar). În cazul detectării duplicatelor, aplicația va notifica utilizatorul și îi va oferi posibilitatea de a realiza referință către un obiect existent în depozit.

Aplicația trebuie să dispună de capabilități intrinseci de transfer de tip batch pentru importul rapid al volumelor mari de documente în depozite, asigurând cel puțin următoarele funcționalități:

a) Încărcarea documentelor în depozite în locațiile corespunzătoare, asigurând totodată atașarea metadatelor din fișierele cu metadescriptorii asociați;
b) Monitorizarea unuia sau mai multor directoare în vederea detectării unui flux de date;
c) Să permită ca structura de stocare să fie definită în funcție de anumite metadate ale documentelor, dar să asigure și posibilitate personalizării structurii.

Aplicația trebuie să asigure transformarea în format electronic a documentelor în format letric, precum și preluarea acestora direct în aplicație prin integrarea cu dispozitive scanner ce dispun de drivere ISIS și/sau TWAIN.

Aplicația trebuie să asigure transformarea în format electronic a documentelor în format letric, folosind echipamente de scanare de rețea, asigurând preluarea automată a acestora în aplicație prin monitorizarea unui sistem de fișiere.

Aplicația trebuie să permită unirea paginilor într-un document electronic (Merge PDF) .

Aplicația trebuie să permită împărțirea documentului electronic în pagini (Split PDF).

Aplicația trebuie să asigure lucrul colaborativ pe documente prin mecanism de Check-în/Check-out, cu blocarea la editare a documentului de către alți utilizatori.

Aplicația trebuie să asigure controlul versiunilor pentru documente și trasabilitatea fiecărui document în parte. Vor fi stocate în sistem versiunile pentru fiecare document după realizarea modificărilor de către utilizatorii cu drepturile de acces corespunzătoare.

Aplicația trebuie să asigure posibilitatea de a reveni la o versiune anterioara – „roll back", precum și posibilitatea de comparare a versiunilor.

Aplicația trebuie să asigure posibilitatea marcării versiunilor blocate la ștergere.

Aplicația trebuie să asigure inclusiv păstrarea de versiuni pentru metadatele asociate documentelor.

Aplicația trebuie să asigure utilizarea șabloanelor de documente și crearea de documente noi pe baza acestor șabloane.

Aplicația trebuie să permită utilizatorilor să creeze alerte atât la nivel de folder cât și la nivel de document prin configurarea următorilor parametri: denumire, prioritate, dată, informații, utilizatori/grupuri de utilizatori care vor fi notificați.

Aplicația trebuie să asigure instrumente de lucru pentru utilizatori, ce vor facilita comunicarea acestora prin mesaje și vor permite schimbul de fișiere, direct din interfața aplicației.

Aplicația trebuie să asigure utilizatorilor un cadru integrat de colaborare pe documente și fluxuri de lucru, prin posibilitatea schimbului de mesaje de colaborare pe document și păstrarea istoricului acestei corespondențe.

Pentru gestionarea informației din sistemul e-Sigur, documentarea anumitor procese și gestionarea know-how-ului instituțional, aplicația va include următoarele funcționalități integrate de tip forum, parametrizabile, care vor permite schimbul de informații rapid între utilizatori și va asigura trasabilitatea și transparenta:

a) Definirea de către utilizatori a unor spații de lucru de tipul: domenii sau subiecte de interes general, etc;
b) Spațiile de lucru vor fi evidențiate vizual în interfața aplicației;
c) La accesarea unui spațiu de lucru, utilizatorul va putea vizualiza lista de postări;.

d) Posibilitatea ca utilizatorii să realizeze postări care să includă text, linkuri, imagini, documente;
e) Posibilitatea ca utilizatorii să posteze comentarii;
f) Posibilitatea utilizatorilor de a se abona la spațiile de lucru pentru a primi notificări cu privire la noutăți;

Aplicația trebuie să permită utilizatorilor cu drepturi corespunzătoare, crearea (configurarea) unor comisii/echipe de lucru pentru un anumit document sau proiect, prin definirea utilizatorilor care vor avea posibilitatea să încarce documente și să modifice/editeze documentele distribuite.

### 2.3.1 CERINȚE PRIVIND FLUXURILE ELECTRONICE

Fluxurile de lucru pre-configurate prezentate utilizatorului vor fi cele pentru care acesta are drept de utilizare în conformitate cu rolul său în sistemul e-SIGUR.

Pentru implementarea proceselor aferente circulației documentelor, aplicația trebuie să permită utilizatorilor să creeze fluxuri ad-hoc, prin stabilirea activităților asociate (avizare, aprobare, semnare, etc.), definirea unuia sau mai multor participanți și a tranzițiilor dintre activități. La definirea unui astfel de flux se va putea stabili: tipul distribuției (secvențial sau paralel), prioritatea, participanții implicați (la nivel de utilizator sau grup), definirea de escaladări (termenul de declanșare, utilizatorul către care se escaladează). Utilizatorul va putea să salveze fluxul astfel definit (ca șablon) pentru utilizarea ulterioară.

Aplicația trebuie să asigure posibilitatea monitorizării fluxurilor de lucru prin vizualizarea datelor relevante sub forma grafică (diagramă), tabelară și listă.

Aplicația trebuie să asigure afișarea diagramei fluxului de lucru, cu indicarea poziției documentului în cadrul fluxului.

Aplicația trebuie să asigure afișarea sarcinilor primite de utilizatori prin intermediul fluxurilor de lucru, precum și posibilitatea filtrării sarcinilor după o perioada de timp selectată de utilizator.

Aplicația trebuie să asigure marcarea sarcinilor ca citite/necitite.

Aplicația trebuie să asigure posibilitatea unui utilizator de a redirecționa o sarcină de lucru către un alt utilizator.

Aplicația trebuie să asigure posibilitatea filtrării listei sarcinilor de lucru, în funcție de utilizatorii implicați pe flux sau starea în care se găsește fluxul de lucru: activ, finalizat, cu termen limită depășit, etc.

Aplicația trebuie să asigure definirea și transmiterea alertelor și notificărilor în platformă cât și via email către utilizatorii participanți la flux, în funcție de evenimentele de pe flux (activitate nouă pe flux, apropierea unui termen limită, depășirea unui termen limită, etc). Utilizatorul va avea posibilitatea de a accesa sarcina/evenimentul direct de pe email.

Aplicația trebuie să asigure posibilitatea repartizării sarcinilor între utilizatori și clasificarea acestora pe nivele de prioritate.

Aplicația trebuie să asigure un mecanism de management al delegărilor pentru sarcinile asociate fluxurilor de lucru. Fiecare utilizator va putea să-și delege sarcinile către unul sau către multipli utilizatori pe o anumită perioada de timp.

Aplicația trebuie să asigure escaladarea în funcție de criterii flexibil predefinite, asigurând ca minim:

a) escaladare în funcție de tipul maxim normat pentru realizarea unui pas din flux;
b) escaladare în funcție de timpul maxim normat pentru finalizarea derulării întregului flux;
c) escaladare graduală către diferitele nivele de superiori ierarhici pentru la atingerea unor praguri de întârziere predefinite.

Aplicația trebuie să asigure asignarea drepturilor de acces în mod diferențiat în ceea ce privește accesarea/utilizarea fluxurilor de lucru – de exemplu, un utilizator va avea acces doar la anumiți pași de flux.

Aplicația trebuie să asigure managementul fluxurilor de lucru definite și va acorda posibilitatea ca utilizatorii cu drept de acces în acest sens, să realizeze modificări asupra fluxurilor de lucru de tipul: versionări, export, creare sau ștergere șabloane de fluxuri de lucru.

Aplicația trebuie să asigure posibilitatea configurării preluării în pașii de flux a documentelor și metadatelor din alte aplicații informatice.

Aplicația trebuie să asigure posibilitatea configurării în pașii de flux a formularelor web (create prin intermediului designer-ului inclus în aplicație). Anumite câmpuri ale formularelor web vor fi completate automat de către aplicație, iar altele vor fi completate de utilizatori.

Aplicația trebuie să permită implementarea de mecanisme de distribuire automată a sarcinilor din fluxurile de lucru către utilizatorii dintr-un grup în funcție de următoarele criterii:

a) Încărcarea utilizatorilor
b) Round robin
c) Valori ale unor indecși

Aplicația trebuie să permită utilizatorilor participanți la fluxurile de lucru să întreprindă acțiuni de aprobare/respingere. În cazul respingerii, să oblige utilizatorul să motiveze respingerea.

### 2.3.2 CERINȚE PRIVIND SEMNAREA ELECTRONICĂ A DOCUMENTELOR

Aplicația trebuie să dispună de mecanisme de aplicare a semnăturii electronice calificate asupra documentelor.

Aplicația trebuie să asigure posibilitatea marcării poziției de aplicare a semnăturii electronice calificate.

Aplicația nu va condiționa semnarea documentelor cu semnătură electronică calificată prin mecanisme de check-out/check-in. Cu alte cuvinte, aplicația va asigura semnarea fără descărcare/încărcare pe/de pe stația de lucru a utilizatorului, a documentelor transmise pe fluxurile de lucru electronice sau stocate în depozit, și fără a fi nevoie de instalarea manuală de utilitare (programe de calculator) pe stațiile locale, în cazul clienților de tip web.

Aplicația trebuie sa permită ca un document ce se afla pe flux să fie semnat multiplu cu diferite certificate calificate (emise de furnizori de servicii de încredere diferiți), de către utilizatori.

### 2.3.3 CERINȚE PRIVIND TRANSMITEREA ȘI EXPORTUL DOCUMENTELOR

Aplicația trebuie să asigure posibilitatea utilizatorilor de a genera referințe (shortcut-uri) ale documentelor și directoarelor din depozit, pentru a facilita accesul controlat și temporar la documente ce nu pot fi transmise prin email din motive diverse (de exemplu: dimensiune prea mare).

Utilizatorii vor putea transmite referințele (shortcut-urile) documentelor și directoarelor din depozit, prin email sau prin alte mijloace de comunicare electronică, direct din interfața de acces a aplicației.

Referințele (shortcut-urile) generate de utilizatori pentru documentele și directoarele din depozit, vor putea fi configurate de către aceștia pentru a se limita la un număr de descărcări sau pentru o anumită perioadă de valabilitate.

Aplicația trebuie să asigure posibilitatea exportului documentelor dintr-un folder, direct din interfața aplicației, în format zip cu posibilitatea configurarea următorilor parametri: intervalul de timp în care au fost încărcate documentele, tipurile de documente, export structura directoare cu documente, export doar documente, export doar structura de directoare, directoare fără documente, versiuni documente, lista metadate.

Aplicația trebuie să permită utilizatorilor exportul unei colecții de documente din depozit, împreună cu toate atributele lor sau doar o parte din acestea, pentru a fi puse la dispoziția unei entități terțe, prin care aceasta, direct dintr-un browser web, fără a fi nevoie de instalarea de programe de calculator de tip utilitar sau plug-in, să poată:

a. Vizualiza organizarea documentelor în structura de directoare stabilită la configurarea exportului;
b. Previzualizarea documentele direct din browser;
c. Căuta documente după cuvinte din denumirea fișierului;
d. Descărca documentele.

### 2.3.4 CERINȚE PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL

Din punct de vedere al alinierii și respectării cerințelor referitoare la protecția datelor cu caracter personal, aplicația va asigura îndeplinirea următoarelor cerințe minimale:

a. Să permită identificarea automată a datelor cu caracter personal (CNP, e-mail) în documentele încărcate în depozit și marcarea acestora printr-o metadată ce evidențiază un document ce conține date cu caracter personal;
b. Să asigure evidențierea vizuală automată a denumirii documentelor care conțin date cu caracter personal

c. Să pună la dispoziție o funcție de export pentru documente și metadate asociate, care să permită mascarea datelor cu caracter personal, cu excepția fișierelor de tip imagine (pentru care este necesară prelucrarea manuală);

### 2.3.5 CERINȚE PRIVIND ADMINISTRAREA ȘI CONFIGURAREA

Aplicația trebuie să permită vizualizarea tuturor utilizatorilor conectați și permite deconectarea unui anumit utilizator.

Aplicația trebuie să permită configurarea perioadei de inactivitate a utilizatorilor în vederea deconectării automate a acestora.

Aplicația trebuie să permită configurarea politicii de parole, referitor la:

a. complexitatea parolei (trebuie să se poată utiliza minim opțiunile : majuscule, litere mici, un număr minim de caractere al parolei);
b. schimbarea forțată a parolei la următoarea/prima logare în sistem;
c. permite definirea politicilor de parolare pentru utilizatori individuali, pentru grupuri, la nivel global din interfața de administrare;
d. schimbarea forțată a parolei la data menționată;
e. schimbarea parolei cu solicitarea de modificare a acesteia – cu opțiunea utilizatorului de a refuza acest lucru și să continue logarea cu parola originală, situație în care cererea de modificare va fi afișată la fiecare încercare noua de logare în sistem, pana la modificarea acesteia.

Aplicația trebuie să permită configurarea mecanismelor de securitate bazate pe grupuri, roluri, utilizatori și funcții din organigramă. Drepturile de securitate și permisiunile vor fi special proiectate astfel încât să permită controlarea accesului utilizatorilor la documente și tipul drepturilor de acces.

Aplicația trebuie să permită organizarea utilizatorilor în grupuri. Un utilizator poate face parte din unul sau mai multe grupuri. Permisiunile de securitate și drepturi de acces se vor putea asocia cu grupurile de utilizatori (aplicându-se tuturor utilizatorilor membri la momentul controlului accesului).

Aplicația trebuie să permită definirea și administrarea drepturilor multiple de acces în cadrul soluției, adăugarea utilizatorilor noi și gruparea/alocarea acestora în grupuri predefinite și moștenirea de drepturi.

Aplicația trebuie să permită definirea drepturilor de acces pe tipurile de fluxuri de lucru pe care un utilizator le va avea disponibile. La nivelul fiecărei activități din flux se vor putea defini drepturi pentru cine va avea acces la acea activitate și drepturi referitoare la acțiunile care se vor putea desfășura de către utilizator.

Aplicația trebuie să permită posibilitatea de asociere de drepturi în mod granular, pe diferite nivele (directoare, documente, tipuri de documente, atribute ale documentelor, grad clasificare, etc), până la nivel de obiect și câmp index.

Aplicația trebuie să permită administratorului să definească și să întrețină un set general de atribute la nivelul organizației din care să se poată selecta ce atribute să apară pe fiecare tip de document.

Aplicația trebuie să permită administratorului să definească mai multe depozite de documente, ce pot fi utilizate în același timp. Fiecare depozit de documente va avea propriile date primare (utilizatori, grupuri de utilizatori, parole, formulare, liste de valori), cât și tranzacționale (foldere, drepturi, restricții aferente obiectelor, informații ierarhice, referințe logice, documente, activități).

Aplicația trebuie să includă un designer dedicat pentru definirea formularelor electronice pentru unele tipuri de documente gestionate, care să fie utilizate ca șabloane de documente.

Designerul de formulare electronice va asigura cel puțin:

a. crearea de formulare dinamice de tip responsiv și interactive;
b. crearea de formulare cu tab-uri și metadate dinamice cu afișare de metadate în funcție de condiționalități;
c. completarea automată a anumitor câmpuri;
d. includerea pe câmpuri a unor formule de calcul;
e. Posibilitatea definirii a câmpurilor de tip: dată, text, casetă de verificare, semnături, imagine, link, de tip buton pentru adăugarea sau ștergerea liniilor;
f. introducerea de reguli și validări pe câmpurile formularului;
g. preluarea de date din surse externe de informație, cum sunt alte sisteme software sau baze de date externe;
h. definirea modului de vizualizare în funcție de echipament: desktop, telefon, tableta.

Aplicația trebuie să asigure definirea și utilizarea de nomenclatoare de documente.

Aplicația trebuie să asigure jurnalizarea tuturor operațiilor, evenimentelor și acțiunilor desfășurate în aplicație. Aceste informații vor putea fi accesate de administratorul de sistem prin intermediul rapoartelor de audit.

Aplicația trebuie să includă un designer de fluxuri care să permită utilizatorilor cu rol de administrator definirea vizuală, direct în aplicație a fluxurilor de lucru aplicabile documentelor.

Designerul de fluxuri va pune la dispoziție cel puțin următoarele instrumente predefinite prin care să se realizeze configurarea pașilor fluxurilor de lucru prin metoda drag-and-drop: nod de tip start, nod de tip end, activitate, conectori, porți logice (noduri de decizie), porți paralele (noduri de distribuție și respectiv noduri de colectare);

Aplicația trebuie să dispună de mecanisme de administrare a fluxurilor electronice de lucru dintr-o interfață grafică, precum acțiuni de definire, configurare, activare, dezactivare butoane de acțiuni, organizare dinamica a secțiunilor din interfață, profile de vizualizare/colecții de teme, posibilitatea de asociere a activităților către utilizatori și roluri din organizație.

Aplicația trebuie să permită modificarea fluxurilor de lucru predefinite prin intermediul designerului grafic, prin operații de drag and drop și asignare de relații. Modificarea nu trebuie să presupună scriere de cod.

Aplicația trebuie să permită configurarea fluxurilor de lucru atât prin intermediul designerului grafic, cât și prin dezvoltarea de scripturi pentru realizarea unor automatizări suplimentare sau implementarea regulilor de proces specifice companiei.

Aplicația trebuie să permită administratorului să configureze funcțiile, a serviciile și meniurile aplicației în conformitate cu rolul, apartenența la grupuri și drepturile utilizatorului. Parametrizările se vor realiza fără a fi necesara dezvoltarea de cod;

Aplicația trebuie să permită administratorului să configureze locațiile de stocare a documentelor, a tipurilor de obiecte, precum și definirea și gestionarea profilurilor de backup ale sistemului, vizualizarea și editarea fișierelor de configurare, instalarea și managementul modulelor soluției, etc;

Aplicația trebuie să permită administratorului să configureze să monitorizeze toate operațiile și evenimentele realizate în sistem, cu evidențierea de date relevante și posibilitatea de a exporta rapoartele de audit;

Aplicația trebuie să permită administratorului să configureze să configureze reguli pentru migrarea automată a conținutului pentru optimizarea stocării, păstrând accesibilitatea și nevoile de conformitate în decursul timpului;

Aplicația trebuie să permită administratorului să configureze mecanismele pentru asigurarea continuității activității în caz de dezastru, prin care să asigure:

i. Sincronizarea bidirecțională a două sau mai multe depozite de documente atât în ceea ce privește datele primare (utilizatori, grupuri de utilizatori, parole, formulare, liste de valori), cât și a celor tranzacționale (foldere, drepturi, restricții aferente obiectelor, informații ierarhice, referințe logice, documente, activități);
ii. Sincronizarea totală sau parțială a unor părți din depozit;

Aplicația trebuie să permită administratorului să configureze integrarea cu soluții de management a utilizatorilor și accesului;

Aplicația trebuie să permită administratorului să configureze noi registre electronice și totodată să definească drepturile de editare/vizualizare pentru acestea la nivel de rol sau de utilizator;

Aplicația trebuie să permită administratorului să definească tipurile de documente;

Aplicația trebuie să permită administratorului să asigure personalizarea interfeței de utilizare în funcție de rolul utilizatorilor, permițând astfel o standardizare a prezentării funcționalităților disponibile;

Aplicația trebuie să permită administratorului să definească chei de criptare prin intermediul interfeței de administrare și să configureze utilizarea de chei de criptare diferite pentru diferite tipuri de documente și/sau pentru diferite depozite de documente;

Aplicația trebuie să permită administratorului să configureze joburi pentru exportul automat de documente din depozit către un spațiu de stocare, în vederea salvării copiilor de siguranță ale documentelor;

Aplicația trebuie să permită administratorului să creeze filtre de căutare care să se aplice fluxurilor de lucru în funcție de:

a. Starea fluxurilor de lucru: active, finalizate, toate fluxurile, fluxurile cu termen depășit
b. Utilizatorii implicați pe fluxurile de lucru: inițiatori, prezenți pe pașii de flux, prezenți pe pașii încă activi
c. Data de start, intervalul de timp

Aplicația trebuie să permită administratorului să creeze formulare electronice printr-un un designer de formulare electronice.

Designer-ul de formulare electronice va permite adăugarea următoarelor tipuri de câmpuri/atribute specifice:

a. Câmpuri de introducere informații (string, numeric, etc)
b. Câmpuri de tip dată
c. Câmpuri de tip text
d. Câmpuri de tip area text
e. Câmpuri de tip check-box
f. Câmpuri de tip radio button
g. Câmpuri de tip combo box
h. Câmpuri de tip semnătură
i. Câmpuri de tip buton, inclusiv adăugare linie sau ștergere linie
j. Câmpuri de tip imagine
k. Câmpuri de tip link

Designer-ul de formulare electronice va permite configurarea parametrilor câmpurilor

Designer-ul de formulare electronice va permite introducerea unor reguli de validare cu privire la numărul de caractere din fiecare câmp

Designer-ul de formulare electronice va permite preluarea de date din surse externe de informație (sisteme software, baze de date externe, etc)

Designer-ul de formulare electronice va permite completarea automată a anumitor câmpuri,

Designer-ul de formulare electronice va permite implementarea formule de calcul,

Designer-ul de formulare electronice va permite posibilitatea de adăugare sau ștergere de câmpuri din formulare,

Designer-ul de formulare electronice va permite utilizarea de script-uri pentru implementarea diverselor automatizări,

Designer-ul de formulare electronice va permite implementarea de liste de valori dinamice

Aplicația trebuie să permită administratorului să expună formulare electronice în exteriorul platformei prin intermediul API;

Aplicația trebuie să permită administratorului să configureze reguli pentru migrarea automată a conținutului pentru optimizarea stocării, păstrând accesibilitatea și nevoile de conformitate în decursul timpului;

### 2.3.6 CERINȚE PRIVIND ARHITECTURA INTERNĂ ȘI PERFORMANȚA

În vederea eliminării riscului de creștere a dimensiunii sistemului de gestiune a bazelor de date relaționale și creșterea timpului de răspuns, documentele vor fi păstrate independent de sistemul de gestiune a bazelor de date relaționale. În sistemul de gestiune a bazelor de date relaționale se vor păstra doar legăturile către fișierele din depozit, alături de metadatele acestora.

Aplicația trebuie să permită funcționarea cu cel puțin trei din următoarele sisteme de gestiune a bazelor de date relaționale: PostgreSQL, Oracle și Microsoft SQL.

Aplicația software de managementul documentelor se va implementa printr-o arhitectură bazată pe servicii, care să asigure o disponibilitate de 99,96 % pentru mediul de producție pentru serviciile aplicative oferite utilizatorilor, în condițiile de performanță și încărcare solicitate mai sus, printr-o combinație de mecanisme care să includă:

a. Gruparea serviciilor aplicative nucleu, din punct de vedere logic și funcțional pe mai multe servere de aplicații (instanțe virtualizate) care să îndeplinească roluri diferite;
b. Clusterizare la nivelul serverelor de aplicații și a celor de baze de date
c. Componentizarea/modularizarea soluției prin descompunerea în microservicii și instalarea în containere sau mașini virtuale, asigurându-se astfel scalabilitatea și portabilitatea soluției..

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 sistemului e-SIGUR aferent CNAIR;
b. Mediul de testare – dezvoltare, va fi utilizat pentru:
   - dezvoltarea de module/funcționalități noi;
   - dezvoltarea de modificări ce vor fi aduse mediului principal de producție;
   - testarea și validarea modificărilor, înaintea promovării acestora pe mediul de producție;
   - validarea integrării cu diverse aplicații și sisteme informatice.
c. Mediul de recuperare în caz de dezastru – asigură stocarea copiilor de siguranță a mașinilor virtuale, bazei de date și depozitelor de documente din centrul de date principal.

Mediul de producție și cel de testare-dezvoltare vor fi găzduite în centrul de date principal.

Pe parcursul implementării se vor elabora proceduri/procese dedicate atât pentru migrarea dezvoltărilor (testate și acceptate) de pe mediul de dezvoltare/testare pe mediul de producție cât și de pe mediul de producție pe mediul de dezvoltare/testare.

### 2.3.7 COMPONENTA BAZA DE DATE

Componenta baze de date va fi un sistem SGBDR care sa asigure atât capabilitățile de tip OLTP, cât și cele de tip OLAP necesare platformei.

Modelul OLTP este o bază de date responsabilă pentru procesarea operațională a tranzacțiilor. Trebuie să fie rapid, dinamic și să răspundă la eșecurile bazei de date cu un plan de rezervă. Acesta este backend-ul de date operațional pentru cazurile de utilizare și, în majoritatea cazurilor, este inclus cu aplicația (în special pentru modelul IaaS). Depozitul de date propus pentru platforma e-SIGUR se bazează pe o bază de date relațională (bază de date SQL) și poate acționa ca un backend unic operațional pentru aplicațiile ce compun platforma.

Scopul procesărilor OLAP este de a salva datele istorice aferente procesului e consultare și de a oferi suport proceselor de extragere, transformare, încărcare (ETL) care sunt utilizate pentru analiza datelor. Bazele de date OLAP sunt folosite pentru a analiza date multidimensionale din mai multe surse și perspective.

Baza de date utilizată va implementa un model hibrid HTAP care să permită ambele modele de procesare fără copierea datelor în arii distincte și va îndeplini următoarele cerințe:

a) să permită importul și exportul de date în format .csv.;
b) datele vor fi stocate in UTF-16 sau UTF-8;
c) să permită minimizarea conflictelor de acces la date și garantarea simultaneității accesului la date;
d) să permită reorganizarea, mutarea, redefinirea de tabele, fără blocarea activității;
e) să ofere suport pentru columnar indexes;
f) să ofere posibilitatea de stocare și gestiune de structuri de date de tip XML utilizând mecanisme native ale bazei de date;
g) să ofere suport pentru proceduri stocate și triggeri;
h) să ofere suport complet pentru folosirea de expresii regulate;
i) să permită salvarea/restaurarea și arhivarea/dezarhivarea datelor în regim de lucru online fără oprirea serviciilor;
j) să asigure refacerea accesului la baza de date în mod automat în caz de incident;
k) să ofere o facilitate pentru înregistrarea tuturor modificărilor bazei de date, pentru a permite recuperarea bazei de date (înregistrarea tranzacțiilor);
l) să ofere mecanisme de control și blocare la nivel de înregistrare și mecanisme de asigurare a consistenței la citire, fără escaladare, pentru a permite accesul în mod concurent al utilizatorilor la date;
m) în interiorul bazei de date tabelele să poată fi relocate sau să își poată modifica tipul și parametrii de stocare, să poată fi adăugați noi indecși sau reconstruiți, adăugate, redenumite sau eliminate coloane fără a întrerupe accesul utilizatorilor finali la datele în curs de modificare;
n) să ofere mecanisme de clustering. Sistemul trebuie să fie disponibil și 100% funcțional pentru utilizatori în cazul apariției unei defecțiuni la unul din membrii cluster-ului;
o) sa ofere stocare nativa si operatori pentru date de tip GIS
p) să ofere posibilitatea de rulare pe diverse platforme hardware, cloud și pe sistemul de operare propus pentru platformă.

### 2.3.8 COMPONENTA GIS ȘI ANALYTICS

Utilizând portalul ca punct unic de intrare, componenta trebuie să fie accesată prin intermediul browserelor web utilizate pe scară largă (cel puțin Chrome, Firefox, Internet Explorer).

Sistemul trebuie să asigure că oricărui formular îi pot fi atașate documente în diferite formate (de ex.: .doc, .pdf, etc.)

Toate interfețele grafice cu utilizatorii ale platformei vor fi localizate în limba română și vor folosi o terminologie adaptată mediului și vocabularului profesional al specialiștilor care vor utiliza sistemul.

Fiecare listă din aplicație va avea atașată o zonă de filtrare după informațiile existente în listă, precum și după criterii specifice definite de către administrator. Filtrarea trebuie să suporte cel puțin controale de tip picklist și text liber.

Platforma trebuie să ofere posibilitatea de a sorta informația din tabel după criterii de ordonare aplicate la nivelul unei coloane.

Sistemul trebuie să ofere o componentă de hartă interactivă web în care trebuie să se asigure:

a) vizualizarea datelor geospațiale gestionate de sistem;
b) vizualizarea informațiilor tehnice la nivel de hartă prin intermediul etichetelor (label) și a casetelor de informare de tip tooltip;
c) navigarea în hartă folosind mouse-ul pentru acțiuni de zoom in/out și pentru acțiuni de tip pan (navigare). Navigarea în hartă trebuie să se poată realiza inclusiv prin intermediul unor butoane dedicate (zoom in/ out) și navigare spre puncte cardinale;
d) instrumente de măsurat care sa permită calculul suprafețelor sau a distantei dintre doua puncte.

Harta interactivă trebuie să asigure funcționalități de tip legendă. La nivel de legendă trebuie să se asigure următoarele funcționalități:

a) vizualizare/ascundere panou legendă;
b) ascundere/afișare strat;
c) afișare strat cu subcategorii (de exemplu, strat de drumuri clasificat în drum național/județean/comunal). Sistemul trebuie să permită inclusiv ascunderea/afișarea unei singure categorii (de exemplu, drumuri comunale).

Utilizatorii sistemului trebuie să poată deschide fișa oricărui obiect din hartă prin intermediul unor acțiuni sau butoane preconfigurate. Deschiderea fișei va fi condiționată de selectarea în hartă a elementului.

Sistemul va permite definirea de analize pe seturi de date multiple in funcție de nevoile existente. Administrarea analizelor se va face prin interfețe grafice fără a necesita cunoștințe de programare.

Sistemul va permite conectarea la una sau mai multe baze de date din care vor fi definite dimensiunile analitice.

Vizualizarea analizelor definite poate fi făcuta de către utilizatorii soluției in baza rolurilor si a drepturilor de acces definite de administrator. Conectarea se va face direct la baza de date, iar

analiza va afișa rezultatele conforme cu informațiile existente in baza de date la momentul accesării.

Sistemul va conține interfețe vizuale prin care sa poată fi vizualizată structura datelor din baza de date și va permite modelarea acestora în vederea definirii dimensiunii analitice. Pentru rezolvarea situațiilor complexe sistemul va conține și o zonă în care să poată fi introdusă fraza SQL.

Sistemul trebuie sa permită crearea analizelor simple și complexe prin punerea la dispoziția utilizatorului cel puțin a următoarelor elemente care pot fi combinate individual sau agregat în funcție de nevoile analitice:

a) liste prin care sa fie afișate informațiile in format tabelar;
b) funcții de tip pivot pentru afișarea perspectivelor cantitative;
c) diagrame de tip bară, plăcinta, arbore sau din puncte;
d) carduri, indicatoare, imagini, casete text;
e) harți prin care să fie analizate informațiile GIS: afișare puncte, afișare agregată ca plăcinte, bule și hărți tematice;
f) elemente de filtrare: filtru interval, filtru casetă combo, filtru casetă listă, vizualizare arborescentă cu posibilitate de selecție, filtru dată.

Poziționarea fiecărui element (control) trebuie să fie la îndemâna prin funcții de tip drag and drop cu opțiuni de așezare în pagina fișă sau automată.

Elementele pot fi configurate ca independente sau interconectate moment în care selecția unei valori să filtreze celelalte elemente incluse în analiză.

Sistemul trebuie să asigure construirea interfeței în funcție de roluri și grupuri de roluri pe baza drepturilor alocate de către administrator.

Componenta de fluxuri de lucru GIS trebuie să ofere independență la nivel de aplicație față de baza de date relațională utilizată.

Componenta platformei care asigură fluxurile de lucru GIS trebuie să dispună de vizualizare la nivelul aplicației a modelului de date construit precum și descrierea acestuia.

### 2.3.9 COMPONENTA CHATBOT

Componenta chatbot va fi utilizată pentru a permite utilizatorilor CNAIR să interfațeze cu platforma utilizând exclusiv limbaj natural, fără a fi necesare cunoștințe speciale de operare a platformei.

Componenta chatbot va putea fi accesată de orice utilizator cu drepturi de acces a platformei. Răspunsurile și acțiunile permise vor fi restricționate la nivelul de acces al utilizatorului.

Componenta chatbot va putea fi accesată prin portalul web, prin email, utilizând limba română.

### 2.3.10 COMPONENTA BI ȘI MONITORIZARE FLUXURI

Platforma de analiză avansată și vizualizare date va fi bazată pe o soluție matură, existentă pe piață și va permite utilizatorilor specializați efectuarea de căutări consolidate în datele încărcate în depozitul de date, precum și efectuarea de analize specifice. Această componentă va permite

definirea unui model de interpretare a datelor încărcate în depozitul de date, pe baza căruia vor fi accesate entitățile și atributele acestora.

Soluția va fi construită pe o arhitectură modernă, bazată pe microservicii, în care modelele și datele să fie procesate în memoria RAM.

În acest scop platforma de analiza avansată și vizualizare date va îndeplini următoarele cerințe:

a) Accesarea platformei să fie prin intermediul unui browser web
b) În funcție de drepturile utilizatorilor, aceștia să aibă acces limitat la anumite modele și date
c) Să pună la dispoziție o zona de lucru comună de tip „repository" în care sa fie accesibile, conform drepturilor, rapoartele, analizele, sursele de date, modelele, etc. putând fi căutate și filtrate pe baza unor criterii, precum si posibilitatea de a organiza și selecta elementele proprii de interes fiecărui utilizator
d) Să ofere posibilitatea de a accesa rapid rapoartele construite;

În ceea ce privește crearea de rapoarte și analize să asigure următoarele funcționalități:

a) Construire automata de grafice și analize doar prin selecția câmpurilor relevante și drag-and-drop în spațiul de lucru, fiind ales cel mai relevant tip de vizualizare
b) In urma selecției unui câmp să se marcheze vizual, automat, alte câmpuri ce sunt relevante din punct de vedere date pentru crearea unei vizualizări
c) Tipurile de vizualizări trebuie sa includă: bar chart, box plot, bubble plot, crosstab, dot plot, vizualizări de serii de timp, heat map, histograme, hărți geografice cu zone, puncte, accelerometre, liste, pie chart, waterfall, hărți cu legături intre puncte/rețele, etc.
d) Prezentarea informației prin aplicarea de filtre, integrarea cu sisteme de vizualizare și prezentare externe prin furnizarea datelor facilitând integrarea cu librării Java Script ( de exemplu D3, C3, Google Chart) pentru vizualizarea datelor;
e) Prognoza – folosind indicatori și date la nivel calendaristic sau orar să se poată crea prognoze bazate pe istoric cât și pe alți factori ce vor fi evaluați automat de către sistem. Prin folosirea prognozelor sistemul va putea furniza și scenarii what-if, utilizatorii putând varia factorii ce influențează indicatorul urmărit, în scopul identificării scenariului relevant pentru viitor.
f) Word Cloud – folosind date nestructurate sa se poată prezenta informația in format de tip word cloud putând fi selectata sursa textului, indicatorul de dimensionare a textului precum si indicatorul folosit pentru selectarea culorii dintr-un gradient selectat
g) Text Topic – folosind date nestructurate de tip text liber sa se poată construi si identifica automat subiecte de interes/discuție ce sumarizează textele furnizate folosind limbaj natural in identificarea termenilor folosiți. Informația se va prezenta vizual sub forma de subiecte (topic-uri) identificate si o harta a termenilor identificați
h) Network Analysis – folosind date ce constituie o rețea (ex: interacțiuni, ierarhii organizaționale, tranzacții, etc) sa se poată construi rețele vizuale pentru analiza atât la nivel de harta cat si independent, daca nu exista date relevante geografice.
i) Explicații automate – folosind tehnologii de tip machine learning sa se poată evidenția automat, în limbaj uman, explicații ale unor variabile, bazat pe celelalte variabile, fiind prezentate vizual legătura, distribuții, histograme, cat si texte ce explica aceste date,

utilizatorii fiind nevoiți doar sa selecteze datele ce vor fi analizate, restul fiind generat automat de către sistem.

În ceea ce privește crearea de analize si rapoarte trebuie sa includă și următoarele capabilități de analiză avansată:

a) Clusterizare/Segmentare - Posibilitatea de a crea clusterizări folosind vizual algoritmi de tipul K-means prin care sa se selecteze numărul de segmente precum și variabilele folosite pentru segmentare. Să se prezinte vizual într-o diagramă segmentele identificate, bazat pe variabilele selectate centroidul fiecărui segment, extinderea precum si suprapunerea cu celelalte segmente. Pe lângă partea vizuală să fie incluse și statistici de tipul: cel mai apropiat segment, distanta către cel mai apropiat centroid, distanta medie a obiectelor dintr-un segment, etc. Pentru a facilita analiza rezultatelor, va putea fi generat ID-ul segmentelor create sub forma unui câmp nou de date ce va putea fi folosit in alte rapoarte si analize, explicând astfel segmentele(clusterele) create.
b) Arbori decizionali - Posibilitatea de a crea arbori decizionali în același mod vizual prin selectarea câmpului „target" – de analizat și a factorilor ce sunt relevanți din punct de vedere business și care vor fi utilizați de către model. Vizualizarea trebuie să ofere imaginea de ansamblu a arborelui, precum și statistici relevante în evaluarea rezultatelor: Gini, KS, F1 Score, Lift, Tau, ASE, Gain, Gamma. Construirea arborelui sa se poată face automat, automat prin specificarea hiperparametrilor: cât timp sa ruleze, câți algoritmi să testeze etc, precum și interactiv, prin care utilizatorul specifică fiecare ramură a arborelui cum sa se extindă în funcție de sugestiile sistemului dar și de nevoile și constrângerile de business. De asemenea, în construirea automată a arborilor să se poată defini parametri de tipul: numărul de ramificații maxim, adâncimea arborelui, dimensiunea minime de observații per ramura, etc. configurând astfel modelul conform cerințelor necesare organizației.
c) Regresii lineare și logistice – Posibilitatea de a crea interactiv, similar cu arborii decizionali modele de tip regresie liniara, logistica, adaptate pentru orice fel de variabile țintă (inclusiv binare). Modelele trebuie sa poată fi construite atât automat cat si prin influenta parametrilor si hiperparametrilor, similar arborilor decizionali.
d) Compararea modelelor – Posibilitatea de a evalua mai multe modele ce sunt create in același context (valoare de analiza, partițiile create) folosind grafice pentru a evidenția importanta câmpurilor de intrare pentru fiecare model in parte, care este modelul campion din cele evaluate.

### 2.3.11 COMPONENTA ESB & API MANAGEMENT

Componenta ESB va fi utilizata atât pentru integrarea modulelor interne ale platformei, cât și cu surse de date si sisteme externe, inclusiv respectarea standardelor de interoperabilitate prevăzute în NRRI (Ordinul MCID nr. 21286 din 26.10.2023) și Legea nr. 242/ 2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate.

Componenta va asigura următoarele funcționalități:

a) să poată realiza transformarea mesajelor de tip CSV, XML, HTML, JSON, RFC în formatul intern al ESB;
b) să suporte protocoalele standard SOAP, REST, FTP, HTTP, HTTPS, SFTP, SMB;

c) să suporte definirea și urmărirea de politici tip QoS (Quality of Service) la nivel de aplicații;
d) să ofere suport pentru soluții de integrare deschise bazate pe principiile SOA;
e) să ofere mecanisme interne pentru asigurare configurații de tip High Availability;
f) să ofere mecanisme de definire și trimitere alerte;
g) să ofere o interfață vizuală intuitivă pentru definirea proceselor;
h) să suporte standardele WS-ReliableMessaging și WS-AtomicTransaction;
i) să funcționeze ca un broker de mesaje cu următoarele cerințe:
    - mesajele în formate incompatibile trebuie să poată fi procesate prin procese de splicing, agregare, clonare și augumentare;
    - mesajele pot fi trimise la unul sau mai multe endpointuri;
    - soluția ESB va garanta ca mesajele sunt livrate către endpointuri o singură dată;
    - soluția ESB va fi capabilă să routeze mesajele conform unor seturi de reguli, oferind în același timp mecanisme de routare de tip „publish and subscribe".
j) soluția ESB trebuie să suporte mecanisme automatizate de failover între noduri;
k) integrările cu alte platforme informatice cum ar fi IGPR si DRPCIV vor respecta următoarele cerințe:
    - Integrările vor fi de tip deschis, utilizând paradigma SOA;
    - Integrările vor respecta standardele WS-I Basic Profile, WSDL, WS-*, XML, SOAP, REST, UDDI sau GraphQL, soluția de tip ESB oferind suport pentru toate acestea;
    - Soluția va avea adaptori incluși pentru: SGBDR, SMTP, HTTP, SOAP, JMS, WS, UDDI precum și capacitatea de a dezvolta noi conectori.

### 2.3.12 CERINȚE DE SECURITATE

Mecanismele de securitate ce vor fi incluse în soluția propusă vor avea la bază norme și concepte de bune practici în domeniu pentru a permite adaptarea cerințelor de securitate, dar, în același timp, să asigure și un nivel ridicat de securizare a sistemelor și datelor manipulate.

Sistemele de operare, aplicațiile software trebuie configurate și protejate corespunzător, atât împotriva atacurilor fizice, cât și logice, atât din interior, cât și din exterior.

Se va folosi principiul AAA (Authentication, Authorization, Accounting). Niciun utilizator nu va avea posibilitatea să facă mai multe tipuri de operațiuni decât cele care îi sunt atribuite inițial și pe care le poate accede prin autentificare. Pentru a se putea face verificări asupra modului în care utilizatorii își folosesc drepturile pe care le au prin autentificare, se vor păstra toate log-urile generate.

Totodată, se vor defini mai multe tipuri de conturi pentru aplicație, fiecare cont având privilegii minime (LEAST privileges).

Se vor asigura soluții de securitate astfel încât datele să nu poată fi accesate decât de utilizatorii autorizați în acest sens. Va fi prevăzută și o cale de auditare care să permită interogări specifice.

Soluția trebuie să răspundă următoarelor cerințe de securitate:

a) pentru accesarea interfeței web se va solicita o pereche validă nume de utilizator și parolă. Aceasta componentă este principalul element care garantează faptul că fiecare utilizator

nu-și poate accesa decât propriile date. Recuperarea numelui de utilizator și a parolei nu se va putea realiza decât prin procese stricte. Detalierea completă a metodei de autentificare folosite se va face în timpul etapei de analiză inițială;

b) se va asigura protecție la atacurile prin injecția de script-uri (XSS);
c) se va asigura protecție la tehnica de injectare a codului ce exploatează breșele de securitate ce ar putea să apară în trimiterea cererilor către baza de date (SQL Injection);
d) soluția va permite definirea de grupuri de utilizatori și autorizarea accesului la funcționalități pe baza de grup. Mai mult, soluția va trebui să permită rafinarea accesului până la nivel de utilizator;
e) acțiunile utilizatorilor în cadrul sistemului vor fi auditate, soluția va trebui să permită controlul dinamic al nivelului de detaliu al informațiilor auditate, activarea/dezactivarea auditului, rafinarea auditului până la nivel de utilizator (dar și la nivel de grup de utilizatori);
f) la nivelul soluției de data warehouse, vor trebui considerate în cadrul soluției cel puțin următoarele elemente:
    - trebuie să se asigure că toate datele stocate nu vor putea fi accesate decât de către persoanele autorizate să utilizeze aplicația; de asemenea, păstrarea parolelor se va realiza în urma unei operații de tip hashing (md5/sha);
    - restricție acces DBA (Database Administrator, administratorul bazelor de date) - una din sarcinile principale ale administratorului de baze de date este de a monitoriza și administra securitatea sistemului de gestiune a bazelor de date. Acest lucru implică adăugarea și eliminarea utilizatorilor, administrarea resurselor sistemului de baze date, auditul bazei de date, precum și verificarea oricăror altor probleme de securitate;
g) se va implementa în cadrul soluției un mecanism specializat care să asigure toate informațiile în ceea ce privește monitorizarea activității utilizatorilor.

Funcționalitățile de auditare și logare vor fi complet configurabile. Acțiunile utilizatorilor vor fi înregistrate. Rezultatele vor fi prezentate într-o manieră agregată și inteligibilă administratorului de sistem. Acest lucru creează posibilitatea de a evidenția numai acele acțiuni sau evenimente care sunt relevante, dată fiind o schemă de prioritizare de la evenimente critice (precum erori de aplicație sau excepții de autorizare) până la operațiuni corespunzătoare unui flux normal de lucru (precum editarea unei entități sau introducerea unei noi înregistrări).

Fiecare cont de utilizator este adăugat în baza de date, iar operațiile ulterioare (modificări sau ștergeri) vor fi adăugate ca informații privitoare la identitatea sa în sistem. Fiecare operațiune care are impact asupra datelor stocate în baza de date este înregistrată împreună cu următoarele informații de control: utilizatorul care efectuează operațiunea, data și ora operațiunii, respectiv tipul operațiunii (adăugare, editare, ștergere).

Platforma va utiliza protocolului HTTPS cu transport TLS, semnat cu certificat furnizat de o autoritate de certificare recunoscută.

Interfața pentru administrare va fi separată de cea de administrare conținut.

Conturile de acces/clienți nu vor putea fi utilizate și pentru administrare.

Va fi implementată o politică de autentificare care să micşoreze riscul de acces neautorizat (politica de parole puternică – criterii minime referitoare la lungime, complexitate, valabilitate, reutilizare, blocare după un număr stabilit de încercări eşuate; utilizarea a 2 factori; CAPTCHA);

Va fi implementată protecţia prin firewall/WAF şi antivirus, precum şi un mecanism de salvare/restaurare.

Componentele software utilizate (inclusiv sistemul de operare) vor avea ultimele versiuni şi actualizări de securitate instalate în vederea limitării posibilităţii de exploatare. Serviciile neutilizate ale sistemului de operare vor fi dezactivate. Nu vor fi utilizate extensii considerate nesigure. Beneficiarul poate efectua o scanare de vulnerabilităţi pentru a putea confirma instalarea actualizărilor.

Instalarea periodică a actualizărilor de securitate după testarea prealabilă (medii separate);

Se va efectua un test penetrare whitebox în etapa de testare pentru a micşora riscul de exploatare a vulnerabilităţilor. Scopul testului de penetrare este de a evalua din punct de vedere al vulnerabilităţilor informatice sistemele importante componente ale soluţiei.

În timpul activităţilor testului de penetrare se vor identifica şi documenta vulnerabilităţile sistemelor informatice menţionate mai sus în ceea ce priveşte:

- Autentificarea şi autorizarea – mecanismele prin intermediul cărora utilizatorii sunt identificaţi, autentificaţi şi autorizaţi să folosească funcţiile sistemului;
- Confidenţialitatea datelor – măsurile implementate pentru a preveni accesarea datelor privind utilizatorii (nume, adrese, date de contact, nume utilizator etc.) şi a datelor stocate şi vehiculate prin intermediul sistemelor informatice, de către persoane neautorizate;
- Integritatea datelor - măsurile implementate pentru a asigura integritatea şi a preveni pierderea, distrugerea sau furtul datelor stocate şi vehiculate de cele două sisteme informatice;
- Disponibilitatea serviciului – aspecte ce privesc furnizarea neîntreruptă a serviciilor furnizate de sistemele informatice;
- Respectarea politicilor şi a practicilor de securitate – modul în care cei ce folosesc aplicaţia web înţeleg şi respectă politicile şi practicile de securitate existente.

Prin testarea securităţii sistemelor componente ale aplicaţiei web se va asigura identificarea posibilelor vulnerabilităţi existente la nivelul sistemelor hardware, bazelor de date şi aplicaţiilor software încorporate, furnizând echipelor care asigură operarea, întreţinerea şi dezvoltarea acestora recomandări/informaţii destinate remedierii vulnerabilităţilor identificate.

Testele de penetrare pentru go-live se vor desfăşura în modul „black box" şi vor fi conforme cu una din metodologiile de pen-testare recunoscute pe plan mondial, cum ar fi: OWASP, OSSTMM, PTF, ISSAF, PCI DSS.

Contractantul va include în propunerea sa un appliance software care să asigure funcţionalităţi de tip web application firewall atât pentru portal, cât şi pentru serviciile web expuse public.

## 2.4 Lucrări din cadrul proiectului „Implementarea sistemului E-sigur"

### 2.4.1 Lucrări de amenajare a terenului si a fundațiilor consolelor rutiere

În valoarea ofertei financiare se va include și contravaloarea fundațiilor și ancorajelor aferente consolei (acestea se vor realiza de către ofertant). În cadrul propunerii tehnice este obligatoriu ca pe lângă proiectul tehnic aferent consolei să fie prezentat și calculul de rezistență pentru fundațiile consolelor.

Aceste fundații vor avea încorporate toate tuburile, cablurile, piesele necesare bunei funcționări a echipamentelor pe care le deservesc, conform proiectelor de instalații. Caracteristicile acestor fundații pot fi modificate înainte de începerea execuției cu realizarea unui proiect specific respectivei locații iar proiectul va fi avizat de un verificator de proiect.

Detaliile se vor corela cu specificațiile tehnice ale furnizorului/producătorului.

**În proiectarea și execuția brațelor consolelor se va avea în vedere adaptarea configurației acestora în funcție de amplasament, după cum urmează:**

- situația în care montajul consolei este destinat acoperirii unei singure benzi de circulație, caz în care dimensiunile și secțiunea brațului vor fi stabilite pentru a asigura rigiditatea și stabilitatea necesare în exploatare;
- situația în care montajul consolei este realizat dincolo de șanțul de scurgere a apei, caz în care poziționarea stâlpului consolei și fundației va fi adaptată pentru a evita interferențele cu infrastructura de colectare a apelor pluviale, asigurând în același timp stabilitatea structurală.

**Toate configurațiile vor fi dimensionate conform normelor tehnice aplicabile, ținând cont de acțiunile de vânt, încărcările utile, condițiile de teren cerințele de siguranță rutieră si sa existe posibilitatea acoperiri a minim 2 benzi de circulație si a șanțului de scurgere.**

La dimensionare trebuie luate în considerare încărcările de calcul definite mai jos precum și cea mai defavorabilă combinație a acestora:

- Încărcări din acțiunea vântului pentru zona meteo a amplasamentului (CR1-1-4/2012);
- Încărcări din greutate proprie (structura + cabinet );
- Încărcări din greutatea unui strat de 20 mm de gheață depusă pe cabinetul și pe structura de rezistență a stâlpului consolei;
- Încărcări din seism pentru tipul solului B conform Eurocod 8;
- Încărcări din echipamentele viitoare (ex. camerele) care vor fi montate pe aceste console, estimate la 100kg ca o forță concentrată aplicată în capătul brațului.
- Încărcări date de cabinetul, care va fi montat pe stâlpul consolei la o înălțime de minim 4m față de bază.

Pentru toate tipurile de încărcări și combinații ale acestora se ține cont de categoria de teren a amplasamentului conform SR EN 1993–3–1:2007.

### 2.4.2 Lucrări de instalare si montaj al consolelor rutiere

Montajul construcțiilor din oțel se face pe baza documentației tehnice elaborate de Ofertant/ Producător, cu respectarea proiectului de execuție și a normelor în vigoare.

- Conform normelor și regulilor de securitatea muncii executantul va asigura instructajul și protecția persoanelor care se află în zona în care se execută lucrările;

- Membrii echipelor vor purta veste reflectorizante;
- Zona de lucru se va semnaliza corespunzător cu normele de securitate în muncă (panouri, indicatoare de semnalizare a lucrărilor, conuri, etc.);
- Se vor transporta echipele de montaj, piesele, materialele şi utilajele necesare montării;
- Se va amenaja corespunzător zona de acces şi de lucru a mijloacelor de ridicat;
- Contractantul va alege procedeul optim de montaj în funcție de mijloacele tehnice din dotare, experiență proprie şi zona de amplasament a produsului;
- În cazul când unele operații urmează să aibă loc la temperaturi scăzute, trebuie respectate toate prevederile prescripțiilor legale în vigoare privind executarea lucrărilor de construcții pe timp friguros;
- Verticalitatea stâlpului consolei se reglează cu ajutorul piulițelor de subplaca de bază, folosind teodolitul. Înaintea începerii montajului se va verifica orizontalitatea suprafeței superioare a fundației stâlpului consolei;

### 2.4.3 Lucrări de conectare la rețeaua națională de distribuție energie electrica

Deoarece din condițiile tehnice de funcționare pentru asigurarea parametrilor tehnici de funcționare a echipamentelor existente in cabinetul si a camerelor video cu radar, exista posibilitatea de a fi aduse modificări la amplasamentele propuse, situații care nu pot fi cunoscute prealabil analizării unei soluții tehnice exacte, orice cost de asigurare a racordării la rețeaua de curent electric, inclusiv cu realizarea de branșamente noi cade in sarcina Ofertantului.

### 2.4.4 Lucrări de conectare fibra optica

Echipamentele vor fi conectate la rețeaua de fibra optică disponibilă , în funcție de situația existentă în teren.

## 3 LIVRARE, AMBALARE, ETICHETARE, TRANSPORT SI ASIGURARE PE DURATA TRANSPORTULUI

### 3.1 LIVRAREA/RECEPTIE

Termenele de livrare pentru produse (console rutiere, cabinete si camere) vor fi conform comenzilor emise de Autoritatea Contractanta, care nu va depăși 60 de zile de la data emiterii comenzii. Livrările pentru primele 50 de bucăți (console rutiere si cabinete si camere video cu radar si unități de procesare) vor începe in luna a 5 - a si nu vor depăși luna a 12- a, pentru restul de pana la 400 de bucăți nu se va depăși termenul contractual si anume 22 de luni. Termenele sunt cele menționate în graficul de implementare al contractului (Anexa nr. 1 la Caietul de sarcini), atât pentru produse cât și pentru servicii si lucrari.

Serviciile de analiza si proiectare software vor începe la Data de începere a contractului si se va încheia in maxim 6 luni. Sunt considerente îndeplinite când proiectul va fi avizat de CNAIR și este acceptat de autoritatea contractantă in urma semnării procesului verbal calitativ si cantitativ.

Serviciile de dezvoltare software sunt considerate a fi realizate când etapele de dezvoltare, customizare, instalare si configurare software sunt finalizate si toate activitățile referitoare la dezvoltarea software în cadrul contractului au fost realizate, sistemul informatic funcționează la parametrii corespunzători (inclusiv integrarea tuturor camerelor) și este acceptat de autoritatea contractantă in urma semnării procesului verbal de acceptanta.

Autoritatea Contractanta nu este responsabila cu masurile necesare asigurării integrității produselor livrate, acestea revin in sarcina Contractantului.

Produsele vor avea toate componentele/subansamblele necesare pentru funcționare (punere și menținere în funcțiune) și vor fi însoțite de documentația specificată.

Produsele vor purta marcajele originale ale producătorului.

Produsele livrate trebuie să fie însoțite obligatoriu de următoarele documente, după caz:

a) aviz de însoțire a mărfii;
b) certificate de conformitate eliberate de producător în original sau în copie conformă cu originalul pentru fiecare produs livrat;
c) CD/DVD-urile suport de la producător (dacă acestea sunt disponibile) sau să se indice în documentație unde se pot descărca de la producător;
d) document/documente în format digital cu liste ce conțin Serial-Number pentru fiecare componentă din cadrul produselor livrate;

În vederea asigurării corespondenței, justificării și trasabilității între reperele menționate în caietul de sarcini și cele ofertate, denumirea produselor din factură, aviz de însoțire a mărfii va fi aceeași cu cea din oferta tehnică/financiară a contractantului.

## 3.2 AMBALAREA ȘI ETICHETAREA

Produsele vor fi ambalate astfel încât să permită depozitarea și transportul acestora în condiții de siguranță, astfel încât să ajungă în bună stare la destinația finală. Contractantul va ambala și eticheta produsele furnizate astfel încât să prevină orice daună sau deteriorare în timpul transportului acestora către destinația stabilită.

Se va aplica o eticheta normala, greu destructibila.

Dacă este cazul, ambalajul trebuie prevăzut astfel încât să reziste, fără limitare, manipulării accidentale, expunerii la temperaturi extreme, sării și precipitațiilor din timpul transportului și depozitării în locuri deschise. În stabilirea mărimii și greutății ambalajului Contractantul va lua în considerare, acolo unde este cazul, distanța față de destinația finală a produselor furnizate și eventuala absență a facilităților de manipulare la punctele de tranzitare.

Toate materialele de ambalare, precum și toate materialele necesare protecției coletelor (folii de protecție, cutii etc.) rămân în proprietatea autorității contractante.

## 3.3 TRANSPORTUL

Contractantul va asigura transportul produselor până la locul de livrare, în spațiile indicate de către un reprezentant al beneficiarului, adresa și persoana de contact fiind comunicate anterior livrării. Predarea produselor către reprezentanții achizitorului se va face de luni până vineri în intervalul orar 07:30 – 15:30.

Transportul și descărcarea până în spațiile indicate de autoritatea contractantă și toate costurile asociate sunt în sarcina exclusivă a contractantului. Până la predarea către beneficiar, produsele vor fi asigurate de contractant împotriva pierderii sau deteriorării intervenite pe parcursul transportului.

Echipamentele se vor transporta marcate și ambalate, conform prevederilor din standardele de execuție a acestora, astfel încât să se asigure integritatea lor pe timpul transportului, manipulării și depozitării până la predarea echipamentelor către achizitor, la destinația finală.

Contractantul este responsabil pentru livrarea în termenul agreat al produselor și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca niciun motiv de întârziere sau costuri suplimentare.

### 3.4 RECEPȚIE - Cerințe generale

Dacă vreunul din produse nu corespunde specificațiilor din oferta propusă, Beneficiarul are dreptul să îl respingă, iar Contractantul, fără a modifica prețul contractului, are una din obligațiile următoare:

a) să înlocuiască produsele refuzate;
b) să facă toate modificările necesare pentru ca produsele să corespundă specificațiilor tehnice.

Recepția produselor/serviciilor se va face de către reprezentanți ai beneficiarului. Mijloacele tehnice fixe destinate măsurării vitezei (camere video cu radar și unitate de procesare locala) vor fi recepționate doar cu condiția existenței verificării metrologice inițiale la momentul recepției.

Constatarea de deficiențe în funcționarea produselor livrate sau neconcordanțe între caracteristicile tehnice și funcționale ofertate și produsele livrate, în timpul recepției, atrage după sine înlocuirea produselor, fără costuri suplimentare, cu produsele corespunzătoare, conform Ofertei tehnice si Caietului de sarcini. Produsele livrate la care s-au constatat neconformități, deficiențe sau lipsuri, vor fi consemnate într-un proces-verbal de recepție și vor fi înlocuite de către Contractant, fără costuri suplimentare, în termen de maxim 10 zile lucrătoare de la data constatării acestora.

După soluționarea eventualelor neconformități se va încheia procesul-verbal final de recepție cantitativă și calitativă, semnat de reprezentanții contractantului și ai beneficiarului.

Dreptul beneficiarului de a inspecta, testa și, dacă este necesar, de a respinge produsele, nu va fi limitat sau amânat din cauza faptului că produsele au fost inspectate și testate de contractant, cu sau fără participarea unui reprezentant al beneficiarului, anterior livrării acestora la destinația finală.

Recepția sistemului informatic integrat implementat este considerată finalizată după parcurgerea cu succes a testelor din cadrul documentației de testare aprobate, în momentul semnării de către Beneficiar, fără obiecții, a procesului verbal de acceptanta.

Componentele hardware si software livrate si recepționate in cadrul acestui contract devin proprietatea CNAIR după semnarea procesului verbal de acceptanta.

# 4 SERVICI DE INSTRUIRE A UTILIZATORILOR ȘI ADMINISTRATORILOR SISTEMULUI

La finalul etapei de dezvoltare/configurare și anterior etapei de testare, așa cum prevede calendarul de proiect prezentat în Caietul de sarcini, se va realiza instruirea administratorilor și utilizatorilor soluției dezvoltate.

Serviciile de instruire vor consta în:

- elaborarea documentațiilor de instruire (Plan de instruire utilizatori, Plan de instruire administratori de sistem, Suport de curs instruire utilizatori, suport de curs instruire administratori de sistem) și transmiterea acestora spre aprobare Autorității contractante cu minim 10 zile lucrătoare anterior demarării etapei de instruire;
- derularea sesiunilor de instruire astfel: o sesiune de instruire de 5 zile lucrătoare pentru 3 administratori de sistem; o sesiune de instruire de 3 zile lucrătoare pentru minim 10 – maxim 15 utilizatori. Sesiunile de instruire se vor desfășura la sediul CNAIR din București și / sau la sediile CMT, conform Planului de instruire elaborat de comun acord cu Beneficiarul.

Tematicile și materialele de curs se elaborează pentru două categorii de personal participant din partea Beneficiarului. Acestea includ prezentarea detaliată a sistemului e-SIGUR, a funcționalităților aplicației, urmând a fi elaborate 2 tematici separate, pentru cursul de administrator de sistem și cel de utilizator.

În cazul utilizatorilor, prin materialele de instruire este obligatorie acoperirea cel puțin a următoarelor teme:

- prezentarea generală a soluției.
- prezentarea funcționalităților, modulelor/componentelor de sistem, interfețelor specifice soluției, modalitatea de operare, reguli de validare.
- prezentarea proceselor automatizate la nivelul soluției implementate.
- exerciții practice.

În cazul administratorilor de sistem, prin materialele de instruire este obligatorie acoperirea cel puțin a următoarelor teme:

**A. Aspecte privind administrarea aplicației software:**

- prezentare componente/funcționalități;
- modalități de instalare, configurare și administrare soluție;
- administrarea structurilor/substructurilor integrate în aplicație;
- administrarea utilizatorilor și drepturilor de utilizare;
- crearea și configurarea fluxurilor și a diagramelor de lucru în cadrul soluției;
- crearea și administrarea formularelor utilizate în cadrul soluției;
- crearea și configurarea/modelarea rapoartelor în cadrul soluției;
- configurare interfețe.
- crearea și administrarea nomenclatoarelor utilizate în cadrul soluției;
- proceduri de administrare tipice pentru toate componentele instalate;
- modalități de corectare a erorilor;

**B. Aspecte privind administrarea infrastructurii de sistem:**

- prezentarea arhitecturii sistemului și a componentelor;
- modalități de instalare, configurare și administrare componente;
- proceduri de administrare tipice pentru toate componentele de infrastructură instalate;
- monitorizarea stării componentelor hw și sw ale platformei și proceduri de diagnosticare și corectare a erorilor;
- operațiuni backup/restore bază de date.

Instruirea trebuie să ofere cunoștințe relevante pentru produsele ofertate (instalare, configurare, utilizare și administrare), conform recomandărilor de instruire ale producătorului acestora și pentru dezvoltările/customizările de aplicație efectuate de Contractant.

Suporturile de curs vor fi elaborate în limba română, cu excepția anumitor aspecte referitoare la administrarea infrastructurii, care se acceptă și în limba engleză.

**Notă:** *Atât materialele de instruire, cât și modul de derulare a activității propriu zise vor pune un accent deosebit pe aspectele practice ale utilizării/administrării platformei, această etapă având totodată rolul unei pre-validări pe care reprezentanții desemnați ai Beneficiarului o vor efectua asupra aplicației dezvoltate și configurate, anterior etapei de testare în vederea acceptanței. Astfel, în cazul în care în etapa de instruire vor fi identificate cerințe care au fost prevăzute în etapa de analiză și proiectare, dar care nu se regăsesc în aplicația dezvoltată sau se regăsesc transpuse eronat față de forma aprobată, acestea vor fi îndeplinite anterior demarării testelor finale, după remedierea celor constatate și reluarea testării interne. Recepția calitativă a livrabilelor aferente activității de dezvoltare/configurare va fi condiționată de derularea și finalizarea cu succes a etapei de instruire.*

Livrabile:

- Plan de instruire utilizatori;
- Plan de instruire administratori de sistem;
- Suport de curs instruire utilizatori;
- Suport de curs instruire administratori de sistem;
- Raport de instruire.

# 5 SERVICII DE TESTARE A SOLUȚIEI IMPLEMENTATE SI OPERAȚIONALIZAREA SISTEMULUI

Testarea sistemului e-SIGUR se va realiza de către reprezentanții Beneficiarului, cu suportul Contractantului și împreună cu responsabilii nominalizați de către structurile beneficiare implicate, pe baza unei documentații de testare (metodologie de testare, plan de testare, scenarii de testare, raport de testare) preaprobate. Se va realiza testarea pe componente (testare unitară), pe interfațare între componente și/sau cu alte sisteme (testare de integrare), pe întreg sistemul (testare de sistem).

În cadrul acestei etape se va realiza testarea calității componentelor de sistem și corectarea oricăror probleme sau disfuncționalități identificate. Activitățile desfășurate presupun verificarea sistemului informatic dezvoltat/configurat, conform specificațiilor din prezentul Caiet de sarcini și a celor rezultate din documentațiile de analiză și proiectare.

Testarea are ca scop validarea modalității corecte de implementare a funcționalităților solicitate și se va realiza utilizând scenariile de testare agreate în prealabil.

Testarea se va realiza în mai multe etape, după cum urmează:

- testare funcțională (verificarea funcționalităților platformei informatice pe niveluri de acces);
- testare de performanță (disponibilitate, număr utilizatori concurenți, timp de răspuns, volum de date etc.).
- teste de conectivitate și interoperabilitate.
- teste de backup și restaurare.

Contractantul trebuie să asigure instrumente automate de testare (aplicații, scripturi etc.) destinate a fi utilizate în timpul procedurilor de testare.

Livrabile:

- Documentația de testare (metodologie de testare, plan de testare pentru acceptanță, scenarii de testare, raport de testare);
- Documentația de administrare infrastructură nucleu central;
- Documentația de administrare platformă e-SIGUR;
- Documentația de utilizare platformă e-SIGUR.

**Operaționalizarea sistemului informatic integrat la nivelul structurilor implicate**

Lansarea în producție a sistemului informatic e-SIGUR se va realiza de către responsabilii tehnici din cadrul echipei de proiect, cu suportul tehnic asigurat de Contractant, după cum urmează:

- verificarea instalării componentelor locale la nivelul tuturor utilizatorilor sistemului (dacă e cazul);
- configurarea rolurilor și utilizatorilor;
- popularea nomenclatoarelor cu date;
- pregătirea bazei de date pentru producție;
- migrarea în sistem a datelor și documentelor gestionate de alte aplicații existente (dacă e cazul);
- verificarea componentelor hardware și software din nucleul central și asigurarea că acestea sunt pe deplin funcționale;
- verificarea documentelor necesare, medii de instalare (dacă e cazul) și asigurarea că licențele aferente componentelor software sunt livrate și activate;
- recepția cantitativă și calitativă a sistemului integrat e-SIGUR.

Livrabile:

- Codul sursă documentat;
- Documentația de migrare.

## DOCUMENTAȚII CE TREBUIE FURNIZATE AUTORITĂȚII CONTRACTANTE

Principalele documentații pe care Contractantul trebuie sa le livreze Autorității Contractante in cadrul contractului sunt:

- ✓ planuri de situație (câte un plan pentru fiecare locație) și plan transversal pentru fundație;
- ✓ avizului Poliției rutiere pentru punctele de amplasare a echipamentelor din teren;
- ✓ Proiectarea soluției informatice
- ✓ certificate de conformitate/constanta performantelor eliberate de producător în original sau în copie conformă cu originalul pentru fiecare produs livrat;
- ✓ document/documente în format digital cu liste ce conțin Serial-Number pentru fiecare componentă din cadrul produselor livrate;
- ✓ declarația de conformitate/declarația de constanță a performanțelor emisă de Producător, potrivit prevederilor *Regulamentului (UE) Nr. 305/2011 al Parlamentului European și al Consiliului de stabilire a unor condiții armonizate pentru comercializarea produselor pentru construcții și de abrogare a Directivei 89/106/CEE a Consiliului*;
- ✓ avizul de însoțire a produsului;

## 6 DURATA DE IMPLEMENTARE A CONTRACTULUI

Durata de implementare a contractului va fi de 22 luni de la Data de de Incepere a Contractului care se va emite de catre Autoritatea contractanta ulteror intrarii in vigoare a Contractului.

Data intrării în vigoare a Contractului va fi în termen de 5 zile lucrătoare de la data semnării Contractului, sub condiția constituirii Garanției de Bună Execuție (10% din valoarea contractului fără TVA). Termenul prevazut mai sus poate fi prelungit, la solicitarea justificata a Furnizorului, fara a depasi 15 zile de la data semnarii contractului de furnizare

## 7 ETAPELE DE IMPLEMENTARE

1. **Analiza punctelor/sectoarelor optime pentru amplasarea echipamentelor în teren**

Se va realiza o analiză bazată pe datele accidentelor din anii 2023, 2024 și 2025. Vor fi identificate primele 400 de puncte în ordinea importanței, conform listei orientative anexate la Caietul de Sarcini, pentru a stabili sectoarele prioritare pentru amplasarea echipamentelor.

2. **Vizite în teren (site-survey)**

Se vor efectua vizite în teren pentru fiecare sector selectat pentru a:

- identifica amplasamentele exacte;
- evalua condițiile optime de instalare și montare;
- documenta activitatea prin măsurători, fotografii și observații tehnice.

3. **Elaborarea planurilor de situație și planului transversal pentru fundație**

Se vor realiza planuri detaliate pentru fiecare locație, inclusiv planul transversal necesar lucrărilor de fundație, pentru a ghida instalarea consolelor și infrastructurii de rețea.

4. **Obținerea avizului Poliției Rutiere**

Se va solicita avizul Poliției Rutiere pentru fiecare punct de amplasare a echipamentelor, conform prevederilor legale (art. 5, alin. 2 din Legea nr. 383/2022).

5. **Întocmirea documentației tehnice pentru obținerea avizelor**

Se va realiza documentația tehnică necesară obținerii avizelor și se vor efectua toate demersurile pentru obținerea acestora, dacă este cazul.

6. **Proiectarea soluției informatice și obținerea avizului CNAIR**

Se va stabili soluția informatică pentru nucleul central și echipamentele din teren, urmând să se obțină avizul CNAIR pentru implementarea acesteia.

7. **Elaborarea Proiectului Tehnic de execuție**

Se va întocmi proiectul tehnic pentru instalarea consolelor în teren, infrastructura de rețea și alte lucrări de conectare, inclusiv obținerea avizului CNAIR.

8. **Dezvoltarea și/sau customizarea soluției informatice**

Se va adapta și implementa software-ul necesar pentru gestionarea sistemului și interfațarea cu echipamentele din teren.

9. **Livrarea consolelor**

Se vor livra consolele destinate instalării în teren conform planului de implementare.

10. **Lucrările de instalare și montare a consolelor și infrastructurii de rețea**

Se vor realiza efectiv lucrările de montare a consolelor și conectarea infrastructurii de rețea necesare funcționării sistemului.

11. **Livrarea componentelor hardware și software pentru teren**

Se vor livra toate echipamentele și soluțiile software pentru cele 400 de sectoare selectate.

12. **Montarea și configurarea echipamentelor în teren și în CMT-uri**

Se vor instala fizic echipamentele și se va realiza configurarea hardware și software pentru funcționarea optimă.

13. **Livrarea componentelor hardware și software pentru nucleul central**

Se vor furniza toate componentele necesare nucleului central al sistemului informatic.

14. **Instalarea și configurarea echipamentelor și soluțiilor software pentru nucleul central**

Aceasta include:

- echipamente pentru procesare și stocare;
- sistem de operare;
- soluții de virtualizare;
- backup-restore;
- securitate aplicații;
- alte componente necesare, conform soluției ofertate, pentru respectarea cerințelor tehnice, funcționale și de performanță.

15. **Livrarea documentației tehnice a infrastructurii software**

Se va furniza documentația completă de instalare, configurare și licențiere a software-ului utilizat.

16. **Integrarea și operaționalizarea echipamentelor și componentelor**

Se va pune în funcțiune sistemul, asigurând integrarea completă a tuturor echipamentelor și soluțiilor software instalate.

**17. Elaborarea documentației de testare și recepție pentru infrastructură**

Se va întocmi documentația necesară testării și recepției tehnice a infrastructurii implementate.

**18. Testarea echipamentelor și a infrastructurii**

Se vor efectua teste de funcționare și performanță pentru echipamentele din teren și infrastructura centrală.

**19. Instruirea personalului beneficiarului**

Se vor organiza sesiuni de instruire pentru personalul care va opera și întreține sistemul.

**20. Lansarea în producție a sistemului**

Sistemul va fi pus în funcțiune pentru operare efectivă.

**21. Recepția lucrărilor și echipamentelor furnizate**

Se va realiza recepția lucrărilor și echipamentelor, precum și a sistemului informatic conform caietului de sarcini.

**22. Punerea la dispoziție a aplicației de ticketing**

Beneficiarul va avea gratuit aplicația de ticketing pe perioada implementării și garanției.

**23. Servicii de mentenanță și suport tehnic pe perioada de garanție**

Se vor furniza servicii de suport și întreținere pentru sistemul implementat.

**24. Recepția finală la expirarea perioadei de garanție**

Se va realiza recepția finală, confirmând conformitatea și funcționalitatea completă a sistemului.

## 8 GARANTIE

**Garanție pentru componentele hardware livrate:**

- 60 de luni garanție de la data semnării procesului-verbal de recepție cantitativă și calitativă de către Beneficiar a echipamentelor livrate.
- În cazul în care producătorii oferă o perioadă de garanție mai mare decât perioada minimă indicată de autoritatea contractantă, perioadele ofertate pentru componentele hardware livrate vor fi cel puțin cât perioadele oferite de producători.
- În cazul în care, pentru remedierea unei defecțiuni, este necesar transportul produselor la service-ul/sediul contractantului, acestea vor fi preluate în primele două zile lucrătoare de la notificarea de către Beneficiar (telefonic, email, fax). Transportul în siguranță a produselor predate de autoritatea contractantă intră în responsabilitatea Contractantului și va fi efectuat fără costuri suplimentare.
- Dacă repunerea în funcțiune a echipamentului defect durează mai mult de 5 zile lucrătoare de la momentul comunicării defecțiunii, contractantul trebuie să asigure temporar în regim NBD (Next-Business Day) un alt echipament similar/superior până la punerea în funcțiune al celui defect. Repunerea în funcțiune nu trebuie să depășească 30 de zile calendaristice.
- În cazul defectării totale a unui echipament, ori în cazul imposibilității depanării din motive neimputabile Contractantului, acesta se obligă să îl înlocuiască cu unul nou cu caracteristici tehnice similare sau superioare, care va rămâne în proprietatea autorității contractante.

Înlocuirea echipamentului se va efectua pe cheltuiala exclusivă a contractantului, în ziua imediat următoare expirării celor 30 de zile menționate mai sus. Contractantul are obligația să prezinte documente justificative pentru motivarea imposibilității depanării. Perioada de garanție va fi extinsă cu o perioadă de timp egală cu durata de indisponibilizare a echipamentelor.

- Indiferent de defectul produsului ofertat, ce necesită, dacă este cazul, a fi înlocuit în perioada de garanție, mediile de stocare de date de tip HDD, SSD, USB stick-uri, tape, defecte sau nu (indiferent de echipamentul în care este instalat) sau orice alt mediu amovibil, nu se vor returna contractantului.
- Verificările metrologice ale mijloacelor tehnice fixe destinate măsurării vitezei cad în sarcina Contractantului pe toată perioada de garanție.

**Garanție pentru componentele software**

Perioada de garanție, atât pentru licențe, cât și pentru soluția software implementată trebuie să fie de minim 60 de luni de la semnarea de către Beneficiar a Procesului verbal de recepție cantitativa si calitativă sau a Procesului verbal de acceptanta a sistemului e-SIGUR. În perioada de garanție și suport tehnic, Contractantul se angajează să asigure:

- majorarea perioadei de garanție cu timpul de nefuncționare a produselor software instalate, respectiv soluțiilor software dezvoltate/configurate;
- remedierea oricărei neconcordanțe a produselor (soluțiilor) software față de cerințele enunțate în Caietul de sarcini și/sau definite/detaliate în perioada de analiză/proiectare a sistemului sau descoperite în exploatarea curentă în faza de producție;
- rezolvarea bug-urilor care nu au fost identificate în timpul implementării/testării și care apar în faza de producție;
- întreținerea și buna funcționare a sistemului furnizat în parametrii agreați (funcțional, performanță, disponibilitate, integritatea datelor etc.);
- instalarea/configurarea de noi versiuni ale aplicațiilor în urma efectuării corecțiilor;
- actualizarea documentațiilor de utilizare, administrare și a altor documente, în urma efectuării corecțiilor, dacă e cazul;
- pentru produsele software livrate, Contractantul va pune la dispoziție toate *patch*-urile care duc la fixarea unor probleme;
- Contractantul va aplica pe toată durata garanției produselor, toate update-urile, patch-urile care duc la fixarea unor probleme sau facilități de care utilizatorul are nevoie. Această operație se face de comun acord cu Beneficiarul, fără a afecta stabilitatea/funcționalitatea soluției;
- în perioada de garanție, Contractantul va notifica și va pune la dispoziția beneficiarului toate update-urile apărute pentru soluția livrată în vederea funcționării acesteia în conformitate cu specificațiile tehnice ale componentelor de sistem;
- transferul de cunoștințe de la Contractant către echipa beneficiarului cu privire la actualizările aduse soluției și la activitățile de administrare aferente soluției implementate;

- asigurarea materialelor necesare pentru desfășurarea activităților de intervenție, fără costuri suplimentare din partea beneficiarului;
- alte cerințe formulate expres în caietul de sarcini.

Dacă în perioada desfășurării achiziției/implementării proiectului apar echipamente/produse software ca și end-of-life/end-of-sale/end-of-support ofertantul trebuie să le înlocuiască cu produse care să asigure minim funcționalitățile și performanța produselor ofertate inițial.

Licențele pentru aplicațiile software trebuie să aibă drept de utilizare acordat life-time (pentru o perioadă nedeterminată de timp).

Contractantul are obligația de a soluționa incidentele constatate de Beneficiar în perioada de garanție, chiar dacă soluționarea acestora va conduce la prelungirea garanției cu perioada de soluționare a problemelor/incidentelor constatate.

De asemenea, Contractantul are obligația de a asigura garanția și suportul pentru produsele livrate, serviciile prestate inclusiv pe toată perioada de derulare a contractului, până la recepția finala a Contractului, fără a afecta perioada de garanție pentru întreg sistemul informatic implementat.

Pentru scopul acestei proceduri, noțiunea de „defect" trebuie interpretată ca un comportament al produsului diferit de parametrii agreați de părți, având ca referință pentru determinarea defectelor cerințele funcționale din caietul de sarcini.
In perioada de garanție, Contractantul are obligativitatea efectuării verificărilor metrologice a sistemelor de măsurare a vitezei, in termenele prevăzute de BRML, pentru continuitate in funcționare.

## 9 SUPORT TEHNIC – SERVICII DE MENTENANTA CORECTIVA

Suportul tehnic trebuie să fie de minim 60 de luni si va fi oferit de Contractant pe întreaga perioada de garanție pentru toate componentele sistemului e-SIGUR implementat (modulele/aplicațiile dezvoltate/configurate, produsele software și echipamentele livrate, inclusiv pentru infrastructura hardware a nucleului central).

Asistența și suportul tehnic asigurat de Contractant sunt de tipul:

- on-site (numai la sediul Beneficiarului);
- telefonic/pe e-mail/aplicație de ticketing (soluție de help desk).

În perioada de suport tehnic, Contractantul va asigura următoarele servicii:

- suport tehnic și sprijin pentru trecerea în producție a soluțiilor livrate – specialiștii cheie din echipa de implementare vor asigura suport on-site la darea în producție (asistență în producție) pe o perioadă de minimum 5 zile lucrătoare. Lista acestor specialiști va fi stabilită de comun acord cu beneficiarul;
- asistență și suport tehnic după lansarea în producție a sistemului, pe perioada garanției:
    - suport pentru echipa tehnică a beneficiarului în investigarea problemelor apărute;

- servicii de HelpDesk (cu administrarea priorităților de deranjament, rapoarte de deranjamente și corelarea erorilor).

Suportul pentru componentele de sistem se va asigura de către Contractant prin experți care fac dovada cunoașterii produsului/produselor. Dovada se poate face prin diplome, certificări, atestări.

Experții pentru componentele de sistem se vor asigura de către Contractant pe toată perioada de garanție și suport a produselor. Prin ofertele elaborate, ofertantul trebuie să demonstreze cum va îndeplini această cerință.

## 9.1 SLA (SERVICE LEVEL AGREEMENT)

În cadrul SLA-ului, Contractantul va acorda următoarele servicii de suport:

- Servicii de Help Desk;
- Rapoarte de deranjamente și remediere a problemelor.

Prin experții puși la dispoziție, Contractantul va:

- administra și monitoriza incidentele;
- lua legătura cu persoana desemnată ca punct de contact din partea beneficiarului, pentru analiza stărilor incidentelor deschise;
- răspunde tuturor întrebărilor legate de incidente;
- înregistra incidentele raportate de către utilizatorii beneficiarului, precum și transmiterea confirmării soluționării incidentului semnalat, în urma rezolvării acestuia;
- înregistra incidentele raportate de către utilizatorii soluției, precum și va transmite confirmarea soluționării incidentului semnalat, în urma rezolvării acestuia (este vorba atât despre incidentele care apar la nivelul aplicațiilor, cât și despre incidentele care afectează bazele de date sau infrastructura hardware/ software);
- marca finalizarea cererii și comunica modalitatea de soluționare completă și definitivă a cererii către beneficiar.

Problemele ridicate de beneficiar vor fi înregistrate de către specialiștii Contractantului, în cadrul unei aplicații de ticketing (soluție de help desk) pusă la dispoziție de Contractant pentru a ajuta beneficiarul în rezolvarea problemelor apărute.

Suportul va fi asigurat conform SLA.

Contractantul va asigura diagnosticarea unui incident pentru determinarea problemei de bază.

Contractantul va efectua toate activitățile necesare pentru remedierea problemelor constatate ca urmare a raportării de către beneficiar a incidentelor, conform nivelurilor SLA stabilite.

Contractantul va monitoriza în permanență incidentul până la închiderea acestuia.

Beneficiarul va avea acces la aplicația de ticketing pentru a monitoriza incidentele.

Aceste servicii (SLA) presupun derularea următoarelor activități de către Contractant:

- preluarea cererilor de suport tehnic prin telefon/fax/e-mail/aplicație de ticketing;
- soluționarea cererii de suport tehnic;
- direcționarea la nivelul superior de suport în cazul în care nu se poate rezolva cererea telefonic;

- marcarea finalizării cererii și comunicarea către beneficiar.

Activitățile efectuate de către Contractant în cadrul serviciilor de suport tehnic presupun comunicarea către beneficiar a posibilelor rezolvări ale erorilor, ale defectelor care afectează funcționarea în parametrii optimi a sistemului și, după caz, intervenția nemijlocită, exclusiv la sediul beneficiarului, a experților Contractantului, atunci când este evident faptul că disfuncționalitatea apărută în sistem este ca urmare a unor erori de configurare sau de funcționare a componentelor sistemului e-SIGUR implementat.

Contractantul va lua toate măsurile administrative și logistice pentru asigurarea timpilor de intervenție și de soluționare specificați în prezentul SLA și va prezenta în cadrul ofertei tehnice modalitățile prin care va putea oferi serviciile la nivelul și în intervalul de timp solicitate.

Neîncadrarea în parametrii de disponibilitate și de continuitate a funcționării serviciilor de garanție și suport tehnic, depășirea timpilor de intervenție și de soluționare a problemelor, neîndeplinirea cantitativă și calitativă a serviciilor în perioadele de timp definite, lipsa de reacție la solicitările de suport tehnic, precum și nesoluționarea acestora atrage după sine aplicarea de penalități contractuale.

Pe tot parcursul tratării unei probleme, Contractantul va asigura trasabilitatea acțiunilor întreprinse de către echipa de suport tehnic, inclusiv a momentelor de timp în care aceste acțiuni au fost stabilite/desfășurate. Pentru o corelare consistentă și o mapare a incidentelor critice/majore și repetitive se va păstra un istoric al tuturor problemelor semnalate, inclusiv al modalităților de soluționare a acestora, acestea putând fi consultate online de către beneficiar.

Nivelul de severitate al unei probleme va fi stabilit de către beneficiar și va fi comunicat în solicitarea de suport tehnic.

| Niveluri de severitate (impact) | Timp de răspuns | Timpi de intervenție pe niveluri de severitate | | |
|---|---|---|---|---|
| | | Diagnosticare | Soluție provizorie | Soluție finală |
| Nivelul de severitate 1 - Impact critic/ Sistem inaccesibil: beneficiarul este în imposibilitatea de a utiliza cel puțin una din componentele principale ale sistemului, rezultând un impact critic asupra disponibilității, securității și performanței acestuia. Această stare necesită o soluție imediată. | 1 oră | 2 ore | 6 ore | 12 ore |
| Nivelul de severitate 2 - Impact semnificativ/major: Sistemul suferă o pierdere masivă a funcționalității, funcțiile importante ale sistemului nefiind accesibile sau cu timpi mari | 2 ore | 3 ore | 8 ore | 24 ore |

| | | | | |
|---|---|---|---|---|
| de răspuns. Problema împiedică desfășurarea în condiții normale a activității utilizatorilor. | | | | |
| Nivelul de severitate 3 – Impact mediu: Funcționalitățile sistemului sunt afectate minor. Impactul asupra disponibilității, securității și performanței sistemului nu este major, dar este necesară o rezolvare a problemei apărute. Impactul reprezintă un inconvenient care necesită soluții alternative pentru refacerea funcționalităților. | 3 ore | 6 ore | 12 ore | 36 ore |
| Nivelul de severitate 4 - Impact minim: O componentă neesențială este nefuncțională, cauzând un impact minim sau beneficiarul solicită o informație/ o îmbunătățire a funcționalității componentelor de sistem sau documentație clarificatoare cu privire la acestea. Rezultatul este o eroare minoră care nu împiedică desfășurarea în bune condiții a activității utilizatorilor. | 4 ore | 8 ore | 48 ore | 72 ore |

*Timp de răspuns* – intervalul de timp în care Contractantul va transmite confirmarea primirii cererii de asistență tehnică și înregistrarea solicitării Beneficiarului;

*Diagnosticare* – intervalul de timp necesar pentru identificarea cauzelor care au produs problemele de funcționare ale sistemului, calculat din momentul notificării incidentului.

*Soluția provizorie* - intervalul de timp necesar pentru a asigura funcționalitățile sistemului informatic, calculat din momentul notificării incidentului până la închiderea acestuia.

*Soluția finală* - intervalul de timp necesar pentru a aduce sistemul la parametrii normali de funcționare și disponibilitate, calculat din momentul notificării incidentului până la închiderea acestuia.

*Aplicație de ticketing (soluție de help desk)*: Problemele ridicate de beneficiar vor fi înregistrate de către specialiști ai Contractantului, în cadrul unei soluții de tip HelpDesk, pe perioada suportului tehnic. Serviciul de HelpDesk al Contractantului va asigura asistență tehnică, diagnosticare, soluții de rezolvare a defecțiunilor/avariilor și va utiliza un instrument de înregistrare și de management al incidentelor care va înștiința beneficiarul asupra stadiului rezolvării problemei, astfel încât acesta să poată controla în mod independent performanța serviciilor de suport și respectarea

criteriilor de performanță solicitate. Ofertanții vor descrie în mod detaliat modalitatea propusă pentru organizarea și furnizarea serviciilor de suport în perioada de garanție. În ultimele 30 de zile ale perioadei de garanție, Contractantul va realiza un transfer (handover) al procedurilor de suport către beneficiar. Acest proces va include proceduri pentru managementul configurației sistemului, precum și recomandări în vederea organizării structurii de suport a beneficiarului.

Dacă soluționarea problemei se realizează prin intervenția experților Contractantului la sediul beneficiarului, aceasta se va realiza în prezența beneficiarului.

În cazul incidentelor cu nivel de severitate 1 și 2, în cazul unor defecte hardware justificate temeinic de către Contractant, soluția provizorie va fi menținută în stare de funcționare până la implementarea soluției finale, dar nu mai mult de 15 zile.

Ofertanții vor descrie detaliat, în oferta tehnică, modalitatea de asigurare a garanției și suportului tehnic pentru toate componentele livrate.

## 9.2 SERVICII DE MENTENANTA PREVENTIVA

**Cerințele de mentenanță / întreținere se referă la următoarele activități:**

| | **Echipamente** | **Activități** | **Periodicitate (inclusiv raport)** |
|---|---|---|---|
| A. Întreținerea echipamentelor din teren în perioada de garanție | Cabinete | verificare vizuala trasee cablaje, prinderi suporți | Trimestrial si ori de cate ori este necesar |
| | | consolidare suporți | Verificare vizuala trimestrial - remediere daca este cazul |
| | | ungere balamale uși/lacăte | Trimestrial si ori de cate ori este necesar |
| | | măsurare priză pământ | Anual si ori de cate ori este necesar |
| | Supraveghere video | verificare vizuala trasee cablaje, prinderi suporți | Trimestrial si ori de cate ori este necesar |
| | | verificare funcționare camere si reglaje, curățare camere | Trimestrial si ori de cate ori este necesar |
| | | verificare înregistrări memorie locala | Trimestrial si ori de cate ori este necesar |
| | UPS | verificare stare acumulatori / funcționare pe acumulatori | Trimestrial si ori de cate ori este necesar |

Pe toata perioada de garanție, Furnizorul trebuie să efectueze minim activitățile de întreținere prezentate în tabelul anterior respectând periodicitatea acestora.
Începutul operațiunilor de întreținere: activitățile de întreținere trebuie să înceapă odată cu instalarea fiecărei componente. Cu toate acestea, perioada de întreținere nu se consideră că a început până la semnarea Procesului Verbal de Recepție cantitativa si calitativă sau a Procesului Verbal de Acceptanta a sistemului e-SIGUR. Întreținerea echipamentelor va începe odată cu începerea perioadei de garanție.

## 10 ORGANIZARE ŞI METODOLOGIE DE PREZENTARE A OFERTEI TEHNICE

Ofertantul va descrie în detaliu modul de îndeplinire a cerinţelor de realizare a activităţilor.

Oferta tehnică va cuprinde minim următoarele:

1. Metodologia de implementare si modalitatea de livrare in care se prezintă strategia propusă de ofertant pentru livrarea produselor si prestarea serviciilor solicitate prin specificaţiile tehnice incluse în caietul de sarcini.

Informaţiile vor fi structurate pe capitole astfel încât să satisfacă in mod corespunzător cerinţele prevăzute in caietul de sarcini.

2. Planul de lucru, care va include Diagrama Gantt pentru toate activităţile proiectului, în ordinea şi succesiunea logică a acestora. Diagrama va fi prezentată la o scară care să permită vizualizarea cel puţin la nivel de lună calendaristică.

3. Fişele tehnice ale echipamentelor propuse de ofertant pentru desfăşurarea activităţilor proiectului din care să reiasă conformitatea cu caietul de sarcini si licenţele software aferente. Caracteristicile tehnice ale produselor vor fi prezentate sub forma de tabel de corespondenta prin care sa demonstreze corespondenta propunerii tehnice cu cerinţele conţinute in caietul de sarcini. Nu se acceptă descrierea detaliată a modului în care este îndeplinită cerinţa din caietul de sarcini **prin copierea conţinutului cerinţei**. Identificarea elementelor de conţinut copiat va face obiectul unei solicitări de clarificări în care ofertantul va trebui să demonstreze pe baza documentelor transmise în cadrul ofertei sale că a descris clar şi relevant modul de îndeplinire a cerinţei.

Pentru echipamentele care vor fi definite după etapa de proiectare, fisele tehnice si licenţele software, după caz, vor fi incluse in Proiectul Tehnic.

## 11 GESTIONAREA RELAŢIEI DINTRE CONTRACTANT ŞI AUTORITATEA CONTRACTANTĂ

Gestionarea relaţiei dintre Contractant şi Autoritatea Contractantă se va face sub forma întâlnirilor de lucru, care poate lua forma întâlnirii de început, a întâlnirilor pentru monitorizarea progresului, a întâlnirilor de lucru sau întâlniri pentru acceptarea rezultatelor parţiale şi a rezultatului final.

Întâlnirea pentru începerea activităţii va avea loc în termen de maxim 15 zile lucrătoare, după intrarea în vigoare a Contractului şi va fi organizată de către Beneficiar.

Întâlnirile de lucru pot fi convocate de oricare dintre părţi, atunci când situaţia o impune; agenda şedinţei va fi întocmită de solicitantul întâlnirii.

Contractantul trebuie să editeze minuta întâlnirii, document ce va fi semnat de reprezentanţii ambelor parţi.

### 11.1 Cerințe privind raportarea

**Contractantul va livra următoarele rapoarte/documente justificative:**

i. ***Raportul inițial ce cuprinde și un plan detaliat*** al derulării activităților pentru toate componentele și fazele contractului va fi depus, în 30 de zile de la Data de de Incepere a Contractului, pentru revizuire, și va cuprinde în mod obligatoriu următoarele aspecte:

- un plan și un grafic detaliat cu toate activitățile ce trebuie realizate pe durata implementării contractului, pentru fiecare structură în parte;
- o descriere a metodologiei care va fi utilizată;
- lista indicatorilor relevanți pentru monitorizarea progresului;
- planificarea în timp, pentru toată durata derulării contractului, a întâlnirilor de lucru.

În cazul în care există vreo modificare propusă la specificațiile tehnice inițiale, datorită apariției anumitor circumstanțe după inițierea activităților, acestea vor fi discutate și agreate cu Beneficiarul înainte de transmiterea raportului.

De asemenea, el trebuie să cuprindă informații despre experții cheie care vor desfășura activitățile contractului atât pentru toate etapele aferente implementării/operaționalizării sistemului informatic integrat cât și pentru instruirea administratorilor și utilizatorilor, programarea activităților, executarea activităților pe perioada de timp alocată fiecărei componente.

Ulterior validării de către beneficiar, raportul inițial va deveni instrumentul de lucru principal pe durata implementării proiectului și va fi documentul de referință pe întreaga durată a proiectului.

Pentru elaborarea raportului de începere în termenul stabilit, beneficiarul va asigura toate informațiile care sunt necesare Contractantului, în condițiile legii și reglementărilor privind legislația și aspectele logistice aplicabile.

Graficul acțiunilor prezentate în acest raport reprezintă o versiune actualizată a ofertei prezentate de Contractant, prin raportare la data reală de începere a contractului.

ii. ***Rapoartele lunare de progres*** vor fi înaintate în primele 10 zile lucrătoare ale lunii următoare celei pentru care se face raportarea. Rapoartele vor detalia:

- progresele înregistrate;
- comparație între evoluția planificată și cea realizată, inclusiv procentajul realizat din activitățile derulate/aflate în derulare;
- rezultatele obținute în cursul perioadei de raportare, resursele utilizate, precum și recomandările sau solicitările aferente și planificarea activităților proiectului pentru perioada următoare.

iii. ***Un raport final inainte de receptie***, care trebuie să fie redactat și predat beneficiarului în termen de 10 zile lucrătoare înainte de semnarea Procesului Verbal de Recepție cantitativa si calitativă sau a Procesului Verbal de Acceptanta a sistemului e-SIGUR. Acesta va cuprinde:

- descrierea întregului proces de furnizare a serviciilor prestate și o evaluare a rezultatelor obținute în termeni, atât calitativi, cât și cantitativi, comparativ cu rezultatele așteptate;
- evaluare a îndeplinirii obiectivelor/indicatorilor propuși;
- recomandări pentru acțiuni viitoare cu scopul asigurării sustenabilității activităților din cadrul proiectului, rezultatele așteptate de la acest proiect după finalizarea lui, precum și măsuri ce trebuie întreprinse în acest sens.

Proiectul de raport va fi revizuit în cazul în care sunt formulate observații și propuneri din partea beneficiarului. Versiunea revizuită a raportului va fi depusă inainte de semnarea Procesului Verbal de Recepție cantitativa si calitativă sau a Procesului Verbal de Acceptanta a sistemului e-SIGUR.

***Transmiterea și aprobarea rapoartelor***

Raportul inițial, Rapoartele lunare și Raportul final trebuie transmise, în trei exemplare, spre aprobare, în atenția Managerului de Proiect al Echipei de proiect din partea Autorității Contractante.

Toate rapoartele vor fi redactate în limba română. Variantele intermediare, de lucru, pot fi transmise Autorității Contractante doar în format electronic editabil. Variantele finale vor fi transmise atât în format electronic editabil cât și pe hârtie. Aprobarea rapoartelor se face de către Comisia de recepție desemnată de Autoritatea Contractantă.

Autoritatea Contractantă, în urma recepției, va aproba rapoartele sau va prezenta observațiile sale în termen de maxim 10 zile lucrătoare de la data depunerii rapoartelor inițial, lunare, respectiv 15 zile lucrătoare pentru raportul final.

În cazul unor modificări, Contractantul are obligația de a răspunde pozitiv solicitărilor Autorității Contractante de modificare/ completare a rapoartelor, corespunzător cu observațiile Autorității Contractante, în termen de maxim 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.

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

Contractantul are obligația de a propune experți calificați și specialiști pentru realizarea activităților prevăzute în prezentul caiet de sarcini și este responsabil pentru activitatea acestora și pentru obținerea rezultatelor cerute.

Contractantul trebuie să asigure personal adecvat din punctul de vedere al pregătirii și al alocării orelor de lucru, pentru efectuarea eficientă a tuturor activităților stipulate în caietul de sarcini și pentru realizarea în final a obiectivelor generale și specifice ale Contractului din punct de vedere al termenelor, al costurilor și al calității.

Pe toată durata de implementare a contractului, Contractantul va lua toate măsurile necesare pentru a preveni orice situație de natură să compromită realizarea cu imparțialitate și obiectivitate a activităților desfășurate pentru realizarea obiectivelor contractului.

Indiferent de durata perioadei de desfășurare a activităților experților propuși, Contractantul serviciilor se va asigura și va urmări cu strictețe ca oricare dintre aceștia să cunoască foarte bine și să înțeleagă cerințele, scopul și obiectivele contractului, cerințele regulilor și regulamentelor Uniunii Europene și legislația națională relevantă, specificul activităților pe care urmează să le desfășoare în cadrul contractului și a componentei/lor acestuia în care sunt direct implicați, precum și a responsabilităților atribuite. Contractantul trebuie să asigure experții, necesarul de birotică, echipamente IT și rechizitele necesare bunei desfășurări a activităților proprii, precum și transportul, cazarea, masa și diurna aferente experților proprii în cazul deplasării în teritoriu în vederea desfășurării activităților necesare conform contractului.

### 11.3 NUMĂRUL DE EXPERȚI PE CATEGORIE DE EXPERTIZĂ NECESARĂ

Contractantul formează echipa de proiect astfel încât să acopere activitățile specifice și să atingă obiectivele contractului.

Pentru realizarea activităților, beneficiarul anticipează că sunt necesare anumite domenii de expertiză sau următoarele categorii de profesii:

| **Categorie de profesii/domeniu al specializării** | **Număr de experți cheie** |
|---|---|
| Manager de proiect | *1 expert cheie* |
| Arhitect de sistem | *1 expert cheie* |
| Analist de business | *1 expert cheie* |

| **Categorie de profesii/domeniu al specializării** | **Număr de experți non-cheie** |
|---|---|
| Expert proiectare și administrare baze de date | *1 expert non-cheie* |
| Expert ITS | *1 expert non-cheie* |

Nominalizarea personalului

- Pentru Experții: Arhitect de Sistem si Analist de business, Ofertanții vor include **in Oferta** lor numele, CV-urile, diplomele si documentele justificative.
  După semnarea contractului de servicii, **Contractantul are obligația de a asigura personalul nominalizat in cadrul Ofertei sale.**
- Pentru ceilalți Experți Contractantul va transmite Beneficiarului, **ulterior semnării Contractului**, CV-urile, diplome (daca este cazul) si documentele justificative sau după caz, actele doveditoare privind atestarea/autorizarea, ale acestor experți.

Cerințele de mai jos sunt aplicabile tuturor experților care ocupa pozițiile respective, indiferent de numărul lor, însă verificarea îndeplinirii acestor condiții in vederea stabilirii conformității

Propunerilor tehnice in cadrul procesului de evaluare a ofertelor **se va face numai pentru experții Arhitect de Sistem si Analist de business**.

Ofertantul va avea in vedere ca pentru experții cheie/ non-cheie trebuie descris in propunerea Tehnica modul in care ofertantul si-a asigurat accesul la serviciile acestora si momentul in care aceștia vor interveni in implementarea contractului.
Pentru personalul nerezident va fi acceptata prezentarea diplomelor/ certificărilor/ autorizărilor corespunzătoare emise in tara de rezidenta, echivalente si/sau echivalate de autoritățile naționale romane.
Pe lângă experții solicitați, Contractantul poate aduce în sprijinul implementării serviciilor și alți experți, dacă va considera acest lucru necesar în vederea acoperirii cerințelor Caietului de sarcini. Costurile acestora sunt suportate de Contractant, în limita bugetului contractului. În plus, Contractantul va asigura personalul administrativ care este necesar echipei sale. Contractantul va stabili cum își organizează echipele, câți experți va aloca/activitate, precum si rolul și responsabilitățile acestora în cadrul contractului.

## 11.4 PROFILUL EXPERȚILOR PRINCIPALI

Contractantul are obligația de a propune experți calificați pentru realizarea activităților prevăzute în documentele contractuale. Calificările, cunoștințele și experiența necesară experților trebuie să fie dovedită prin documentele care însoțesc oferta. Contractantul este responsabil pentru activitatea experților, pentru atingerea indicatorilor și pentru calitatea rezultatelor obținute în cadrul contractului.

## 11.5 ALTE CERINȚE LEGATE DE PERSONALUL DIRECT IMPLICAT ÎN PRESTAREA SERVICIILOR

Niciunul dintre experții propuși nu trebuie să se afle în nici un fel de situație de incompatibilitate cu responsabilitățile acordate lor și/sau cu activitățile pe care le vor desfășura în cadrul contractului. În plus, pe toată durata de implementare a contractului, Contractantul ia toate măsurile necesare pentru a preveni orice situație de natură să compromită realizarea cu imparțialitate și obiectivitate a activităților desfășurate pentru realizarea obiectivelor asociate Contractului.

Contractantul trebuie să se asigure de disponibilitatea experților propuși conform perioadelor evidențiate în contract.

Contractantul trebuie să se asigure și să urmărească cu strictețe ca toți experții propuși să cunoască foarte bine și să înțeleagă cerințele, scopul și obiectivele contractului, cerințele legislației relevante, specificul activităților pe care urmează să le desfășoare în cadrul Contractului precum și a responsabilităților atribuite.

Contractantul nu va face schimbări de personal fără aprobarea Beneficiarului. Înlocuirea oricărui expert se face printr-un act adițional la contract. Este recomandat ca înlocuirea acestora să se facă numai în cazuri excepționale (de ex: demisie sau ineficiență în implementare, caz de boală, accident, etc.), cu îndeplinirea tuturor cerințelor privind criteriile de selecție pentru experiența

profesională a experților, calificările și experiența profesională a experților cheie din cadrul echipei de implementare pe baza cărora s-a selectat ofertantul.

Autoritatea contractantă poate să solicite înlocuirea experților pe perioada derulării contractului, pe baza unei cereri scrise motivate și justificate, dacă apreciază că un membru al personalului este ineficient sau nu își îndeplinește sarcinile la nivelul cerințelor stabilite.

Pentru înlocuirea unui expert, Contractantul va avea în vedere prevederile art. 162 alin. (1), lit. b) din HG nr. 395/2016, respectiv va transmite pentru noul personal documentele solicitate prin documentația de atribuire fie în vederea demonstrării îndeplinirii criteriilor de calificare/selecție stabilite, fie în vederea calculării punctajului aferent factorilor de evaluare.

Toate costurile generate de înlocuirea personalului cheie sunt exclusiv în sarcina Contractantului.

**Experți – cerințe minime**

A. Cerințe minime ale Expertului cheie nr. 1: Manager de proiect (1 expert)
   a) *studii superioare* dovedite prin diplomă de licență sau echivalent;
   b) *studii de specializare în managementul proiectelor* dovedite prin deținerea unui certificat de absolvire pentru ocupația manager de proiect (COR 241919) sau echivalent;
   c) Experiența deținuta în poziția de Manager proiect/contract si/sau Adjunct Manager proiect/contract si/sau Coordonator proiect/contract si/sau Adjunct Coordonator proiect/contract si/sau Director proiect/contract si/sau Adjunct Director proiect/contract si/sau Project Manager si/sau Project Manager Adjunct si/ sau Șef echipa proiectare si/ sau Adjunct Șef Echipa proiectare si/ sau Șef Proiect si/ sau Adjunct Șef Proiect in cadrul unui contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în contract.

**Nota 1:** In vederea îndeplinirii cerinței de mai sus, **ulterior semnării contractului**, Contractantul va prezenta Diploma de studii, CV-ul si documente justificative (recomandări/ documente emise de beneficiari/angajatori / fișă de post/ contract de muncă sau orice alte documente similare care să ateste activitatea desfășurată ca manager de proiect si din care să rezulte funcția ocupata).

**Responsabilități:**

- Activități specifice de management de proiect (legat de obiectul contractului, dezvoltare software)
- Punct principal de contact in relația cu beneficiarul
- Managementul contractului
- Managementul proiectului in ansamblul sau, managementul ariei de cuprindere, managementul schimbărilor, planificarea generala a proiectului, managementul riscurilor, managementul problemelor, managementul comunicării
- Asigurarea resurselor proiectului
- Managementul, organizarea, alocarea si planificarea echipei de proiect
- Identificarea riscurilor si propunere de soluții pentru diminuarea/evitarea riscurilor
- Rezolvarea problemelor in scopul evitării situațiilor de criza
- Urmărirea respectării tuturor termenelor conform planului de proiect
- Analiza modalității prin care livrabilele proiectului corespund cerințelor de business
- Realizarea rapoartelor periodice/ad-hoc ale proiectului.

- Elaborează planurile de calitate

Verifica si asigura calitatea livrabilelor

B. Cerințe minime ale Expertului-cheie nr. 2: Arhitect de sistem (1 expert)

a) *studii superioare încheiate în unul din domeniile:* matematică, informatică, calculatoare și tehnologia informației, ingineria sistemelor, inginerie electronică și telecomunicații, cibernetică, statistică și informatică economică, contabilitate(specializarea contabilitate și informatică de gestiune), inginerie electrică (specializarea inginerie electrică și calculatoare), științe inginerești aplicate (specializările informatică industrială, informatică aplicată în inginerie electrică, matematică și informatică aplicată în inginerie), dovedite prin diplomă de licență sau echivalent;

b) Experiența deținuta în poziția de Arhitect de sistem sau similar*) in cadrul unui contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în contract.

**Nota 1:** In vederea îndeplinirii cerinței de mai sus, Ofertanții vor prezenta Diploma de studii, CV-ul si documente justificative (recomandări/ documente emise de beneficiari/ angajatori / documentații tehnice aferente implementării sau orice alte documente similare care să ateste activitatea desfășurată în cadrul unui astfel de proiect și arhitectura sistemului).

**Nota 2:** Cerința de mai sus reprezintă cerința minima pe care ofertanții au obligația sa o îndeplinească in vederea stabilirii conformității propunerii tehnice.

**Responsabilități:**

- Este responsabil pentru imaginea, comunicarea și evoluția arhitecturii întregului sistem
- Definește împreuna cu ceilalți coordonatori proiectarea sistemului
- Urmărește respectarea cu strictețe a obiectivelor asumate in documentele de proiectare
- Are rol de mediator intre membrii echipelor proiectului pe teme tehnice si rol decizional in alegerea soluțiilor informatice legate de sisteme , framework-uri si standarde implementate
- Întreține si livrează documentul de arhitectura al sistemului
- Colaborează cu specialiștii autorității contractante pe teme legate de arhitectura sistemului informatic

C. Cerințe minime ale Expertului cheie nr. 3: Analist de business (1 expert)

a) *studii superioare* dovedite prin diplomă de licență sau echivalent;

b) *certificat de absolvire* a unui curs de specialitate în domeniul analizei de business prin certificare/de tip Certified Business Analysis Professional sau echivalent;

c) Experiența deținuta in poziția de Analist de business sau similar*) in cadrul unui contract de dezvoltare/implementare/extindere sistem informatic in care s-au realizat servicii similare activităților ce urmează să le îndeplinească în contract.

**Nota 1:** In vederea îndeplinirii cerinței de mai sus, Ofertanții vor prezenta Diploma de studii, Certificatul de absolvire / adeverința / documente justificative similare sau echivalente care atesta

absolvirea cursului, CV-ul si documente justificative (recomandări/ documente emise de beneficiari/ angajatori / documentații tehnice aferente implementării sau orice alte documente similare care să ateste rolul, activitatea desfășurată în cadrul unui astfel de proiect, precum și informații relevante referitoare la sistem (module, funcționalități, scop etc.).

**Nota 2:** Cerința de mai sus reprezintă cerința minima pe care ofertanții au obligația sa o îndeplinească in vederea stabilirii conformității propunerii tehnice.

**Responsabilități:**

- Coordonează activitățile de analiza a cerințelor de business, elaborare a documentelor de specificații funcționale si a scenariilor de testare
- Activități de implementare, asistenta si suport tehnic
- Suport acordat utilizatorilor cheie pentru testarea de acceptanta a sistemului

Nota: *) pentru experții Arhitect de sistem si Analist de business experiența in poziții similare va fi analizata raportat la responsabilitățile expertului din acest contract

D. Cerințe minime ale Expertului non-cheie nr. 1: Expert proiectare și administrare baze de date (1 expert)
   a) *studii superioare* dovedite prin diplomă de licență sau echivalent;
   b) *Certificare profesională* atestată de un producător de tehnologie care să demonstreze specializarea în domeniul software-lui administrării bazelor de date pentru produsul și/sau tehnologia SGBD ofertată;
   c) *experiență specifică în calitate de expert baze de date constând în implicarea în cel puțin un proiect/contract de implementare sau administrare a unei baze de date clusterizată în tehnologia SGBD ofertată,*

   **Nota 1:** In vederea îndeplinirii cerinței de mai sus, **ulterior semnării contractului,** Contractantul va prezenta Diploma de studii, CV-ul si documente justificative (recomandări/ documente emise de beneficiari/angajatori / documentații tehnice aferente implementării sau orice alte documente similare care să ateste rolul, activitatea desfășurată în cadrul unui astfel de proiect, precum și informații relevante referitoare la produsul și/sau tehnologia SGBD implementată).

E. Cerințe minime ale Expertului non-cheie nr. 2: ITS (1 expert)
   a) *studii superioare* dovedite prin diplomă de licență sau echivalent;
   b) *certificare profesională* atestată de angajatori (recomandări)
   c) *experiență:* implicare in minim doua proiecte care implica activități de proiectare sau implementare a sistemelor de transport inteligente sau sisteme de telecomunicații

   **Nota 1:** In vederea îndeplinirii cerinței de mai sus, **ulterior semnării contractului,** Contractantul va prezenta Diploma de studii, CV-ul si documente justificative (recomandări/ documente emise de beneficiari/angajatori).

Suplimentar, Contractantul va asigura personal calificat pentru derularea activităților prevăzute in caietul sarcini.

## 12 MODALITĂŢI ŞI CONDIŢII DE PLATĂ

Contractantul va emite factura pentru produsele livrate, serviciile prestate si lucrarile executate.
In conformitate cu prevederile legale privind e-Factura, Furnizorul are obligația de a emite facturi electronice pe care sa le transmită prin sistemul național privind factura electronica RO e-Factura.
In conformitate cu prevederile legale in vigoare, exemplarul original al facturii electronice se considera fișierul de tip XML, însoțit de sigiliul electronic al Ministerului Finanțelor.
Orice factura trimisa fizic sau la adresa de e-mail registraturacnair@andnet.ro, care nu va avea atașat indexul încărcării in sistemul RO e-Factura se va restitui Furnizorului.
După înregistrarea facturilor in sistemul național RO e-Factura, Furnizorul va transmite Autorității Contractante, in termen de maxim 2 zile lucrătoare, indexul de încărcare a facturii in sistemul RO e-Factura, pentru a putea fi identificate si descărcate din Spațiul Privat Virtual (SPV).
Netransmiterea indexului de încărcare către Autoritatea Contractanta, in termenul menționat, face ca termenul de plata menționat la alin. (2) in cuprinsul prezentului articol, sa nu curgă pana la data transmiterii oficiale a indexului de încărcare, conform alin. (6).
Termenul de plata, menționat la alin. (2), va curge de la primirea de către Autoritatea Contractanta a indexului de încărcare, potrivit prezentului alineat.
Indexul de încărcare in Sistemul RO e-factura al facturii emise se comunica Autorității Contractante prin următoarele metode: posta cu confirmare de primire sau prin delegat direct la sediul Beneficiarului sau in format electronic la adresa de e-mail: registraturacnair@andnet.ro. In caz de divergente, dovada comunicării indexul de încărcare in Sistemul RO e-Factura al facturii emise către Autoritatea Contractanta o constituie, după caz, mandatul poștal sau stampila aplicata de Registratura Autorității Contractante pe document sau dovada electronica de primire.
Factura va avea menționat obligatoriu: numărul de înregistrare, data emiterii, numărul si data contractului, data scadenta, perioada in care au fost executate lucrările / prestate serviciile, denumirea subunității (după caz), precum si alte informații specifice contractului, inclusiv Codul CPV.
Plata se va face eșalonat în funcție de livrări și recepții parțiale sau recepție finală, conform prevederilor Contractului.
Plățile se vor face pe baza preturilor unitare comunicate in propunerea financiara.

## 13 CERINTE PRIVIND PROTECŢIA DATELOR CU CARACTER PERSONAL

### 13.1 CONTEXT

Legea nr. 383/2022 reglementează instituirea sistemului informatic e-SIGUR pentru monitorizarea traficului rutier în România. Acest sistem integrat urmărește eficientizarea monitorizării și îmbunătățirea siguranței rutiere conform Strategiei naționale privind siguranța rutieră. Sistemul informatic e-SIGUR va include diverse tehnologii și dispozitive de monitorizare, inclusiv radare

fixe, pentru a detecta și preveni încălcările regulilor de circulație. Prin intermediul e-SIGUR, autoritățile vor putea gestiona mai eficient fluxul de trafic și vor avea mai multe instrumente disponibile pentru a reduce accidentele și congestiile rutiere, având un impact semnificativ asupra siguranței și eficienței rutiere în România.

Implementarea proiectului e-SIGUR trebuie să respecte cerințele privind protecția datelor cu caracter personal stabilite în Legea nr. 190/2018, care transpune Regulamentul (UE) 2016/679 (GDPR).

### 13.2 METODOLOGIE

Pentru a evalua impactul datelor cu caracter personal asupra unui sistem informatic nou, cum este sistemul e-SIGUR, precum și pentru a asigura respectarea principiilor "*Privacy by Design*" și "*Privacy by Default*" cerute de GDPR, trebuie urmărite câteva obiective importante, care presupun o serie de activități:

**Identificarea datelor cu caracter personal**: Se efectuează o analiză a tuturor datelor prelucrate de sistemul informatic pentru a identifica informațiile care pot fi considerate date cu caracter personal conform GDPR. Apoi se identifică și se notează toate datele care se referă la persoane fizice identificate sau identificabile, inclusiv dacă sunt date cu caracter personal.

**Evaluarea impactului asupra protecției datelor** (*DPIA*): Realizarea unei DPIA pentru a identifica și evalua riscurile potențiale pentru confidențialitate și securitatea datelor cu caracter personal.

**Protecția datelor introdusă în arhitectura sistemului e-SIGUR**: Asigurarea că atât confidențialitatea cât și securitatea datelor sunt încorporate în designul și arhitectura sistemului informatic, fără a fi necesare modificări ulterioare.

**Proiectarea cerințelor de confidențialitate** (*Privacy by Design*): Integrarea principiilor de confidențialitate încă din faza de concepție a sistemului informatic, inclusiv selectarea și configurarea adecvată a tehnologiilor, astfel încât să se minimizeze colectarea și prelucrarea datelor cu caracter personal.

**Setări implicite pentru protecția datelor** (*Privacy by Default*): Configurarea implicită a sistemului să fie orientată spre protecția datelor, astfel încât să ofere niveluri ridicate de confidențialitate încă de la început, fără intervenția utilizatorilor.

Desfășurarea acestor activități asigură că sistemul informatic e-SIGUR va respecta cerințele GDPR și că protecția datelor cu caracter personal este o prioritate încă de la etapa inițială a dezvoltării sistemului informatic.

### 13.3 IDENTIFICAREA DATELOR CU CARACTER PERSONAL

Pentru identificarea datelor cu caracter personal procesate de sistemul e-SIGUR, trebuie identificate toate categoriile de date procesate de sistemul informatic și analizat care din aceste date sunt cu caracter personal (informații despre o persoană identificată sau identificabilă). În

principiu, sistemul e-SIGUR este un sistem care agregă date din sistemele informatice ale Centrelor de Monitorizare și Informare (CMI) aparținând CNAIR, care le stochează temporar, cu scopul de a genera alerte către CNAIR pentru verificare rovinietă sau IGPR pentru constatarea altor contravenții.

Astfel, distingem 3 categorii de date:

**Date importate (preluate din CMI)**

| Date prelucrate | Format | Date cu caracter personal | Justificare |
|---|---|---|---|
| Imagini domeniu public (drum, acostament, parcare, clădire, persoane, etc) | Video | DA, în anumite circumstanțe | Camerele pot înregistra imagini ale unor persoane (exemplu: o persoana care traversează strada, o persoană care conduce un autovehicul sau este pasager, o persoana care coboară sau urcă într-un vehicul, etc.). |
| Detalii autovehicul (marcă, model, culoare) | Video | DA, în anumite circumstanțe | În cazul modelelor auto exclusiviste, se poate identifica proprietarul autovehiculul. |
| Număr de înmatriculare autovehicul | Text | DA, corelat cu alte informații | Pe baza numărului de înmatriculare, se poate identifica proprietarul autovehiculul (mai ales a numerelor personalizate, aparținând persoanelor publice). |
| Parametrii tehnici autovehicul (viteză, greutate, geolocație) | Text | NU | Parametrii tehnici autovehicul nu pot conduce la identificarea unei persoane. |
| Înregistrări senzori (bucle, FOS, stații meteo) | Text | NU | Parametrii tehnici autovehicul nu pot conduce la identificarea unei persoane. |

**Date prelucrate de e-SIGUR**

| Date prelucrate | Format | Date cu caracter personal | Justificare |
|---|---|---|---|
| Stocare date video preluate din CMI | Video | DA, în anumite circumstanțe | Imaginile pot conține date ale unor persoane (șoferi, pietoni) sau date care pot duce la identificarea unor persoane (proprietari) |

| Date prelucrate | Format | Date cu caracter personal | Justificare |
|---|---|---|---|
| Lista vehicule căutate (import IGPR) | Tabelar | DA, corelat cu alte informații | Lista conține numere de înmatriculare ale unor autovehicule. |
| Parametrii tehnici agregați (număr de înmatriculare, viteză) | Bază de date | DA, corelat cu alte informații | Conține numărul de înmatriculare. |
| Notificări IGPR – alertă cazuri | XML | DA, corelat cu alte informații | Cazurile vor fi notificate printr-un API. Pe baza acestor notificări din e-SIGUR, IGPR va identifica proprietarul autovehiculului pe baza numărului de înmatriculare. |
| Notificări CNAIR – alertă rovinietă | API | DA, corelat cu alte informații | Pe baza acestor notificări din e-SIGUR, CNAIR va identifica autovehiculele care circulă pe drumurile publice naționale fără a avea rovinietă și pe baza numărului de înmatriculare identifică proprietarul autovehiculului. |
| Rapoarte BI (export raport consolidat) | Diverse formate | NU | Rapoartele nu conțin numere de înmatriculare ci sunt doar date statistice. |
| Chatbot (imput/output) | Text | DA, în anumite circumstanțe | Poate furniza în răspunsuri date cu caracter personal, precum numărul de înmatriculare. Cu toate acestea, conversațiile nu sunt salvate ci se pierd la finalizarea interacțiunii. |
| Arhivare cazuri | Bază de date | NU | Cazurile închise de operatori sunt arhivate și oprite de la procesare. Metadatele aferente cazurilor închise și arhivate sunt date statistice ce nu conțin informații care pot duce la identificarea unei persoane. |

**Date tehnice ale sistemului**

| Date prelucrate | Format | Date cu caracter personal | Justificare |
|---|---|---|---|
| Cont utilizator | Text | DA | Este necesar pentru identificarea utilizatorului și revizuirea drepturilor de acces. |
| Jurnale de audit | Text | DA | Conțin date despre utilizator și acțiunile lui, inclusiv despre adresa IP privată de la care s-a efectuat conexiunea. |
| Backup baza de date | Arhivă | DA | Este o copie a bazei de date de producție și conține aceleași informații. |
| Date operaționale IT, de monitorizare a bunei funcționări a sistemului e-SIGUR | Diverse formate | NU | Monitorizarea performanței și a disponibilității platformei e-SIGUR nu duce la identificarea unei persoane. |
| Semnătură electronică calificată | Text | DA | Este o semnătură calificată, care împreună cu marca temporală calificată, garantează unicitatea și autenticitatea unui înregistrări electronice. |

## 13.4 ANALIZA DE IMPACT

### 13.4.1 PRELUCRAREA DATELOR SENSIBILE

Întrucât sistemul e-SIGUR nu folosește imaginile video pentru identificarea automată a persoanelor, ci doar a numerelor de înmatriculare, considerăm că sistemul NU procesează date cu caracter sensibil, conform Art.9 Alin.(2) punctul (g) din Regulamentul GDPR. Acesta prevede excluderea prelucrării datelor cu caracter SPECIAL, în cazul în care "*prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate*". Astfel, identificarea proprietarului unui autovehicul se face manual de către personalul IGPR și/sau CNAIR, în afara platformei e-SIGUR, consultând alte baze de date (exemplu: DRPCIV), pentru asocierea numărului de înmatriculare cu proprietarul autovehiculului.

<u>În concluzie:</u>

- Identificarea proprietarului autovehiculului <u>nu se face</u> pe baza înregistrărilor video ale persoanei vizate, ci pe baza numărului de înmatriculare
- Identificarea proprietarului autovehiculului <u>nu se face automat</u> de un sistem ci manual de o persoană din IGPR/CNAIR, consultând alte baze de date

- Identificarea proprietarului autovehiculului nu se face exclusiv pe baza datelor din e-Sigur, ci consultând alte baze de date

Sistemul e-Sigur nu prelucrează date cu caracter personal sensibile referitoare la condamnări penale și infracțiuni, conform Articolului 10 din Regulamentul GDPR. Aceste informații sunt disponibil exclusiv în bazele de date ale IGPR. Căutarea unui autovehicul în cadrul platformei e-SIGUR, poate fi făcut doar de către IGPR și nu presupune automat existența unei infracțiuni. De asemenea proprietarul autovehiculului nu poate fi asociat cu o infracțiune, el putând fi chiar victima unei infracțiuni (exemplu: căutarea unui autovehicul furat).

**Scopul prelucrării datelor**

| Scopul prelucrării datelor | Categoria de date | Date cu caracter personal | Temeiul prelucrării |
|---|---|---|---|
| Îmbunătățirea siguranței rutiere | Înregistrări video | Imagini domeniu public, detalii autovehicul, număr înmatriculare | Obligație legală/ Interes public |
| Îmbunătățirea siguranței rutiere | Parametrii tehnici | Detalii autovehicul, număr înmatriculare, parametrii tehnici | Obligație legală/ Interes public |
| Verificare rovinietă | Număr de înmatriculare | Număr înmatriculare, clasă autovehicul | Obligație legală/ Interes public |
| Suport pentru IGPR | Vehicule căutate | Număr de înmatriculare | Protejarea intereselor persoanei vizate/ Interes public |
| Eficientizarea monitorizării | Date statistice | Date de trafic, volumetrii, parametrii tehnici, rapoarte BI | Interes public |
| Funcționarea sistemului e-SIGUR | Date tehnice ale sistemului informatic | Date de autentificare, jurnale de acces (log-uri), backup | Interes legitim – pentru buna funcționare a sistemului IT |

## 13.5 PERIOADA DE RETENȚIE A DATELOR

Perioada de retenție a datelor diferă în funcție de categoria de date și de temeiul prelucrării. Astfel, platforma e-SIGUR va trebui sa asigure o perioadă de retenție personalizabilă, pe tipurile de date, configurată în conformitate cu legile în vigoare. De asemenea va trebui să asigure ștergerea automată a datelor, la expirarea perioadei de retenție definită. În anumite cazuri, în care este necesară păstrarea datelor peste perioada de retenție implicită (de exemplu ca urmare a solicitării instanțelor de urmărire penală sau a instanțelor judecătorești), parametrul de retenție va putea fi modificat de către utilizatorul care gestionează cazul respectiv. Justificarea acestei situații o regăsim în Regulamentul GDPR Art.9 Alin.(2) punctul (f) "*prelucrarea este necesară pentru*

*constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare*".

## 13.6 DREPTURILE PERSOANEI VIZATE

O persoană vizată, conform GDPR (Regulamentul General privind Protecția Datelor), este o persoană fizică identificată sau identificabilă, ale cărei date cu caracter personal sunt prelucrate de către un operator sau un împuternicit de prelucrare a datelor. Aceste date cu caracter personal includ orice informații care se referă la persoana respectivă și care o pot identifica direct sau indirect, cum ar fi numele, adresa, numărul de înmatriculare al autovehiculului, datele de localizare, etc.

Persoana vizată poate fi orice cetățean român sau străin care circulă pe drumurile publice din România, drumuri care sunt monitorizate de CNAIR cu scopul îmbunătățirii siguranței rutiere.

Persoana vizată are drepturi și protecții specifice în ceea ce privește prelucrarea datelor sale personale conform prevederilor GDPR. Aceste drepturi includ:

| Art. GDPR | Drepturi ale persoanei vizate | Aplicabilitate | Justificare |
|---|---|---|---|
| Art.13 | Dreptul la informare | Aplicabil | Persoana vizată trebuie informată că este înregistrată pe respectivele tronsoane de drum (ex: Politica de confidențialitate a sistemului e-SIGUR publicată pe website-ul CNAIR). |
| Art.12 | Dreptul la transparență informațională | Aplicabil | CNAIR trebuie să ia măsuri adecvate pentru a oferi persoanei vizate informații clare, concise, transparente și ușor accesibile referitoare la prelucrarea datelor sale cu caracter personal (Ex: panou rutier de informare asupra monitorizării video, campanii publice de informare) |
| Art.15 | Accesul la datele personale | Aplicabil | Persoana vizată poate solicita în anumite condiții prevăzute de lege, înregistrări video cu propria persoană. |
| Art.5 | Dreptul de rectificare | Neaplicabil | Imaginile video nu pot fi rectificate. |
| Art.17 | Ștergere sau restricționare a prelucrării datelor | Neaplicabil | Cerință legală – datele nu pot fi șterse la cererea persoanei vizate. |
| Art.69 | Dreptul la portabilitatea datelor | Neaplicabil | Persoana vizată nu poate solicita portarea datelor. |
| Art.21 | Dreptul de a se opune prelucrării datelor | Neaplicabil | Prelucrarea este în baza unei legi. |
| Art.70 | Dreptul de a depune o plângere la ANSPDCP | Aplicabil | Persoana vizată se poate adresa ANSPDCP pentru a depune o plângere legată de drepturile sale. CNAIR trebuie să ofere o procedură prin care să reglementeze dreptul persoanei vizate de a depune o plângere la autorități. |

# 14 IPOTEZE SI RISCURI

## 14.1 IPOTEZELE

Ipotezele avute în vedere sunt:

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

În pregătirea Ofertei, Ofertantul trebuie să aibă în vedere cel puțin riscurile și ipotezele descrise mai sus. În acest sens, la întocmirea ofertei, Ofertantul trebuie să ia în considerare resursele necesare (de timp, financiare și de orice alta natură), pentru implementarea strategiilor de risc propuse.

## 14.2 Registru Riscuri

| Arie | Descrie risc | Impact | Măsuri de securitate recomandate |
|---|---|---|---|
| e-SIGUR | Implementarea finala a sistemului e-SIGUR sa fie diferita de arhitectura inițială | Mare | Audit de proiect, la finalizarea implementării, pentru a valida ca sistemul corespunde cu arhitectura inițială. |
| e-SIGUR | Neimplementarea funcționalităților definite în cadrul proiectului, inclusiv cele de securitate | Mare | Audit de proiect, la finalizarea implementării, pentru a valida fiecare funcționalitate. |
| Personal | Erori umane în operarea platformei e-SIGUR | Mediu | Identificarea cazurilor de utilizare eronata și/sau abuzivă și corectarea acestor situații. Acest lucru poate fi făcut ori la nivel tehnic, prin modificarea platformei e-SIGUR sau a drepturilor de acces ale utilizatorilor, ori la nivel organizatoric prin instruirea operatorilor. Recomandăm documentarea operării într-un manual de operare al sistemului e-SIGUR și instruirea persoanelor care operează sistemul (înainte de acordarea dreptului de acces, dar și periodic în cadrul instruirilor anuale). O bună practică este testarea cunoștințelor după fiecare instruire. |
| Personal | Alocarea de drepturi excesive utilizatorilor sistemului e-SIGUR | Mare | Definirea pofilelor de utilizator cu drepturi granulare. Instituirea unui proces periodic de revizuire a drepturilor de acces, care să cuprindă atât utilizatorii interni CNAIR cât și |

| Arie | Descrie risc | Impact | Măsuri de securitate recomandate |
|---|---|---|---|
| | | | utilizatorii externi ai sistemului e-SIGUR (utilizatori IGPR, administratori de la furnizori, etc.) |
| e-SIGUR | Utilizarea parolelor slabe în procesul de autentificare | Mare | Recomandăm integrarea platformei e-SIGUR cu sistemul Active Directory al CNAIR, pentru aplicarea unitară a politicii de parole la nivelul CNAIR. Alternativ, mecanisme similare de complexitate a parolei trebuie implementate în sistemul e-SIGUR. |
| e-SIGUR | Interconectări ale platformei e-SIGUR cu alte sisteme informatice din CNAIR sau din alte instituții, care nu au un nivel de securitate echivalent | Mare | Audit de securitate (teste tehnice), la fiecare interconectare cu un nou sistem informatic. |
| e-SIGUR | Platforma nu jurnalizează toate acțiunile utilizatorului. | Mare | Platforma trebuie să jurnalizeze (logheze) toate acțiunile utilizatorului. Întrucât GDPR consideră "vizualizarea" o prelucrare de date cu caracter personal, trebuie să existe log-uri pentru toate acțiunile efectuate de utilizator, inclusiv pentru zonele de "*search*" pe numerele de înmatriculare auto. |
| Security | Lipsa unui proces sistematic de monitorizare a evenimentelor de securitate | Mare | Integrarea evenimentelor de securitate din sistemul e-SIGUR într-o platforma de tip SIEM (*Security Incident and Event Management*) – managementul evenimentelor și al incidentelor de securitate. |
| DPO | Păstrarea datelor mai mult decât este necesar / setarea eronată a perioadei de retenție. | Mare | Datele trebuie păstrate doar dacă există un temei în acest sens. Analiza necesității păstrării datelor și justificarea perioadei de retenție depinde de actualizările legislative. De aceea este important să se revizuiască periodic Registrul prelucrărilor de date personale din CNAIR, în care să se identifice perioadele de retenție a datelor din platforma e-SIGUR. |
| e-SIGUR | Lipsa unui proces sistematic de actualizare a componentelor software: sistem de operare, baze de date, server web, firmware, etc. | Mediu | Recomandăm elaborarea unui plan anual de mentenanță care să includă toate componentele Hardware și Software ale sistemului e-SIGUR (inclusiv echipamente de rețea, storage, dispozitive de securitate) |
| e-SIGUR | Utilizarea de librarii open-source neîntreținute | Mare | Dezvoltatorul software al sistemului e-SIGUR, va trebui să își asume securitatea pentru toate componentele terțe (3rd party) pe care le utilizează. Dacă nu poate garanta acest lucru, este mai bine să nu se folosească componente care nu se află sub controlul său (librarii open-source dezvoltate de comunitate).<br>Recomandăm dezvoltatorului să includă procesul de testare de securitate în ciclul de viața al dezvoltării produsului. |

| Arie | Descrie risc | Impact | Măsuri de securitate recomandate |
|---|---|---|---|
| CNAIR | Atacuri informatice cu malware (ex: criptarea bazei de date cu ransomware) | Mare | Implementarea unui proces sistematic de backup care să asigure disponibilitatea datelor în cazul în care acestea sunt criptate de un malware. Soluția de backup trebuie să asigure o capacitate de stocare suficientă pentru o perioadă de retenție a metadatelor pentru cel puțin o lună de zile.<br>Implementarea de soluții anti-malware de ultimă generație superioare clasicului antivirus: EDR/XDR (*endpoint detection and response / extended detection and response*). |
| CNAIR | Scurgeri de informații | Mare | Implementarea unui sistem de clasificare și etichetare a datelor exportate din e-SIGUR, împreună cu o soluție DLP (*Data Loss Prevention*) care să detecteze și să alerteze posibilele scurgeri de informații, pe toate stațiile de lucru ale operatorilor platformei e-SIGUR. Dacă în fluxurile operaționale sunt implicate transmisii de date prin intermediul poștei electronice (e-mail) atunci soluția DLP trebuie să vizeze și acest serviciu. De asemenea trebuie impus și terților care utilizează sistemul e-SIGUR (exemplu: utilizatori din IGPR) să implementeze măsuri de securitate cel puțin egale cu cele ale CNAIR pentru a asigura un nivel de securitate echivalent. |
| CNAIR | Acces neautorizat la date | Mic | Trebuie efectuat un audit periodic al drepturilor de acces care să includă analize privind accesul la informații (ce informație a fost accesată, de către cine și în ce scop). Aceasta este o activitate operațională manuală, care trebuie efectuată periodic de responsabilul cu securitatea sistemului e-SIGUR. |
| CNAIR | Configurații eronate ale sistemelor IT&C ce alcătuiesc sistemul e-SIGUR sau care se interfațează cu sistemul e-SIGUR | Mediu | Efectuarea periodica a auditurilor de configurație, prin validarea manuală sau automată a setărilor tehnice. |
| CNAIR | Măsuri de securitate care nu sunt sistematic aplicate pe tot ciclul de viață al sistemului e-SIGUR | Mediu | Adoptarea unui Sistem de Management al Securității informației (SMSI) bazat pe bunele practici de securitate. Recomandăm utilizarea standardului internațional ISO 27001 care este centrat pe managementul riscurilor și pe o îmbunătățire continuă a controalelor de securitate. |

### 14.3 Măsuri tehnice și organizatorice (TOMs) GDPR

| Nr. | Cerință GDPR | Articol GDPR | Controale de securitate |
|---|---|---|---|
| 1 | *Privacy by design*<br>*Privacy by default* | 25 | Cerințele de *privacy* trebuie respectate atât în faza de proiectare a sistemului e-SIGUR, cât și în faza de implementare efectivă. Astfel, în cadrul proiectului de implementare trebuie desemnată o persona responsabilă cu monitorizarea |

| Nr. | Cerință GDPR | Articol GDPR | Controale de securitate |
|---|---|---|---|
| | | | respectării cerințelor de *privacy*. Această persoana va face parte din proiect și va fi responsabilă cu identificarea, analiza și gestionarea riscurilor de securitate la adresa datelor cu caracter personal.<br><br>Pentru a sprijini evaluările eficace ale riscurilor la adresa vieții private și a securității IT&C, ar trebui menținut un inventar actualizat al datelor, al componentelor informatice și corelării acestora.<br><br>La finalul proiectului, datele personale gestionate de sistemul e-SIGUR vor trebui să se regăsească în registrul prelucrării datelor la nivelul instituției (CNAIR). |
| 2 | Minimizarea datelor | 5, 25 | Vizualizarea, exportul și transferul datelor cu caracter personal trebuie să se limiteze la ceea ce este necesar în raport cu scopurile în care sunt prelucrate. Toate exporturile vor fi jurnalizate (cine a exportat, ce a exportat, când a exportat). Fișierele exportate vor avea pe fundal ca *watermark* eticheta CONFIDENȚIAL și *timestamp* cu numele și data utilizatorului care a efectuat exportul. |
| 3 | Dreptul de a fi uitat | 5, 25 | Sistemul e-SIGUR trebuie să includă mecanisme pentru ștergerea în condiții de siguranță a datelor cu caracter personal, la atingerea perioadei de retenție stabilită. Datele nu trebuie să mai poată fi recuperate după o ștergere sigură. |
| 4 | Păstrarea datelor | 5, 25 | Datele păstrate în scop statistic vor fi anonimizate (ex: se va înlocui numărul de înmatriculare cu orașul, modelul auto cu categoria auto, etc.). Acolo unde nu este posibil, datele vor fi *pseudonimizate* (înlocuirea datelor directe identificabile cu pseudonime sau coduri pentru a limita accesul la informații sensibile). |
| 5 | Minimizarea datelor în rapoarte și schimburi de date | 5, 25 | Rapoartele și exporturile de date din aplicațiile care conțin date cu caracter personal ar trebui controlate, deoarece acestea oferă o cale de acces necontrolată la informații. După caz, astfel de rapoarte ar trebui protejate prin controale compensatorii pentru a preveni divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal din fișierele de date exportate (exemplu: fișier protejat cu parolă, marcarea proprietarului cu numele celui care a efectuat exportul, aplicare eticheta sau metadata, etc.) |
| 6 | Minimizarea datelor pentru mediul de testare | 5, 32 | Definirea proceselor de management al testelor ar trebui să includă cerințe pentru anonimizarea / pseudonimizarea datelor pentru toate mediile de dezvoltare / testare ale sistemului e-SIGUR. Recomandăm utilizarea datelor sintetice în toate mediile de dezvoltare / testare. |
| 7 | Trasabilitatea prelucrării și pregătirea pentru incidente | 32, 33 | Mecanismele de monitorizare a jurnalelor ar trebui să includă colectarea securizată a înregistrărilor și mecanisme de alertă pentru detectarea activităților care prezintă riscuri în materie de securitate și confidențialitate. Astfel recomandăm ca jurnalele de securitate să fie transmise în timp real către un sistem de tip SIEM (*Security Information and Event Management*). Un astfel de sistem, împreună cu alte soluții de securitate la nivel de gazdă: EDR (*Endpoint Detection and Response*), FIM (*File Integrity Monitoring*), |

| Nr. | Cerință GDPR | Articol GDPR | Controale de securitate |
|---|---|---|---|
| | | | DLP (*Data Loss Prevention*), vor asigura detectarea în cel mai scurt timp a unui eveniment/incident de securitate.<br><br>Activitățile utilizatorilor privilegiați trebuie monitorizate pentru a preveni distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal în mod accidental sau ilegal și pentru a preveni eludarea/dezactivarea controalelor aplicațiilor. Astfel recomandăm ca toate acțiunile privilegiate să fie înregistrate într-un sistem PAM (*Privileged Access Management*) în special în cazul terților (subcontractori, dezvoltatori software, administratori de la alte instituții, etc.) |
| 8 | Abilitatea de a restabili disponibilitatea și accesul la datele cu caracter personal | 32 | Copiile de rezervă ale datelor cu caracter personal trebuie luate și testate în mod regulat, în conformitate cu o politică de backup convenită. Copiile de rezervă ar trebui protejate prin intermediul unei protecții similare sistemelor sursă (criptare backup).<br><br>Copiile de siguranță ale sistemului e-SIGUR trebuie să asigure o dimensionare corectă, astfel încât să poată fi restaurate toate datele, fără a exista perioade de pierderi. În cadrul proiectului vor fi incluse licențele software de backup și capacitățile de stocare necesare pentru acoperirea volumului de date pentru care este necesară o copie de siguranță. Se vor păstra minim 3 copii de date ale bazelor de date (ce conțin date, metadate, cazuri deschise, arhiva cazurilor). Nu se vor include în backup datele row mai vechi de 30 de zile, datorită volumului uriaș de date. |
| 9 | Gestionarea accesului utilizatorilor | 32 | Toate profilurile de utilizator care prelucrează date cu caracter personal ar trebui definite astfel încât să se reducă la minimum accesul la datele cu caracter personal transmise, stocate sau prelucrate în alt mod. În urma analizei detaliate a fluxurilor operaționale gestionate de e-SIGUR, se vor defini profile de utilizatori care vor respecta principiile "*need to know*" (dreptul de știi) și "*need to have*" (dreptul de a avea). |
| 10 | Punerea în aplicare a unor măsuri pentru a asigura un nivel de securitate corespunzător riscului | 32 | Ar trebui definite standarde de securitate de referință pentru a proteja informațiile accesate, stocate și comunicate între sisteme. Pentru implementarea măsurilor de securitate de tip *hardening*, recomandăm să se utilizeze standardele tehnice *CIS Security Controls* v8. |
| 11 | Securitate OS/DB | 32 | Sistemul e-SIGUR trebuie să utilizeze doar componente hardware și software care sunt în ciclul de viață al producătorului. Pentru fiecare componentă în parte trebuie urmărit care este ciclul de viață și trebuie planificată înlocuirea/ upgrade-ul componentei înainte ca producătorul să oprească suportul acesteia. Nu recomandăm utilizarea de componente care sunt *End-of-Life* sau *End-of-Support* și pentru care producătorul nu mai oferă suport sau actualizări de securitate. |

| Nr. | Cerință GDPR | Articol GDPR | Controale de securitate |
|---|---|---|---|
| | | | Componentele IT&C trebuie scanate periodic (recomandăm săptămânal) pentru a identifica vulnerabilități de securitate. Se vor aplica imediat corecțiile de securitate, care pot include: aplicarea de patchuri de securitate conform specificațiilor producătorului, modificarea unor parametri tehnici, upgrade-ul la o versiune superioară, înlocuirea componentei cu una echivalentă, etc. Aceste modificări asupra componentelor sistemului e-SIGUR ar trebui făcute prin procesul regular de Management al schimbărilor, care să asigure atât trasabilitatea modificărilor, cât și aprobările necesare. Toate modificările se vor face în perioada de mentenanță definită în planul anual de mentenanță, plan ce cuprinde toate activitățile IT&C care sunt necesare a fi desfășurat pe parcursul unui an calendaristic. Respectarea cu strictețe al planului de mentenanță se va face lunar de către de administratorii tehnici ai platformei e-SIGUR ar procesele verbale cu furnizorii externi vor fi păstrate ca evidențe de audit.<br><br>Activitățile administratorilor DB și ale utilizatorilor cu acces direct la bazele de date trebuie monitorizate pentru a preveni distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul accidental sau ilegal la datele cu caracter personal stocate. Recomandam implementarea unei soluții de tip DAM (Database Access Management) care să monitorizeze interogările SQL ale bazelor de date, vulnerabilitățile tehnice specifice bazelor de date, activități suspecte/neobișnuite precum și alte măsuri de prevenție de tip firewall de baze de date. |
| 12 | Securitate aplicație | 32 | Pentru securizarea aplicației front-end (aplicație web) precum și a API-urilor, recomandăm implementarea unei soluții firewall de tip WAF (*Web Application Firewall*) care înțelege cum funcționează sistemul e-SIGUR, care se adaptează automat și care protejează aplicația de o multitudine de tipuri de atac cibernetic. |
| 13 | Securitatea codului sursă | 32 | Pentru a asigura securitatea codului sursă pe tot parcursul ciclului de viață al dezvoltării de software (SDLC), se vor implementa următoarele măsuri de securitate:<br><br>Analiza de securitate la începutul procesului: Realizarea unei analize de securitate în faza de planificare a dezvoltării pentru a identifica și evalua posibilele amenințări și vulnerabilități ale codului sursă.<br><br>Aplicarea unor standarde de codare sigură: Adoptarea și respectarea unor standarde stricte de codare sigură pentru a evita vulnerabilitățile și erorile comune care pot duce la probleme de securitate.<br><br>Testare automată și manuală a securității: Utilizarea unor instrumente automate și revizuirea manuală a codului pentru a detecta și remedia vulnerabilitățile de securitate înainte de implementare - scanare de tip SAST (*Static Application Security Testing*) |

| Nr. | Cerință GDPR | Articol GDPR | Controale de securitate |
|---|---|---|---|
| | | | Actualizarea și remedierea continuă: Monitorizarea și actualizarea constantă a codului sursă pentru a remedia rapid eventualele vulnerabilități descoperite ulterior.<br><br>Controlul accesului la codul sursă: Limitarea accesului la codul sursă doar la personalul autorizat și implementarea unor politici stricte de gestionare a accesului.<br><br>Securizarea codului sursă: Utilizarea unor mecanisme de securitate pentru a proteja codul sursă împotriva accesului neautorizat și a manipulării, versionarea codului sursă, etc. |
| 14 | Confidențialitatea, integritatea, disponibilitatea și reziliența continuă a componentelor sistemului e-SIGUR | 32 | Luând în considerare expunerea la risc a aplicațiilor prelucrează date cu caracter personal, se vor planifica și se vor executa evaluări periodice de securitate. Aceste evaluări ar trebui să conțină cel puțin:<br><br>Scanarea de vulnerabilități a infrastructurii (cel puțin lunar, pe toată infrastructura)<br><br>Scanarea componentelor web pentru identificarea vulnerabilităților de tip OWASP Top 10 – scanare de tip DAST (*Dynamic Application Security Testing*) (cel puțin trimestrial și la orice modificare efectuată)<br><br>Audit de configurație – verificarea manuală a configurațiilor (cel puțin anual, prin verificări manuale de către un auditor de securitate sau automat prin intermediul aplicațiilor de securitate)<br><br>Teste de penetrare (cel puțin anual și la orice nouă integrare a sistemului e-SIGUR cu alte componente informatice sau alte instituții)<br><br>Pentru asigurarea securității datelor cu caracter personal procesate de sistemul e-SIGUR, trebuie să se asigure criptarea datelor. Datele trebuie criptate "*at-rest*" (date stocate) la nivelul bazei de date și la nivelul echipamentului de stocare (storage). De asemenea datele trebuie criptate și "*in-transit*" (la transmitere) utilizând exclusiv protocoale securizate (HTTPS, SSH, Secure FTP, etc. dar și canale de comunicare criptate (tuneluri VPN IPSEC). |

## 15 DREPTURI DE PROPRIETATE INTELECTUALĂ

Toate documentele ce vor fi elaborate în executarea Contractului (Livrabile, studii, analize, rapoarte, planuri, proceduri, metodologii, materiale de instruire și prezentare 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.

Drepturile patrimoniale de autor asupra soluției tehnice create de către Contractant (contractant sau membrii asocierii), aferente serviciilor livrate, se transferă către Autoritatea Contractantă, CNAIR (cf. art. 12, alin. (1) din Ordonanța de urgență nr. 41/2016 privind stabilirea unor măsuri de simplificare la nivelul administrației publice centrale și pentru modificarea și completarea unor acte normative: *„Instituțiile publice, organele de specialitate ale administrației publice centrale și locale, precum și persoanele juridice de drept privat care, potrivit legii, au obținut statut de utilitate publică sau sunt autorizate să presteze un serviciu public, în regim de putere publică, au obligația de a prevedea explicit în caietele de sarcini și în contractele aferente procedurilor de achiziție publică demarate, care includ dezvoltări de programe informatice la solicitarea instituției sau autorității, faptul că toate drepturile patrimoniale de autor asupra tuturor operelor create de către contractant sau membrii asocierii, aferente produsului sau serviciului livrat, se transferă către autoritatea contractantă".*

Pe toata durata desfășurării proceselor de dezvoltare a soluțiilor informatice, se vor utiliza depozitare de cod sursa aflate in patrimoniul CNAIR. Codul sursa nu va fi stocat, sub nici o forma in alta locație decât cea indicate de către autoritatea contractanta.

Înainte de plata facturii finale, autoritatea contractanta preia integral codul sursă al aplicațiilor informatice dezvoltate, documentația aferentă și kit-urile de instalare.

## 16 Alte mențiuni

Limba de lucru este limba romana. Ofertele care se vor prezenta numai pentru anumite activități sau care nu vor respecta toate condițiile prevăzute in prezentul caiet de sarcini pot fi considerate neconforme.

## ANEXA 1 - GRAFICUL DE IMPLEMENTARE

| Activitate (denumire sintetica) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Efectuarea de vizite în teren (site-survey) pentru identificarea amplasamentului exact și a condițiilor optime de instalare/montare | | | | | | | | | | | | | | | | | | | | | | |
| Întocmirea documentației tehnice pentru obținerea avizelor si Elaborarea Proiectului Tehnic de execuție pentru instalarea consolelor în teren, infrastructura de rețea și alte lucrări de conectare | | | | | | | | | | | | | | | | | | | | | | |
| Livrarea/instalarea/montarea consolelor și infrastructurii de rețea electrica | | | | | | | | | | | | | | | | | | | | | | |
| Livrare echipamente, componentelor hardware și software in teren | | | | | | | | | | | | | | | | | | | | | | |
| Instalare echipamente, componentelor hardware și software in teren | | | | | | | | | | | | | | | | | | | | | | |
| Analiză detaliata a cerintelor software pentru Sistemul E-sigur | | | | | | | | | | | | | | | | | | | | | | |
| Proiectare solutie software | | | | | | | | | | | | | | | | | | | | | | |
| Livrare și instalare componentele hardware și software pentru nucleul central | | | | | | | | | | | | | | | | | | | | | | |
| Dezvoltare/ customizare, instalare, configurare software | | | | | | | | | | | | | | | | | | | | | | |
| Instruire utilizatori și | | | | | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **administratori sistem** | | | | | | | | | | | | | | | | | | | | | | |
| **Testare sistem în vederea acceptanței** | | | | | | | | | | | | | | | | | | | | | | |
| **Lansarea în producție a sistemului** | | | | | | | | | | | | | | | | | | | | | | |

**ANEXA 2 – Lista orientativa a sectoarelor care poate suporta modificări in implementarea contractului**

Tabelul de mai jos indică cele 400 de sectoare roșii și galbene unde este recomandată amplasarea de sisteme de monitorizare viteza și comportament rutier, identificate de centrul sectorului.

| Nr. crt. | Latitudine | Longitudine | Tip sector | Indicativ drum | Poz. km. aprox. |
|---|---|---|---|---|---|
| 1 | 44.43809 | 25.94604 | roșu | A1 | 12 + 718 |
| 2 | 45.81478 | 22.06233 | galben | A1 | 442 + 009 |
| 3 | 45.94734 | 21.28369 | roșu | A1 | 515 + 250 |
| 4 | 46.21044 | 20.7975 | roșu | A1 | 581 + 787 |
| 5 | 44.44098 | 26.67314 | roșu | A2 | 48 + 408 |
| 6 | 44.44263 | 26.76344 | galben | A2 | 55 + 747 |
| 7 | 44.39831 | 27.56358 | roșu | A2 | 120 + 418 |
| 8 | 44.33851 | 28.02278 | galben | A2 | 159 + 608 |
| 9 | 44.31985 | 28.03281 | galben | A2 | 161 + 993 |
| 10 | 44.21477 | 28.21578 | galben | A2 | 182 + 877 |
| 11 | 44.88475 | 26.03242 | roșu | A3 | 68 + 793 |
| 12 | 44.21652 | 28.55186 | galben | A4 | 5 + 648 |
| 13 | 44.10847 | 28.63453 | roșu | A4 | 21 + 820 |
| 14 | 44.48919 | 26.21515 | galben | DNCB | 14 + 921 |
| 15 | 44.40126 | 26.22894 | roșu | DNCB | 24 + 332 |
| 16 | 44.34271 | 26.16688 | roșu | DNCB | 33 + 425 |
| 17 | 44.35936 | 26.03611 | galben | DNCB | 44 + 939 |
| 18 | 44.47053 | 25.95863 | galben | DNCB | 60 + 117 |
| 19 | 44.58729 | 26.07074 | roșu | DN1 | 18 + 300 |
| 20 | 44.65893 | 26.07551 | galben | DN1 | 26 + 460 |
| 21 | 45.00428 | 25.88034 | galben | DN1 | 74 + 069 |
| 22 | 45.27782 | 25.62173 | galben | DN1 | 111 + 919 |
| 23 | 45.37904 | 25.5391 | roșu | DN1 | 126 + 990 |
| 24 | 45.40152 | 25.53451 | roșu | DN1 | 129 + 679 |
| 25 | 45.45629 | 25.56649 | roșu | DN1 | 137 + 160 |
| 26 | 45.73508 | 25.43735 | roșu | DN1 | 187 + 229 |
| 27 | 45.82619 | 24.90045 | roșu | DN1 | 240 + 269 |
| 28 | 45.7957 | 24.7233 | roșu | DN1 | 254 + 598 |
| 29 | 45.7837 | 24.63955 | galben | DN1 | 261 + 329 |
| 30 | 45.75717 | 24.48684 | roșu | DN1 | 274 + 458 |
| 31 | 45.71873 | 24.3284 | galben | DN1 | 288 + 499 |
| 32 | 45.70526 | 24.29106 | roșu | DN1 | 292 + 049 |
| 33 | 45.78863 | 24.05068 | roșu | DN1 | 317 + 648 |
| 34 | 46.76957 | 23.3401 | galben | DN1 | 497 + 698 |
| 35 | 46.87098 | 22.98257 | galben | DN1 | 530 + 398 |

| Nr. crt. | Latitudine | Longitudine | Tip sector | Indicativ drum | Poz. km. aprox. |
|---|---|---|---|---|---|
| 36 | 46.88237 | 22.90833 | roșu | DN1 | 536 + 269 |
| 37 | 46.88675 | 22.89539 | roșu | DN1 | 537 + 679 |
| 38 | 46.94755 | 22.81449 | roșu | DN1 | 548 + 319 |
| 39 | 46.95356 | 22.78413 | galben | DN1 | 551 + 618 |
| 40 | 46.94695 | 22.71591 | galben | DN1 | 558 + 718 |
| 41 | 47.02532 | 22.50701 | galben | DN1 | 581 + 159 |
| 42 | 47.05872 | 22.36156 | roșu | DN1 | 593 + 558 |
| 43 | 47.07321 | 22.25475 | roșu | DN1 | 602 + 049 |
| 44 | 47.06278 | 22.17205 | roșu | DN1 | 609 + 459 |
| 45 | 47.06158 | 22.14851 | roșu | DN1 | 611 + 259 |
| 46 | 47.05446 | 22.07937 | roșu | DN1 | 616 + 608 |
| 47 | 44.67141 | 25.89296 | roșu | DN1A | 33 + 140 |
| 48 | 44.69978 | 25.89475 | roșu | DN1A | 36 + 250 |
| 49 | 44.8557 | 25.92314 | galben | DN1A | 55 + 810 |
| 50 | 44.9505 | 26.09436 | galben | DN1A | 80 + 619 |
| 51 | 44.95432 | 26.0796 | galben | DN1A | 81 + 897 |
| 52 | 45.12112 | 26.03408 | galben | DN1A | 104 + 670 |
| 53 | 45.13725 | 26.03074 | galben | DN1A | 106 + 640 |
| 54 | 45.24818 | 26.02375 | roșu | DN1A | 119 + 569 |
| 55 | 45.518485 | 25.843943 | galben | DN1A | 167 + 659 |
| 56 | 44.96287 | 26.14539 | galben | DN1B | 18 + 408 |
| 57 | 44.95704 | 26.19028 | roșu | DN1B | 22 + 119 |
| 58 | 44.95479 | 26.23327 | galben | DN1B | 25 + 530 |
| 59 | 45.02027 | 26.4875 | galben | DN1B | 47 + 039 |
| 60 | 45.05367 | 26.56912 | galben | DN1B | 54 + 708 |
| 61 | 45.11857 | 26.74165 | galben | DN1B | 70 + 099 |
| 62 | 46.83353 | 23.7461 | galben | DN1C | 17 + 450 |
| 63 | 46.86786 | 23.76672 | roșu | DN1C | 21 + 589 |
| 64 | 46.91779 | 23.78062 | roșu | DN1C | 27 + 549 |
| 65 | 47.00532 | 23.84157 | roșu | DN1C | 38 + 808 |
| 66 | 47.05511 | 23.91985 | galben | DN1C | 48 + 179 |
| 67 | 47.16698 | 23.87251 | galben | DN1C | 63 + 010 |
| 68 | 47.71277 | 23.36014 | galben | DN1C | 169 + 768 |
| 69 | 47.74407 | 23.29906 | galben | DN1C | 175 + 678 |
| 70 | 44.94324 | 26.24568 | galben | DN1D | 1 + 829 |
| 71 | 44.92696 | 26.27045 | galben | DN1D | 4 + 569 |
| 72 | 44.83461 | 26.39808 | galben | DN1D | 19 + 240 |
| 73 | 44.81446 | 26.41917 | galben | DN1D | 22 + 299 |
| 74 | 44.736663 | 26.577266 | galben | DN1D | 37 + 758 |
| 75 | 45.63262 | 25.56193 | roșu | DN1E | 5 + 448 |
| 76 | 45.61686 | 25.54645 | roșu | DN1E | 9 + 369 |
| 77 | 46.79904 | 23.50617 | roșu | DN1F | 8 + 897 |

| Nr. crt. | Latitudine | Longitudine | Tip sector | Indicativ drum | Poz. km. aprox. |
|---|---|---|---|---|---|
| 78 | 46.86949 | 23.41357 | galben | DN1F | 23 + 059 |
| 79 | 46.91775 | 23.42322 | roșu | DN1F | 29 + 129 |
| 80 | 47.64986 | 22.50508 | galben | DN1F | 163 + 928 |
| 81 | 47.22618 | 22.965 | galben | DN1H | 66 + 888 |
| 82 | 47.22888 | 23.00083 | galben | DN1H | 71 + 359 |
| 83 | 45.21933 | 26.7185 | roșu | DN10 | 8 + 807 |
| 84 | 45.27365 | 26.67758 | roșu | DN10 | 15 + 999 |
| 85 | 45.2269 | 26.44443 | roșu | DN10 | 38 + 876 |
| 86 | 45.23908 | 26.38183 | roșu | DN10 | 44 + 190 |
| 87 | 45.28278 | 26.35447 | galben | DN10 | 50 + 118 |
| 88 | 45.439 | 26.30703 | galben | DN10 | 70 + 681 |
| 89 | 45.62761 | 26.11612 | galben | DN10 | 104 + 137 |
| 90 | 45.67766 | 25.96838 | galben | DN10 | 121 + 018 |
| 91 | 45.69194 | 25.67551 | galben | DN11 | 6 + 928 |
| 92 | 45.72765 | 25.73335 | roșu | DN11 | 12 + 938 |
| 93 | 45.73829 | 25.75059 | galben | DN11 | 14 + 729 |
| 94 | 45.74874 | 25.76764 | galben | DN11 | 16 + 489 |
| 95 | 45.96248 | 26.05919 | galben | DN11 | 50 + 669 |
| 96 | 46.04492 | 26.32746 | roșu | DN11 | 75 + 838 |
| 97 | 46.16959 | 26.47538 | galben | DN11 | 100 + 639 |
| 98 | 46.20931 | 26.54505 | roșu | DN11 | 108 + 219 |
| 99 | 46.2866 | 26.75403 | rosu | DN11 | 133 + 340 |
| 100 | 46.30375 | 26.75275 | roșu | DN11 | 135 + 250 |
| 101 | 46.3429 | 26.73593 | galben | DN11 | 140 + 090 |
| 102 | 46.35352 | 26.74095 | galben | DN11 | 141 + 309 |
| 103 | 46.49596 | 26.79599 | roșu | DN11 | 160 + 788 |
| 104 | 46.21743 | 27.46963 | galben | DN11A | 77 + 522 |
| 105 | 46.08366 | 26.00114 | roșu | DN11C | 15 + 559 |
| 106 | 46.01181 | 25.83824 | galben | DN12 | 28 + 270 |
| 107 | 46.19051 | 25.89966 | galben | DN12 | 50 + 979 |
| 108 | 46.4773 | 25.74951 | roșu | DN12 | 91 + 529 |
| 109 | 46.55102 | 25.96982 | roșu | DN12A | 32 + 180 |
| 110 | 46.31263 | 26.55042 | roșu | DN12A | 95 + 709 |
| 111 | 46.26266 | 26.73407 | roșu | DN12A | 112 + 907 |
| 112 | 46.77839 | 25.72581 | galben | DN12C | 17 + 299 |
| 113 | 46.82875 | 25.87822 | galben | DN12C | 36 + 449 |
| 114 | 46.85422 | 25.9351 | roșu | DN12C | 42 + 299 |
| 115 | 46.88663 | 26.00527 | roșu | DN12C | 49 + 339 |
| 116 | 46.03676 | 25.20408 | galben | DN13 | 64 + 657 |
| 117 | 46.08995 | 25.11891 | roșu | DN13 | 74 + 789 |
| 118 | 46.23751 | 24.86135 | roșu | DN13 | 109 + 415 |
| 119 | 46.36055 | 24.71961 | roșu | DN13 | 139 + 411 |

| Nr. crt. | Latitudine | Longitudine | Tip sector | Indicativ drum | Poz. km. aprox. |
|---|---|---|---|---|---|
| 120 | 46.38041 | 24.72909 | galben | DN13 | 141 + 822 |
| 121 | 46.49001 | 24.63074 | roșu | DN13 | 158 + 435 |
| 122 | 46.42027 | 25.23627 | roșu | DN13A | 61 + 599 |
| 123 | 46.5295 | 25.14329 | roșu | DN13A | 45 + 668 |
| 124 | 46.33039 | 25.27482 | roșu | DN13A | 75 + 849 |
| 125 | 46.35713 | 25.4586 | galben | DN13A | 95 + 858 |
| 126 | 46.36552 | 25.70417 | roșu | DN13A | 121 + 169 |
| 127 | 45.85579 | 25.74006 | roșu | DN13E | 21 + 089 |
| 128 | 45.89347 | 24.16426 | roșu | DN14 | 12 + 910 |
| 129 | 46.12719 | 24.29576 | roșu | DN14 | 48 + 458 |
| 130 | 46.17329 | 24.42844 | galben | DN14 | 60 + 927 |
| 131 | 46.20228 | 24.49958 | roșu | DN14 | 67 + 508 |
| 132 | 46.22622 | 24.74467 | galben | DN14 | 87 + 209 |
| 133 | 46.28281 | 24.30069 | galben | DN14A | 18 + 460 |
| 134 | 46.34048 | 24.27105 | galben | DN14A | 27 + 729 |
| 135 | 46.468181 | 24.050072 | galben | DN15 | 27 + 339 |
| 136 | 46.60233 | 24.6378 | galben | DN15 | 84 + 289 |
| 137 | 46.61767 | 24.63959 | roșu | DN15 | 86 + 289 |
| 138 | 46.74684 | 24.71259 | galben | DN15 | 102 + 690 |
| 139 | 46.8356 | 24.74405 | galben | DN15 | 114 + 170 |
| 140 | 46.97567 | 25.59988 | roșu | DN15 | 204 + 269 |
| 141 | 46.9838 | 25.60797 | roșu | DN15 | 205 + 419 |
| 142 | 46.98187 | 25.81978 | galben | DN15 | 225 + 519 |
| 143 | 46.97375 | 25.72078 | roșu | DN15 | 216 + 708 |
| 144 | 47.22602 | 26.17583 | galben | DN15B | 29 + 189 |
| 145 | 47.14087 | 26.31788 | galben | DN15C | 34 + 928 |
| 146 | 47.24045 | 26.37107 | roșu | DN15C | 48 + 489 |
| 147 | 47.33803 | 26.34859 | galben | DN15C | 60 + 409 |
| 148 | 46.9433 | 26.42467 | galben | DN15D | 3 + 448 |
| 149 | 47.1749 | 26.24899 | galben | DN15F | 6 + 000 |
| 150 | 46.81167 | 23.8182 | roșu | DN16 | 5 + 728 |
| 151 | 47.18404 | 24.20516 | galben | DN17 | 27 + 798 |
| 152 | 47.10727 | 24.34982 | galben | DN17 | 44 + 748 |
| 153 | 47.06385 | 24.41707 | galben | DN17 | 51 + 908 |
| 154 | 47.07237 | 24.42335 | galben | DN17 | 53 + 040 |
| 155 | 47.17901 | 24.55395 | roșu | DN17 | 68 + 928 |
| 156 | 47.18189 | 24.56807 | galben | DN17 | 70 + 139 |
| 157 | 47.28465 | 25.04296 | galben | DN17 | 116 + 419 |
| 158 | 47.28924 | 25.07647 | roșu | DN17 | 119 + 179 |
| 159 | 47.3826 | 25.3221 | roșu | DN17 | 150 + 819 |
| 160 | 47.45929 | 25.3326 | roșu | DN17 | 163 + 569 |
| 161 | 47.46445 | 25.36 | roșu | DN17 | 168 + 507 |

| Nr. crt. | Latitudine | Longitudine | Tip sector | Indicativ drum | Poz. km. aprox. |
|---|---|---|---|---|---|
| 162 | 47.53588 | 25.5179 | roșu | DN17 | 184 + 388 |
| 163 | 47.51963 | 25.63439 | roșu | DN17 | 194 + 369 |
| 164 | 47.54563 | 25.77508 | galben | DN17 | 210 + 578 |
| 165 | 47.56157 | 25.95409 | galben | DN17 | 226 + 579 |
| 166 | 47.57276 | 25.97535 | roșu | DN17 | 228 + 897 |
| 167 | 47.57883 | 25.99297 | roșu | DN17 | 230 + 408 |
| 168 | 47.64806 | 26.19056 | roșu | DN17 | 249 + 129 |
| 169 | 47.17482 | 25.7928 | roșu | DN17B | 67 + 600 |
| 170 | 47.27167 | 24.42543 | galben | DN17C | 18 + 548 |
| 171 | 47.19945 | 24.20198 | roșu | DN17D | 5 + 424 |
| 172 | 47.27578 | 24.30973 | roșu | DN17D | 18 + 317 |
| 173 | 47.28904 | 24.32657 | roșu | DN17D | 20 + 393 |
| 174 | 47.27973 | 24.53277 | roșu | DN17D | 38 + 860 |
| 175 | 47.44015 | 24.86333 | galben | DN17D | 75 + 260 |
| 176 | 47.88602 | 23.93085 | galben | DN18 | 58 + 411 |
| 177 | 47.83031 | 24.21375 | galben | DN18 | 100 + 084 |
| 178 | 47.20177 | 23.85495 | galben | DN18B | 79 + 750 |
| 179 | 47.31614 | 22.03998 | galben | DN19 | 34 + 073 |
| 180 | 47.54642 | 22.22553 | galben | DN19 | 72 + 304 |
| 181 | 47.92953 | 23.49103 | galben | DN19 | 188 + 813 |
| 182 | 47.24418 | 22.20016 | roșu | DN19E | 24 + 719 |
| 183 | 47.7804 | 23.08181 | galben | DN19F | 14 + 169 |
| 184 | 44.52239 | 26.26468 | roșu | DN2 | 17 + 249 |
| 185 | 44.59663 | 26.40892 | roșu | DN2 | 34 + 159 |
| 186 | 45.06035 | 26.76852 | roșu | DN2 | 97 + 110 |
| 187 | 45.09928 | 26.77682 | roșu | DN2 | 101 + 560 |
| 188 | 45.13532 | 26.7622 | galben | DN2 | 105 + 628 |
| 189 | 45.22075 | 26.86228 | galben | DN2 | 121 + 159 |
| 190 | 45.33753 | 26.97645 | galben | DN2 | 137 + 359 |
| 191 | 45.44978 | 27.0575 | roșu | DN2 | 152 + 300 |
| 192 | 45.573 | 27.10315 | galben | DN2 | 167 + 279 |
| 193 | 45.62287 | 27.12136 | galben | DN2 | 173 + 329 |
| 194 | 45.65651 | 27.16042 | galben | DN2 | 178 + 179 |
| 195 | 45.71556 | 27.19842 | galben | DN2 | 185 + 992 |
| 196 | 45.82015 | 27.2111 | galben | DN2 | 197 + 800 |
| 197 | 45.91692 | 27.20931 | galben | DN2 | 208 + 560 |
| 198 | 45.9596 | 27.2042 | galben | DN2 | 213 + 390 |
| 199 | 46.24285 | 27.08505 | galben | DN2 | 247 + 549 |
| 200 | 46.35892 | 26.99068 | roșu | DN2 | 262 + 420 |
| 201 | 46.38744 | 26.95412 | roșu | DN2 | 266 + 729 |
| 202 | 46.43734 | 26.92187 | roșu | DN2 | 272 + 769 |
| 203 | 47.25635 | 26.5502 | roșu | DN2 | 379 + 708 |

| Nr. crt. | Latitudine | Longitudine | Tip sector | Indicativ drum | Poz. km. aprox. |
|---|---|---|---|---|---|
| 204 | 47.41991 | 26.30838 | galben | DN2 | 406 + 289 |
| 205 | 47.97241 | 26.06724 | roșu | DN2 | 480 + 439 |
| 206 | 44.6274 | 26.98435 | roșu | DN2A | 31 + 688 |
| 207 | 44.5772 | 27.40702 | galben | DN2A | 68 + 089 |
| 208 | 44.63857 | 27.62358 | roșu | DN2A | 87 + 059 |
| 209 | 44.39557 | 28.35498 | galben | DN2A | 174 + 099 |
| 210 | 44.31901 | 28.50796 | galben | DN2A | 189 + 899 |
| 211 | 44.27226 | 28.55781 | galben | DN2A | 196 + 465 |
| 212 | 45.16325 | 27.73325 | galben | DN2B | 84 + 867 |
| 213 | 45.22483 | 27.90456 | roșu | DN2B | 100 + 569 |
| 214 | 45.23227 | 27.91684 | galben | DN2B | 101 + 838 |
| 215 | 44.6321 | 27.30102 | galben | DN2C | 72 + 250 |
| 216 | 45.75218 | 27.13341 | roșu | DN2D | 8 + 099 |
| 217 | 45.91209 | 26.94719 | roșu | DN2D | 32 + 069 |
| 218 | 47.5063 | 26.04768 | roșu | DN2E | 21 + 558 |
| 219 | 46.68965 | 27.19957 | roșu | DN2F | 29 + 781 |
| 220 | 46.64366 | 27.50499 | galben | DN2F | 62 + 451 |
| 221 | 46.53306 | 26.61718 | galben | DN2G | 35 + 568 |
| 222 | 47.91206 | 25.62928 | galben | DN2H | 38 + 222 |
| 223 | 45.17827 | 27.8829 | galben | DN21 | 8 + 509 |
| 224 | 45.09493 | 27.81528 | galben | DN21 | 19 + 160 |
| 225 | 44.53597 | 27.38795 | galben | DN21 | 93 + 300 |
| 226 | 44.47915 | 27.38551 | roșu | DN21 | 99 + 640 |
| 227 | 44.3325 | 27.36013 | galben | DN21 | 116 + 130 |
| 228 | 44.3119 | 27.3565 | galben | DN21 | 118 + 410 |
| 229 | 44.30082 | 27.35462 | galben | DN21 | 119 + 660 |
| 230 | 45.1707 | 28.73954 | galben | DN22 | 170 + 628 |
| 231 | 45.14831 | 28.78525 | galben | DN22 | 179 + 929 |
| 232 | 45.05547 | 28.73701 | roșu | DN22 | 192 + 460 |
| 233 | 44.48995 | 28.56769 | roșu | DN22 | 261 + 320 |
| 234 | 44.30347 | 28.55225 | roșu | DN22 | 283 + 659 |
| 235 | 45.05944 | 28.62789 | galben | DN22A | 10 + 997 |
| 236 | 44.2679 | 28.18236 | galben | DN22C | 17 + 149 |
| 237 | 44.25319 | 28.32315 | galben | DN22C | 30 + 169 |
| 238 | 45.22415 | 28.17297 | roșu | DN22D | 4 + 259 |
| 239 | 45.67884 | 27.2187 | roșu | DN23 | 2 + 289 |
| 240 | 45.62308 | 27.40295 | galben | DN23 | 18 + 598 |
| 241 | 45.84333 | 27.24637 | roșu | DN24 | 2 + 787 |
| 242 | 46.30444 | 27.73803 | galben | DN24 | 79 + 619 |
| 243 | 46.62172 | 27.75712 | galben | DN24 | 118 + 959 |
| 244 | 47.21522 | 27.55016 | galben | DN24 | 203 + 519 |
| 245 | 46.5896 | 27.88453 | galben | DN24B | 10 + 445 |

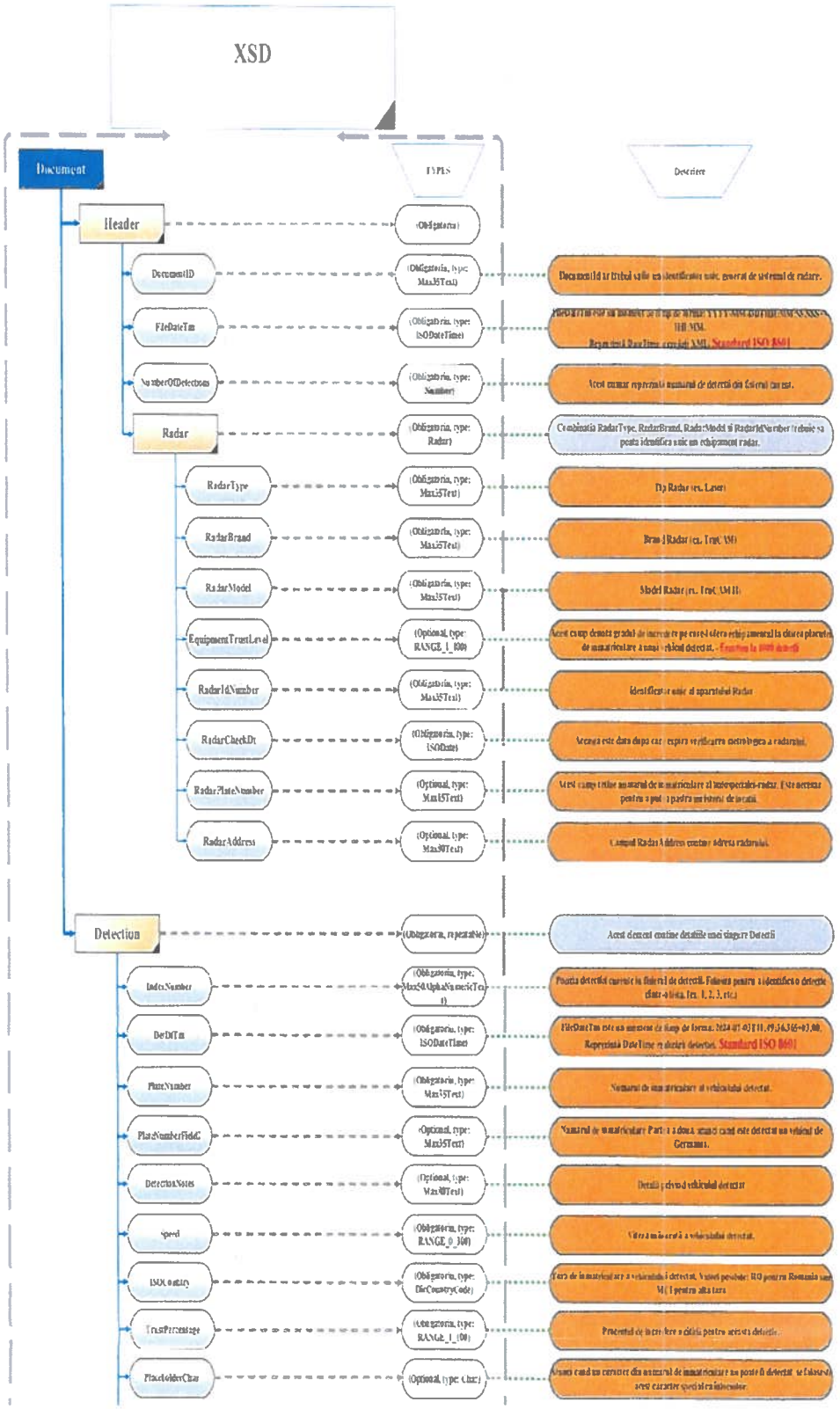
| Nr. crt. | Latitudine | Longitudine | Tip sector | Indicativ drum | Poz. km. aprox. |
|---|---|---|---|---|---|
| 246 | 46.77421 | 28.13573 | roșu | DN24B | 45+530 |
| 247 | 47.44532 | 27.48987 | galben | DN24C | 24 + 959 |
| 248 | 46.15674 | 27.66329 | galben | DN24D | 6 + 387 |
| 249 | 45.80828 | 27.87904 | roșu | DN24D | 51 + 407 |
| 250 | 45.69382 | 27.50942 | roșu | DN25 | 18 + 649 |
| 251 | 45.59597 | 28.04381 | galben | DN26 | 17 + 769 |
| 252 | 47.19522 | 26.99591 | galben | DN28 | 24 + 757 |
| 253 | 47.2188 | 27.31128 | galben | DN28 | 50 + 837 |
| 254 | 47.13345 | 27.68726 | galben | DN28 | 82 + 309 |
| 255 | 47.12586 | 27.70164 | galben | DN28 | 83 + 799 |
| 256 | 47.10246 | 27.76943 | roșu | DN28 | 90 + 119 |
| 257 | 47.24124 | 26.60729 | galben | DN28A | 36 + 039 |
| 258 | 47.26791 | 26.97801 | galben | DN28B | 7 + 681 |
| 259 | 47.64884 | 26.76708 | roșu | DN28B | 62 + 090 |
| 260 | 47.65093 | 26.3751 | galben | DN29 | 12 + 220 |
| 261 | 48.00084 | 26.43277 | roșu | DN29A | 46 + 011 |
| 262 | 47.77324 | 27.07211 | roșu | DN29D | 37 + 590 |
| 263 | 44.46603 | 26.35665 | galben | DN3 | 21 + 189 |
| 264 | 44.50845 | 26.7171 | roșu | DN3 | 51 + 947 |
| 265 | 44.38727 | 26.90967 | galben | DN3 | 74 + 389 |
| 266 | 44.07956 | 27.66634 | roșu | DN3 | 166 + 849 |
| 267 | 44.07077 | 28.2324 | roșu | DN3 | 224 + 149 |
| 268 | 44.16596 | 28.46372 | galben | DN3 | 246 + 996 |
| 269 | 44.20771 | 27.4301 | roșu | DN3B | 11 + 927 |
| 270 | 44.41545 | 27.85417 | galben | DN3B | 59 + 687 |
| 271 | 43.92583 | 28.35414 | galben | DN38 | 29 + 709 |
| 272 | 44.04302 | 28.64487 | galben | DN39 | 16 + 120 |
| 273 | 44.02257 | 28.64478 | galben | DN39 | 18 + 409 |
| 274 | 44.13073 | 28.61418 | galben | DN39E | 0 + 319 |
| 275 | 44.31329 | 26.06426 | galben | DN5 | 14 + 080 |
| 276 | 44.32644 | 26.25905 | galben | DN4 | 18 + 469 |
| 277 | 44.1601 | 25.99868 | galben | DN5 | 32 + 570 |
| 278 | 44.06469 | 25.9806 | roșu | DN5 | 43 + 470 |
| 279 | 43.9463 | 25.35249 | galben | DN51 | 3 + 310 |
| 280 | 43.70027 | 25.33581 | roșu | DN51A | 4 + 770 |
| 281 | 43.96557 | 25.28578 | galben | DN52 | 2 + 898 |
| 282 | 44.10218 | 24.35526 | roșu | DN54 | 1 + 420 |
| 283 | 44.09332 | 24.36232 | roșu | DN54 | 2 + 569 |
| 284 | 44.01416 | 24.41246 | galben | DN54 | 12 + 320 |
| 285 | 43.85022 | 24.45805 | galben | DN54 | 30 + 880 |
| 286 | 43.74338 | 24.77805 | roșu | DN54 | 63 + 857 |
| 287 | 43.74473 | 24.8017 | galben | DN54 | 65 + 897 |

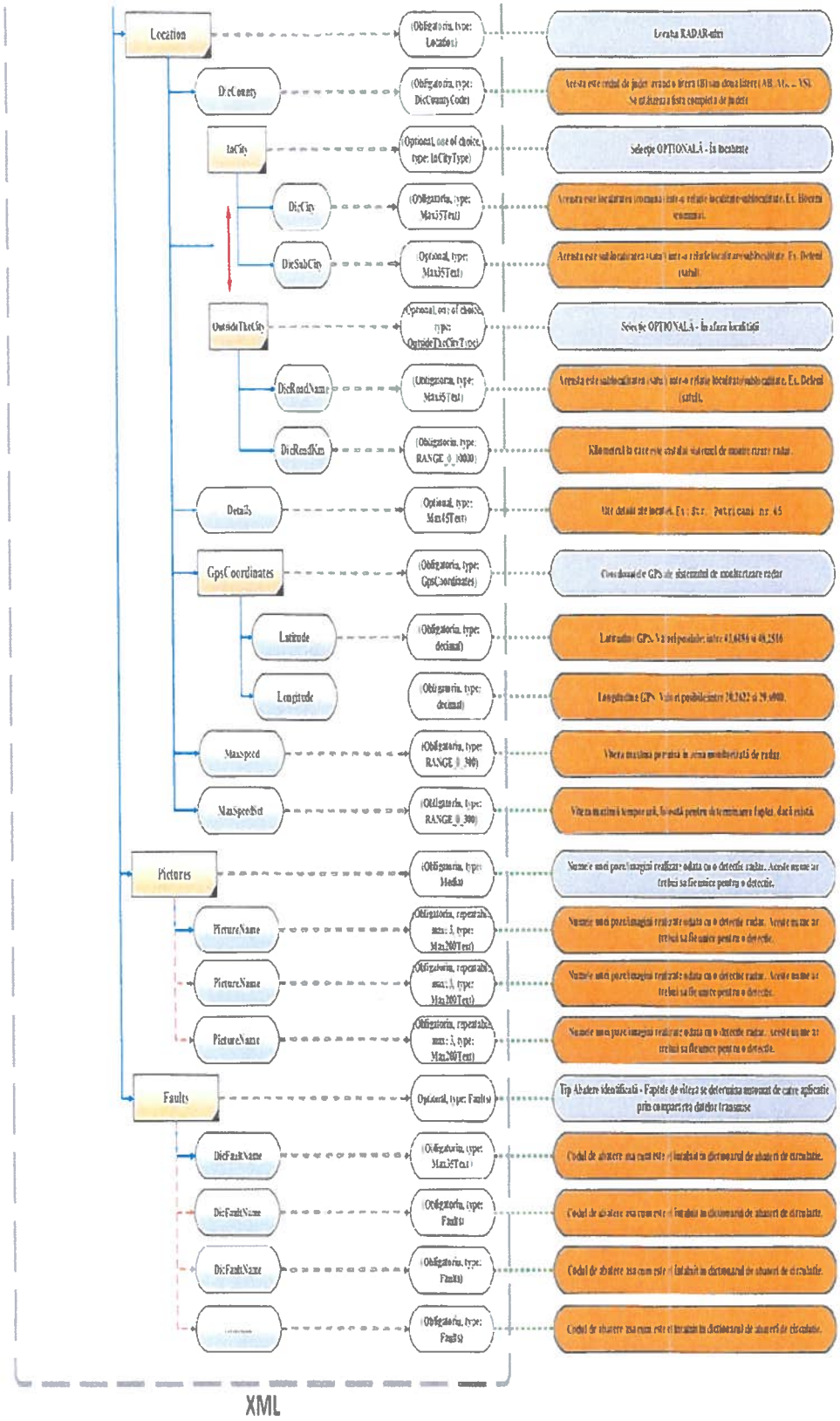
| Nr. crt. | Latitudine | Longitudine | Tip sector | Indicativ drum | Poz. km. aprox. |
|---|---|---|---|---|---|
| 288 | 43.79664 | 24.11117 | galben | DN54A | 31 + 698 |
| 289 | 44.27061 | 23.82089 | galben | DN55 | 6 + 149 |
| 290 | 44.00314 | 22.99178 | roșu | DN56 | 79 + 279 |
| 291 | 44.48703 | 22.776 | galben | DN56A | 62 + 758 |
| 292 | 44.72298 | 22.36626 | roșu | DN57 | 5 + 489 |
| 293 | 44.68828 | 22.36325 | roșu | DN57 | 10 + 359 |
| 294 | 44.97416 | 21.59401 | roșu | DN57 | 142 + 739 |
| 295 | 45.05059 | 21.74297 | galben | DN57B | 5 + 711 |
| 296 | 45.3472 | 21.8351 | roșu | DN58B | 5 + 838 |
| 297 | 45.35526 | 21.82791 | roșu | DN58B | 7 + 149 |
| 298 | 45.36378 | 21.81708 | roșu | DN58B | 8 + 918 |
| 299 | 45.76128 | 21.12372 | galben | DN59A | 8 + 478 |
| 300 | 45.50624 | 20.88025 | galben | DN59B | 37 + 179 |
| 301 | 44.25793 | 25.83559 | roșu | DN6 | 32 + 069 |
| 302 | 44.18288 | 25.76572 | roșu | DN6 | 42 + 639 |
| 303 | 44.1253 | 25.68252 | roșu | DN6 | 53 + 149 |
| 304 | 44.07903 | 25.5572 | roșu | DN6 | 65 + 419 |
| 305 | 44.04654 | 25.49076 | roșu | DN6 | 72 + 019 |
| 306 | 44.03058 | 25.45802 | roșu | DN6 | 75 + 149 |
| 307 | 43.99115 | 25.37092 | galben | DN6 | 83 + 289 |
| 308 | 44.06502 | 25.03748 | galben | DN6 | 114 + 389 |
| 309 | 44.11668 | 24.25664 | roșu | DN6 | 181 + 847 |
| 310 | 44.27742 | 23.87189 | galben | DN6 | 219 + 699 |
| 311 | 44.39386 | 23.71956 | galben | DN6 | 238 + 440 |
| 312 | 44.50606 | 23.59136 | roșu | DN6 | 255 + 089 |
| 313 | 44.51986 | 23.56922 | roșu | DN6 | 257 + 479 |
| 314 | 44.60877 | 22.88404 | galben | DN6 | 316 + 678 |
| 315 | 44.61532 | 22.85994 | galben | DN6 | 318 + 828 |
| 316 | 44.61213 | 22.83365 | galben | DN6 | 320 + 947 |
| 317 | 44.60871 | 22.72609 | roșu | DN6 | 330 + 947 |
| 318 | 44.73497 | 22.41499 | galben | DN6 | 364 + 090 |
| 319 | 44.78235 | 22.39414 | roșu | DN6 | 371 + 360 |
| 320 | 45.19443 | 22.30951 | roșu | DN6 | 426 + 129 |
| 321 | 45.48944 | 22.16465 | galben | DN6 | 464 + 220 |
| 322 | 45.72086 | 21.89682 | galben | DN6 | 500 + 577 |
| 323 | 45.86101 | 20.99306 | galben | DN6 | 580 + 209 |
| 324 | 45.89674 | 20.94552 | galben | DN6 | 585 + 908 |
| 325 | 44.69308 | 25.31241 | galben | DN61 | 75 + 290 |
| 326 | 44.1376 | 24.35331 | roșu | DN64 | 2 + 860 |
| 327 | 44.21549 | 24.34963 | roșu | DN64 | 11 + 820 |
| 328 | 44.80927 | 24.2458 | roșu | DN64 | 80 + 780 |
| 329 | 44.92654 | 24.23462 | galben | DN64 | 94 + 050 |

| Nr. crt. | Latitudine | Longitudine | Tip sector | Indicativ drum | Poz. km. aprox. |
|---|---|---|---|---|---|
| 330 | 44.52566 | 24.52003 | roșu | DN65 | 67 + 778 |
| 331 | 44.56839 | 24.59439 | roșu | DN65 | 75 + 957 |
| 332 | 44.58889 | 24.60558 | roșu | DN65 | 78 + 720 |
| 333 | 44.72007 | 24.7948 | roșu | DN65 | 101 + 530 |
| 334 | 44.7549 | 24.82855 | galben | DN65 | 106 + 389 |
| 335 | 44.76874 | 24.83987 | roșu | DN65 | 108 + 679 |
| 336 | 44.81891 | 24.88706 | galben | DN65B | 1 + 169 |
| 337 | 43.83378 | 25.14722 | galben | DN65E | 34 + 579 |
| 338 | 44.28808 | 23.90672 | galben | DN65F_VOS | 3 + 230 |
| 339 | 44.58176 | 23.49354 | galben | DN66 | 2 + 740 |
| 340 | 45.01334 | 23.26513 | galben | DN66 | 71 + 060 |
| 341 | 45.20914 | 23.3751 | roșu | DN66 | 97 + 629 |
| 342 | 45.23632 | 23.38942 | galben | DN66 | 101 + 849 |
| 343 | 45.44502 | 23.26186 | galben | DN66 | 143 + 758 |
| 344 | 45.52286 | 23.0542 | galben | DN66 | 165 + 329 |
| 345 | 45.37537 | 23.30664 | galben | DN66A | 5 + 000 |
| 346 | 44.6895 | 22.69794 | roșu | DN67 | 7 + 600 |
| 347 | 44.91765 | 22.99915 | roșu | DN67 | 57 + 089 |
| 348 | 44.99448 | 23.13857 | galben | DN67 | 71 + 378 |
| 349 | 44.99752 | 23.15723 | roșu | DN67 | 72 + 907 |
| 350 | 45.00592 | 23.17848 | roșu | DN67 | 74 + 818 |
| 351 | 45.01707 | 23.20649 | galben | DN67 | 77 + 329 |
| 352 | 45.03389 | 23.40383 | roșu | DN67 | 94 + 059 |
| 353 | 45.02861 | 23.42642 | roșu | DN67 | 95 + 917 |
| 354 | 45.13865 | 23.73908 | galben | DN67 | 126 + 728 |
| 355 | 45.12498 | 23.91933 | galben | DN67 | 144 + 628 |
| 356 | 45.12652 | 23.94685 | roșu | DN67 | 146 + 837 |
| 357 | 45.12992 | 24.04028 | galben | DN67 | 156 + 489 |
| 358 | 45.05084 | 24.27834 | galben | DN67 | 186 + 059 |
| 359 | 45.07568 | 24.34187 | galben | DN67 | 191 + 947 |
| 360 | 44.66149 | 24.2797 | galben | DN67B | 117 + 380 |
| 361 | 44.79961 | 24.7337 | galben | DN67B | 173 + 991 |
| 362 | 45.05463 | 23.217 | galben | DN67D | 3 + 646 |
| 363 | 45.08157 | 23.17657 | roșu | DN67D | 8 + 434 |
| 364 | 45.08681 | 23.0914 | roșu | DN67D | 15 + 454 |
| 365 | 45.85053 | 22.32263 | roșu | DN68A | 45 + 369 |
| 366 | 45.86592 | 22.34645 | galben | DN68A | 48 + 529 |
| 367 | 44.59251 | 25.77315 | roșu | DN7 | 32 + 518 |
| 368 | 44.88662 | 24.77941 | galben | DN7 | 122 + 817 |
| 369 | 45.0141 | 24.57007 | roșu | DN7 | 147 + 997 |
| 370 | 45.09871 | 24.38228 | roșu | DN7 | 173 + 110 |
| 371 | 45.11998 | 24.38242 | roșu | DN7 | 175 + 549 |

| Nr. crt. | Latitudine | Longitudine | Tip sector | Indicativ drum | Poz. km. aprox. |
|---|---|---|---|---|---|
| 372 | 45.15861 | 24.37185 | galben | DN7 | 181 + 709 |
| 373 | 45.18267 | 24.36529 | galben | DN7 | 184 + 630 |
| 374 | 45.2514 | 24.3364 | roșu | DN7 | 193 + 998 |
| 375 | 45.29295 | 24.29429 | roșu | DN7 | 200 + 139 |
| 376 | 45.29977 | 24.28397 | roșu | DN7 | 201 + 528 |
| 377 | 45.309214 | 24.28486 | roșu | DN7 | 202 + 280 |
| 378 | 45.35525 | 24.27385 | galben | DN7 | 211 + 389 |
| 379 | 45.47313 | 24.29303 | roșu | DN7 | 228 + 539 |
| 380 | 45.55009 | 24.26566 | galben | DN7 | 240 + 099 |
| 381 | 45.61704 | 24.26604 | roșu | DN7 | 248 + 979 |
| 382 | 46.09023 | 21.79648 | galben | DN7 | 501 + 837 |
| 383 | 46.17503 | 21.01616 | galben | DN7 | 571 + 767 |
| 384 | 44.93576 | 25.52025 | galben | DN72 | 38 + 878 |
| 385 | 44.92659 | 25.85703 | roșu | DN72 | 68 + 149 |
| 386 | 45.16042 | 24.99486 | roșu | DN73 | 37 + 333 |
| 387 | 45.58196 | 25.41274 | roșu | DN73A | 24 + 468 |
| 388 | 45.92614 | 22.86891 | galben | DN76 | 2 + 909 |
| 389 | 46.03697 | 22.83516 | galben | DN76 | 17 + 099 |
| 390 | 46.0645 | 22.81652 | roșu | DN76 | 22 + 169 |
| 391 | 46.16513 | 22.75214 | roșu | DN76 | 37 + 059 |
| 392 | 46.18458 | 22.63763 | galben | DN76 | 46 + 797 |
| 393 | 46.26519 | 22.59624 | galben | DN76 | 60 + 738 |
| 394 | 46.64049 | 22.37948 | galben | DN76 | 118 + 979 |
| 395 | 46.99168 | 21.98357 | galben | DN76 | 175 + 889 |
| 396 | 46.35472 | 21.4239 | roșu | DN79 | 21 + 479 |
| 397 | 46.51844 | 21.50964 | roșu | DN79 | 41 + 510 |
| 398 | 46.75012 | 21.59382 | roșu | DN79 | 69 + 799 |
| 399 | 46.86122 | 21.72608 | galben | DN79 | 86 + 939 |
| 400 | 45.44872 | 22.22183 | roșu | VO_CARANSEBES | 456 + 759 |

## ANEXA 3 - Formatul semnalărilor și al datelor de monitorizare a traficului




Location
(Obligatoriu, type: Location)
Locatia RADAR-ului
DicCounty
(Obligatoriu, type: DicCountyCode)
Acesta este codul de judet avand o litera (B) sau doua litere (AB, AG, ... SV). Se utilizeaza lista completa de judete
IsCity
(Optional, one of choice, type: IsCityType)
Selectie OPTIONALĂ - In localitate
DicCity
(Obligatoriu, type: Max35Text)
Acesta este localitatea (comuna) intre-o relatie localitate-sublocalitate. Ex. Bucuresti sectorul
DicSubCity
(Optional, type: Max35Text)
Acesta este sublocalitatea (sat) intre-o relatie localitate-sublocalitate. Ex. Dobroti (sat)
OutsideTheCity
(Optional, one of choice, type: OutsideTheCityType)
Selectie OPTIONALĂ - In afara localitatii
DicRoadName
(Obligatoriu, type: Max35Text)
Acesta este sublocalitatea (sat) intre-o relatie localitate/sublocalitate. Ex. Dobroti (sat).
DicRoadKm
(Obligatoriu, type: RANGE_0_10000)
Kilometrul la care este amplasat radarul de masurare viteza radar.
Details
(Optional, type: Max45Text)
Alte detalii ale locatiei. Ex: Str. ... Pentru cazul nr. 45
GpsCoordinates
(Obligatoriu, type: GpsCoordinates)
Coordonate GPS ale sistemului de monitorizare radar
Latitude
(Obligatoriu, type: decimal)
Latitudine GPS. Valori posibile intre 43,6436 si 48,2516
Longitude
(Obligatoriu, type: decimal)
Longitudine GPS. Valori posibile intre 20,2432 si 29,6900.
MaxSpeed
(Obligatoriu, type: RANGE_0_300)
Viteza maxima permisa in zona monitorizata de radar.
MaxSpeedSet
(Obligatoriu, type: RANGE_0_300)
Viteza maxima temporara, la nevoie pentru determinarea faptei, daca exista.
Pictures
(Obligatoriu, type: Media)
Numele unei poze/imagini realizate odata cu o detectie radar. Acestea nu ar trebui sa fie unice pentru o detectie.
PictureName
(Obligatoriu, repetabil: max: 3, type: Max200Text)
Numele unei poze/imagini realizate odata cu o detectie radar. Acestea nu ar trebui sa fie unice pentru o detectie.
PictureName
(Obligatoriu, repetabil: max: 3, type: Max200Text)
Numele unei poze/imagini realizate odata cu o detectie radar. Acestea nu ar trebui sa fie unice pentru o detectie.
PictureName
(Obligatoriu, repetabil: max: 3, type: Max200Text)
Numele unei poze/imagini realizate odata cu o detectie radar. Acestea nu ar trebui sa fie unice pentru o detectie.
Faults
Optional, type: Faults)
Tip Abatere identificata - Faptele de viteza se determina automat de catre aplicatie prin compararea datelor transmise
DicFaultName
(Obligatoriu, type: Max35Text)
Codul de abatere asa cum este el inregistrat in dictionarul de abateri de circulatie.
DicFaultName
(Obligatoriu, type: Faults)
Codul de abatere asa cum este el inregistrat in dictionarul de abateri de circulatie.
DicFaultName
(Obligatoriu, type: Faults)
Codul de abatere asa cum este el inregistrat in dictionarul de abateri de circulatie.
(Obligatoriu, type: Faults)
Codul de abatere asa cum este el inregistrat in dictionarul de abateri de circulatie.
XML

**Anexa nr. 4 - DOCUMENTE SUPORT**

## Proces-verbal de recepţie cantitativă nr...../.....

| | |
|---|---|
| *Contract nr.* | |
| *Denumire contract* | |
| *Contractant* | |
| *Dată livrare produs* | |

| *Nr.* | *Denumirea (conform Caiet de Sarcini/Contract)* | *Referinţă (conform Caiet de Sarcini/Contract)* |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. ..... | | |

**Contractant** **Autoritatea Contractantă**

**Dată:**

**Nume:**

**Funcţia:**

**Semnătura:**

**Proces-verbal de recepție calitativă**

**nr...../.....**

1. Context

| | |
|---|---|
| *1.1. Contract nr.* | |
| *1.2. Denumire contract* | |
| *1.3. Contractant* | |

2.Lista produselor

| 2.1. Produs | 2.2 Referință (conform Caiet de Sarcini/Contract) | 2.3. Termenul de livrare |
|---|---|---|
| | | |
| | | |
| | | |

3. Concluzii cu privire la acceptare

| | | | |
|---|---|---|---|
| ☐ | 3.1. Acceptare (fără observatii/rezerve) | | |
| ☐ | 3.2. Acceptare cu observatii minore | | |
| ☐ | 3.3. Acceptare cu rezerve (Contractantul se angajează să corecteze - în timpul convenit - defectele constatate și descrise la punctul 5 din prezentul document). | | |
| ☐ | 3.4. Este aplicabilă perioada de garanție? | Data finalizării: | |
| ☐ | 3.5. Refuzat (Contractantul se angajează să corecteze greșelile constatate și descrise la punctul 5 din prezentul document). Remedierea defectelor trebuie efectuată în conformitate cu cele stabilite în Contract. | | |

4. Semnături

| 4.1. CONTRACTANT | | 4.2. AUTORITATE CONTRACTANTĂ | | | |
|---|---|---|---|---|---|
| Data: | | Data: | | Data: | |
| Nume: | | Nume: | | Nume: | |
| Funcția: | | Funcția: | | Funcția: | |
| Aprobat: | | Aprobat: | | Aprobat: | |
| Acceptare finală *[dacă este cazul]*: | | | | | |
| Data: | | Data: | | Data: | |
| Nume: | | Nume: | | Nume: | |
| Funcția: | | Funcția: | | Funcția: | |
| Aprobat: | | Aprobat: | | Aprobat: | |

5. Observații *[introduceți]*