Nr. 367/IICG-PNRR/13.07.2023

CAIET DE SARCINI

revizuit după Avizul Conform Condiționat nr 9855/27.06.2023

pentru atribuirea contractului de achiziție publică având ca obiect

prestarea de servicii pentru dezvoltarea și implementarea soluției informatice, inclusiv furnizarea de software pentru implementarea „Portalul Digital Unic al României – PDURo”

1. INFORMATII GENERALE

1.1.Informații despre autoritatea contractantă

AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI (ADR)

Sediul principal:	Bd. Libertății nr 14, sector 5, București, România, cod poștal 050706
Sediul secundar:	Str. Italiană nr 22, sector 2, București, România, cod poștal 020976
Cod fiscal:	R042283735
Telefon:	021 3052710
Fax:	021 3032899

Autoritatea pentru Digitalizarea României (ADR), este organizată și funcționează ca structură cu personalitate juridică în cadrul aparatului de lucru al Guvernului și în subordinea Ministerului Cercetării Inovării și Digitalizării având rolul de a realiza și coordona implementarea strategiilor și a politicilor publice în domeniul transformării digitale și societății informaționale. Printre atribuțiile legale pe care ADR le are este și implementarea prevederilor Regulamentului 1724/ 2018 privind înființarea unui portal digital unic (single digital gateway) pentru a oferi acces la informații, la proceduri și la servicii de asistență și de soluționare a problemelor. Aceste prevederi sunt complementare proiectului Punctului de Contact Unic electronic care la rândul său acomodează implementarea mai multor prevederi legislative de la nivel european și național.

1.2.Informații despre contextul achiziției

1.2.1. Denumirea investiției

„Portalul Digital Unic al României – PDURo face parte din investiția 1 „Implementarea infrastructurii de CLOUD GUVERNAMENTAL" din cadrul Componentei 7 TRANSFORMAREA DIGITALĂ aferentă Planul Național de Redresare și Reziliență (PNRR).

Prezentul document utilizează informațiile cuprinse în *Raportul analizei opțiunilor privind arhitectura Cloud-ului Guvernamental*, document elaborat în vederea atingerii milestone-ului 143 din cadrul Componentei 7 Transformarea Digitală vizând:

- ✓ opțiunile strategice și tehnologice și pachetul legislativ și de reglementare pentru stabilirea realizării Cloud-ului Guvernamental;
- ✓ posibilitățile de construcție, livrare, instalare și funcționare a infrastructurilor

civile și tehnologice conform termenelor prevăzute în plan;

- ✓ inventarierea aplicațiilor/serviciilor publice oferite în prezent de autoritățile publice;
- ✓ planul de dezvoltare/migrare în Cloud a aplicațiilor inventariate.

1.2.2. Scopul investiției

În data de 3 noiembrie 2021 Consiliul Uniunii Europene a aprobat Planul Național de Redresare și Reziliență al României (PNRR) conform art. 20 din Regulamentul nr. 241/2021 al Parlamentului European și al Consiliului de instituire a Mecanismului de redresare și reziliență, a Deciziei de punere în aplicare a Consiliului de aprobare a evaluării planului de redresare și reziliență al României (Regulamentul (UE) 2021/241).

În conformitate cu prevederile Regulamentului (UE) 2021/241, ale Deciziei de punere în aplicare a Consiliului de aprobare a evaluării Planului de Redresare și Reziliență al României, ale O.U.G. nr. 155/2020, cu modificările și completările ulterioare, MCID, ADR, SRI și STS realizează Investiția 1 „Implementarea infrastructurii de CLOUD GUVERNAMENTAL" din cadrul Componentei 7 TRANSFORMAREA DIGITALĂ aferentă Planului Național de Redresare și Reziliență (PNRR).

În conformitate cu Anexa la Decizia de punere în aplicare a Consiliului de aprobare a evaluării Planului de Redresare și Reziliență al României, scopul Investiției 1 este de a implementa infrastructura de Cloud Guvernamental, utilizând tehnologii sigure și eficiente din punct de vedere energetic pentru a asigura caracterul sigur, interoperabil și standard al datelor publice.

Implementarea acestei investiții include:

i) amenajarea de Centre de Date Tier IV de la momentul conceperii pentru cele două Centre Principale de Date și Tier III de la momentul conceperii pentru cele două Centre Secundare de Date;

ii) furnizarea unei infrastructuri specifice pentru tehnologia informației și comunicațiilor;

iii) dezvoltarea și extinderea infrastructurii de sprijin (energie electrică, măsuri de securitate fizică);

iv) implementarea unei infrastructuri TIC scalabile și cu disponibilitate ridicată în fiecare centru de date.

Centrele de date vor respecta Codul european de conduită privind eficiența energetică a centrelor de date.

Punerea în aplicare a acestei investiții se bazează pe opțiunile strategice și tehnologice și pachetul legislativ și de reglementare prin care se stabilește realizarea Cloud-ului raport

lunarGuvernamental, posibilitățile de amenajare, livrare, instalare și exploatare a infrastructurilor civile și tehnologice în conformitate cu termenele stabilite în plan, cartografierea aplicațiilor/serviciilor digitale publice oferite în prezent de autoritățile de stat, proiectarea proceselor și a procedurilor puse în aplicare în etapele de producție și/sau de implementare, precum și planul de dezvoltare/migrare la Cloud a aplicațiilor cartografiate.

1.2.3. Locațiile investiției

Locațiile celor 4 Centre de Date sunt municipiul București, localitatea Giroc din jud. Timiș, localitatea Cristian din jud. Brașov, municipiul Sibiu din jud. Sibiu.

- Centrul de Date Principal 1 este de nivel Tier IV.
- Centrul de Date Principal 2 este de nivel Tier IV.
- Centrul de Date Secundar 1 este de nivel Tier III.
- Centrul de Date Secundar 2 este de nivel Tier III.

Referitor la stadiul construcției clădirilor, o clădire este finalizată, iar celelalte trei sunt în curs de execuție, în diferite stadii.

Aceste facilități, aflate în diferite faze de implementare, au fost selectate ca urmare a faptului că au fost special concepute și proiectate pentru a funcționa ca Centre de Date, reducându-se astfel timpul de implementare a proiectelor și asigurând astfel respectarea termenelor impuse de Regulamentul 241/2021, referitor la angajarea cheltuielilor (contractare) și la plata acestora.

1.3.Situația actuală și cerințele funcționale pentru PDURo

În majoritatea statelor membre, precum și la nivelul UE, e-guvernarea reprezintă o prioritate majoră pe ordinea de zi deoarece contribuie la reducerea birocrației, la creșterea eficienței și la economisirea de bani pentru autoritățile publice.

La nivel european au fost stabilite viziunea, obiectivele și căile pentru a asigura o transformare digitală reușită a Europei până în 2030. Acest lucru este esențial și pentru realizarea tranziției către o economie neutră din punct de vedere climatic, circulară și reziliență. Ambiția UE este să fie suverană din punct de vedere digital într-o lume deschisă și interconectată și să aplice politici digitale care să permită cetățenilor și întreprinderilor să beneficieze de un viitor digital sustenabil și mai prosper, care pune oamenii pe primul plan. Pentru aceasta este nevoie, printre altele, de abordarea vulnerabilităților și a dependențelor, precum și de accelerarea investițiilor.

Busola pentru dimensiunea digitală a Europei

Comisia propune o **Busolă pentru dimensiunea digitală** prin care să se transpună ambițiile digitale ale UE pentru 2030 în dispoziții concrete. Acestea se axează pe patru elemente esențiale:

1) **cetățeni cu competențe digitale și profesioniști cu înaltă calificare în domeniul digital**: până în 2030, cel puțin 80% dintre adulți ar trebui să aibă competențe digitale de bază, iar în UE ar trebui să existe 20 de milioane de specialiști angajați în sectorul TIC; de asemenea, mai multe femei ar trebui să ocupe astfel de posturi;

2) **infrastructuri digitale securizate, performante și sustenabile**: până în 2030, toate gospodăriile din UE ar trebui să aibă conectivitate de ordinul gigabiților, iar toate zonele populate ar trebui să fie acoperite de tehnologia 5G; producția de semiconductori de ultimă generație și sustenabili în Europa ar trebui să reprezinte 20% din producția mondială; în UE ar trebui să fie instalate 10.000 de noduri de procesare la periferie (*edge computing*) foarte securizate, neutre din punct de vedere climatic, iar Europa ar trebui să dispună de primul său calculator cuantic;

3) **transformarea digitală a întreprinderilor**: până în 2030, trei din patru companii ar trebui să utilizeze servicii de cloud computing, sisteme de tip big data și inteligență artificială, peste 90% dintre IMM-uri ar trebui să ajungă cel puțin la un nivel de bază de adoptare a tehnologiilor digitale, iar numărul de start-up-uri de tip unicorn din UE ar trebui să se dubleze;

4) **digitalizarea serviciilor publice**: *până în 2030, toate serviciile publice esențiale ar trebui să fie disponibile online, toți cetățenii vor avea acces la dosarele lor medicale electronice, iar 80% dintre cetățeni ar trebui să utilizeze o soluție de identificare electronică.*

Busola stabilește o structură de guvernanță solidă, comună cu statele membre, bazată pe un sistem de monitorizare cu raportare anuală sub forma unor coduri de culoare. Obiectivele vor fi înscrise într-un program strategic care urmează să fie convenit cu Parlamentul European și cu Consiliul.

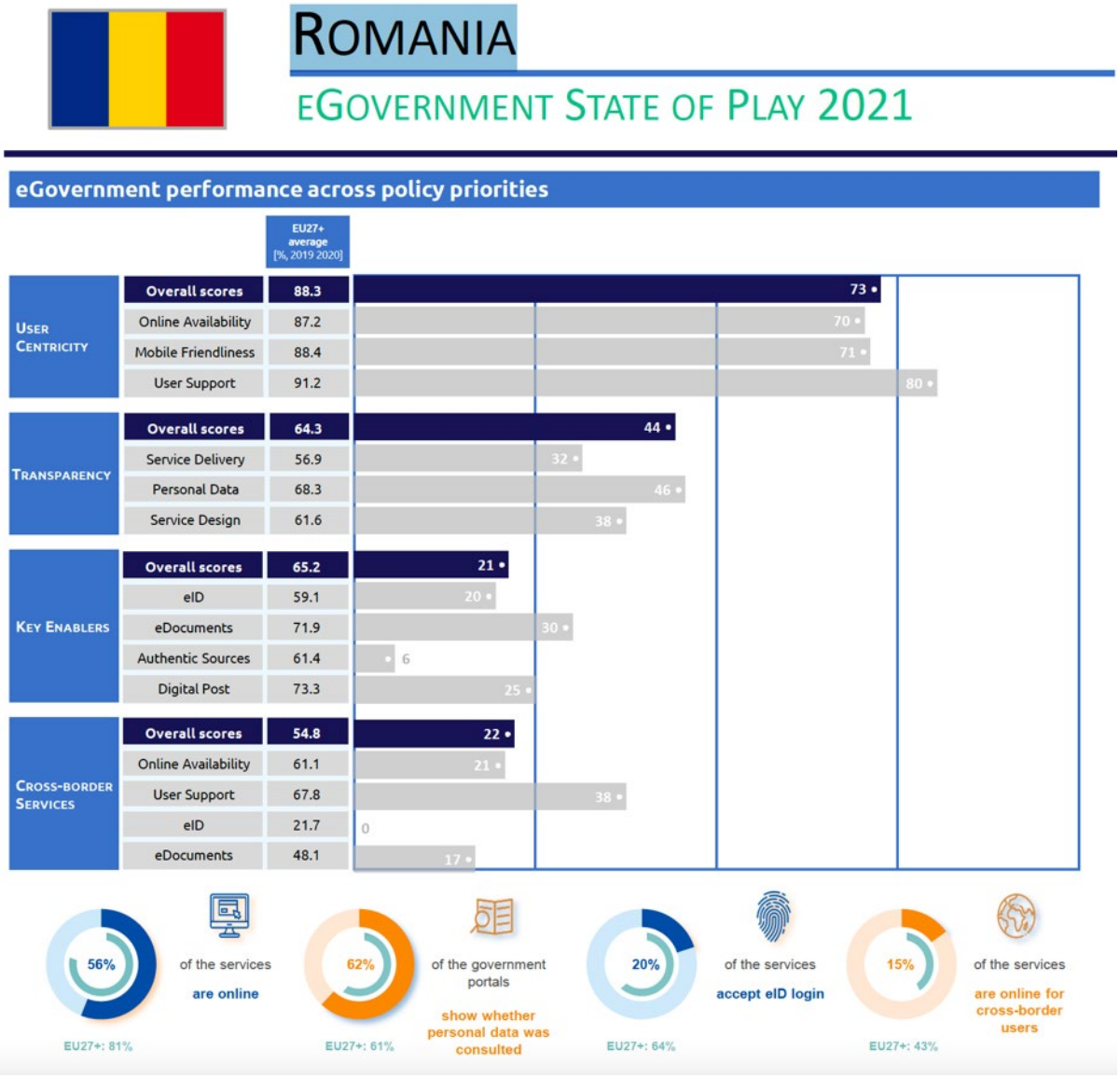
Drepturile și principiile digitale pentru europeni

Drepturile și valorile UE se află în centrul abordării europene a domeniului digital, centrată pe factorul uman, iar aceste drepturi și valori ar trebui să se reflecte pe deplin în spațiul online, la

fel ca în lumea reală. Din acest motiv, Comisia propune dezvoltarea unui **cadru de principii digitale**, cum ar fi accesul la conectivitate de înaltă calitate, la competențe digitale suficiente, la servicii publice, la servicii online echitabile și nediscriminatorii și, în general, asigurarea faptului că drepturile care se aplică offline pot fi exercitate pe deplin și online. Aceste principii ar urma să fie discutate în cadrul unei ample dezbateri la nivelul întregii societăți și ar putea fi consacrate într-o **declarație solemnă, interinstituțională**, formulată de Parlamentul European, Consiliu și Comisie. Aceasta ar urma să se bazeze pe Pilonul european al drepturilor sociale, completându-l. În fine, Comisia propune ca, în cadrul unui sondaj Eurobarometru anual, să se monitorizeze dacă europenii consideră că drepturile lor digitale sunt respectate.

O Europă digitală pe scena mondială

Transformarea digitală dă naștere la **provocări globale**. UE va depune eforturi pentru a-și promova agenda digitală pozitivă și centrată pe factorul uman în cadrul organizațiilor internaționale și prin intermediul unor parteneriate digitale internaționale solide. Combinarea investițiilor interne ale UE cu fondurile semnificative disponibile în cadrul noilor instrumente de cooperare externă va permite UE să colaboreze cu parteneri din întreaga lume în vederea atingerii obiectivelor globale comune. Comisia a propus deja înființarea unui nou Consiliu pentru comerț și tehnologie UE-SUA. Comunicarea de astăzi subliniază importanța investițiilor în îmbunătățirea conectivității cu partenerii externi ai UE, de exemplu prin crearea unui Fond pentru conectivitate digitală.



Dimensiunea cheie Centricitatea utilizatorului indică la ce măsură (informațiile despre) un serviciu este furnizat online, cum este realizata parcurgerea procedurii online și dacă site-urile web publice sunt prietenoase cu dispozitivele mobile.

Disponibilitate online: indică dacă un serviciu este online. Variind din offline (0%), doar informații online (50%), integral online (100%).

Asistență utilizator: indică dacă asistență, ajutor și (interactiv) funcționalitățile de feedback sunt online.

Utilizarea mobilelor: indică dacă site-ul oferă servicii printr-o interfață prietenoasă cu dispozitivele mobile; o interfață care este „adaptata” pe dispozitivul mobil.

Transparența: este o dimensiune cheie care indică în ce măsură guvernele sunt transparente

Transparența prestării serviciilor: indică în ce măsură guvernele sunt transparente în ceea ce privește procesul de livrare a serviciilor publice.

Transparența proiectării serviciilor: indică în ce măsură guvernele sunt transparente în ceea ce privește procesul de proiectarea serviciului public.

Transparență sau Date personale: indică în ce măsură guvernele sunt transparente în ceea ce privește datele personale implicate.

Key Dimension Key Enablers indică măsura în care 4 precondiții tehnice sunt disponibile online. Acestea sunt:

- identificare electronică (eID);
- documente electronice(eDocumente);
- surse autentice și
- poștă digitală.

Poșta digitală se referă la posibilitatea ca guvernele să poată comunica doar electronic cu cetățenii sau antreprenorii prin cutiile poștale personale sau alte soluții digitale de corespondență.

Dimensiunea cheie pentru serviciile transfrontaliere indică în ce măsură cetățenii UE pot utiliza online în serviciile din altă țară.

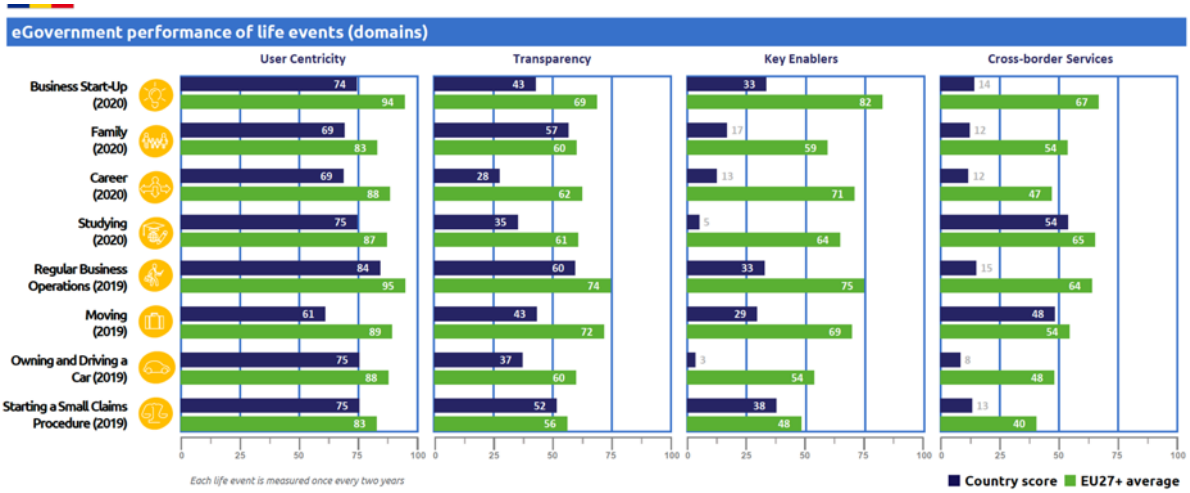
Disponibilitate online: indică dacă un serviciu este online. Variind din offline (0%), doar informații online (50%), integral online (100%).

Asistență utilizator: indică dacă asistența, ajutorul și (interactiv) funcționalitățile de feedback sunt online.

eID: indică dacă un eID național din țara A poate fi utilizat în țara B.

eDocuments: indică dacă eDocumentele pot fi transmise din țara A în țara B.

România conform **eGovernment benchmark 2021** se situează sub media europeană pentru aproape toate serviciile publice electronice**.**



De mulți ani, Benchmark-ul anual de eGovernment al Comisiei Europene a evaluat serviciile publice digitale din diferite țări în funcție de mai mulți indicatori ce se încadrează în 4 teme generale:

- Centrarea pe utilizator – măsura în care serviciile sunt online și accesibile;
- Transparență – deschiderea comunicării despre modul în care sunt furnizate serviciile;
- Factori cheie – tehnologia minima necesara care permite furnizarea de servicii digitale;
- Mobilitatea transfrontalieră – ușurința cu care cetățenii din străinătate pot folosi serviciile.

Dar rezultatele acestei metode de evaluare au părut uneori în contradicție cu propriile experiențe ale utilizatorilor: raportul European Benchmark 2020 a acordat țărilor UE un scor mediu uimitor de mare de 87% pentru utilizarea serviciilor de e-guvernare.
Ultimele evaluări comparative a guvernării electronice au folosit 3 indicatori pentru a evalua centrarea pe utilizator:

- Disponibilitate online – dacă serviciile publice oferite de către administrația publică pentru anumite evenimente de viață ale cetățenilor (cum ar fi începerea unei afaceri și mutarea acasă) sunt online; dacă există doar informații despre serviciul online sau dacă nu există informații online;
- Utilizarea dispozitivelor mobile – dacă site-urile web sunt optimizate pentru utilizarea mobilă;
- Asistență pentru utilizatori – dacă există proceduri de reclamație (inclusiv alte canale decât un site web). Acestea ar putea include forumuri de discuții sau rețele sociale,

mecanisme de feedback, detalii de contact, o demonstrație sau un chat live și secțiunea Întrebări frecvente (FAQs).

Multe dintre aceste măsuri sunt destul de elementare – nu ajung la calitatea experienței reale a unui utilizator. Unele ar putea fi ușor de realizat și de implementat. Spre exemplu, implementarea unei secțiuni de tip "*Întrebări frecvente*" ar conta în favoarea unui serviciu, chiar dacă nu s-a dovedit extrem de util utilizatorului.

Majoritatea măsurilor de remediere se încadrează în 3 domenii:

- Măsuri cantitative – inclusiv timpul necesar pentru a finaliza "*user journey*", durata încărcării paginii și numărul de clicuri (și măsurile privind costul pe tranzacție al rulării serviciului);
- Măsuri de proxy sau de proces – dacă echipele care construiesc servicii digitale au procedurile și resursele potrivite, cum ar fi utilizarea unor metrici pentru a urmări performanța serviciilor, reunirea unei echipe multidisciplinare și utilizarea opiniei utilizatorilor;
- Indicatori pentru User Experience (UX) și User Journey – stabilirea așteptărilor, de exemplu, oferind o idee exactă a duratei unei tranzacții), accesibilitatea (folosirea unui limbaj simplu), ajutor și feedback (mesaje de eroare, dacă reclamațiile au fost rezolvate) și succesul general al serviciului (dacă utilizatorul a obținut rezultatul corect).

Realizarea pașilor necesari pentru implementarea corectă și completă a Regulamentului Single Digital Gateway (Regulamentul 2018/1724 din 2 octombrie 2018) în România este o oportunitate pentru a reduce din decalajul existent faţă de media europeană.

Implementarea Single Digital Gateway (SDG) prin Portalul Digital Unic va ajuta cetățenii și firmele europene să acceseze informații și proceduri administrative online, spre exemplu pentru a solicita finantarea studiilor în învățământul superior, solicitarea recunoașterii academice a unei diplome sau pentru a înmatricula o mașină.

Acest punct unic de intrare european va fi integrat în portalul „Europa ta", disponibil în toate limbile. Acesta va oferi acces și link-uri către site-uri web și pagini web naționale și ale UE, într-un mod ușor de utilizat, pentru a le permite utilizatorilor să-și exercite drepturile și să își respecte obligațiile în cadrul pieței unice.

O transformare digitală a UE: situația actuală și următorii pași

Pentru a sprijini o adevărată piață unică digitală, Comisia Europeană și autoritățile naționale lucrează împreună pentru a-și actualiza informațiile și a-și digitaliza procedurile și serviciile.

Implementate până acum:

- portalul *Your Europe* oferă acum acces la multe mai multe informații practice privind drepturile și procedurile administrative pentru cetățenii și companiile din UE.
- un instrument de căutare a serviciilor de asistență, care îi ajută pe utilizatori să găsească informații privind drepturile, obligațiile și normele care decurg din dreptul Uniunii și dreptul național..
- un instrument de feedback al utilizatorilor pentru a raporta problemele sau obstacolele întâmpinate la utilizarea portalului și a altor resurse online furnizate de administrațiile UE și naționale. Acest lucru ajută la îmbunătățirea calității informațiilor și serviciilor publice.

"*Europa ta*" va trebui să ofere:

- **acces la 21 de proceduri digitalizate, în toate țările UE**: cele mai importante proceduri administrative pentru utilizatorii transfrontalieri vor fi complet disponibile online, cu instrucțiuni clare pentru utilizatori în toate statele membre ale UE;
- **servicii publice digitale fără granițe**: Indiferent de locul în care un cetățean se află în UE, ar trebui să poată accesa procedurile online ale oricărei unități administrative relevante, la fel ca și localnicii;
- **principiul „o singură dată":** utilizatorii trebuie să trimită documente sau date, la nivel transfrontalier (de exemplu, înmatricularea vehiculului) o singură dată; nu trebuie să le depună din nou dacă o altă autoritate din UE le deține deja. Schimbul transfrontalier de informații înseamnă că documentele și datele pot și trebuie să fie partajate între autoritățile din diferite țări ale UE.

DIRECTIVA (UE) 2019/1024 A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 20 iunie 2019 privind datele deschise și reutilizarea informațiilor din sectorul public

Pentru a obține accesul la datele deschise pentru reutilizare prin Directiva 1024/2019, trebuie să se asigure accesul la date dinamice prin API bine concepute. API reprezintă un set de funcții, proceduri, definiții și protocoale pentru comunicarea dintre mașini și schimbul fără sincope de date. API ar trebui să fie sprijinite de o documentație tehnică clară care să fie completă și

disponibilă online. Atunci când este posibil, ar trebui utilizate API deschise. Trebuie aplicate protocoalele standard ale Uniunii sau protocoale standard recunoscute la nivel internațional și vor trebui utilizate standarde internaționale pentru seturile de date acolo unde este cazul. API pot avea diferite niveluri de complexitate și pot consta într-o simplă conexiune la o bază de date pentru extragerea unor seturi de date specifice, într-o interfață web sau în configurații mai complexe. Reutilizarea și partajarea datelor printr-o utilizare corespunzătoare a API prezintă o valoare generală, întrucât le permit dezvoltatorilor și întreprinderilor nou-înființate să creeze noi servicii și produse. Acestea reprezintă, de asemenea, un ingredient esențial pentru crearea unor ecosisteme valoroase în jurul unor date exploatabile care rămân adesea neutilizate. Configurarea și utilizarea API trebuie să se bazeze pe mai multe principii: disponibilitate, stabilitate, întreținere de-a lungul ciclului de viață, uniformitate a utilizării și a standardelor, ușurință în utilizare și securitate. În cazul datelor dinamice, cu alte cuvinte al datelor actualizate frecvent, adesea în timp real, organismele din sectorul public și întreprinderile publice ar trebui să le pună la dispoziție imediat după colectare, prin intermediul unor API corespunzătoare, și, dacă este cazul, prin descărcare în masă, cu excepția cazurilor în care acest lucru ar impune un efort disproporționat.

Adoptarea de măsuri practice care să faciliteze căutarea documentelor disponibile pentru reutilizare, cum ar fi listele de resurse ale principalelor documente, împreună cu metadatele relevante, accesibile, în cazurile în care acest lucru este posibil și oportun, online și în formate prelucrabile automat, și site-uri portal cu legături spre listele de resurse. În cazurile în care acest lucru este posibil, statele membre facilitează căutarea în mai multe limbi a documentelor, în special prin facilitarea agregării metadatelor la nivelul Uniunii.

1.3.1. Legislație

Ordonanța de urgență nr. 89/2022 privind unele măsuri pentru adoptarea sistemului de guvernanță a Platformei de cloud guvernamental, precum și pentru stabilirea cadrului legal de organizare și funcționare a infrastructurilor informatice și a serviciilor de tip cloud în procesul de transformare digitală (Text publicat în Monitorul Oficial, Partea I nr. 638 din 28 iunie 2022.) prevede, printre altele, următoarele:

- modul de utilizare a Platformei și modul de realizare a interconectării la nivel de servicii între componentele prevăzute la alin. (2) sunt prevăzute în Ghidul de guvernanță a platformei.

- ADR asigură interconectarea la nivel de SaaS la serviciile specifice Cloudului privat guvernamental pentru entitățile găzduite și conectate în cloud.

Hotărârea nr. 112 din 8 februarie 2023 privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental (Text publicat în Monitorul Oficial, Partea I, nr. 118 din 10 februarie 2023) care fixează politica cloud first, precum și standardele, regulile și obligațiile necesare operaționalizării și guvernanței sistemelor informatice și a serviciilor de tip cloud.

Legislația care prevede obligativitatea punerii la dispoziția cetățenilor/mediului de afaceri a serviciilor electronice prin intermediul PCU este:

Conform legislației europene, naționale și sectoriale, instituțiile din administrația publică centrală și locală, ordinele profesionale, sunt obligate să se înroleze în PCU și să-și configureze procedurile administrative, în vederea obținerii unor servicii/beneficii pe cale electronică.

Ordonanța de urgență nr.49/2009 și Legea 68/2010 prevăd amenzi în cazul în care nu respectă cerințele impuse de legislație.

Legislația europeană

Regulamentul (UE) 2018/1724 privind înființarea unui portal digital unic (gateway) pentru a oferi acces la informații, la proceduri și la servicii de asistență și de soluționare a problemelor și de modificare a Regulamentului (UE) nr. 1024/2012

- Regulamentul de punere în aplicare (UE) 2020/1121 al Comisiei din 29 iulie 2020 referitor la colectarea și partajarea statisticilor privind utilizatorii și a observațiilor din partea utilizatorilor cu privire la serviciile portalului digital unic în conformitate cu Regulamentul 2018/1724 al Parlamentului European și al Consiliului;
- Regulamentul de punere în aplicare (UE) 2022/143 al Comisiei din 5 august 2022 de stabilire a specificațiilor tehnice și operaționale ale sistemului tehnic pentru schimbul transfrontalier automatizat de elemente justificative și aplicarea principiului „doar o singură dată” în conformitate cu Regulamentul (UE) 2018/1724 al Parlamentului European și al Consiliului;
- Directiva 2006/123/EC privind serviciile în cadrul pieței interne (Directiva Servicii);
- Directiva 2013/55/UE a Parlamentului European și a Consiliului privind recunoașterea calificărilor profesionale;
- Directiva 2005/35/EC a Parlamentului European și al Consiliului din 7 septembrie 2005 privind recunoașterea calificărilor profesionale;

- Directiva 2014/24/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE;
- Directiva 2014/25/UE a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile efectuate de entitățile care își desfășoară activitatea în sectoarele apei, energiei, transporturilor și serviciilor poștale și de abrogare a Directivei 2004/17/CE;
- Directiva (UE) 2019/1024 a Parlamentului European și a Consiliului din 20 iunie 2019 privind datele deschise și reutilizarea informațiilor din sectorul public;
- Regulamentul (UE) 2018/1807 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind un cadru pentru libera circulație a datelor fără caracter personal în Uniunea Europeană;
- Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor)
- Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE.

Legislația națională

- Ordonanța de urgență nr. 49/2009 privind libertatea de stabilire a prestatorilor de servicii și libertatea de a furniza servicii în România;
- Legea 68/2010 pentru aprobarea OUG 49/2009 privind libertatea de stabilire a prestatorilor de servicii și libertatea de a furniza servicii în România;
- Hotărârea de guvern nr. 922/2010 privind organizarea și funcționarea Punctului de contact unic electronic;
- OUG nr. 41/2016 - stabilirea unor măsuri de simplificare la nivelul administrației publice centrale și pentru modificarea și completarea unor acte normative cu modificarile și completările ulterioare
- Legea nr. 200 din 25 mai 2004 privind recunoașterea diplomelor și calificărilor profesionale pentru profesiile reglementate din România, cu modificările și completările ulterioare care transpune Directiva 2005/36/CE din 7 septembrie 2005;

- Ordonanța nr.43/2015 pentru modificarea și completarea Legii nr.200/2004 privind recunoașterea diplomelor și calificărilor profesionale pentru profesiile reglementate din România

- Legea nr. 98 din 19 mai 2016 privind achizițiile publice care transpune Directivele 2014/24/UE și 2014/25/UE din 26 februarie 2014
- Lege nr 242 / 2022 privind schimbul de date între sisteme informatice și crearea Platformei naționale de interoperabilitate;
- Ordonanța de urgență nr. 89/2022 privind unele măsuri pentru adoptarea sistemului de guvernanță a Platformei de cloud guvernamental, precum și pentru stabilirea cadrului legal de organizare și funcționare a infrastructurilor informatice și a serviciilor de tip cloud în procesul de transformare digitală;
- Hotărârea de guvern nr. 112 din 8 februarie 2023 privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental;
- Legea nr. 190/2018 privind masurile de aplicare a GDPR;
- celelalte acte normative incidente în domeniul achizițiilor publice și în domeniul contractului.

1.3.2. PCUe

1.3.2.1.Situația actuală

PCU este un sistem informatic pus la dispoziția cetățenilor /mediului de afaceri /instituțiilor publice, pentru a obține /furniza informații și servicii/beneficii pe cale electronică.
PCUe cuprinde două componente:

- **Componenta informațională**: Documentele necesare obținerii unui serviciu pot fi descărcate pentru a fi prezentate în format letric la sediul instituției pentru obținerea unui serviciu/beneficiu.
- **Componenta operațională**: Pentru obținerea unui serviciu/ beneficiu solicitarea se inițiază și se finalizează pe o cale în întregime electronică. Pentru furnizarea unui serviciu orice instituție publică își poate configura un flux electronic în cadrul platformei.

Punctul de Contact Unic electronic s-a implementat ca urmare a transpunerii *Directivei 2006/123/CE numită și "Directiva Servicii"* în legislația națională, prin următoarele acte normative: OUG nr. 49/2009 privind libertatea de stabilire a prestatorilor de servicii și libertatea

de a furniza servicii în România, aprobată cu modificări și completări, prin Legea nr. 68/2010 și HG nr. 922/2010. Conform cadrului legal existent, prin Punctul de Contact Unic electronic, sistem disponibil la adresa www.edirect.e-guvernare.ro, va fi conectată administrația publică centrală și locală, precum și alte autorități competente, putându-se îndeplini de la distanță, prin mijloace electronice, următoarele proceduri și formalități:

- ansamblul procedurilor și formalităților necesare pentru accesul la activitățile de servicii ale acestora, în special declarațiile, notificările sau cererile necesare pentru obținerea autorizării, inclusiv cererile de înscriere într-un registru.
- orice cereri de autorizare necesare pentru exercitarea activităților de servicii.

PCUe este bazat pe tehnologie Microsoft: Sharepoint 2016 și bază de date SQL. Astfel, sistemul informatic existent îndeplinește funcțiile de bază ale portalului de Punct de Contact Unic, însă există o serie de **aspecte de securitate, compatibilitate de rulare pe browserele uzuale și bug-uri de sistem care limitează utilizarea portalului la potențialul dorit**.

Una dintre soluțiile informatice existente cu relevanță pentru proiectul în cauză o constituie Sistemul National Electronic de Plata a taxelor și impozitelor utilizând cardul bancar (SNEP), care funcționează în baza următoarelor acte normative: Hotărârea nr. 1235/2010, Ordinul nr. 95/2011, Ordinul nr. 173/2011 și HG nr. 1070/2013 și este disponibil la adresa web www.ghiseul.ro. Sistemul este conceput ca o soluție deschisă ce are ca atribut principal facilitățile de integrare cu alte sisteme informatice funcționale.

Sistemul Național Electronic de Plată asigură:

- punct central de acces, punct central de informare, punct central de serviciu electronic;
- acces la informații actualizate și consolidate privind taxele și impozitele către oricâte dintre instituțiile publice înregistrate în sistem;
- posibilitatea plății electronice cu cardul bancar, parțială sau totală, a datoriilor înregistrate;
- creșterea satisfacției cetățenilor în relația cu administrația publică;
- o platformă solidă de interoperabilitate la nivel național, standardizarea documentelor, nomenclatoarelor, comunicației și fluxurilor electronice;
- utilizarea unor tehnologii noi și creșterea gradului de cunoaștere în IT&C în administrația publică
- fluxuri automatizate, intervenție umană minimală.

Modalitatea actuală de conectare în sistem:

Se alege una dintre opțiunile de autentificare:

- **eDirect** – autentificarea se realizează folosind credențialele de acces obținute în urma completării informațiilor din secțiunea „Cont nou”- Persoana fizică”;
- **ghișeul.ro** – autentificarea se realizează folosind credențialele de acces utilizate pe portalul Ghiseul.ro;
- **Certificat digital calificat** – dacă utilizatorul are deja un cont activ în portal, autentificarea se poate realiza în mod automat, folosind un certificat digital calificat (în condițiile în care adresa de email din certificat este identică cu adresa de email asociată contului de utilizator din portal);
- **ROeID** - autentificarea se realizează folosind credențialele platformei de management al identității electronice.

Categoriile de utilizatori ale PCUe:

- administrator portal;
- administrator instituție;
- operator instituție;
- cetățeni/persoane juridice.

Cetățeni

Modalitatea actuală de autentificare:

- creare cont pe eDirect -„Persoana fizică”;
- credențialele de la ghișeul.ro;
- certificat digital calificat;
- credențialele de la ROeID.

PDURo va implementa la nivel național obiectivele Regulamentului Single Digital Gateway (Regulamentul 2018/1724) prin care se urmărește :

- reducerea sarcinilor administrative suportate de cetățeni și companii;
- libera circulație a cetățenilor și companiilor;
- eliminarea discriminării și asigurarea funcționării pieței interne europene;
- simplificarea și debirocratizarea administrativă..

Persoanele juridice

Modalitatea de autentificare:

- creare cont pe eDirect - „Persoana juridică”, sistemul validează corectitudinea datelor din cadrul formularului, prin interogarea bazei de date a ONRC prin intermediul platformei BIG DATA;
- administratorul firmei poate să acorde drepturi de operator.

Fluxul procedural prin PCUe

Inițierea fluxului de către cetățeni/persoane juridice:

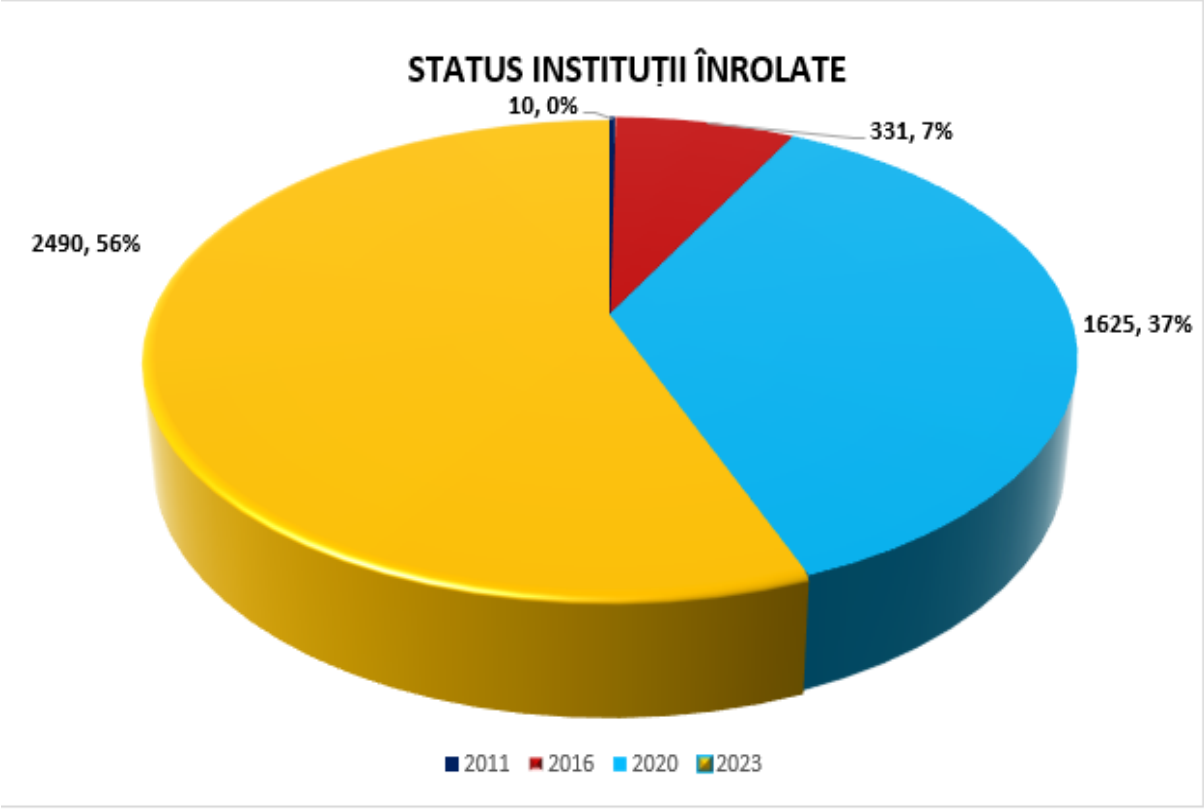
- de pe contul de cetățean/operator firmă, pe baza filtrelor, se identifică instituția și procedura;
- se atașează documentele și se transmite solicitarea;
- sistemul generează pentru fiecare solicitare un **număr unic** PCUe
- în contul de cetățean /operator firma se pot vizualiza informații cum sunt:
    - stare solicitare;
    - termen estimat până la soluționare;
    - data solicitării;
    - număr PCUe;
    - CNP/CUI solicitant;
    - istoric stare solicitare (elemente referitoare la solicitare : data, stare, utilizator curent);
    - elemente referitoare la solicitare (data transmiterii solicitării, expeditor, destinatar, mesaj, documente atașate, număr intern de înregistrare).
- comunicarea între cetățeni/persoane juridice și operatorul din instituție se poate vizualiza în contul de pe PCUe și pe email.

Procesarea dosarului de către instituții:

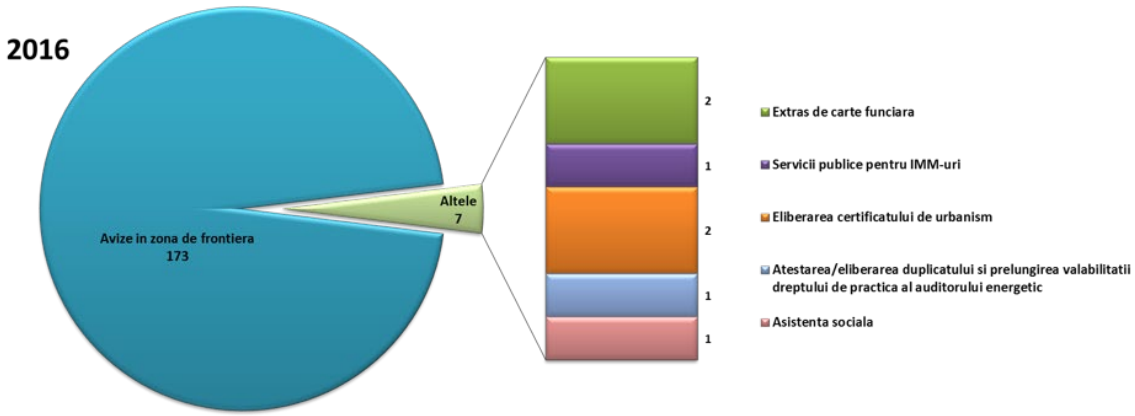
- solicitarea este preluată de operatorul instituției și i se atribuie un număr de înregistrare intern;
- dacă este nevoie de documente suplimentare se solicită clarificări;
- dacă dosarul este complet, instituția poate să soluționeze solicitarea.
- Solicitarile transmise care nu indeplineasc cerintele procedurale pot fi trecute in starea de „Expirat”, “Arhivat” sau “Clasat”.

Instituții înrolate în PCUe

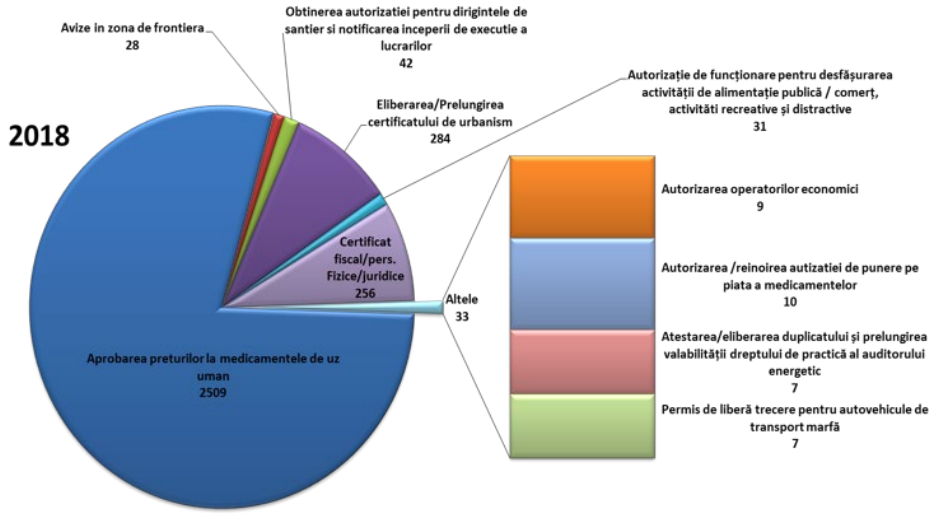
- Dacă în anul **2011**, când s-a lansat în producție, erau înscrise în PCUe un număr de **10 instituții**, în prezent peste 2500 de de autorități, structuri teritoriale și ordine profesionale oferă cetățenilor/mediului de afaceri din țară și din spațiul comunitar posibilitatea de a vizualiza, dar și de a accesa online servicii publice, prin intermediul unui portal unic.
- Până la data de **06.06.2023 in PCUe** au fost configurate un număr de **5390** proceduri din care, **1568** cu caracter informațional și 1606 cu caracter operațional, fiind înrolate **731 de autorități** acestea reprezentând: primării municipale, orășenești și comunale, autorități ale administrației publice centrale, agenții și servicii publice deconcentrate, inspectorate școlare județene, universități, academii, biblioteci, ordine profesionale, alte instituții.



Diversificarea serviciilor puse la dispoziție prin PCU - 2016-2018



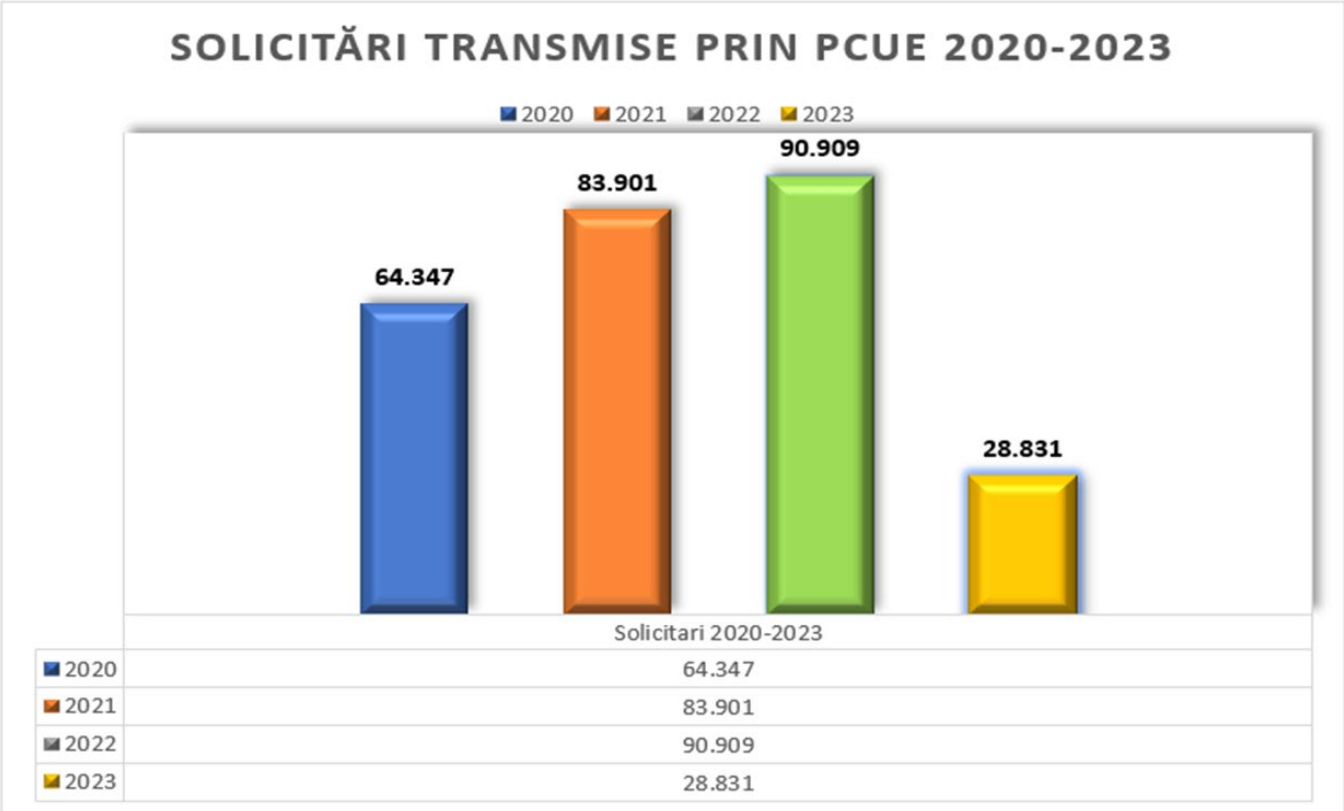
Sursa: ADR



Sursa: ADR

Solicitări transmise prin PCUe

Eliminarea deplasării fizice la ghișeul instituțiilor publice



	Solicitari 2020-2023
2020	64.347
2021	83.901
2022	90.909
2023	28.831

1.3.2.2.Cerințe funcționale PDURo

Portalul PDURo, dezvoltat în cadrul proiectului, va înlocui PCUe cu toate funcționalitățile existente, se va integra cu ROeID - care va oferi identitatea digitală pentru persoanele fizice române - și cu nodul EIDAS pentru validarea identității cetățenilor străini.

PDURo își propune să dezvolte tehnologic PCUe pentru a permite digitalizarea mai multor procese ale administrației publice și să îl integreze cu SDG.

Portalul PDURo va implementa sistemul tehnic pentru schimbul transfrontalier automatizat de elemente justificative (prevăzut la articolul 14 al Regulamentului Single Digital Gateway). Prin intermediul acestui sistem tehnic, statul membru care eliberează propriilor cetățeni în format electronic un act administrativ (element justificativ), are obligația de a pune și la dispoziția autorităților competente solicitante din alte state membre același act administrativ în vederea îndeplinirii procedurilor administrative esențiale (enumerate în Regulamentul Single Digital Gateway), la cererea expresă a unui cetățean european.

1.3.3. Portal digital unic (single digital gateway)

Conform evoluției legislative, dar și a deciziilor strategice și politice de implementare a e-guvernării în România, la început a fost realizat PCUe, un portal de tip one stop shop pentru interacțiunea cetățenilor și mediului privat cu autoritățile publice din perspectiva libertății de circulație și prestare a serviciilor sau de recunoaștere a diplomelor de studii. Cu timpul, acest portal a evoluat – e-guvernarea a început să fie construită în jurul său – și a ajuns să faciliteze inclusiv interacțiunea între autoritățile publice (vezi interacțiuni între primării și Direcțiile de Sănătate Publică – DSP sau Agenții Județene pentru Plăți și Inspecție Socială – AJPIS) la acest moment asigurând relații funcționale de tip G2C, G2B și G2G.

Portalul digital unic (single digital gateway) - PDURo își propune să ofere un acces facil la informații, proceduri și servicii de asistență și de soluționare a problemelor.
Urmând această logică, odată cu apariția Regulamentului Single Digital Gateway – SDG (1724/2018), viziunea strategică a fost de a dezvolta portalul PCUe și de a-l transforma pentru a asigura servicii de tip G2C, G2B și G2G la un nivel de calitate și eficiență ridicat. În acest sens, se propune realizarea acestui proiect care din punct de vedere tehnic va trebui să îmbunătățească funcționalitățile deja existente ale PCUe, dar și să asigure implementarea *Regulamentului 1724/2018*:

- realizarea interoperabilității bazelor de date aferente serviciilor publice furnizate prin mijloace electronice **inclusiv posibilitatea configurării de noi fluxuri procedurale electronice pentru serviciile administrației publice care nu au trecut la furnizarea lor online;**
- realizarea unui catalog al serviciilor publice care să cuprindă atât serviciile publice electronice, cât și cele clasice – fără a se limita la serviciile prevăzute de PCUe și Regulamentul (UE)1724/2018;
- asigurarea modalității de plată a unor taxe/tarife/sume aferente procedurilor specifice de furnizare a serviciilor publice dezvoltând / reutilizând / utilizând funcționalitățile GHISEUL.RO;
- asigurarea unui sistem de autentificare unic pentru toate serviciile publice (Single Sign On).

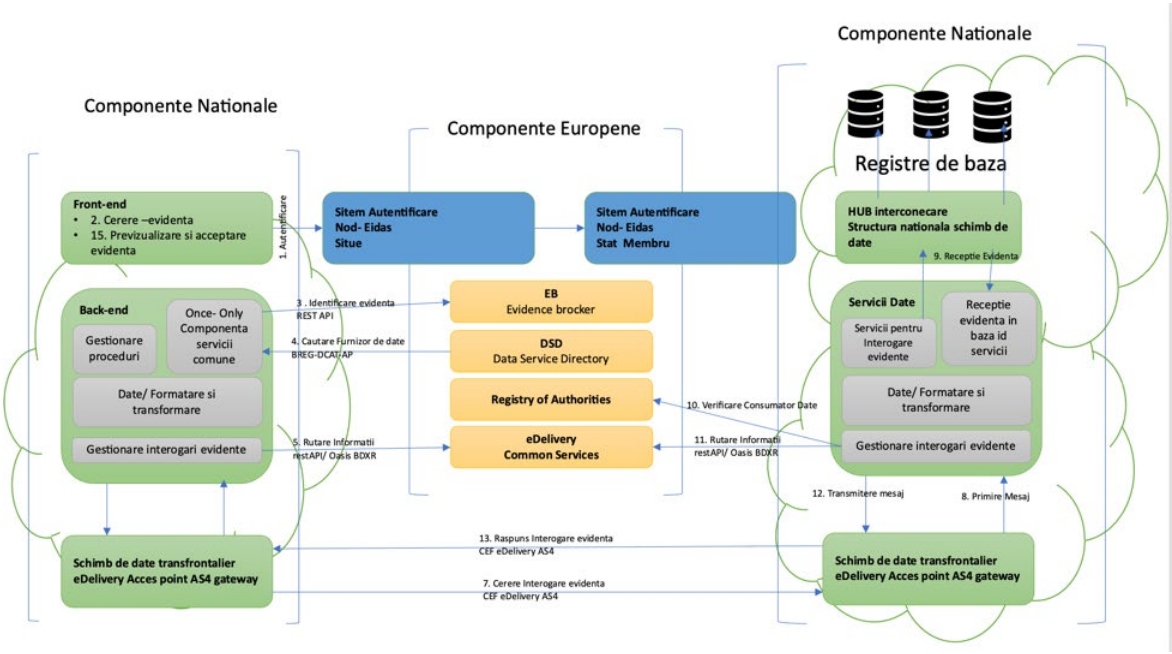
1.3.3.1.Introducere

Piața unică este una dintre cele mai mari realizări ale UE, promovând creșterea și îmbunătățirea vieții de zi cu zi a întreprinderilor și a cetățenilor deopotrivă prin garantarea liberei circulații a mărfurilor și serviciilor.

Cu toate acestea, barierele în calea activității transfrontaliere persistă în continuare, sarcinile administrative fiind impuse atât organizațiilor, cât și persoanelor fizice, pe măsură ce interacționează cu administrațiile publice din alte state membre ale UE.

Portalul Digital Unic (Gateway) promite sfârșitul multora dintre aceste bariere. Aplicarea principiului o singură dată la nivel transfrontalier va duce la o economie semnificativă de timp pentru multe proceduri publice. Cetățenii și întreprinderile se vor putea baza pe administrațiile care vor reutiliza informațiile despre acestea deja transmise altor autorități publice din alte state membre atunci când efectuează aceste proceduri. În plus, implementarea sistemului va avea un efect de spillover, încurajând dezvoltarea și implementarea altor soluții pentru livrarea serviciilor publice transfrontaliere cetățenilor .

Pentru a realiza aplicarea efectivă a acestui principiu este însă necesară o nouă infrastructură, ce prevede noi obligații pentru statele membre de a se conecta la aceasta. **Sistemul tehnic Single Digital Gateway Once Only Technical System (SDG OOTS)** va furniza această infrastructură, cea mai recentă arhitectură a sistemului fiind prezentat în figura următoare:



Partea stângă a figurii prezintă principalele componente arhitecturale gestionate de statul membru A (SM A) - consumatorul de date - în timp ce partea dreaptă prezintă componentele

gestionate de statul membru B (SM B) - furnizorul de date. Componentele UE sunt prezentate în centrul figurii și oferă informații despre, cum și unde pot fi preluate probele solicitate de SM A de la SM B. Pentru a realiza interacțiunea transfrontalieră, statele membre trebuie să dezvolte componente funcționale atât pentru consumatori, cât și pentru furnizor și conexiunile aferente cu Componentele UE (folosind API-uri specifice).

Pe scurt, statele membre sunt responsabile pentru dezvoltarea următoarelor componente, care intră în domeniul de aplicare al SDG:

1. **Portalul eProcedure și back-end;**
2. **Infrastructura transfrontalieră de schimb de date (punct de acces eDelivery);**
3. **Serviciul de date.**

În plus:

- Nodul eIDAS ar trebui utilizat ca sistem de autentificare transfrontalier, astfel cum este implementat în temeiul regulamentului eIDAS;
- O infrastructură nouă sau existentă de schimb de date poate fi utilizată pentru a prelua dovezile din interiorul granițelor unei țări (accesarea registrelor de bază naționale sau a bazelor de date locale).

Componentele centrale ale CE sunt următoarele (reprezentate în portocaliu în figură):

1. **Broker de probe;**
2. **Director de servicii de date;**
3. **Registrul Autorităților;**
4. **Servicii comune eDelivery.**

Pentru aceste componente centrale se discută în prezent următoarele strategii de implementare:

1. *Centralizat*: o singură componentă la nivelul UE este implementată și întreținută de către CE, SM furnizează/sincronizează datele în mod interactiv sau printr-un API de management al ciclului de viață;

2. *Federat*: o singură componentă la nivelul UE este desfășurată și întreținută de către CE, în timp ce mai multe sunt desfășurate în fiecare stat membru. Componenta centrală va transmite interogări către cele naționale pentru a obține informații;

3. *Descentralizat*: nu există o singură componentă la nivelul UE, fiecare stat membru își desfășoară și întreține componentele și le conectează la alte state membre;

4. *Hibrid* : combinație de abordare centralizată și descentralizată.

În tabelul următor, diferitele componente funcționale ODD sunt descrise mai detaliat, subliniind, de asemenea, împărțirea diferită a responsabilităților între statele membre și Comisia Europeană:

Componentele arhitecturii SDG

Componentă funcțională SDG	Descriere	Responsabilitatea statului membru	Responsabilitatea Comisiei Europene
eProcedure Portal și Backend	Este un portal web pe care un stat membru A îl pune la dispoziție pentru a permite utilizatorilor, inclusiv utilizatorilor din alt stat membru B, să execute o procedură a unui stat membru UE. Interfața va oferi următoarele funcții: autentificarea utilizatorilor, managementul, selecția dovezilor și previzualizarea. Pe de altă parte, backend-ul portalului trebuie să includă funcționalități pentru a gestiona procedura și starea sesiunii, pentru a se integra cu sistemele informaționale și/sau baza de date și pentru a efectua transformarea datelor sau a formatului, pentru a crea cereri de dovezi și pentru a transmite și a primi răspunsul la dovezi.	<u>Consumatorii de date ale statelor membre:</u> Proiectarea, dezvoltarea, operarea și întreținerea portalurilor naționale de procedură online, oferind o singură integrare la nodul eIDAS, la punctele de acces eDelivery și la serviciile centrale Evidence Broker, Data Service Directory și eDelivery Common Service.	Unele elemente vor fi incluse în specificațiile sau în ghidurile sistemului tehnic OOTS (inclusiv funcționalitatea de previzualizare, scenariile alternative și de eroare, instrucțiunile de arhivare, liniile directoare de securitate și altele).
Infrastructură transfrontalieră de schimb de date (eDelivery)	Este folosit pentru a solicita dovezi unui alt stat membru și pentru a le primi ca răspuns. Acest punct de acces trebuie utilizat pentru interacțiunile transfrontaliere (atât la cerere, cât și la primire).	Implementarea, operarea și configurarea unuia sau mai multor puncte de acces eDelivery pentru portalurile naționale de procedură online și serviciile de date și integrarea acestora la serviciile centrale eDelivery.	Definirea și întreținerea specificațiilor tehnice ale sistemului tehnic OOTS, precum și a specificațiilor pentru blocuri reutilizabile, inclusiv eIDAS și eDelivery.
Sistem de autentificare transfrontalier (nodul eIDAS)	Nodurile eIDAS ale celor două state membre pot fi utilizate pentru autentificarea transfrontalieră. Această funcționalitate va fi accesată din partea frontală a Portalului de proceduri online, deoarece implică interacțiunea cu utilizatorul.	Funcționarea unui nod eIDAS.	Definirea și întreținerea specificațiilor tehnice OOTS, precum și a specificațiilor pentru blocuri reutilizabile, inclusiv eIDAS și eDelivery.

Componentă funcțională SDG	Descriere	Responsabilitatea statului membru	Responsabilitatea Comisiei Europene
Serviciu de date	Serviciul de date este o componentă operată de autoritățile competente din statele membre ca răspuns la solicitările portalurilor eProcedure. Un serviciu de date trebuie să aibă două servicii de aplicație standardizate, o singură dată, un „Serviciu de interogare a dovezilor” și un „Servicii de preluare a dovezilor prin ID”. Aceste servicii se bazează pe standardul OASIS RegRep4.	Furnizorii de date ale statelor membre: Proiectarea, dezvoltarea, operarea și întreținerea serviciilor naționale de date, oferind o singură integrare la punctele de acces eDelivery și la serviciul central Registrul autorităților.	
Broker de dovezi	Sistemul va permite statelor membre să gestioneze și să partajeze informații despre regulile referitoare la criteriile dovezilor din statele membre, în special pentru tipurile standardizate de dovezi (de exemplu, certificatele de naștere) care nu necesită o evaluare detaliată substanțială. Sistemul ar trebui să ofere o interfață de management care să permită reprezentanților statelor membre să creeze și să actualizeze reguli referitoare la echivalența probelor.	Furnizarea de date referitoare la autoritățile competente din statul lor membru. *Responsabilitățile s-ar putea schimba dacă sunt alese strategii de implementare federate, descentralizate sau hibride*	Proiectare, dezvoltare, operare și întreținere. *Responsabilitățile s-ar putea schimba dacă sunt alese strategii de implementare federate, descentralizate sau hibride*
Director de servicii de date	Directorul de servicii de date face parte din sistemul OOP și va permite consumatorilor MS să caute și să găsească serviciul de date al furnizorului MS care poate prelua dovezile solicitate.	Furnizarea de date referitoare la autoritățile competente din statul lor membru. *Responsabilitățile s-ar putea schimba dacă sunt alese strategii de implementare federate, descentralizate sau hibride*	Proiectare, dezvoltare, operare și întreținere. *Responsabilitățile s-ar putea schimba dacă sunt alese strategii de implementare federate, descentralizate sau hibride*
Registrul Autorităților	Acesta enumeră, pentru administrațiile publice din statele membre UE, procedurile pentru care administrațiile străine sunt autorizate să solicite ce tipuri de probe.	Furnizarea de date referitoare la autoritățile competente din statul lor membru. *Responsabilitățile s-ar putea schimba dacă sunt alese strategii de*	Proiectare, dezvoltare, operare și întreținere. *Responsabilitățile s-ar putea schimba dacă sunt alese strategii de implementare federate, descentralizate sau hibride*

Componentă funcțională SDG	Descriere	Responsabilitatea statului membru	Responsabilitatea Comisiei Europene
Servicii comune eDelivery	Dacă eDelivery este configurat utilizând descoperirea dinamică, se recomandă utilizarea serviciilor comune eDelivery pentru a localiza serviciul de metadate al punctului de acces al receptorilor.	Asigurarea integrării cu portalurile naționale de procedură online și serviciul de date.	Proiectare, dezvoltare, operare și întreținere.

Implementarea corectă și completă a Regulamentului Single Digital Gateway în toate componentele sale este obligatorie pentru toate Statele Membre. România are așadar obligația de a publica toate informațiile necesare privind drepturile, obligațiile și normele care decurg din dreptul Uniunii și dreptul național pentru ca cetățenii europeni să le exercite în cadrul pieței interne, de colecta și de a publica informațiile referitoare la serviciile de asistență și de soluționare a problemelor. Mai mult, România are obligația de a digitaliza serviciile publice esențiale, atât din perspectiva obiectivelor Decadei Digitale 2030, cât și din perspectiva Regulamentului Single Digital Gateway care fixează o listă obligatorie a procedurilor administrative care vor deveni accesibile online nu doar pentru cetățenii români, ci și pentru cetățenii europeni prin intermediul sistemului tehnic Once-Only.

Platforma PDURo va fi așadar instrumentul care va permite transpunerea cât mai completă a Regulamentului Single Digital Gateway.

Portalul digital unic și Europa ta

Portalul digital unic facilitează accesul online la informații, proceduri administrative și servicii de asistență de care cetățenii și întreprinderile din UE ar putea avea nevoie în altă țară din UE. Accesul la portal se realizează prin intermediul unei funcții de căutare pe portalul „Europa ta”. În urma adoptării Regulamentului privind portalul digital unic (Single Digital Gateway) în 2018, Comisia Europeană și administrațiile naționale dezvoltă o rețea de portaluri naționale pentru a oferi informații cetățenilor și întreprinderilor cu privire la modul în care normele UE sunt aplicate în fiecare țară din UE pentru utilizatorii transfrontalieri, precum și cu privire la serviciile de asistență disponibile. Din decembrie 2020, unele dintre aceste servicii sunt disponibile de la punctul unic de intrare de pe portalul „Europa ta”. Site-urile naționale care participă la portal pot fi ușor recunoscute prin prezența logoului „Europa ta”.

Conform Regulamentului, până la sfârșitul anului 2023, sistemul tehnic „doar o singură dată” (Once-Only Technical System - OOTS) va oferi acces la 21 de proceduri online în toate țările

UE, proceduri precum înmatricularea unei mașini sau solicitarea unei pensii fiind complet digitalizate și eliminând nevoia de documente fizice. Cele mai importante proceduri administrative pentru utilizatorii transfrontalieri **vor trebui să fie disponibile pe deplin online în toate țările UE.**

Once-only la nivel european

Conform considerentului (42) al Regulamentului Single Digital Gateway, serviciile online oferite de autoritățile competente sunt esențiale pentru îmbunătățirea calității și siguranței serviciilor oferite cetățenilor și întreprinderilor. Administrațiile publice din anumite state membre depun eforturi din ce în ce mai mari în vederea reutilizării datelor, renunțând la cerința ca cetățenii și întreprinderile să furnizeze aceleași informații în mod repetat. Reutilizarea datelor ar trebui să fie stimulată în cazul utilizatorilor transfrontalieri, în scopul de a reduce sarcinile suplimentare. Sistemul tehnic Once-Only, prevăzut de Regulamentul Single Digital Gateway și de Regulamentul de punere în aplicare 2022/1463, va urmări îndeplinirea acestui obiectiv, fiind un sistem de transfer al documentelor necesare pentru aceste proceduri între autoritățile naționale din diferite țări ale UE. De exemplu, o diplomă obținută într-o țară poate fi partajată cu autoritățile naționale ale altei țări, în cazul în care este necesară pentru a începe o afacere.
Pentru a îmbunătăți procesul de elaborare a politicilor, utilizatorii sunt, de asemenea, în măsură să ofere feedback prin intermediul portalului privind obstacolele cu care se confruntă pe piața unică.

De ce este nevoie de un portal digital unic

Cetățenii și întreprinderile din UE, în special cei care își desfășoară activitatea într-o altă țară a UE, se străduiesc adesea să înțeleagă normele care se aplică cazului lor particular sau măsurile necesare pentru a efectua proceduri simple. Căutarea informațiilor reprezintă adesea un proces obositor și confuz. Rezultatele tind să fie împrăștiate pe diferite site-uri web care adesea nu au nicio garanție de calitate sau fiabilitate, iar lacunele semnificative în materie de informații rămân în multe domenii, lăsând întrebări importante fără răspuns. Pentru cetățeni, există și mai puține cerințe europene pentru ca furnizarea de informații să fie accesibilă decât pentru mediul de afaceri. În consultarea publică a Regulamentului SDG s-a arătat că 60% dintre cetățenii care au încercat să afle ce cerințe naționale ar trebui să îndeplinească atunci când se mută într-un alt

stat membru au găsit acest lucru extrem de dificil și, bineînțeles, extrem de greu de îndeplinit. Motivele principale au fost că site-urile web au fost greu de găsit și de înțeles și că acestea conțineau informații inexacte sau învechite. O serie de proceduri sunt încă doar pe suport de hârtie sau necesită coadă de așteptare într-un birou, ceea ce este o pierdere de timp și bani. De asemenea, utilizatorii transfrontalieri întâmpină adesea obstacole în calea procedurilor administrative naționale, deoarece administrațiile publice naționale lucrează doar cu numere de telefon naționale, coduri poștale sau metode de plată neclare. În plus, mulți cetățeni și companii nu sunt conștienți de serviciile de asistență disponibile pentru a-i ajuta să își rezolve problemele. Așa cum a arătat analiza de impact efectuată de către Comisia europeană, administrațiile naționale proiectează serviciile publice din perspectiva lor și nu din cea a utilizatorului.

Atât la nivelul UE, cât și la nivel național, proiectarea serviciilor centrate pe nevoile administrației a fost modul tradițional de implementare a transformării digitale și de aceea a produs servicii publice care adresează nevoile administrației mult mai mult decât pe cele ale utilizatorului (cetățeanului, firmei) în termeni de explicații online clare și ușor de înțeles. Este mai ușor pentru administrație să „lanseze și să părăsească” un nou portal web decât să organizeze pentru cetățeanul obișnuit actualizări sistematice ale conținutului acestuia.

Digitalizarea serviciilor publice generează în cele din urmă beneficii substanțiale în administrație și o eficiență sporită din perspectiva funcționării acesteia. Această transformare necesită însă și investiții inițiale considerabile, ceea ce poate fi un obstacol pentru lansarea rapidă a serviciilor publice electronice.

Administrațiile naționale se concentrează pe soluții digitale naționale neglijând utilizatorul non-național, iar accesibilitatea pentru utilizatorii serviciilor publice care provin din afara țării este în cel mai bun caz o idee marginală. Utilizatorii cetățeni străini au o voce inexistentă în procesul decizional, iar nevoile lor, în ceea ce privește acoperirea lingvistică și accesul la proceduri, sunt, în general, ignorate. Astfel, utilizatorii non-naționali întâmpină dificultăți , cum ar fi faptul că în câmpurile de formulare ale procedurilor sunt acceptate doar formatele datelor naționale, dovezile străine (de exemplu, documentele administrative eliberate de alte State Membre) nu sunt acceptate ca parte a procedurii online, posibilitățile de plată fiind accesibile doar cetățenilor naționali, schemele de identificare eID străine nefiind acceptate și procedurile fiind dezvoltate numai în limbile naționale. O reală problemă pentru un utilizator de servicii publice cetățean european este aceea de a înțelege limba națională dintr-un alt stat membru. Conform aceleiași consultări efectuate de CE, 81% dintre cetățeni doresc ca autoritățile să aibă obligația de a oferi

minimum de informații pentru desfășurarea activităților transfrontaliere și 72% ar dori să vadă acest lucru cel puțin într-o altă limbă a UE.

În ultimii zece ani, circulația cetățenilor UE în statele membre a crescut în mod constant, pe măsură ce tot mai mulți cetățeni se deplasează în interiorul continentului european pentru a trăi, a lucra sau a studia. O parte tot mai însemnată a populației UE are reședința într-un alt stat membru decât în statul membru de origine și de asemenea un număr tot mai mare de cetățeni din UE-27 profita de dreptul la libera circulație.

Toate aceste obstacole împiedică consolidarea unei veritabile piețe unice, în care libertatea bunurilor, a serviciilor, a capitalului și a persoanelor este pe deplin asigurată. De asemenea, acestea împiedică crearea unei piețe unice digitale creând bariere online inutile între cetățenii din diferite țări ale UE.

Pentru a aborda aceste probleme, Parlamentul European și Consiliul Uniunii Europene au adoptat Regulamentul de instituire a unui portal digital unic – Regulamentul Single Digital Gateway (Regulamentul (UE) 2018/1724) la 2 octombrie 2018. Se preconizează că portalul digital unic va economisi întreprinderilor peste 11 miliarde EUR pe an și va stimula activitatea transfrontalieră.

Regulamentul (UE) 2018/1724 al Parlamentului european și al Consiliului din 2 octombrie 2018 privind înființarea unui portal unic digital (gateway) pentru a oferi acces la informații, la proceduri și la servicii de asistență și soluționare a problemelor și de modificare a Regulamentului (UE) nr. 1024/2012 (Regulamentul Single Digital Gateway) prevede crearea unui portal digital unic pentru a servi drept punct de intrare unic prin intermediul căruia cetățenii și întreprinderile să aibă acces la informații cu privire la regulile și cerințele pe care trebuie să le respecte, în conformitate cu dreptul Uniunii sau dreptul intern. Portalul va trebui să simplifice contactul cetățenilor și întreprinderilor cu serviciile de asistență și de soluționare a problemelor, stabilite la nivelul Uniunii sau la nivel național și să îl facă mai eficace. Anexa I a Regulamentului stabilește domeniile (ex. Călătorii în interiorul Uniunii Europene, munca și pensionarea în Uniunea Europeană) în care portalul va trebui să ofere acces la informații privind drepturile, obligațiile și normele care decurg din dreptul Uniunii și din dreptul național. Astfel, Regulamentul răspunde nevoii cetățenilor și întreprinderilor de asistență în desfășurarea activităților lor transfrontaliere punând la dispoziția acestora accesul facil la informațiile, la procedurile și la serviciile de asistență și de soluționare a problemelor de care au nevoie pentru a-și exercita drepturile în cadrul pieței interne. Regulamentul instituie un portal interactiv și ușor de utilizat, care în funcție de nevoile utilizatorilor, îi îndrumă către serviciile cele mai

potrivite. Portalul „Europa ta” facilitează interacțiunile dintre cetățeni și întreprinderi pe de o parte, și autoritățile competente, pe de altă parte, prin asigurarea unui acces la soluții online și la informații exacte și actualizate, la proceduri și la servicii de asistență și de soluționare a problemelor.

Programul de lucru al Comisei pentru 2023 „O uniune fermă și unită”, arată că stimularea transformării digitale a administrațiilor publice rămâne o prioritate de vârf pentru Uniunea Europeană. Comisia împreună cu statele membre au dezvoltat cadrul de reglementare necesar pentru a stabili reguli și stimulente clare, armonizate și obligatorii pentru produsele și serviciile digitale pe Piața Unică. Mai mult, în urmărirea obiectivelor deceniului digital al UE, Europa își propune să ofere tuturor cetățenilor europeni acces online la toate serviciile publice cheie până în 2030. Mai mult, Europa își propune să ofere cetățenilor UE acces la un mijloc de identificare electronică securizat, recunoscut în întreaga Uniune, permițând utilizatorilor să acceseze servicii publice și private, asigurând totodată ca utilizatorii să păstreze controlul deplin asupra tranzacțiilor de identitate și a datelor personale partajate. Investiții și politici fundamentale au fost implementate pentru a facilita transformarea digitală, astfel că acestui obiectiv au fost alocați cel puțin 20% din fondurile Mecanismului de Redresare și Reziliență și ale politicii de coeziune. Aproximativ 37% din aceste fonduri alocate transformării digitale au fost direcționați către implementarea Regulamentului Single Digital Gateway și a portofelului european de identitate digitală (Regulamentul eIDAS 2), identificate drept instrumente cheie pentru depășirea barierelor în oferirea accesului cetățenilor și întreprinderilor la servicii publice digitale transfrontaliere.

Proceduri online și completarea acestora

Regulamentul (UE) 2018/1724 – Single Digital Gateway va intermedia așadar accesul la proceduri online și completarea acestora.

Regulamentul identifică în Anexa II o serie de proceduri considerate esențiale **care vor trebui digitalizate complet – proceduri care vor trebui oferite integral online de către toate statele membre** . Ordonate în logica evenimentelor de viață (naștere, reședință, studii, aspecte legate de muncă, mutarea, pensionarea, demararea, desfășurarea și închiderea unei activități comerciale), acestea includ serviciile publice esențiale de care au nevoie cetățenii europeni transfrontalier. Fiecare eveniment de viață cuprinde proceduri administrative diferite. Spre exemplu, evenimentul de viață **Studii** cuprinde următoarele proceduri administrative:

- depunerea unei cereri inițiale de acces în instituțiile publice de învățământ superior;

- solicitarea recunoașterii academice a diplomelor, a certificatelor sau a altor dovezi a studiilor sau cursurilor;
- solicitarea finanțării studiilor în învățământul superior, cum ar fi granturile de studiu și împrumuturile acordate de un organism public sau o instituție publică.

Mai mult, în anumite State Membre aceste proceduri pot să nu existe. Spre exemplu, în România nu există un sistem de finanțare a studiilor în învățământul superior la cerere sau împrumuturi pentru studii. Aceste aspecte trebuie înțelese în detaliu la nivel național pentru a putea fi corect înregistrate și mai apoi identificate în **Brokerul de dovezi** existent în serviciile comune dezvoltate la nivel european.

O procedură este considerată ca fiind integral online în cazul în care utilizatorul poate urma toți pașii de la acces până la finalizarea acesteia, în ceea ce privește interacțiunea dintre utilizator și autoritatea competentă („serviciul relații cu clienții”), în format electronic, de la distanță și prin intermediul unui serviciu online. Acest serviciu online trebuie să ghideze utilizatorul printr-o listă cu toate cerințele care trebuie să fie îndeplinite și cu toate elementele justificative care trebuie furnizate, și trebuie să permită utilizatorului să prezinte informații și dovada conformității cu toate aceste cerințe și trebuie să ofere utilizatorului o recunoaștere automată a primirii, cu excepția cazului în care rezultatul procedurii este livrat imediat. Acest lucru nu ar trebui să împiedice autoritățile competente să contacteze utilizatorii direct dacă pentru procedura respectivă sunt necesare precizări suplimentare. Rezultatul procedurii ar trebui și el transmis pe cale electronică, dacă este posibil, în conformitate cu dreptul aplicabil la nivelul Uniunii și la nivel intern.

Mai mult, același Regulament prevede ca procedurile transfrontaliere ce ar trebui oferite integral online (menționate la Anexa II, precum și procedurile privind serviciile conform Directivei 2006/123/CE, procedurile privind recunoașterea calificărilor profesionale conform Directivei 2005/36/CE, procedurile privind achizițiile publice conform Directivelor 2014/24/UE și 2014/25/UE) trebuie să sprijine utilizarea principiului „doar o singură dată” (Once-Only Principle) la nivel european. În vederea facilitării utilizării procedurilor online, Regulamentul reprezintă baza pentru crearea și utilizarea unui sistem tehnic pe deplin operațional, sigur și securizat pentru schimbul automatizat de elemente justificative între părțile angajate într-o procedură transfrontalieră, atunci când acest lucru este cerut în mod expres de cetățeni și întreprinderi. Aplicarea transfrontalieră a principiului „doar o singură dată” ar trebui să rezulte în faptul că cetățenii și întreprinderile nu sunt nevoiți să furnizeze în mod repetat aceleași date autorităților publice și că ar trebui să fie posibil ca respectivele date să poată fi

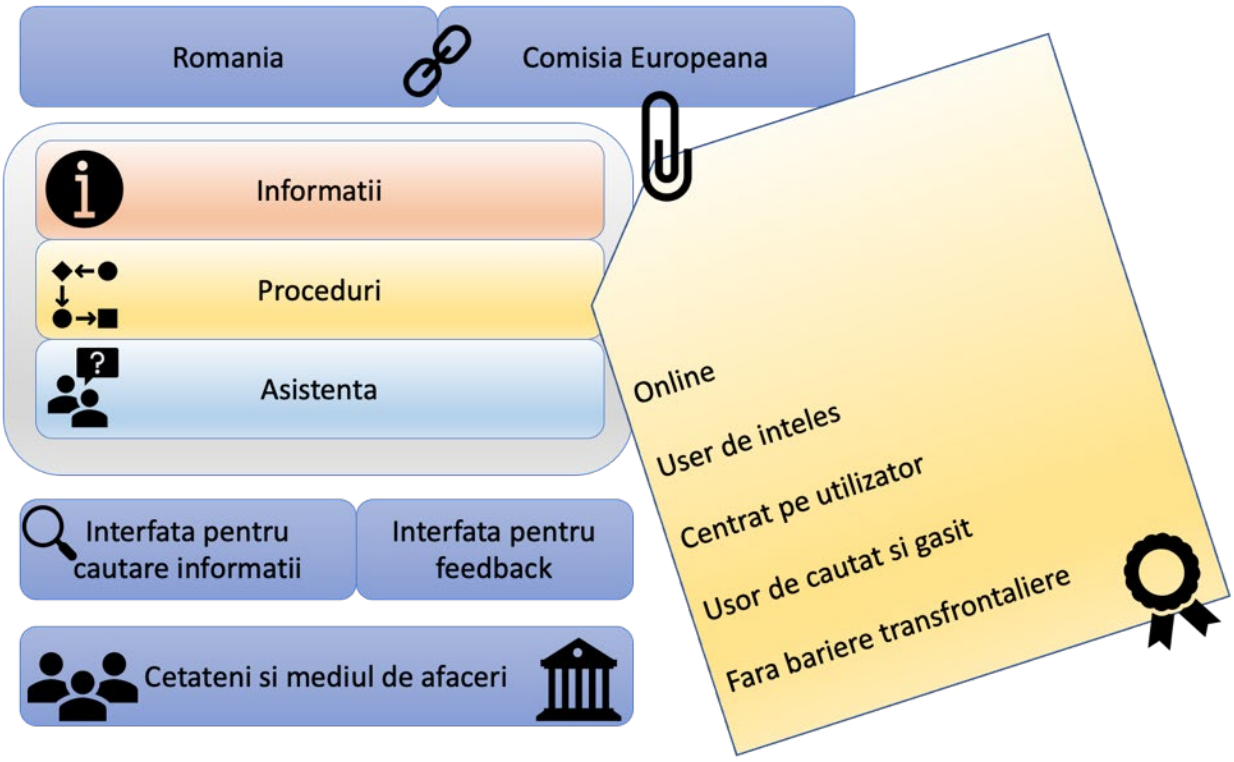
folosite la cererea utilizatorului pentru efectuarea procedurilor online transfrontaliere care implică utilizatori transfrontalieri.

Regulamentul privind portalul digital unic facilitează accesul online la informații și la procedurile de e-guvernare. Pentru a reduce sarcina administrativă și pentru a se asigura că procedurile administrative reglementate de propunere sunt conforme cu Regulamentul privind portalul digital unic, există propuneri de modificare a anexelor de la regulamentul menționat. Se vor considera și cerințele **privind colectarea și schimbul de date referitoare la serviciile de închiriere de locuințe pe termen scurt și de modificare a Regulamentului (UE) 2018/1724.**

Din punct de vedere tehnic propunerea de modificare presupune pentru acces la date următoarele funcționalități pentru sistem sau atribuții ale autorităților competente în calitate de utilizatori ai datelor:

1. Sistemul va permite stabilirea unei liste a autorităților competente responsabile pentru zonele în care se aplică o procedură.
2. Accesul la informațiile transmise poate fi acordat numai autorității competente după ce este verificat temeiul legal conform procedurilor administrative.
3. Autoritățile competente incluse pe lista menționată mai sus păstrează datele privind activitatea în mod securizat și confidențial atât timp cât este necesar pentru scopurile menționate în cadrul legal. Autoritățile competente respective pot, în conformitate cu legislația să transmită date privind activitatea care nu includ niciun fel de date care cu caracter personal de exemplu: numerele de înregistrare și URL-urile.
4. Sistemul permite agregarea datelor privind activitatea și transmiterea acestora (de exemplu pentru institutul național de statistică și/sau către Eurostat).

1.3.3.2.Componente SDG - PDURo



Portalul Unic Digital (Single Digital Gateway) are trei componente care vor trebui implementate:

A) Componenta de informare a cetățenilor privind legislația și obligațiile aplicabile în domeniile ce se regăsesc în Anexa I la Regulamentul (UE) 2018/1724 al Parlamentului European și al Consiliului din 2 octombrie 2018;

B) Componenta de digitalizare a procedurilor menționate în Anexa II Regulamentul (UE) 2018/1724 al Parlamentului European și al Consiliului din 2 octombrie 2018, proceduri ce vor trebui oferite integral online;

C) Componenta de implementare a sistemului tehnic Once-Only („doar o singură dată") care va permite schimbul transfrontalier de documente administrative.

A. Componenta de informare privind legislația și obligațiile aplicabile în domeniile ce se regăsesc la Anexa I la Regulamentul (UE) 2018/1724 al Parlamentului European și al Consiliului din 2 octombrie 2018

Componenta de informare va fi instalată pe infrastructura platformei de cloud guvernamental. Informațiile existente vor fi migrate.

Funcționalități ale Portalului Digital Unic – PDURo

Conform articolului 2 alineatul (1) al Regulamentului, portalul unic digital constă într-o interfață comună pentru utilizatori administrată de Comisie („interfața comună pentru utilizatori”), care este integrată în portalul „Europa ta” și care oferă acces la paginile web relevante ale Uniunii și naționale.

Alineatul (2) al aceluiași Regulament prevede că portalul trebuie să ofere acces la:

a) informații privind drepturile, obligațiile și normele prevăzute în dreptul Uniunii și în dreptul intern, aplicabile utilizatorilor care își exercită sau intenționează să își exercite drepturile care decurg din dreptul Uniunii în materia pieței interne, în domeniile enumerate în Anexa I;

Prin PDURo, la care se vor conecta administrația publică centrală și alte autorități competente, se pot îndeplini la distanță, prin mijloace electronice, ansamblul procedurilor și formalităților necesare pentru accesul la activitățile de servicii ale acestora, în special declarațiile, notificările sau cererile necesare pentru obținerea autorizării, inclusiv cererile de înscriere într-un registru și orice cereri de autorizare necesare pentru exercitarea activităților de serviciu.

b) informații privind procedurile online și offline și linkuri către procedurile online, inclusiv prin procedurile vizate de anexa II și celelalte texte europene care intră în scopul Regulamentului Single Digital Gateway, stabilite la nivelul Uniunii sau la nivel național pentru a le permite utilizatorilor să își exercite drepturile și să respecte obligațiile și normele în materia pieței interne enumerate în anexa I;
c) informații și linkuri către serviciile de asistență și soluționare a problemelor enumerate în anexa III sau menționate la articolul 7 cărora cetățenii și întreprinderile li se pot adresa cu întrebări sau probleme legate de drepturile, obligațiile, normele sau procedurile menționate la literele (a) și (b) de la prezentul alineat.

Platforma e-guvernare.ro (care va fi integrata în PDURo) afișează un buton „Servicii de asistență și de soluționare a problemelor” care informează utilizatorii despre punctele de asistență disponibile la nivel național:

- Punctul de Contact Unic electronic;
- Punct de informare despre produs;
- Punct de informare despre produse pentru construcții;
- Centrul de asistență pentru recunoașterea calificărilor profesionale – Centrul Național de Recunoaștere și Echivalare a Diplomelor;
- Punctul Național de Contact – Asistență medicală transfrontalieră;
- Centrul European al Consumatorilor din România;

- EURES România – Portalul mobilității europene pentru forța de muncă.

Pentru a obține informații adecvate în vederea evaluării și a îmbunătățirii performanței portalului, Regulamentul obligă atât autoritățile competente, cât și Comisia să colecteze și să analizeze datele referitoare la utilizarea diferitelor domenii de informații, a diverselor proceduri și servicii oferite prin intermediul portalului. Colectarea de statistici vizează utilizatorii, precum date referitoare la numărul de vizite pe anumite pagini web, numărul de utilizări din cadrul unui stat membre în comparație cu numărul de utilizatori din alte state membre, termeni de căutare utilizați, paginile web cele mai vizitate, paginile web de referință sau numărul, originea și obiectul cererilor de asistență. Aceste statistici au drept obiectiv îmbunătățirea calității serviciilor oferite.

Articolul 24 din Regulamentul Single Digital Gateway prevede obligația autorităților competente din statele membre și a Comisiei de a se asigura că se colectează statistici în legătură cu vizitele utilizatorilor pe portalul digital unic și pe paginile web cu care este conectat portalului. Acesta prevede, de asemenea, obligația autorităților competente, a furnizorilor de servicii de asistență și de soluționare a problemelor și a Comisiei de a colecta și a partaja, într-o formă agregată, numărul, originea și obiectul solicitărilor de servicii de asistență și de soluționare a problemelor și timpii de răspuns ai acestora.

Regulamentul de punere în aplicare (UE) 2020/1121 al Comisiei din 29 iulie 2020 referitor la colectarea și partajarea statisticilor privind utilizatorii și a observațiilor din partea utilizatorilor cu privire la serviciile portalului digital unic în conformitate cu Regulamentul (UE) 2018/1724 al Parlamentului European și al Consiliului.

Conform considerentului (4) al Regulamentului de punere în aplicare 2020/1121 din 29 iulie 2020, pentru a colecta statistici și observații din partea utilizatorilor, care sunt comparabile și utilizabile în scopurile prevăzute în Regulamentul (UE) 2018/1724 și pentru a facilita corelarea datelor cu serviciul conex, trebuie să se specifice datele contextuale care trebuie să fie puse la dispoziție împreună cu statisticile și observațiile din partea utilizatorilor. Aceste date contextuale trebuie să includă URL-ul și informații referitoare la conținutul paginii web relevante. Furnizorii de servicii trebuie să includă aceste informații ca etichete în metadatele paginilor web sau să le introducă direct în registrul pentru linkuri.

Pentru redarea automată a informațiilor de etichetare de pe paginile web, Comisia folosește un instrument denumit EC Crawler.

În vederea automatizării procesului la nivel național, prestatorul va trebui să dezvolte un instrument care permite colectarea automată centralizată a statisticilor prevăzute de Regulamentul Single Digital Gateway și de Regulamentul de punere în aplicare 2020/1121 și conectarea acesteia la API EC Crawler al Comisiei. (anexa I,II, III Regulament 2020/1121 respectiv punctele 11.7, 11.8, 11.9 din prezentul)

B. Componenta de digitalizare a procedurilor menționate în Anexa II, proceduri ce vor trebui oferite integral online

Regulamentul (UE) 2018/1724 prevede la articolul 6 care vizează procedurile oferite integral online că fiecare stat membru se asigură că utilizatorii pot să acceseze și să finalizeze, în întregime online, oricare dintre procedurile enumerate în Anexa II (punctul 11.3 din preentul) în cazul în care procedura relevantă a fost stabilită în statul membru în cauză.

Articolul 6 alineatul (2) fixează criteriile pentru ca procedurile să fie considerate integral online:

a) identificarea utilizatorilor, furnizarea de informații și de elemente justificative, semnarea și transmiterea finală pot fi realizate în întregime prin mijloace electronice de la distanță, prin intermediul unui canal de servicii care le permite utilizatorilor să îndeplinească cu ușurință și în mod structurat cerințele legate de procedură;

Cerințe funcționale minimale ale sistemului:

- identificarea utilizatorilor - procedurile trebuie să permită identificarea utilizatorilor folosind atributele precizate în Regulamentul eIDAS (Regulamentul (UE) 910/2014);
- sistemul trebuie să permită furnizarea de informații și de elemente justificative;
- sistemul trebuie să permită semnarea și transmiterea finală prin mijloace electronice de la distanță;

b) utilizatorii beneficiază de o confirmare de primire automată, cu excepția cazului în care rezultatul procedurii este livrat imediat;

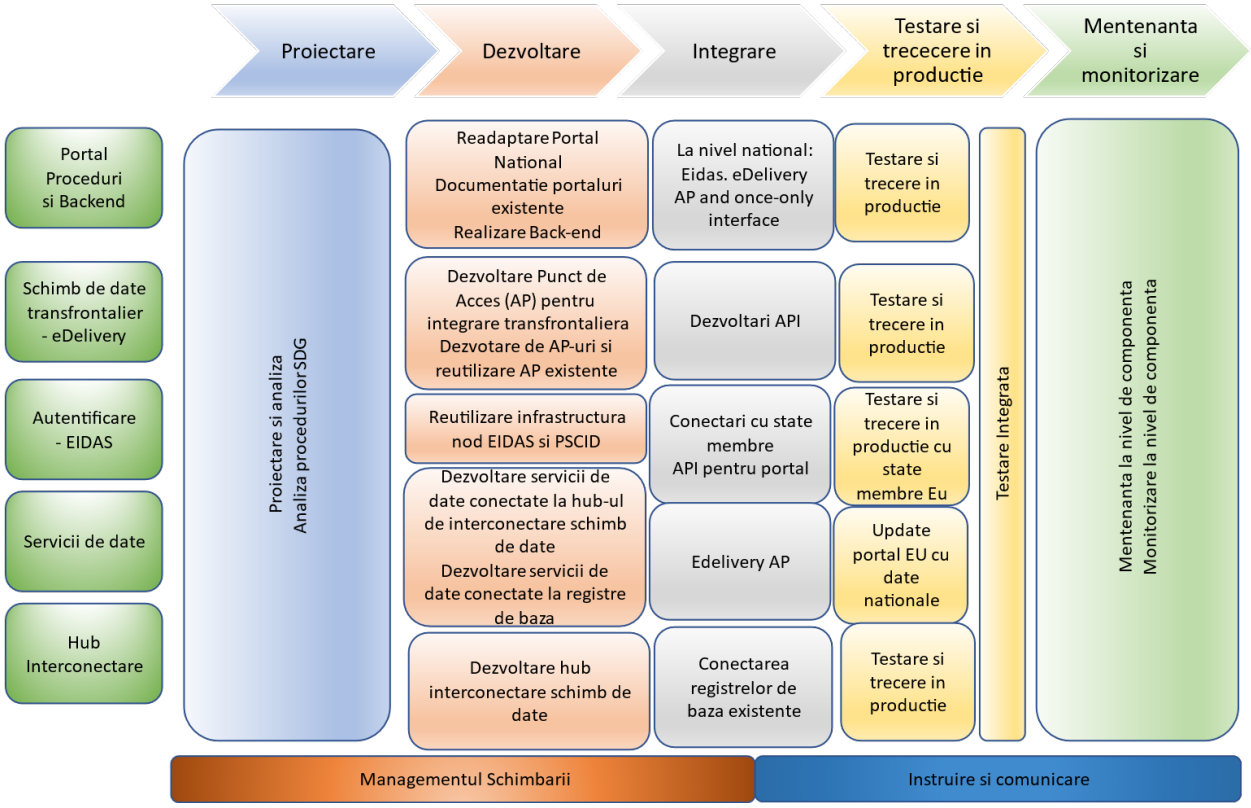
c) rezultatul procedurii este furnizat în format electronic sau, după caz, pentru a se conforma cu dreptul Uniunii sau dreptul intern aplicabil, este furnizat prin mijloace fizice;

d) utilizatorilor li se transmite o notificare electronică privind finalizarea procedurii.

Alineatul (3) stabilește situațiile în care statele membre pot deroga de principiul „***integral online”*** în ceea ce privește anumite proceduri enumerate în Anexa II a Regulamentului. Astfel, în situații excepționale, justificate de motive imperative de interes public în domeniile securității publice, sănătății publice sau combaterii fraudelor, obiectivul urmărit nu poate fi realizat în întregime online, statele membre pot solicita utilizatorului să se prezinte personal în fața autorității competente, ca etapă din procedură.

În astfel de situații excepționale, statele membre limitează această prezență fizică la ceea ce este strict necesar și justificat în mod obiectiv și se asigură că alte etape ale procedurii pot fi finalizate în întregime online. Statele membre se asigură, de asemenea, că cerința privind prezența fizică nu duce la discriminarea utilizatorilor transfrontalieri.

În cazul în care identifică astfel de proceduri, conform alineatului (4) al articolului sus-menționat, statele membre au obligația de a notifica și de a explica printr-un registru comun, accesibil Comisiei și celorlalte state membre, motivele pentru care ar putea fi necesară prezența fizică a utilizatorului pentru procedura exemplificată.



Analiza procedurilor SDG

Procedurile din Anexa II a Regulamentului (UE) 2018/1724 se vor analiza după cum urmează:

- Etapa 1 – Identificarea procedurilor care nu există la nivelul României

Regulamentul (UE) 2018/1724 impune obligația de a oferi procedurile enumerate în Anexa II doar dacă procedura relevantă a fost stabilită în statul membru. Așadar, primul pas reprezintă identificarea corectă a procedurilor existente în România. În urma acestei analize, va rezulta lista procedurilor pe care România va trebui să le ofere integral online.

- Etapa 2 – Identificarea acelor proceduri care pot fi deja considerate online sau au o componentă digitală

În urma analizei (al cărui exemplu superficial îl reprezintă capitolul de mai jos intitulat „Procedurile ce se regăsesc la Anexa II a Regulamentului (UE) 2018/1724), vor rezulta două liste: Proceduri online sau în curs de a deveni online/ Proceduri offline.

Atât pentru acele proceduri identificate drept proceduri online sau în curs de a deveni online, cât și pentru acele proceduri offline, prestatorul va realiza o nouă analiză mai detaliată a procedurilor administrative, conform exemplului din **Tabelul 4 - Efortul de analiză al procedurilor administrative românești pentru a permite implementarea Regulamentului Single Digital Gateway (Anexa II).** Această analiză va cuprinde cel puțin:

1) Identificarea procedurii la nivel național – prestatorul va trebui să determine dacă procedura identificată în Anexa II a Regulamentului există sau nu la nivel național. Mai mult, o procedură al cărei rezultat este menționat în Anexa II se poate traduce la nivel național în mai multe proceduri care sunt gestionate de autorități competente diferite.
   Ex: eveniment de viață **Aspecte legate de muncă** – Procedură *Notificarea modificărilor privind circumstanțele personale sau profesionale ale persoanei care primește prestații de securitate socială, relevante pentru prestațiile respective* care cuprinde la nivel național atât Beneficiile de asistență socială pentru prevenirea și combaterea sărăciei și riscului de excluziune socială (precum ajutorul social), cât și Beneficiile pentru susținerea copilului și a familiei ce au în vedere nașterea, educației și întreținerea copiilor (precum alocația de stat pentru copii) și Beneficiile de asistență socială pentru sprijinirea persoanelor cu nevoi speciale (precum drepturile acordate persoanelor cu handicap). Pe lângă acestea, cade sub incidența aceleiași proceduri a Anexei II indemnizația de șomaj, acordarea concediului medical și al indemnizației temporare de muncă, indemnizației pentru maternitate, pensia de invaliditate și pensia de urmaș;
2) Identificarea actelor necesare îndeplinirii procedurilor, care se traduce în limbajul Actului de implementare 2022/1463 a Regulamentului 2018/1724 prin cerințe în vederea îndeplinirii procedurilor administrative electronic prin intermediul sistemului

tehnic pentru schimbul transfrontalier automatizat de elemente justificative și aplicarea principiului „o singură dată” (sistemul tehnic „o singură dată” – *Once Only Technical System*). Identificarea acestor cerințe vor servi drept bază pentru efortul de digitalizare și integrare în sistem a procedurilor online sau parțial online, cât și a procedurilor disponibile doar offline la nivel național;

3) Identificarea documentelor administrative eliberate în urma îndeplinirii procedurilor administrative identificate în Etapa 2.2. și procedura eliberării documentului final este etapa în care prestatorul va identifica legislația aplicabilă procedurii administrative și autoritatea competentă pentru îndeplinirea procedurii. Astfel, pentru procedurile deja digitalizate va fi identificat actul normativ care permite aceasta, precum și legislația conexă care fixează etapele procedurii administrative.

   În ceea ce privește procedurile offline, prestatorul va realiza în plus o analiză a schimbărilor legislative necesare pentru digitalizarea procedurilor, conform cerințelor sistemului prevăzut de Regulamentul Single Digital Gateway, respectiv sistemul tehnic „doar o singură dată” și o foaie de parcurs în vederea digitalizării acestora. Foaia de parcurs va cuprinde cel puțin obiectivele urmărite, etapele pentru digitalizarea procedurilor și activitățile ce vor trebui efectuate.

Prestatorul va continua cu analiza procedurilor digitalizate total sau parțial urmărind:

1) Guvernanța procedurii digitale – analiza nivelului de digitalizare și a actorilor implicați din perspectiva implementării sistemului tehnic „doar o singură dată”, care sunt transformările ce trebuie efectuate pentru a digitaliza procedura și a o integra în platforma PDURo și în sistemul tehnic „o singură dată” ;
2) Elementele pe care le cuprinde documentul final ce ar trebui transmis de manieră transfrontalieră în vederea înregistrării documentului administrativ și a descrierii acestuia din Brokerul de dovezi (*Evidence Broker*) european;
3) Identificarea autorității/ autorităților (dacă sunt autorități locale) competente pentru eliberarea acestor documente;
4) Traducerea oficială a documentelor într-o limbă de circulație internațională, certificând astfel conținutul documentului original care va fi schimbat.

- Etapa 3 – Verificarea îndeplinirii criteriilor pentru a considera procedurile integral online

Pentru a verifica îndeplinirea criteriilor vizate de articolul 6 alineatul (2) al Regulamentului, va fi realizată o analiză a rezultatelor Etapei a 2-a, verificând nivelul de îndeplinire al criteriilor

fixate de Articolul 6 alineatul (2). Rezultatul va măsura așadar gradul de îndeplinire al criteriilor și următoarele etape pentru ca toate procedurile menționate în regulament să poată fi oferite integral online.

- Etapa 4 – Identificarea acelor proceduri care nu pot fi niciodată oferite integral online

Analiza vizează identificarea acelor proceduri care din motive imperative de interes public în domeniile securității publice, sănătății publice sau combaterii fraudelor, nu pot fi oferite integral online, astfel că statele membre pot solicita utilizatorului să se prezinte personal în fața autorității competente, ca etapă din procedură. Lista procedurilor ce nu pot fi oferite integral online, precum și motivele acestei decizii, vor fi notificate prin registrul comun Comisiei și celorlalte state membre. Aceste proceduri vor fi identificate dintre procedurile care acum se desfășoară complet offline (astfel de obstacole din motive de interes public vor fi identificate în Etapa a 3-a pentru acele procedurii care se desfășoară în acest moment parțial online).

- Etapa 5 – Modificarea acelor proceduri oferite online pentru a îndeplini toate criteriile Articolului 6 alineatul (1)

Elaborarea unor foi de parcurs individuale pentru fiecare procedură identificată în Etapa a 2-a și Etapa a 3-a și a criteriilor care trebuie îndeplinite (ex. Procedura poate permite autentificarea, dar nu schimbul de elemente justificative sau permite ambele procese, însă nu permite recepționarea rezultatului – în cazul în care legislația națională o permite).

- Etapa 6 – Elaborarea unor foi de parcurs individuale pentru a transforma procedurile oferite offline în proceduri integral online

Foile de parcurs individuale vor avea drept punct de plecare strategiile de digitalizare ale instituțiilor vizate de procedurile enumerate în Anexa II. În funcție de aceste strategii și intenții, foile de parcurs vor viza această transformare a procedurilor pe termen scurt/ mediu/ lung.

Analiza celorlalte proceduri care cad sub incidența Regulamentului Single Digital Gateway

Prestatorul va trebui să analizeze în același mod descris sumar în **Tabelul 4 - Efortul de analiză al procedurilor administrative românești pentru a permite implementarea Regulamentului Single Digital Gateway (Anexa II)**, urmând cele șase etape de analiză descrise mai sus, și procedurile prevăzute de celelalte acte normative europene care cad sub incidența Regulamentului Single Digital Gateway:

1) **Directiva 2006/123/CE** a Parlamentului European și a Consiliului din 12 decembrie 2006 privind serviciile în cadrul pieței interne transpusă în legislația națională prin

Ordonanța de urgență a Guvernului nr. 49/2009 privind libertatea de stabilire a prestatorilor de servicii și libertatea de a furniza servicii în România aprobată cu modificări și completări prin Legea 68/2010 și Hotărârea de guvern 922/2010 privind organizarea și funcționarea Punctului de contact unic electronic;

2) **Directiva 2005/36/CE** a Parlamentului European și a Consiliului din 7 septembrie 2005 privind recunoaștere calificărilor profesionale transpusă în legislația națională transpusă în legislația națională prin Legea nr. 200 din 25 mai 2004 privind recunoașterea diplomelor și calificărilor profesionale pentru profesiile reglementate din România, cu modificările și completările ulterioare și a legislației conexe necesare la momentul stabilirii procedurilor administrative prevăzute de Directivă ce vor trebui digitalizate, conform Regulamentului;
3) **Directiva 2014/24/UE** a Parlamentului European și a Consiliului din 26 februarie 2014 privind achizițiile publice și de abrogare a Directivei 2004/18/CE transpusă în legislația națională prin Legea nr. 98 din 19 mai 2016 și a legislației conexe necesare la momentul stabilirii procedurilor administrative prevăzute de Directivă ce vor trebui digitalizate, conform Regulamentului.

Livrabilele și activitățile prestatorului**:**

Etapa 1 – Identificarea procedurilor care nu există la nivelul României

Prestatorul va proceda la o analiză a procedurilor enumerate în Anexa II pentru a determina dacă procedura respectivă există sau nu în România.

În cazul acelor proceduri administrative care nu există, prestatorul va analiza dacă motivul pentru care această procedură nu există este logica administrației românești (pentru procedura Solicitarea finanțării studiilor în învățământul superior, cum ar fi granturile de studiu și împrumuturile acordate de un organism public sau o instituție publică, logica administrației românești nu prevede astfel de finanțări ale studiilor, precum sistemul olandez spre exemplu). Dacă răspunsul este afirmativ, prestatorul va exclude procedura din lista procedurilor în vederea implementării Regulamentului Single Digital Gateway.

Dacă răspunsul este negativ, iar motivul pentru care procedura aceasta nu există este că nu a fost încă implementată (ex: dovada de reședință, prevăzută de Lege, dar care nu este încă eliberată), prestatorul va discuta detaliile viitoarei proceduri cu reprezentanții Ministerului care are competență în elaborarea respectivei proceduri administrative. Reprezentanții ADR vor facilita discuțiile dintre prestator și autoritățile competente.

Rezultatul va fi un livrabil care mapează procedurile existente în România și autoritățile competente pentru îndeplinirea acestora și va sublinia procedurile prevăzute de Regulament. Analiza va arăta așadar lista procedurilor administrative pe care România va trebui să le ofere integral.

Înainte de definitivare, rezultatele analizei vor fi validate de reprezentanții ADR și reprezentanții autorităților competente.

Livrabilul 1 - Identificarea procedurilor prevăzute de Regulamentul SDG care nu există la nivelul României

Etapa 2 – Identificarea acelor proceduri care pot fi deja considerate online sau au o componentă digitală

Pentru fiecare procedură administrativă identificată în Livrabilul 1, prestatorul va realiza o primă analiză în trei etape:

1) Identificarea acesteia la nivel național. O singură procedură administrativă prevăzută de Regulament se poate traduce în mai multe proceduri administrative naționale, iar prestatorul are obligația de a analiza fiecare dintre aceste proceduri ex: Eveniment de viață Aspecte legate de muncă, descris mai sus.

Livrabilul 2.1 – Identificarea procedurilor administrative prevăzute de Regulamentul Single Digital Gateway la nivel național

2) Identificarea actelor necesare îndeplinirii procedurilor care se traduce în limbajul Actului de Implementare 2022/1463 prin cerințe în vederea îndeplinirii procedurilor administrative electronic prin intermediul sistemului tehnic OOTS

Livrabilul 2.2 – Identificarea cerințelor necesare îndeplinirii procedurilor administrative identificate în Livrabilul 2.1

3) Identificarea documentelor administrative eliberate în urma îndeplinirii procedurilor administrative identificate și a legislației aplicabile eliberării documentului și autoritatea competentă pentru îndeplinirea procedurii. Aceasta este etapa de analiză a modalității de operaționalizare a procedurii, care va arăta dacă aceasta este digitalizată (care este modalitatea de digitalizare a acesteia și în baza cărui text normativ) sau nu (care este textul normativ care prevede etapele pentru eliberarea respectivului document)

Livrabilul 2.3 – Documentele administrative rezultate și descrierea procedurilor pentru eliberarea acestora (din perspectivă operațională și legislativă – online/offline/parțial online)

4) Realizarea unei foi de parcurs pentru digitalizarea acelor proceduri administrative care au fost identificate drept proceduri administrative offline conform cerințelor sistemului prevăzut de Regulamentul Single Digital Gateway și de sistemul tehnic OOTS. Foaia de parcurs va cuprinde cel puțin obiectivele urmărite, etapele pentru digitalizarea procedurilor și activitățile ce vor trebui efectuate.

Livrabilul 2.4.1 – Elaborarea unui plan concret cu pași clari în vederea digitalizării a procedurilor conform cerințelor sistemului tehnic OOTS, pornind de la specificațiile tehnice ale sistemului și a obiectivelor urmărite de acesta, cerințelor serviciilor comune. Baza de lucru va fi reprezentată de livrabilele elaborate de grupul de lucru european Evidence-Mapping care vor fi furnizate prestatorului de reprezentanții Autorității pentru Digitalizarea României.

5) **Livrabilul 2.4.2 – Realizarea unor etape clare pentru digitalizarea procedurilor administrative care intră în scopul Regulamentului Single Digital Gateway, dar care nu sunt încă disponibile online la nivel național,** Analiza procedurilor administrative identificate în Livrabilul 2.3 drept proceduri digitalizate sau parțial digitalizate și identificarea compatibilității acestora cu OOTS și identificarea elementelor pe care le cuprinde documentul administrativ final ce ar trebui transmis prin sistemul tehnic în vederea înregistrării în Intermediarul de elemente justificative (*Evidence Broker) și* în Registrul Serviciilor de date (*Data Service Directory*)

Livrabil 2.5 - Ajutor în înscrierea documentelor administrative și a autorităților competente în serviciile comune ale Comisiei

6) Traducerea oficială a documentelor într-o limbă de circulație internațională, certificând astfel conținutul documentului original care va fi schimbat și sprijinirea autorității contractante în vederea înscrierii documentelor și autorităților care eliberează dovezi administrative în serviciile comune aferente SDG ale Comisiei

Analiza prestatorului referitoare la implementarea Regulamentului Single Digital Gateway:

Etapa 3 – Verificarea îndeplinirii criteriilor articolului 6 alineatul (2) al Regulamentului Single Digital Gateway pentru a considera procedurile integral digitalizate și elaborarea unei

foi de parcurs pentru activitățile ce vor trebui îndeplinite pentru a considera articolul 6 alineatul (2) perfect implementat

Livrabilul 3 – Analiza va măsura gradul de îndeplinire al criteriilor prevăzute de articolul 6 alineatul (2) de procedurile administrative identificate în Livrabilul 2.1 și va oferi sugestii clare pentru fiecare procedură administrativă analizată astfel încât aceasta să respecte condițiile serviciului public digitalizat complet, conform articolului 6 alineatul (2)

Etapa 4 –– Identificarea acelor proceduri care nu pot fi niciodată oferite integral online

Analiza vizează identificarea acelor proceduri care din motive imperative de interes public în domeniile securității publice, sănătății publice sau combaterii fraudelor, nu pot fi oferite integral online, astfel că statele membre pot solicita utilizatorului să se prezinte personal în fața autorității competente, ca etapă din procedură. Lista procedurilor ce nu pot fi oferite integral online, precum și motivele acestei decizii, vor fi notificate prin registrul comun Comisiei și celorlalte state membre. Aceste proceduri vor fi identificate dintre procedurile care acum se desfășoară complet offline (astfel de obstacole din motive de interes public vor fi identificate în Etapa a 3-a pentru acele procedurii care se desfășoară în acest moment parțial online).

Rezultatele Livrabilului vor fi validate de reprezentanții ADR și de reprezentanții Ministerelor care sunt autorități competente pentru procedurile administrative identificate.

Livrabilul 4 – Identificarea acelor proceduri care nu pot fi niciodată oferite integral online

C. Componenta de implementare a sistemului tehnic Once-Only („doar o singură dată”) care va permite schimbul transfrontalier

Articolul 14 al Regulamentului (UE) 2018/1724 reglementează modalitatea de implementare a sistemului tehnic pentru schimbul transfrontalier automatizat de elemente justificative și aplicarea principiului „doar o singură dată”.

Alineatul (1) fixează perimetrul de aplicare al sistemului tehnic pentru schimbul automatizat de elemente justificative între autoritățile competente din state membre diferite. Deși acesta vizează mai multe domenii, incluzând recunoașterea calificărilor profesionale reglementate prin Directiva 2005/36/CE a Parlamentului european și a Consiliului din 7 septembrie 2005 privind recunoașterea calificărilor profesionale, sistemul tehnic va trebui aplicat cu precădere procedurilor enumerate la Anexa II a Regulamentului (UE) 2018/1724.

Astfel, prin aplicarea alineatului (2), în cazul în care eliberează legal, în propriul stat membru și într-un format electronic care permite schimbul automatizat, elemente justificative care sunt relevante pentru procedurile online sus-menționate, autoritățile competente pun aceste elemente justificative și la dispoziția autorităților competente solicitante din alte state membre într-un format electronic care permite schimbul automatizat.

- **Obiectivul - Sprijin pentru punerea în aplicare a sistemului Once Only în temeiul Regulamentului Single Digital Gateway**

În vederea implementării Regulamentului SDG, portalul de informații „Europa ta" va fi extins, modernizat și legat de portalurile statelor membre UE - în România și integrat în PDURo. **Regulamentul SDG prevede informații privind drepturile și obligațiile, procedurile online și offline și serviciile de asistență care urmează să fie furnizate. În România, acestea sunt colectate prin intermediul rețelei de portal de gateway online și puse la dispoziție portalului ADR. În acest fel se vor transmite metadate în limbile română și engleză către portalul Europa ta. Scopul proiectului este realizarea unui portal național aliniat cu cerințele SDG.**

Regulamentul de punere în aplicare (UE) 2022/1463 al Comisiei din 5 august 2022 de stabilire a specificațiilor tehnice și operaționale ale sistemului tehnic pentru schimbul transfrontalier automatizat de elemente justificative și aplicarea principiului „doar o singură dată" în conformitate cu Regulamentul (UE) 2018/1724 al Parlamentului European și al Consiliului stabilește principalele componente ale arhitecturii OOTS (Once-Only Technical System), definește rolurile și obligațiile tehnice și operaționale ale Comisiei, ale statelor membre, ale solicitanților de elemente justificative, ale furnizorilor de elemente justificative și ale platformelor intermediare.

Regulamentul de punere în aplicare prevede obligația ca arhitectura OOTS să se bazeze, în măsura posibilului pe soluții reutilizabile, să fie neutră din punct de vedere al tehnologiei de implementare.

O astfel de soluție reutilizabilă dezvoltată la nivelul Uniunii este **sistemul de noduri eIDAS** prevăzut de Regulamentul de punere în aplicare (UE) 2015/1501 al Comisiei care, datorită faptului că permite comunicarea cu alte noduri ale rețelei eIDAS, poate procesa atât cererea de autentificare transfrontalieră a unui utilizator, cât și furnizarea respectivei autentificări. Nodurile eIDAS trebuie să le permită solicitanților de elemente justificative și, după caz,

furnizorilor de elemente justificative să identifice utilizatorii care solicită schimbul de elemente justificative prin intermediul sistemului, astfel încât furnizorii de elemente justificative să poată corela datele de identificare cu propriile evidențe.

În scopul **autentificării transfrontaliere a unui utilizator**, arhitectura OOTS trebuie aliniată cu Regulamentul nr. 910/2014 al Parlamentului European și al Consiliului (**Regulamentul eIDAS**). Mai mult, pentru a asigura securitatea serviciilor de livrare electronică transfrontalieră în scopul OOTS, sistemul va utiliza **puncte de acces pentru livrarea electronică (eDelivery)** pentru a crea o rețea de noduri pentru schimbul securizat de date digitale. Pentru a asigura flexibilitatea în aplicarea Regulamentului de implementare 2022/1463, statele membre trebuie să poată decide dacă doresc să dispună de unul sau mai multe puncte de acces eDelivery, în cadrul OOTS. Prin urmare, un stat membru trebuie să aibă posibilitatea să implementeze un singur punct de acces care să gestioneze toate mesajele eDelivery legate de OOTS adresate solicitanților de elemente justificative sau furnizorilor de elemente justificative printr-o platformă intermediară, după caz, sau, în mod alternativ, să implementeze mai multe puncte de acces la orice nivel ierarhic sau pentru domenii, sectoare sau niveluri geografice specifice ale administrațiilor sale publice.

Pentru a permite schimbul automatizat transfrontalier de elemente justificative, Comisia va constitui servicii comune la nivel european al sistemului tehnic OOTS:

a) Registrul serviciilor de date - catalogul european furnizorilor de elemente justificative și a tipurilor de elemente justificative eliberate de aceștia;

b) Intermediarul de elemente justificative (Broker de dovezi – *Evidence broker*) – ce permite solicitanților de elemente justificative să stabilească ce tipuri de elemente justificative emise în alte state membre corespund tipurilor de elemente justificative solicitate în contextul procedurilor pentru care respectivul solicitant de elemente justificative este competent;

c) Repertoriul semantic – ce oferă acces la modelul generic de metadate OOTS, care este conceput pentru a afișa metadatele care identifică în mod unic elementele justificative și furnizorul de elemente justificative. Astfel, pentru toate tipurile de elemente justificative structurate

convenite în cadrul grupului de coordonare a portalului, repertoriul semantic trebuie să conțină un model de date OOTS format din componentele prevăzute de Regulament de implementare 2022/1463 din 5 august 2022.

Platforma PDURo va reprezenta platforma intermediară națională care va asigura punctul de acces ce va gestiona toate mesajele eDelivery legate de OOTS. Platforma va permite autentificarea cetățenilor români prin intermediul schemei naționale ROeID (în curs de implementare) și va permite recunoașterea identității digitale a utilizatorilor europeni prin intermediul nodului eIDAS (pre-notificat la Comisie).

Având în vedere că principiul de bază al Regulamentului SDG este să nu pornești de la zero, ci să se clădească pe serviciile de informare și asistență existente la nivel UE, trebuie luate în considerare câștigurile deja existente. Astfel, multe state membre au făcut progrese excelente în lansarea programelor de e-guvernare și au dezvoltat foarte bune practici în acest proces care ar trebui folosit ca model pentru dezvoltarea PDURo. De exemplu, Franța, Olanda, Luxemburg, Cipru și Malta au reușit să depășească logica insulelor administrative și au dezvoltat pentru cetățeni și pentru mediul de afaceri portaluri pe deplin integrate. Franța gestionează și calitatea conținutului de pe portalul guvernamental cu un set elaborat de criterii de calitate și de indicatori de performanță. Mecanismul de feedback al utilizatorilor este în vigoare în majoritatea platformelor performante din Austria, Danemarca, Franța, și Suedia şi arată că este posibil să ghidezi utilizatorii prin zona complexă a regulilor online (a se vedea anexa 13 din documentul SWD(2017) 213 final Impact Assessment Accompanying the document Proposal for a regulation of the European parliament and of the Council on establishing a single digital gateway to provide information, procedures, assistance and problem solving services and amending Regulation (EU) No 1024/2012 {COM(2017) 256 final} {SWD(2017) 211 final} {SWD(2017) 212 final} {SWD(2017) 214 final}, pentru exemple suplimentare de bune practici naționale). Serviciile de informare și asistență au fost incluse în cadrul instrumentului juridic, ceea ce înseamnă că acestea trebuie să îndeplinească criteriile de calitate, să fie parte din acțiunile de promovare, să integreze mecanismul de feedback al utilizatorilor și să se conecteze la interfața de căutare a utilizatorului din cadrul SDG european. Alte inițiative oferă soluții pentru raportarea comună privind obstacolele care împiedică piața unică și, chiar dacă nu sunt acoperite ca atare de Regulamentul SDG,

acestea sunt complementare și contribuie la realizarea unui sistem fără sincope în mediul online pentru cetățeni și mediul de afaceri.

- **Ergonomie**

Ușurința de utilizare a serviciilor online ale administrației publice este o abordare centrală ADR. Pentru a consolida și mai mult acest lucru și pentru a îmbunătăți calitatea informațiilor și a serviciilor furnizate, Regulamentul SDG obligă statele membre ale UE să ofere și utilizatorilor posibilitatea de a oferi feedback cu privire la serviciile online oferite. Pe baza feedback-ului, Comisia UE va defini măsuri pentru îmbunătățirea calității serviciilor online în statele membre, ca parte a unui program de lucru anual. Colectarea statisticilor utilizatorilor ar trebui, de asemenea, să ajute la evaluarea și, dacă este necesar, la îmbunătățirea calității ofertelor online. Pentru paginile de informare, acestea vor fi colectate și în portalul ADR și transmise anonim Comisiei Europene.

La momentul elaborării documentației prezente, specificațiile tehnice ale sistemului tehnic Once-only sunt încă în curs de evoluție, iar Prestatorul va folosi la momentul implementării cele mai noi specificații din acel moment.

- **Activități și implementare**

O cerință centrală a Regulamentului SDG este digitalizarea completă a 21 pachete și proceduri denumite în mod specific (în anexa II) și analizate în capitolul <u>B. Componenta de digitalizare a procedurilor menționate în Anexa II și procedurile prevăzute de alte texte europene prin intermediul sistemului tehnic OOTS</u>. Aceste proceduri trebuie să poată fi gestionate integral online. În plus, principiul *o singură dată* urmează să fie implementat pentru aceste proceduri administrative și procedurile din patru directive UE și conectate la sistemul tehnic unic al EU. Acest lucru ar trebui să facă inutil ca cetățenii și companiile să ofere dovezi de mai multe ori.

PDURo, platforma intermediară OOTS

Prestatorul va dezvolta componenta Platformei PDURo care va reprezenta Platforma intermediară conform Regulamentului de implementare 2022/1463 și a specificațiilor tehnice ale sistemului OOTS.

Din punct de vedere tehnic aceasta va trebui să permită:

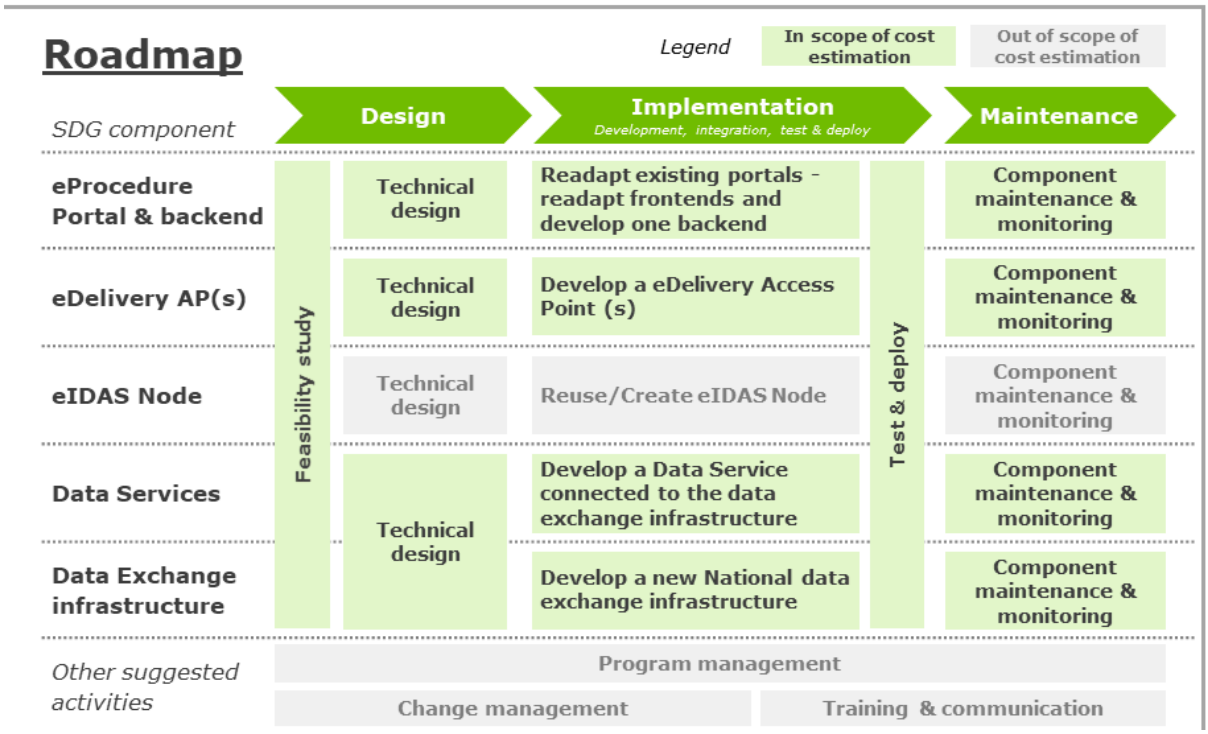
1) Autentificarea cetățenilor români prin intermediul schemei naționale de identificare ROeID (schemă în curs de implementare);

2) Autentificarea cetățenilor europeni prin intermediul nodului eIDAS (pre-notificat Comisiei);
3) Punctul de acces eDelivery care va gestiona toate mesajele eDelivery legate de OOTS adresate solicitanților de elemente justificative sau furnizorilor de elemente justificative;
4) Asigurarea conexiunii Platformei la serviciile comune europene, respectiv la Registrul Serviciilor de date, la Intermediarul de elemente justificative, precum și la Repertoriul semantic în cazul în care autoritățile competente dispun de elemente justificative sub forma datelor structurate.

În plus, prestatorul va implementa metodologia de înscriere a furnizorilor de elemente justificative și a elementelor justificative în serviciile comune europene, respectiv în Registrul Serviciilor de Date și în Intermediarul de elemente justificative.

În Registrul Serviciilor de Date vor fi înscrise toate elementele justificative (documentele administrative) inventariate și descrise în livrabilul din capitolul **B. Componenta de digitalizare a procedurilor menționate în Anexa II și procedurile prevăzute de alte texte europene prin intermediul sistemului tehnic OOTS.**

Prestatorul va identifica furnizorii de dovezi naționali după regula „furnizorul urmărește elementul justificativ". Astfel, dacă un document administrativ (element justificativ) este eliberat urmare a unei proceduri administrative aflate sub incidența Regulamentului Single Digital Gateway, autoritatea competentă pentru eliberarea respectivului document administrativ este furnizor de elemente justificative, așa cum este el înțeles prin Regulamentul de punere în aplicare 2022/1463 din 5 august 2022.



Portal eProceduri și back-end

Este un portal web pe care un stat membru, în cazul de faţă România, îl pune la dispoziție pentru a permite utilizatorilor, inclusiv utilizatorilor din alt stat membru B, să execute o procedură a unui stat membru UE. Interfața va oferi următoarele funcții: autentificarea utilizatorilor, managementul, selecția dovezilor și previzualizarea. Pe de altă parte, backend-ul portalului trebuie să includă funcționalități pentru a gestiona procedura și starea sesiunii, pentru a se integra cu sistemele informaționale și/sau baza de date și pentru a efectua transformarea datelor sau a formatului, pentru a crea cereri de dovezi și pentru a transmite și a primi răspunsul la dovezi.

Activități:

- proiectare tehnică;
- dezvoltare portal pe infrastructura cloudului guvernamental;
- dezvoltare back-end;
- documente de proiectare pentru portalurile conectate la Portalul Digital Unic - PDURo.

eDelivery AP(s)

Este folosit pentru a solicita dovezi unui alt stat membru și pentru a le primi ca răspuns. Acest punct de acces trebuie utilizat pentru interacțiunile transfrontaliere (atât la cerere, cât și la primire).

Activități:

- proiectare tehnică;
- implementarea punctului de acces electronic AP de tip eDelivery.

eIDAS Node:

Nodurile eIDAS ale celor două state membre pot fi utilizate pentru autentificarea transfrontalieră. Această funcționalitate va fi accesată din partea front-end a portalului pentru proceduri online, ce implică autentificarea.

Activități:

- Reutilizarea infrastructurii nodului existent.

Servicii Date:

Serviciul de date este o componentă operată de autoritățile competente din statele membre ca răspuns la solicitările portalurilor eProcedure. Un serviciu de date trebuie să aibă două servicii de aplicație standardizate, o singură dată, un „Serviciu de interogare a dovezilor" și un „Servicii de preluare a dovezilor prin ID". Aceste servicii se bazează pe standardul OASIS RegRep4.

Activitate: Dezvoltarea serviciilor electronice pentru schimb de date.

Infrastructura Schimb de date

Dezvoltarea de la zero a unei infrastructuri națională de schimb de date care poate simplifica recuperarea dovezilor în interiorul granițelor țării (situate în registrele de bază ale țării sau bazele de date locale).

Activitate: Dezvoltarea hubului național de interconectare pentru Single Digital Gateway (descris în capitolul Hub de Interconectare).

- **Funcționalități și detalii tehnice ale sistemului OOTS**

Conform alineatului (3) al articolului 14, **sistemul tehnic va fi implementat și va trebui să permită:**

  - **Prelucrarea cererilor pentru furnizarea elementelor justificative la cererea expresă a utilizatorului**

Conform Actului de implementare, pentru a autentifica utilizatorii, solicitanții dovezilor se vor baza pe identificarea electronică (notificată conform Regulamentului 2014/910 - eIDAS). Pentru a solicita însă aceste dovezi, instituțiile abilitate să solicite aceste dovezi trebuie să fi fost sesizați de o cerere expresă în acest sens de către utilizatori (Articolul 11 și Articolul 12 din Actul de implementare).

- **Prelucrarea cererilor pentru furnizarea elementelor justificative care urmează să fie accesate sau partajate**

Conform Actului de implementare, instituțiile abilitate să solicite dovezile trebuie să transmită cererea către furnizorii (providers) de dovezi împreună cu o serie de elemente enumerate la Articolul 13 (Cererea de furnizare de elemente justificative), care include printre altele identificatorul unic al utilizatorului, tipul de dovada necesară, procedura vizată, dar și data și ora la care solicitarea a fost primită.

- **Schimbul de elemente între autoritățile competente**

Elementele nu pot fi schimbate înainte de a i se oferi utilizatorului un preview al dovezii (Articolul 14 al Actului de implementare). Cererile pentru eliberarea dovezilor și dovezile vor fi procesate prin punctele de acces eDelivery (eDelivery Access Points – Articolul 15 – Rolul în schimbul de elemente justificative).

Dovezile nu vor fi eliberate de furnizorii (providers) de dovezi decât dacă au reușit să identifice fără echivoc utilizatorul și (dacă este cazul) atributele transmise pentru eliberarea dovezii (Articolul 16 – Corelarea identităților și a elementelor justificative).

- **Prelucrarea elementelor justificative de către autoritatea competentă solicitantă**

Autoritățile competente solicitante trebuie să se asigure că solicitanții sunt conectați la nodul eIDAS pentru a permite autentificarea utilizatorilor, iar statele membre trebuie să se asigure că punctele de acces eDelivery sunt instalate și configurate în portalurile solicitanților, în serviciile de date ale furnizorilor de dovezi sau în platformele intermediare.

- **Asigură confidențialitatea și integritatea elementelor justificative**

Pentru a demonstra confidențialitatea și integritatea elementelor justificative, atât solicitanții dovezilor cât și furnizorii acestora vor trebui să afișeze timp de 12 luni, cel puțin, dovada solicitării dovezilor cu elementele aferente, informațiile incluse în răspunsul pentru eliberarea dovezii și data privind evenimentul eDelivery privind schimbul de dovezi/ răspunsuri/ erori (Articolul 17 din Actul de implementare – Sistemul de înregistrare).

- **Asigură posibilitatea utilizatorului de a vizualiza elementele justificative care urmează să fie utilizate de către autoritatea competentă solicitantă și să aleagă dacă continuă sau nu cu schimbul de elemente justificative**

Actul de implementare vizează la articolul 14 – Redirecționarea utilizatorului către furnizorul de elemente justificative, funcționalitatea ca utilizatorul să previzualizeze dovada eliberată de furnizor și să aleagă dacă o folosește sau nu.

- **Asigură un nivel adecvat de interoperabilitate cu alte sisteme**

Sistemul tehnic OOTS trebuie să fie interoperabil cu portalurile care oferă procedurile menționate în Anexa II. Statele membre vor trebui să asigure integrarea acestor portaluri cu acelea ale solicitanților de dovezi, cu registrele electronice naționale și, acolo unde este aplicabil, cu serviciile comune (data service repository/ evidence broker/ semantic repository), conform articolului 14 al Actului de implementare.

- **Asigură un nivel înalt de securitate pentru transmiterea și prelucrarea elementelor justificative**

Solicitanții de dovezi specifică exact nivelul de securitate (*assurance*) așteptat pentru dovezi, precum și nivelul de securitate al elementelor justificative transmise (Articolul 5 alineatul (3) (a), alineatul (5) – Data service directory).

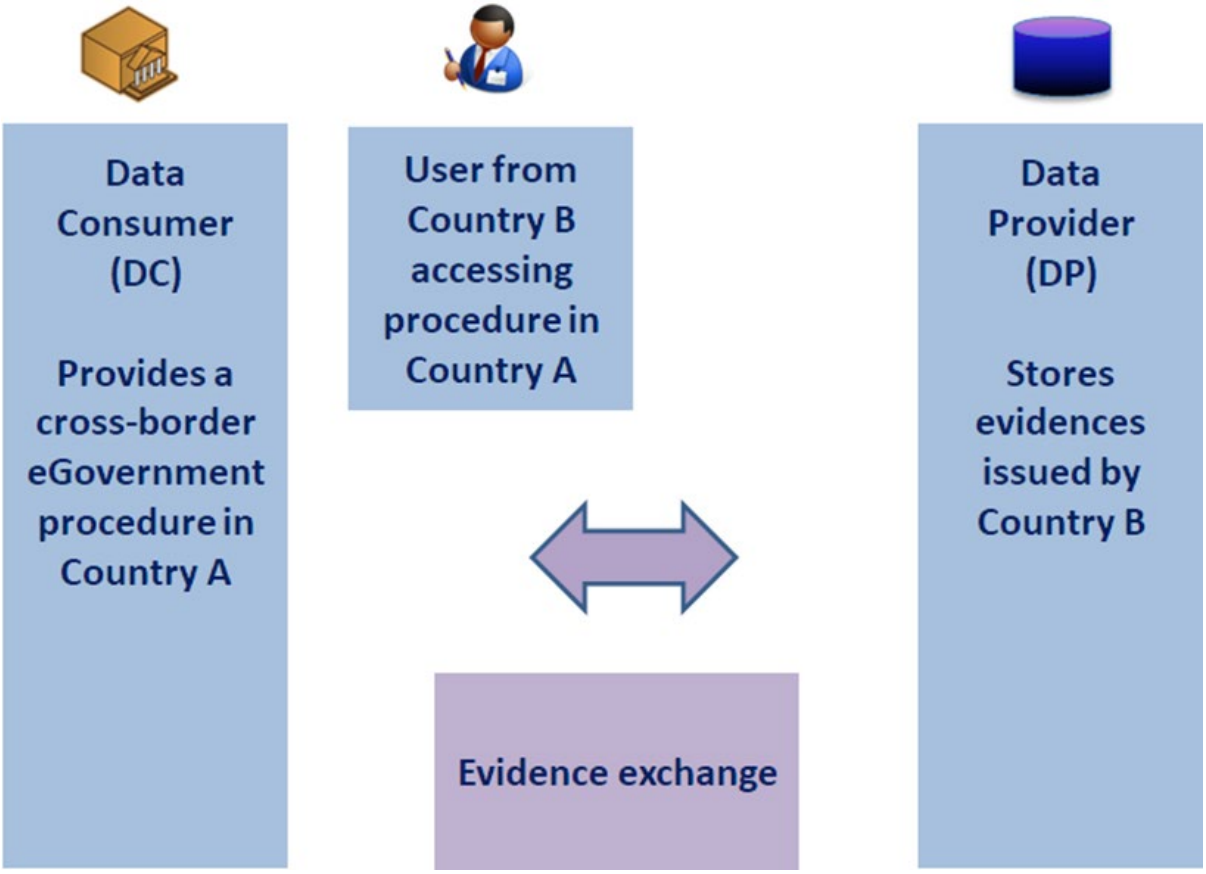
- **Nu prelucrează elemente justificative dincolo de ceea ce este necesar din punct de vedere tehnic pentru schimbul de elemente justificative și numai pe durata necesară în acest scop**

- **Principalele componente și specificații ale sistemului tehnic OOTS**
  - **Once Only**

Arhitectura soluției OOTS furnizează o imagine pentru funcționalități și design tehnic, care contribuie în mare măsură la implementarea *Schimbului de dovezi* la nivel transfrontalier în cadrul Uniunii Europene.

Procesul de schimb date transfrontalier pentru documente de tip evidenta este nucleul arhitecturii soluției care asigura principiul "*once only*". Pentru aplicarea Principiului O singură dată, un Consumator de Date are nevoie de un anumit tip de date, pentru a executa corect o procedură. Pentru a face acest lucru, există mai mulți pași ai proceselor care trebuie executate cu mai multe interacțiuni care trebuie să aibă loc între serviciile centrale ale infrastructurii OOTS și sistemele actorilor.

Figură – Arhitectura soluției OOTS



Sursa: https://wiki.ds.unipi.gr/display/TOOP/Conceptual+Architecture

- **Utilizator**

Utilizatorul este actorul care inițiază execuția unei proceduri în cadrul uni sistem de tip Sistem Data Consumer. În cazul schimbului transfrontalier de probe/evidente Utilizatorul este din aceeași țară cu Furnizorul de Date (Țara B), în timp ce Consumatorul de Date se află într-o țară diferită (Țara A).

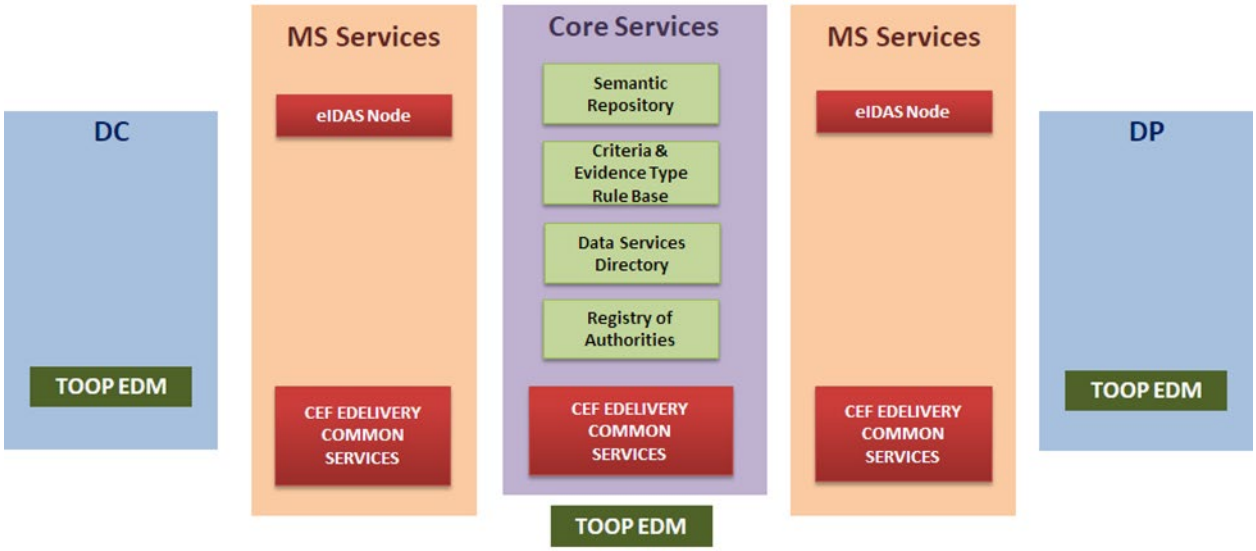
- **Solicitantul Elementelor justificative (Evidence Requester – ER)**

ER este termenul generic pe care îl folosim pentru serviciul public al unei organizații publice care execută o procedură pentru un anumit utilizator care este subiectul de date al procedurii. Pentru buna derulare a procedurii, ER trebuie să solicite date care îndeplinesc anumite cerințe ale procedurii. Aceste date pot fi furnizate fie manual de către utilizator, fie de către o Autoritate Competentă care acționează ca Furnizor de Date, în numele utilizatorului.

- **Furnizor de elemente justificative (EP – Evidence provider)**

EP este o organizație publică (de exemplu, Registrul de bază) sau o organizație privată care este capabilă să furnizeze date despre un subiect al datelor, la cererea unui EP.

Figură – Blocuri de arhitectură software



Sursa: https://wiki.ds.unipi.gr/display/TOOP/Conceptual+Architecture

- **eIDAS Node**

  Nodul eIDAS oferă un mijloc de autentificare transfrontalieră a Utilizatorului.

- Registrul de reguli pentru criterii și tipuri de dovezi **(Criterion & Evidence Type Rule Base (CERB)**

CERB este un sistem central care mapează seturi specifice de date ca dovezi care dovedesc cerințe specifice. DC consultă CERB pentru a afla ce tip de Date (Setul de date) poate fi solicitat ca dovadă pentru un anumit Utilizator, ținând cont de țara și/sau jurisdicția Utilizatorului.

- **Director de servicii de date (DSD)**

DSD este un serviciu central care acționează ca un catalog de seturi de date pe care DP-urile le pot furniza la cerere. Leagă anumite DP-uri cu seturi de date, astfel încât DC să le poată descoperi și să trimită cereri de probe.

- **Registrul Autorităților (RoA)**

Registrul Autorităților este un serviciu de bază care enumeră, pentru administrațiile publice din statele membre UE, procedurile pentru care aceste administrații sunt autorizate să solicite anumite tipuri de probe. Registrul autorităților poate completa și poate oferi un context pentru, dar nu este un înlocuitor, cererea/intrarea explicită a utilizatorului.

- **Servicii comune CEF eDelivery**

Service Metadata Publisher (SMP) and Business Document Metadata Service Location (BDXL)

Împreună, serviciile de localizare a serviciilor de metadate a documentelor de afaceri și a editorului de metadate a serviciilor furnizează metadatele despre punctele de acces eDelivery utilizate de consumatorii și furnizorii de date în procesul de schimb de dovezi.

Punct de acces CEF eDelivery

CEF eDelivery ajută actorii să facă schimb de date și documente electronice între ei într-un mod fiabil și de încredere. Soluția CEF eDelivery se bazează pe un model distribuit numit „modelul în 4 colțuri". În acest model, sistemele back-end ale utilizatorilor nu fac schimb de date direct între ele, ci fac acest lucru prin puncte de acces. Aceste puncte de acces sunt conforme cu aceleași specificații tehnice și, prin urmare, sunt capabile să comunice între ele.
Drept urmare, utilizatorii care adoptă CEF eDelivery pot face schimb de date cu ușurință și în siguranță, chiar dacă sistemele lor IT au fost dezvoltate independent unul de celălalt.

Modelul de date de schimb TOOP (EDM)

Modelul de date de schimb de mesaje oferă un model de mesaj bazat pe standarde care este utilizat pentru a exprima uniform cererile și răspunsurile de probe.
Pentru blocurile arhitecturale se vor utiliza blocurile arhitecturale puse la dispoziție de Comisia europeană, precum: https://ec.europa.eu/digital-building-blocks/code/projects/OOP
Comisia europeană publică codul open source în mod transparent: https://ec.europa.eu/digital-building-blocks/code/projects.

1.3.3.3.Documentație suplimentară

- O serie de workshopuri privind evaluarea procedurilor:

https://ec.europa.eu/digital-building-blocks/wikis/display/SDGOOPE/SDG+OOP+Evidence
https://ec.europa.eu/digital-building-blocks/wikis/display/SDGOOPE/1+-+Workshop+Report+-+Requesting+proof+of+registration+of+birth

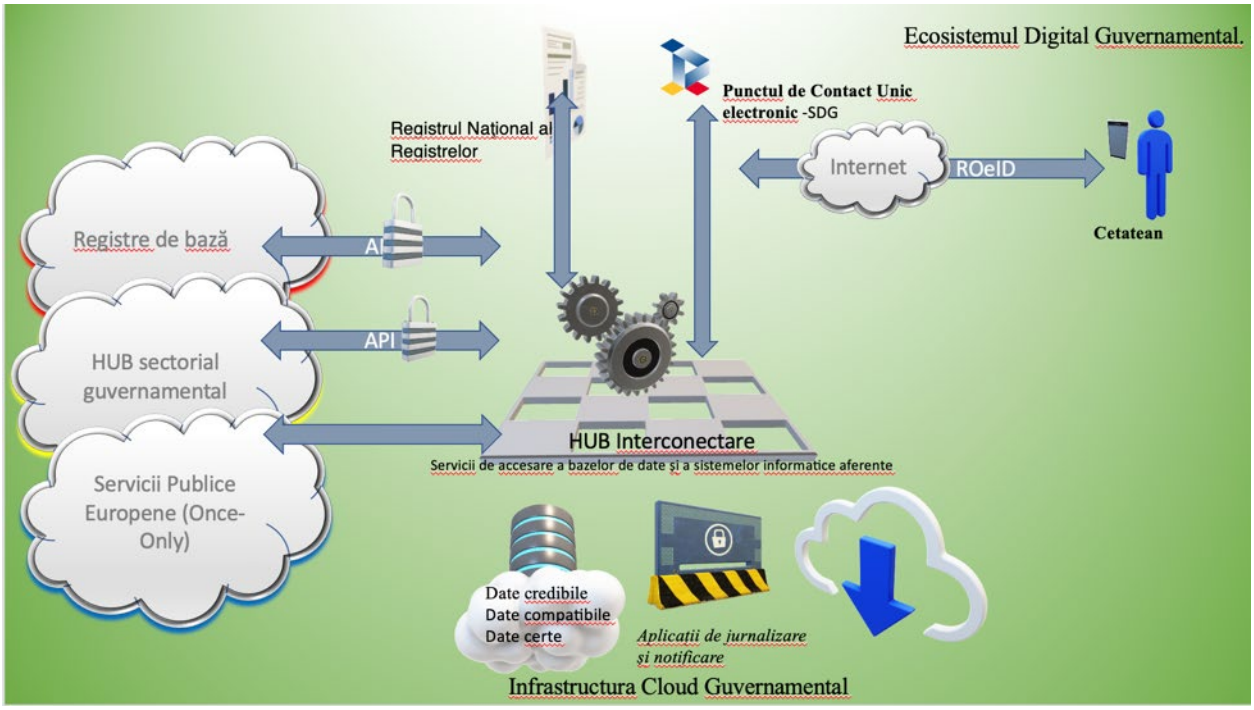
- Detalierea arhitecturii sistemului tehnic OOTS, prezentată anexat în documentul **„Once Only Technical System - architecture"**

1.3.4. HUB de Interconectare

HUB-ul de interconectare va trebui să permită un sistem de management al API-urilor prin care vor fi interconectate sistemele informatice ale administrației publice.

HUB-ul de interconectare va trebui să permită inițiativele de tip Open Government prin punerea la dispoziție a informațiilor către terțe părți.

HUB-ul de interconectare va avea următoarea structură:



HUB-ul de interconectare va fi implementat folosind soluția definită la capitolul "Componentele software".

*1.4.*Obiectivul achiziției

Obiectivul achiziției constă în îmbunătățirea și simplificarea modalității de acces a cetățenilor la serviciile electronice guvernamentale, precum și punerea la dispoziție către instituțiile publice a unor instrumente digitale de management de procese și interconectare.

În cadrul proiectului se vor integra și implementa cerințele funcționale ale PCUe, SDG și ale HUB-ului de interconectare așa cum sunt prezentate mai sus.

Obiectivele specifice sunt:

- **Modernizarea serviciilor publice prin digitizare și retehnologizarea proceselor operaționale.** Cetățenii și întreprinderile pot accesa cu ușurință, printr-un singur portal guvernamental, informații și servicii electronice furnizate de autoritățile publice centrale. Aceste servicii pot fi accesibile prin diferite canale: Internet, mobil, chioșcuri, terminale interactive și altele.
- **Optimizarea operațiunilor guvernamentale prin interconectarea, consolidarea activelor IT și reutilizarea datelor.** Cetățenii vor beneficia de un guvern conectat și eficient. Instituțiile publice vor opera și vor interacționa printr-o platformă tehnologică comună pentru a oferi servicii de înaltă calitate. Cetățenii vor putea să ofere date cu caracter personal guvernului o singură dată, iar instituțiile publice vor putea reutiliza aceste date pentru furnizarea de servicii.
- **Digitizarea serviciului public.** Portalul unic al guvernului - PDURo- va simplifica accesul electronic și utilizarea serviciilor publice. Paginile web ale guvernului vor fi revizuite și consolidate, iar accesul electronic la serviciile publice va fi integrat în portalul unic, astfel încât oamenii să poată găsi informații și servicii mult mai ușor. Măsurile de securitate ale portalului guvernamental vor fi sporite pentru a răspunde noului rol al portalului în tranziția de la serviciile de informare la serviciile interactive și tranzacționale. Cetățenii vor avea o experiență personalizată în interacțiunile lor cu autoritățile și vor beneficia de servicii de calitate pentru clienți.

  Implementarea Regulamentului (UE) 1724/2018 prevede minim:

  - instituirea și funcționarea unui portal digital unic, care să ofere cetățenilor și întreprinderilor un acces ușor la informații de înaltă calitate, la proceduri eficiente și la servicii eficace de asistență și soluționare a problemelor în ceea ce privește normele Uniunii și normele naționale aplicabile cetățenilor și întreprinderilor care își exercită sau intenționează să își exercite drepturile care decurg din dreptul Uniunii în domeniul pieței interne, în sensul articolului 26 alineatul (2) din TFUE;
  - utilizarea unor proceduri de către utilizatorii transfrontalieri și punerea în aplicare a principiului „doar o singură dată” în legătură cu procedurile enumerate în anexa II la prezentul regulament și procedurile prevăzute în Directivele 2005/36/ CE, 2006/123/CE, 2014/24/UE și 2014/25/UE;

- raportarea cu privire la obstacolele existente pe piața internă bazându-se pe colectarea observațiilor formulate de utilizatori și a statisticilor de la serviciile acoperite de portal;
- punerea la dispoziție către instituțiile publice a unor instrumente digitale de management de procese și interconectare;
- realizarea hub-ului de interconectare a serviciilor publice electronice.

- **Dezvoltarea și accesibilizarea portalului de servicii** prin integrarea acestuia cu sistemele ROeID (platforma de management al identității electronice), integrarea și dezvoltarea SNEP (www.ghiseul.ro), nodul eIDAS național.
- **Realizarea HUB-ului de interconectare** care să ofere servicii de schimb de date care să permită schimbul de elemente justificative pentru procedurile online, prin aplicarea principiului „once-only".
- Integrări cu sistemele informatice ale instituțiilor publice.
- Integrarea cu nodul EIDAS și proiectul PSCID care va furniza identitatea digitala a cetățenilor români.
- Integrări cu serviciile electronice din portalurile instituțiilor guvernamentale sectoriale (sistemele de tip hub de servicii – ex. MAI, MMJS, ONRC, ANAF, Ministerul Educației, MAE).
- Realizarea Catalogului Serviciilor Electronice de eGuvernare și a Registrului Furnizorilor de Servicii Electronice de eGuvernare. În cadrul catalogului se vor publica Normele de referință pentru asigurarea schimbului de date între sistemele informatice deținute de participanții la schimbul de date;

Realizarea acestor obiective va schimba modul în care sectorul public gestionează și utilizează tehnologia. Aplicarea unui cadru de investiții IT inteligent și colaborarea extinsă cu sectorul privat vor conduce la o abordare coordonată și coerentă în IT, inclusiv planificarea strategică, bugetarea achizițiilor din domeniul IT, conceptualizarea, managementul, contractarea și controlul calității în IT.

Reformele bazate pe IT vor elimina practicile ineficiente ale interacțiunii guvernamentale cu cetățenii și funcționarea internă. Procesele ineficiente și redundante vor fi restructurate pentru a reduce duplicarea resurselor și a eforturilor prin standardizarea proceselor și partajarea resurselor similare.

Rezultate așteptate

- eficientizarea furnizării serviciilor publice furnizate de către autoritățile publice;
- reducerea costurilor necesare asigurării serviciilor publice furnizate;
- reducerea timpului în care cetățenii/operatorii economici beneficiază de aceste servicii;
- îmbunătățirea interacțiunii dintre cetățeni/mediul de afaceri cu autoritățile/instituțiile publice;
-asigurarea continuității serviciilor IT chiar și în cazul evenimentelor neașteptate cu impact major asupra dezvoltării normale a activităților.

1.5. Entități implicate

Din punct de vedere al actorilor care vor participa în fluxul de oferire al serviciilor publice electronice prin hub vor exista următoarele categorii importante de entități conectate:

- ADR – administratorul PDURo;
- Instituțiile administrației publice centrale și locale care oferă servicii de e-Guvernare;
- Instituții care se vor conecta și se vor interconecta cu PDURo;
- Ordinele profesionale;
- Cetățeni și mediul de afaceri.

2. CERINTE PRIVIND SOLUȚIA TEHNICĂ

2.1. Cerințe generale

Pentru implementarea proiectului cu succes este necesară realizarea următoarelor nivele:

- **la nivel legal** - Se va avea în vedere cap "Legislație".
- **la nivel organizațional** - alinierea proceselor operaționale presupune documentarea acestora într-un mod stabilit de comun acord și cu ajutorul unor tehnici de modelare general acceptate, inclusiv a informațiilor schimbate, astfel încât toate administrațiile publice participante la furnizarea serviciilor publice naționale și europene să poată înțelege ansamblul procesului operațional („end-to-end") și rolul care le revine în cadrul acestuia. Documentarea proceselor operaționale în cadrul proiectului se va realiza folosind tehnici de modelare general acceptate și presupune realizarea unor acorduri cu furnizorii de servicii din administrația publică asupra modului în care procesele vor trebui să fie aliniate pentru furnizarea unui serviciu public electronic către cetățeni și mediul de afaceri.

- **La nivel semantic** – Se va utiliza pentru setul minim de date vocabularul ISA Core Natural Person și Core Legal Persons
- **La nivel tehnic**

La nivel tehnic sistemul va trebui să asigure:

- platforma tehnică trebuie să suporte standarde deschise, fiind necesar a fi compatibilă cu serverele care respectă specificațiile non-proprietare și cu standardele existente;
- sistemul informatic trebuie proiectat, instalat, testat și pus în funcțiune ca un sistem complet integrat, scalabil, deschis, extensibil, flexibil, cu atribute înalte de securitate și disponibilitate, interoperabil cu alte sisteme informaționale, prin interfețe care vor fi descrise mai jos;
- utilizarea unei arhitecturi modulare care să permită o cuplare redusă între componente și în care responsabilitățile fiecărei componente sunt specializate;
- structura modulară permite adăugarea de noi module fără modificări în modulele software finalizate;
- pentru schimbul de date cu alte sisteme se solicită utilizarea de standarde deschise (de exemplu bazate pe XML/JSON);
- sistemul va expune o interfață bazată pe servicii WEB prin care aplicațiile instituțiilor pot transmite informație folosind un canal de comunicare *sistem la sistem*;
- sistemul propus va permite exportul informațiilor stocate în diverse formate (de exemplu bazate pe XML/JSON);
- Prestatorul va avea în vedere că toate cerințele și caracteristicile sunt minime și obligatorii;
- Prestatorul are obligativitatea de a include în propunerea tehnică și comercială toate componentele software și de servicii pe care le consideră necesare, chiar dacă acestea nu sunt individualizate sau solicitate în mod explicit.

Prezentul caiet de sarcini cuprinde regulile de bază care trebuie respectate astfel încât potențialii furnizori/ofertanți să elaboreze propunerea tehnică corespunzător cu necesitățile autorității contractante/beneficiarului. Cerințele impuse prin Caietul de sarcini sunt considerate ca fiind minimale. Specificațiile tehnice care indică o anumită origine, sursă, producție, un produs special, o marcă de fabricație sau de comerț, un brevet de invenție, standard, 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”.

Principiile care trebuie aplicate pentru implementarea PDURo sunt următoarele:

- Only once - definește conceptul de reutilizare și definirea unor servicii specializate cu funcțiuni clar definite ce sunt partajate cu diverși consumatori de servicii;
- Open services - presupune că fiecare funcționalitate implementată la nivelul unui sistem informatic să fie definită și ca un serviciu deschis, în acord cu politica de securitate și acces la date;
- One-stop-shop - presupune definirea unei interfețe unitare ce oferă un set complet de servicii într-o formă simplificată și coerentă. Într-o exprimare tehnică, aceasta presupune publicarea acestor servicii către consumatori externi sub forma unor cataloage de servicii corespunzător documentate;
- End2End - definește conceptul de consolidare și orchestrare unitara a diverselor funcțiuni unitare care vin să definească un proces de business complet, astfel, procesul de business va fi încapsulat unitar și ușor de utilizat ulterior (de exemplu, serviciul de aprobare al unei cereri este încapsulat unitar fără a fi nevoie de o cunoaștere în detaliu a procesului de aprobare, persoane, nivel de management, instituții ce sunt implicate în acest proces de aprobare etc);
- Digital by default - recomandă proiectarea fiecărui nou serviciu public sau intern ca serviciu digital, utilizând tehnologii moderne și inovatoare, ce poate fi consumat/accesat de diverse entități interne sau externe (cetățeni, instituții externe etc);
- Cloud ready - flexibilitatea de a beneficia de avantajele conceptului de Cloud (utilizarea de standarde deschise, API driven, scalabilitate, independenta de locația de instalare: on-prem, Cloud privat, Cloud public etc).

2.2. Prevederi de securitate

PDURo va reprezenta principalul punct de acces către servicii de eGuvernare, precum și faptul cĂ va gestiona date cu caracter personal, vor trebui respectate următoarele principii:

- **Confidențialitate** - asigurarea protecției datelor împotriva acceselor neautorizate.

- **Integritate** - asigurarea protecției, exactității și completitudinii datelor atât la nivelul modalității de stocare și gestionare a acestora, cât și pentru asigurarea împotriva manipulării frauduloase a datelor/informațiilor
- **Disponibilitate -** sistemul trebuie să asigure un proces de disponibilitate prin asigurarea redundanței tuturor componentelor sistemului pentru asigurarea păstrării coerentei și necoruperii datelor.

În cadrul proiectului se va implementa o serie întreagă de soluții și instrumente de securitate printre care enumerăm:

- asigurarea posibilităților de autentificare folosind două modalități de tipul carduri electronice cu certificate digitale, OTP, etc prin interconectarea cu sisteme de furnizare de identitate notificate conform regulamentului EIDAS (de exemplu PSCID) și reutilizare nod EIDAS conform documentației publice privind implementarea once-only.
- posibilitatea de criptare a datelor în trafic și în modul de stocare în baza de date;
- auditarea activităților realizate în sistem și a solicitărilor de acces la serviciile de e-Guvernare expuse prin intermediul platformei.

3. DESCRIEREA TEHNICĂ A PROIECTULUI

*3.1.*Cerințele funcționale ale sistemului

Cerințele funcționale care stau la baza sistemului integrat PDURo sunt:

- ***Consolidarea*** și ***interconectarea*** sistemelor IT existente în instituțiile publice;
- ***Alinierea*** - prin folosirea unei soluții de tip BPM - a sistemelor IT ***cu procesele guvernamentale*** în vederea realizării serviciilor publice electronice care vor fi puse la dispoziția cetățenilor;
- Noile sisteme IT vor fi dezvoltate pe baza unei ***arhitecturi orientate pe servicii (SOA)*** și a folosirii **HUB-ului de Interconectare**;
- Identificarea serviciilor electronice de eGuvernare existente și definirea ***Catalogului Național de servicii de e-Guvernare;***
- Este necesară ***implementarea unei platforme de livrare a serviciilor de e-Guvernare către cetățeni și mediul de afaceri,*** care să ofere o viziune de 360°

asupra serviciilor de tip e-Guvernare (așa cum acestea vor fi definite în „***Catalogul National de servicii de e-Guvernare”)*** prin extinderea PCU;

- ***Componentele platformei de livrare a serviciilor*** de e-Guvernare sunt:
  - **Portal de interacțiune** care să reprezinte canalul de interacțiune G2C/G2B/G2G și nivelul integrat de publicare a serviciilor;
  - **Infrastructura completă de integrare de tip HUB de servicii** (de tip API management) pentru:
    - procesele de livrare a serviciilor
    - interacțiunea umană cu fluxuri de aprobare, revizuire
    - aplicații existente, aplicații migrate, aplicații noi
  - **Integrarea** cu HUB-urile de servicii sectoriale (de ex. MAI, ONRC, MMJS, ANAF), platforma guvernamentală de identități electronice (PSCID), nodul național eIDAS
- **Obligativitatea utilizării datelor primare**

Instituțiile și autoritățile publice au obligația de a utiliza platforma de interconectare pentru accesarea datelor necesare furnizării serviciilor publice electronice și la ghișeu.
Interconectarea este definita în OUG89/2022 ca fiind un proces care constă în totalitatea activităților operaționale, procedurale și tehnice necesar a fi realizate în vederea transmiterii/accesării datelor dintr-un sistem informatic, care furnizează servicii publice electronice în Cloudul privat guvernamental;

Mijloace tehnice pentru furnizarea G2G a unor dovezi sau certificări ale datelor deja colectate. Datele utilizate în furnizarea serviciilor publice trebuie preluate exclusiv din registrele de bază disponibile prin intermediul platformei.
Mijloace tehnice pentru distribuirea sau reutilizarea informației într-o manieră transparentă și securizată, cu respectarea principiului colectării și stocării exclusiv a informațiilor necesare și a regulilor de protecție a datelor personale.
Datele furnizate prin platforma de interconectare au aceeași valoare juridică cu datele conținute în documentul prezentat fizic care conține sau confirmă datele respective, a unei copii conforme cu originalul sau a unui document electronic semnat cu semnătură electronică calificată. Pentru managementul disputelor toate operațiile necesare se vor jurnaliza.

În scopul verificării legalității prelucrării datelor cu caracter personal, automonitorizării și asigurării integrității și securității corespunzătoare a datelor, administratorul platformei cloud

guvernamental are obligația de a stoca informații cu privire la toate acțiunile derulate prin intermediul platformei (jurnale) și de a prezenta în mod transparent și nemijlocit titularului datelor informații despre colectarea, accesarea, modificarea, combinarea, dezvăluirea, reutilizarea sau ștergerea datelor cu caracter personal. Jurnalele nu vor fi supuse niciunor modificări și se vor comunica la cerere către ANSPDCP, către responsabilul cu protecția datelor cu caracter personal și, dacă este necesar pentru o investigație specifică, autorității competente. Jurnalele vor fi șterse după trei ani, cu excepția cazului în care datele pe care le conțin sunt necesare în continuare pentru asigurarea controlului.

- Funcționalități minime ale sistemului:
    - Livrarea serviciilor de e-Guvernare prin implementarea conceptului de portal One Stop Shop către cetățeni și mediul de afaceri;
    - Implementarea HUB-ului de Interconectare;
    - Realizarea Catalogului Național de servicii de e-Guvernare;
    - Realizarea în format electronic al registrului registrelor. Acesta va conține informații privind autenticitatea datelor conținute de aceste registre sub formă de listă de încredere, proceduri documentate pentru instituțiile și autoritățile publice care au acces la aceste date, fundamentele legale pentru transmiterea datelor, descrierea proceselor colectării datelor, precum și modalitatea utilizării datelor colectate. Lista de atribute de încredere și un mecanism de pentru utilizarea atributelor de încredere în cadrul regulamentului EIDAS;
    - Realizarea procedurii de conectare și participare la platforma de interconectare pentru SDG și la schimbul de date;
    - Implementarea unui modul de tip managementul proceselor (BPM) care va fi pus la dispoziția instituțiilor administrației publice pentru digitalizarea proceselor în relația cu cetățeanul;
    - Integrare cu platforma de management al identității electronice ROeID;
    - Interconectarea cu nodul eIDAS;
    - Modul de plată;
    - Multilingvism;
    - Conexiune securizată;
    - Statistică;
    - Configurare și emitere rapoarte

- Analiză și auditare

ADR își propune să realizeze un HUB pentru interconectare de tip middleware (în conformitate cu bunele practici europene prezentate mai sus) bazat pe tehnologii API prin care să realizeze interconectarea între sistemele informaționale ale instituțiilor publice în vederea implementării principiilor "digital-by-default" și "once only" în furnizarea serviciilor publice electronice pentru cetățeni și mediul de afaceri.

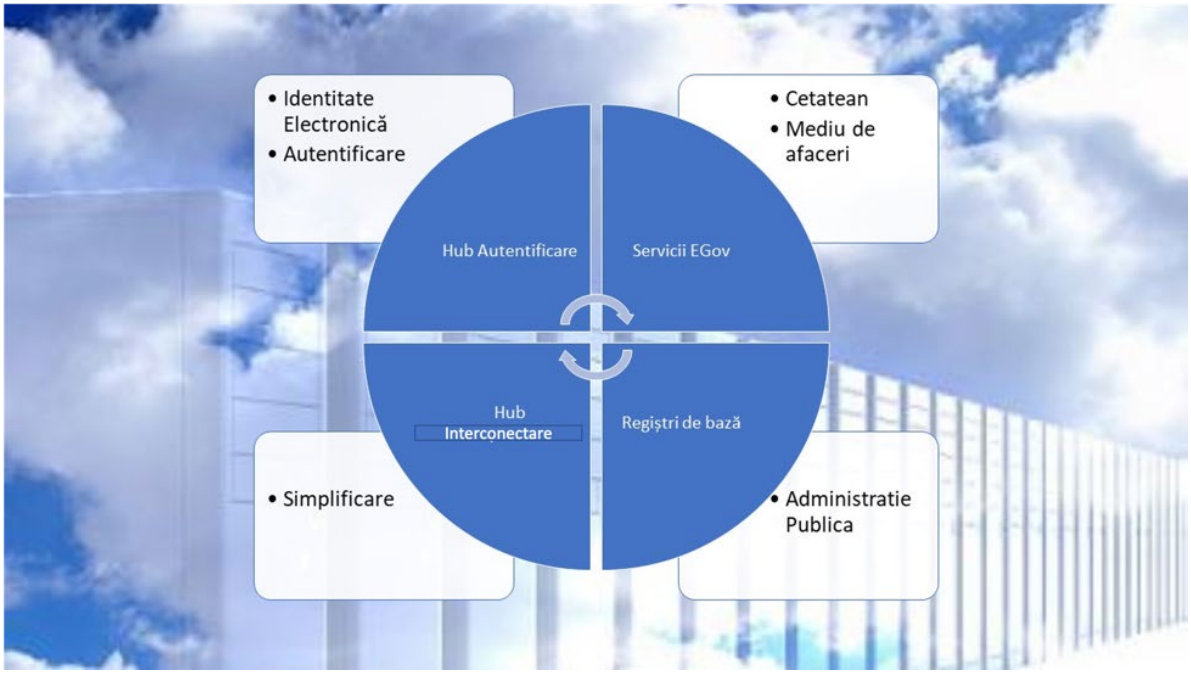
HUB-ul de interconectare va implementa următoarele tipuri de API-uri:

- **Open - Deschise rețelelor publice către publicul larg**: API-urile sunt de tip open/deschise (adică este necesară permisiunea de a le utiliza) și reprezintă punctul de acces pentru dezvoltatori pentru a utiliza sursele publice de date publice, cum ar fi informații despre recensământ sau alte date statistice similare pe care aceștia le folosesc pentru a crea aplicații pentru cetățenii.
- **Open - Deschise pentru dezvoltatori comerciali**: similar cu cele pentru publicul larg, dar destinate dezvoltatorilor care doresc să adune date disponibile în mod liber pentru utilizare, în general, în aplicații care pot fi vândute. Aceștia pot adăuga valoare prin combinarea ("mashing") datelor, de exemplu combinarea datelor privind rețelele de transport public cu datele de localizare disponibile pe telefonul inteligent al unui individ pentru a ajuta cetățenii să facă alegeri de călătorie în timp real. Dezvoltatorii au acces la API în orice moment, astfel încât aceștia să se poată asigura că este corectă comunicarea bidirecțională între anumite produse software.

  Accesul persoanelor fizice și persoanelor juridice de drept privat la date deținute de instituții publice și accesul instituțiilor publice la date deținute de primele: participanții la schimbul de date pot avea simultan rol de furnizor și de consumator de date.

  Costurile vor fi stabilite de administratorul platformei de interconectare și vor depinde de costurile operaționale ale administratorilor registrelor de bază consultate, respectiv ale administratorului platformei de Interconectare. Soluția va jurnaliza metrici care să poată cuantifica costul pentru operarea platformei pentru schimburile de date.
- **Furnizori de servicii publice/servicii securizate**: API-urile sunt deschise partenerilor și pot include, de exemplu, furnizorii de asistență medicală care, în anumite state membre, sunt interesați să împărtășească dosarele medicale sau să confirme eligibilitatea pentru tratament gratuit sau subvenționat utilizând datele deținute de o instituție guvernamentală.

- **Open Securizat pentru Instituții guvernamentale**: aceste API-uri sunt disponibile altor instituții guvernamentale și le permit să facă schimb de date numai după autentificarea lor. **Aceasta susține multe dintre principiile fundamentale ale guvernării digitale, permițând instituțiilor să colecteze datele despre un cetățean o singură dată și apoi să le împărtășească în siguranță.**
- **Open Securizat - Dezvoltatori servicii noi:** în mod similar cu cele de mai sus, dar în locul schimbului de date de tip inter-instituțional datele sunt consumate și apoi completate pentru a fi utile dezvoltatorilor de noi servicii în cadrul unei instituții guvernamentale. Acestea sunt folosite pentru a crea aplicații personalizate, în jurul datelor interne, pentru îndeplinirea scopurilor instituțiilor.



La nivel tehnic, transpunerea **Regulamentului (UE) 2018/1724 al Parlamentului European și al Consiliului din 2 octombrie 2018 privind înființarea unui portal digital unic (gateway) pentru a oferi acces la informații, la proceduri și la servicii de asistență și de soluționare a problemelor și de modificare a Regulamentului (UE) nr. 1024/2012 (Text cu relevanță pentru SEE.)** se realizează prin implementarea HUB-ului de Interconectare și a portalului pentru cetățean care vor fi parte componenta a cloudului guvernamental.

Baza platformei de interconectare pentru SDG, la nivel tehnic, este o magistrală de servicii.

Această magistrală trebuie să transporte mesaje structurate predefinite în catalogul semantic. HUB-ul trebuie să asigure securitatea mesajelor transmise.

Toate sistemele informatice conectate la platformă vor fi înregistrate într-un **catalog de sisteme**. Pentru a asigura coerența, înregistrarea în HUB se efectuează pe baza unui identificator de sistem al ADR.

Catalogul sistemelor va conține detalii tehnice despre sistemele informatice conectate, definițiile mesajelor pe care sistemele le pot trimite și le pot primi, precum și resursele de informații disponibile pentru interogările distribuite.

Sistemele vor fi conectate la platformă prin adaptoare care vor transforma, valida și cripta/decripta mesajele din/în formatul specific sistemului conectat, într-un format unificat, operat de platformă.

Procesul de conectare a unui sistem la platformă va fi reglementat la nivel tehnic și va include reguli de utilizare a standardelor și catalogului semantic, politici de versiune, precum și detalii tehnice privind conectarea la rețelele fizice, testarea/pilotarea și acceptarea sistemelor.

Toate serviciile HUB-ului de Interconectare vor fi disponibile pentru reutilizare în vederea uniformizării conectării sistemelor informatice ce informatizează serviciile publice electronice.

Pentru optimizarea sistemului portalului național al SDG se vor realiza, în conformitate cu documentația europeană a SDG:

- Sisteme de autentificare ale aplicațiilor de tip portal ale instituțiilor publice, pentru a realiza funcții de tip single sign-on cu acestea. Integrarea se va face cu proiectul PSCID și cu nodul EIDAS;
- Sisteme de integrare cu aplicațiile de tip management de documente folosite de către instituții, pentru automatizarea gestiunii solicitărilor pe întreaga durată de viață a acestora. Integrarea se va realiza prin dezvoltarea unor servicii web care se vor pune la dispoziția instituțiilor;
- Integrare cu sistemele de plată ale instituțiilor (inclusiv europene), prin integrarea acestora cu PDURo. Prin intermediul unor servicii web se vor putea vizualiza elementele de plată, respectiv se vor putea și trimite plățile realizate în aceste sisteme. De asemenea, se va permite direcționarea utilizatorului portalului PDURo către categoria de plată a instituției printr-un link creat dinamic, în conformitate cu prevederile portalului SDG european;

Interacțiunile complexe, care implică mai multe servicii conectate, vor fi orchestrate de soluția de tip API management.

Securitatea datelor și confidențialitatea în cadrul hub-ului de interconectare vor fi asigurate prin aplicarea unor mecanisme de securitate centralizate, în conformitate cu principiile fundamentale stabilite pentru prelucrarea acestor categorii de date.

HUB-ul de interconectare va asigura accesul la datele cu caracter personal în conformitate cu principalele condiții de prelucrare, stocare și utilizare a datelor respective, condiții prevăzute în regulamentele europene privind protecția datelor cu caracter personal, respectiv în actele normative naționale relevante, inclusiv cerințele pentru asigurarea securității datelor cu caracter personal la prelucrarea datelor, de către sistemele care prelucrează astfel de date.

HUB-ul de interconectare va implementa mecanisme pentru asigurarea unui nivel ridicat de disponibilitate, fiabilitate și performanță.

3.2.Arhitectura funcțională a sistemului

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

- *Nivel de prezentare* – portalul pentru accesul la serviciile de e-Guvernare expuse de furnizorii de servicii publice electronice;
- *Nivel de aplicații* – componentele necesare funcționării HUB-ului de Interconectare și a soluției de management al proceselor;
- *Nivelul de date* – componentele de stocare a datelor gestionate în cadrul platformei respectiv a datelor de auditare a activităților realizate în cadrul sistemului;
- *Nivel de suport* – componentele de administrare, monitorizare, backup, help desk și suport ale întregului sistem;
- *Securitate* – componentele de securizare a datelor la nivelul sistemului și la nivelul bazelor de date (criptare, firewall de date), auditare suplimentare față de securitatea oferită de cloudul guvernamental;
- *Infrastructura hardware și de comunicații* – vor fi asigurate de cloudul guvernamental

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

- Componenta de **portal** prin intermediul căreia se expun către cetățeni serviciile de e-Guvernare;

- Componenta de management al proceselor – de tip BPM;
- HUB-ul de interconectare– bazat pe tehnologie de tip API management;
- O soluție de **management al identităților electronice** care va asigura procesele:
    - Integrarea cu platforma identităților electronice PSCID;
    - Crearea și mentenanța identităților digitale, pentru identitățile care nu fac obiectul PSCID (exemplu: reprezentanți ai administrației); se estimează un număr de minim 10.000 de utilizatori;
    - Auditarea și raportarea informațiilor corespunzătoare proceselor executate în cadrul soluției
- O soluție de **management al accesului** care va asigura procesele:
    - Definirea privilegiilor și serviciilor care vor fi gestionate de sistemul HUB interconectare;
    - Autorizare și acces la serviciile electronice;
- O soluție de **stocare centralizată a profilelor de utilizatori** aferente identităților digitale **(atribute, roluri, grupuri, etc.)** care va asigura stocarea centralizată a tuturor informațiilor corespunzătoare conturilor de utilizatori, a credențialelor utilizate și a permisiunilor acordate pentru rolurile mapate pe privilegiile definite în cadrul sistemelor țintă
- O soluție de **autentificare securizată** care să permită utilizarea de credențiale de tipul „dispozitive de autentificare virtuale” (token/software de tip onetime password etc), respectiv utilizarea de instrumente anti-malware și anti-phishing prin care utilizatorul certifica ca serviciul utilizat este autentic (prin personalizare) și prin care se asigură securitatea autentificării împotriva atacurilor;
- O componenta de **analiză și raportare**;
- O componenta de gestiune a informațiilor necesare proceselor de **auditare;**
- Sistem de **gestiune a bazelor de date** în cadrul căruia se vor stoca toate instanțele bazelor de date aferente modulelor funcționale și portalului;
- **Soluții de securitate** pentru prevenirea accesului neautorizat la funcționalitățile sistemului respectiv la datele stocate pentru identitățile electronice;

- Componente suport ale sistemului de **administrare, monitorizare, asigurare proceduri de salvare** a datelor și aplicațiilor platformei.

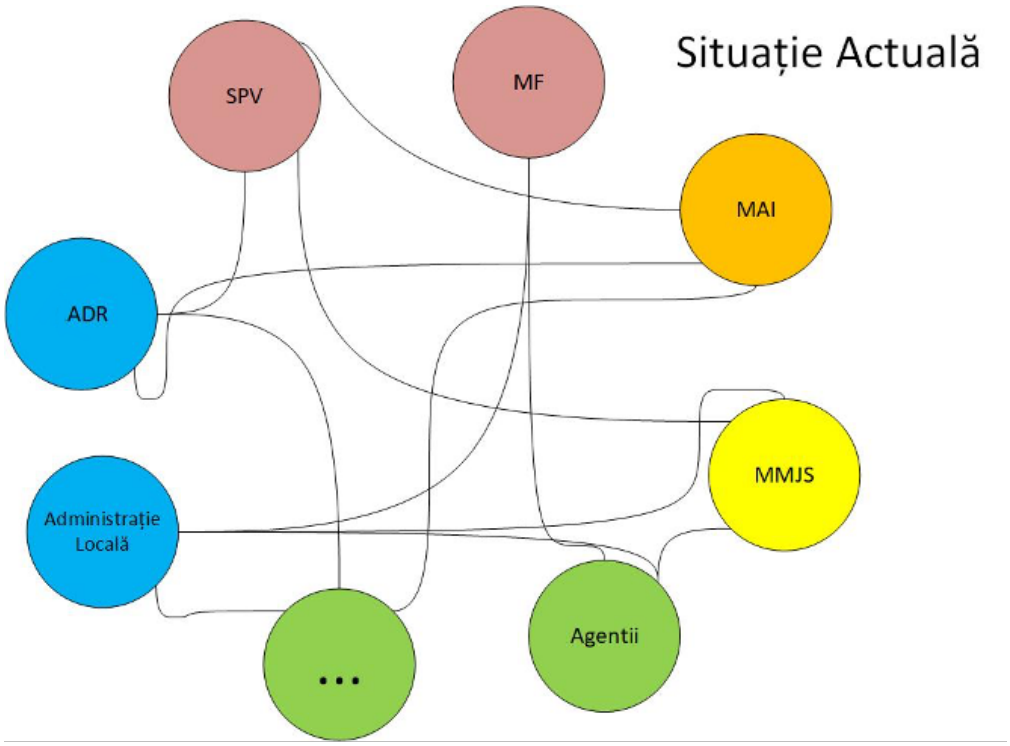


Fig 1. Situația actuală a schimbului de date între sistemele guvernamentale

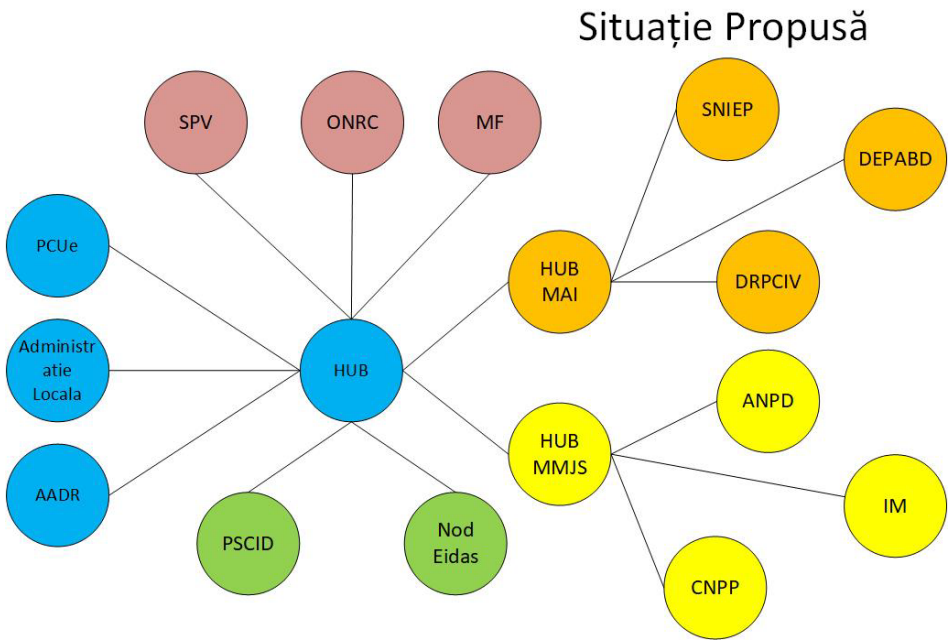
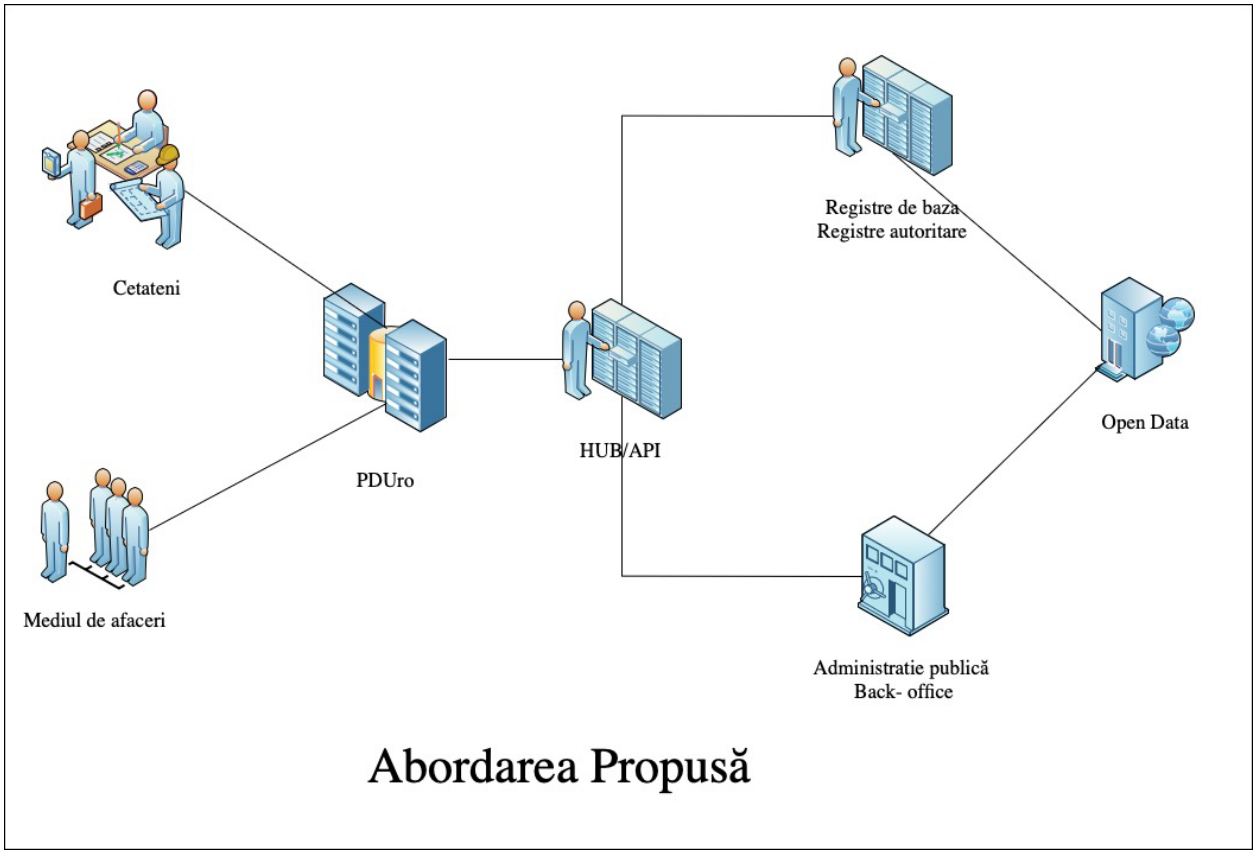


Fig 2. Situația propusă



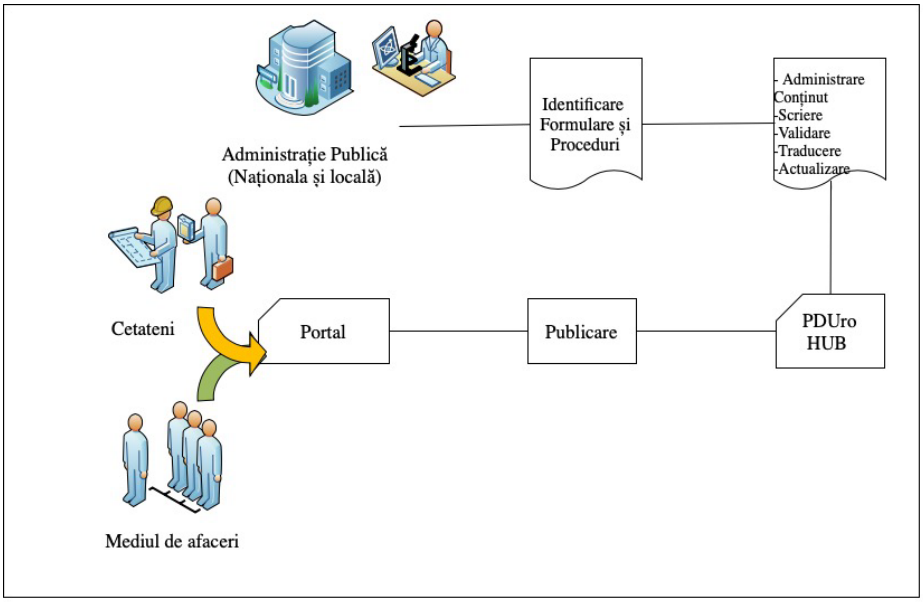


Fig 3. Arhitectura sistemului

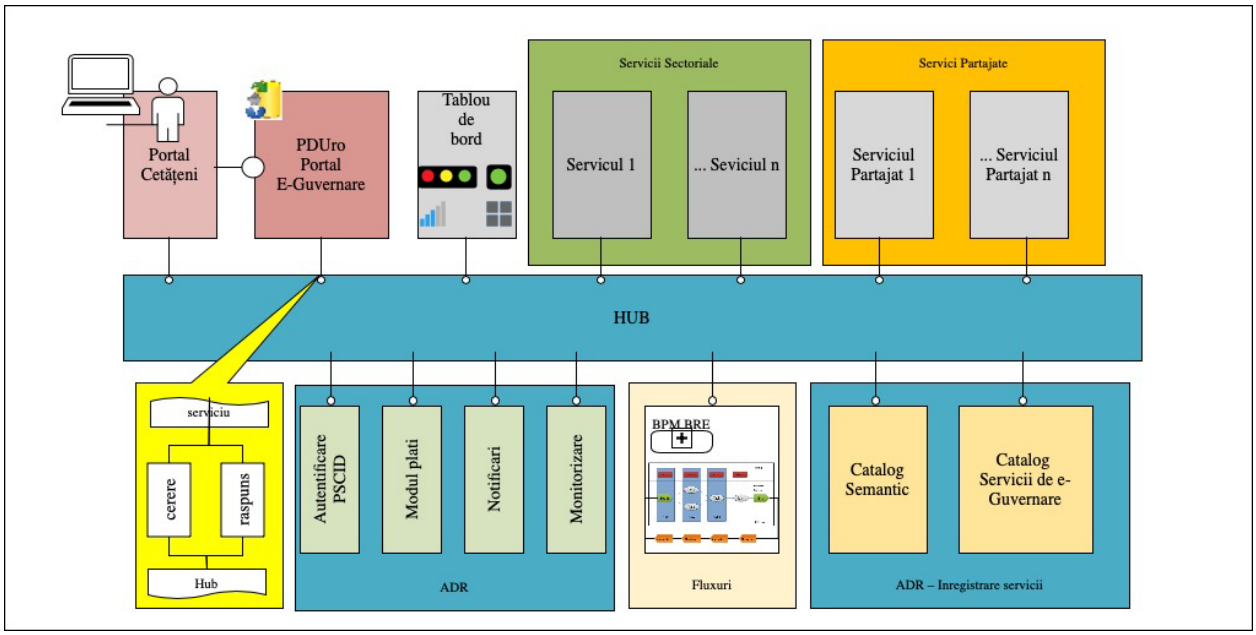
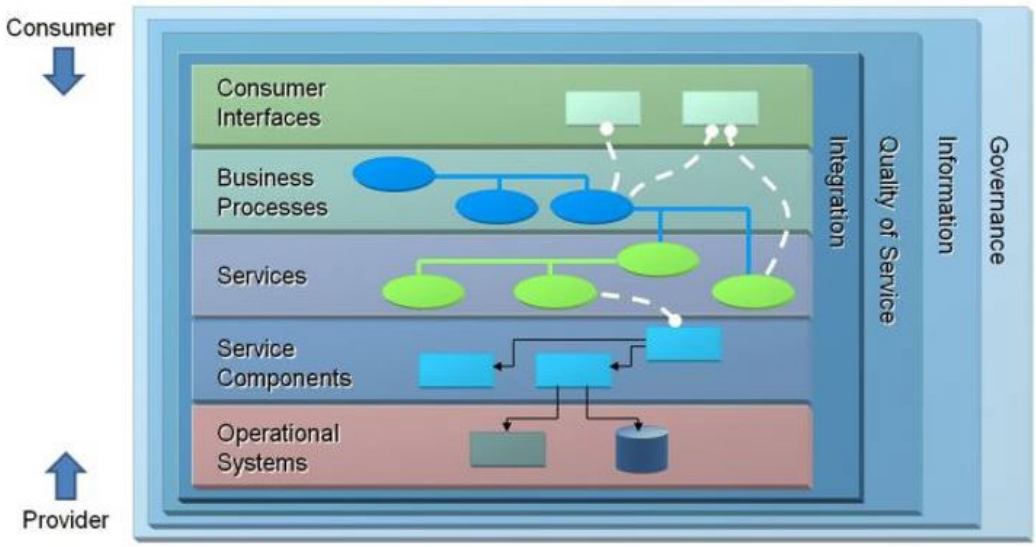


Fig 4. Arhitectura HUB-ului de Interconectare



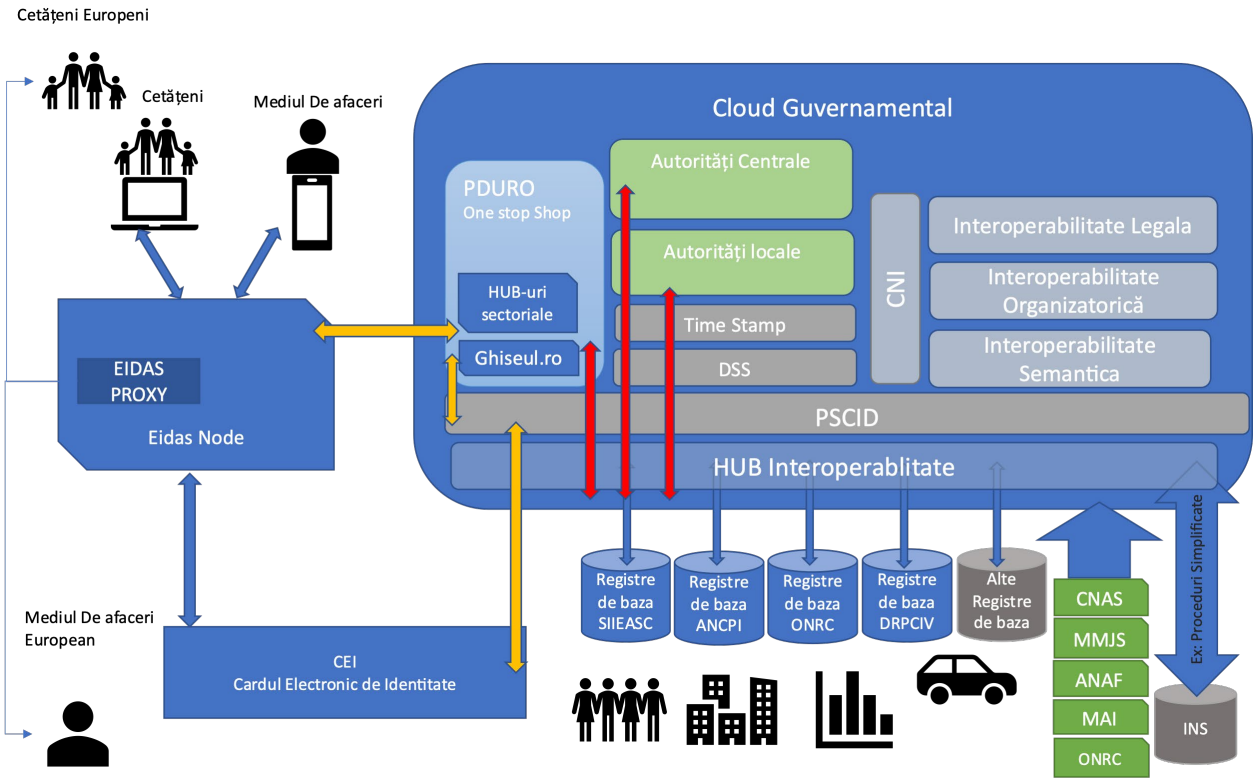


Fig 5. Arhitectura consolidată

3.3.Arhitectura tehnică

Din punct de vedere tehnic, arhitectura sistemului va fi constituită din soluții redundante în toate subcomponentele sistemului cu câte două noduri alocate fiecărei componente în parte astfel:

- Soluție cu asigurarea disponibilității și balansarea încărcării (cluster HA) pentru toate componentele funcționale ale sistemului:
    - servere web și poarta securizare servicii electronice;
    - portal;
    - BPM;
    - HUB Interconectare;
    - analiza și raportare;
    - managementul identităților electronice;
    - managementul accesului;

- stocare centralizată a profilelor de utilizatori aferente identităților digitale (LDAP);
- sistem de gestiune a bazelor de date în cadrul căreia se vor stoca toate instanțele bazelor de date aferente modulelor funcționale și portalului.

- Soluție cu asigurarea disponibilității de tip failover pentru componentele de suport:
  - Auditare;
  - administrare și monitorizare.

Pentru asigurarea funcționării în bune condiții a performanței sistemului PDURo vor fi asigurate următoarele medii:

a) **Mediul de producție** - asigură funcționarea în producție a sistemului PDURo și reprezintă mediul care va fi utilizat în mod direct de către cetățeni și instituțiile publice pentru definirea identităților electronice și furnizarea serviciilor electronice expuse prin intermediul platformei;

b) **Mediul de dezvoltare** și **testare** – asigură mediul pe care vor fi dezvoltate și apoi testate - într-un mod integrat, înainte ca acestea să fie trecute în producție - toate componentele sistemului;

Toate mediile vor avea, din punct de vedere al numărului de noduri respectiv al modalității de asigurare a disponibilității și scalabilității sistemului, aceeași arhitectură tehnică, diferențe existând doar la nivelul dimensionării acestor medii.

Mediul de producție va fi dimensionat fără limitarea din punct de vedere al licențierii pe infrastructura virtuală minimă solicitată; în cazul soluțiilor cu altĂ metrică sau modalitate de licențiere, sistemul informatic va trebui să asigure accesul a minim 10.000.000 de cetățeni către serviciile de e-guvernare dezvoltate în cadrul proiectului. **Se estimează că se va conecta un număr minim de 3000 de instituții ale administrației publice la HUB-ul de interconectare.**

Mediul de dezvoltare și testare va fi dimensionat pentru asigurarea unui număr minim de 50 de utilizatori.

Deoarece în scopul prezentului caiet de sarcini nu intră livrarea de echipamente, infrastructura hardware și de comunicații, inclusiv pentru mediul de dezvoltare și testare, urmând a fi asigurată de cloudul guvernamental (achiziție și implementare nefinalizate la acest moment), poate apărea situația ca la momentul începerii activității de dezvoltare din prezentul contract

infrastructura din cloudul guvernamental să nu fie disponibilă. În cazul apariției unei astfel de situații, care ar conduce la întârzierea începerii activităților de dezvoltare și testare, respectiv blocarea și întârzierea acestui proiect, ofertantul trebuie să dispună de infrastructura hardware și de comunicații necesară în vederea realizării temporare a mediului de dezvoltare și testare pe această infrastructură până la momentul la care infrastructura hardware și de comunicații din cloudul guvernamental va fi disponibilă. În acest sens, în cadrul ofertei, ofertantul trebuie să prezinte dovada capacității sale de a dispune de infrastructura hardware și de comunicații necesară în vederea realizării temporare a mediului de dezvoltare și testare. Pentru a fi asigurate conformitatea arhitecturală, integritatea și securitatea dezvoltărilor realizate pe acest mediu, este necesar ca acesta să fie un mediu de dezvoltare și testare distinct (să fie izolat de mediul de dezvoltare și testare utilizat de către ofertant în cadrul altor proiecte) și să respecte toate cerințele, inclusiv pe cele de arhitectură, dimensiune și securitate, impuse prin cerințele caietului de sarcini pentru mediul de dezvoltare și testare care va fi realizat pe infrastructura cloudului guvernamental. După operaționalizarea mediului de dezvoltare și testare pe infrastructura cloudului guvernamental, atunci când aceasta va deveni disponibilă, intră în responsabilitatea prestatorului migrarea de pe mediul de dezvoltare și testare temporar pe cel din cloudul guvernamental, trebuind ca după finalizarea migrării să facă dovada faptului că nimic din dezvoltările realizate nu se mai regăsește pe mediul de dezvoltare și testare temporar. Ofertantul va prezenta în oferta tehnică infrastructura hardware și de comunicații și abordarea sa avute în vedere pentru realizarea acestui mediu de dezvoltare și testare temporar.

Ținând cont de sensibilitatea datelor și nivelului de securitate solicitat în cadrul proiectului cât și de asigurarea de către producători a suportului tehnic pentru toate componentele funcționale, de securitate și suport ale platformei, prestatorul este solicitat să ofere versiunea comercială (COTS) pentru tot software-ul standard.

Pentru a reduce complexitatea arhitecturii, precum și costurile administrative și operaționale, platforma de aplicații propusă trebuie să fie pe deplin integrată la nivelul componentelor de management al fluxurilor și proceselor de emitere, aplicații software personalizate pentru acest sistem.

Sistemul informatic va fi proiectat astfel încât să funcționeze în regim de înaltă performanță și disponibilitate și va fi structurat pe trei niveluri, conform celor mai bune practici în domeniu: stocarea datelor, prelucrare și prezentare.

Dimensionarea componentelor funcționale și a celor de suport ale mediului de producție va trebui să asigure minimul de resurse de procesare după cum urmează:

Nr. crt.	Componenta	Număr minim de noduri	Disponibilitate minimă	Număr core-uri fizice minime pe nod	Memorie RAM (GB) minim necesară per nod
1.	Portal	4	Cluster HA	16	128
2.	Server web/Reverse proxy	2	Cluster HA	8	64
3.	SGBD	2	Cluster HA	8	256
4.	BPM	2	Cluster HA	8	256
5.	Hub de interconectare	2	Cluster HA	8	256
6.	Analiza și Raportare – BI	2	Cluster	16	256
7.	Gestiunea accesului utilizatorilor	2	Cluster	32	64
8.	Securizare acces servicii electronice	2	Cluster	16	64
9.	Monitorizare date, sisteme și aplicații	1	....	24	128
10.	Componenta de mascare a datelor	1	...	16	128

Nr. crt.	Componenta	Număr minim de noduri	Disponibilitate minimă	Număr core-uri fizice minime pe nod	Memorie RAM (GB) minim necesară per nod
11.	Componenta de securizare a accesului la bazele de date	2		16	128
12.	Backup	1	....	16	64

3.4.Managementul utilizatorilor și accesul la sistem

Prezentul proiect are ca obiectiv dezvoltarea și implementarea, cu acces național al cetățenilor și mediului de afaceri, al Hub-ului de interconectare

În cadrul serviciilor de eGuvernare oferite în prezent de diferite instituții publice există implementate mai multe modalități și soluții de asigurare a accesului la serviciile electronice care sunt strâns legate de sistemele informatice ce oferă aceste servicii. De regulă un sistem este configurat pentru a permite utilizarea unui singur tip de credențial, iar credențialele cel mai des utilizate sunt cele de tipul *nume utilizator/parola*.

Platforma va folosi pentru gestiunea identităților persoanelor fizice soluția de IAM a PSCID.

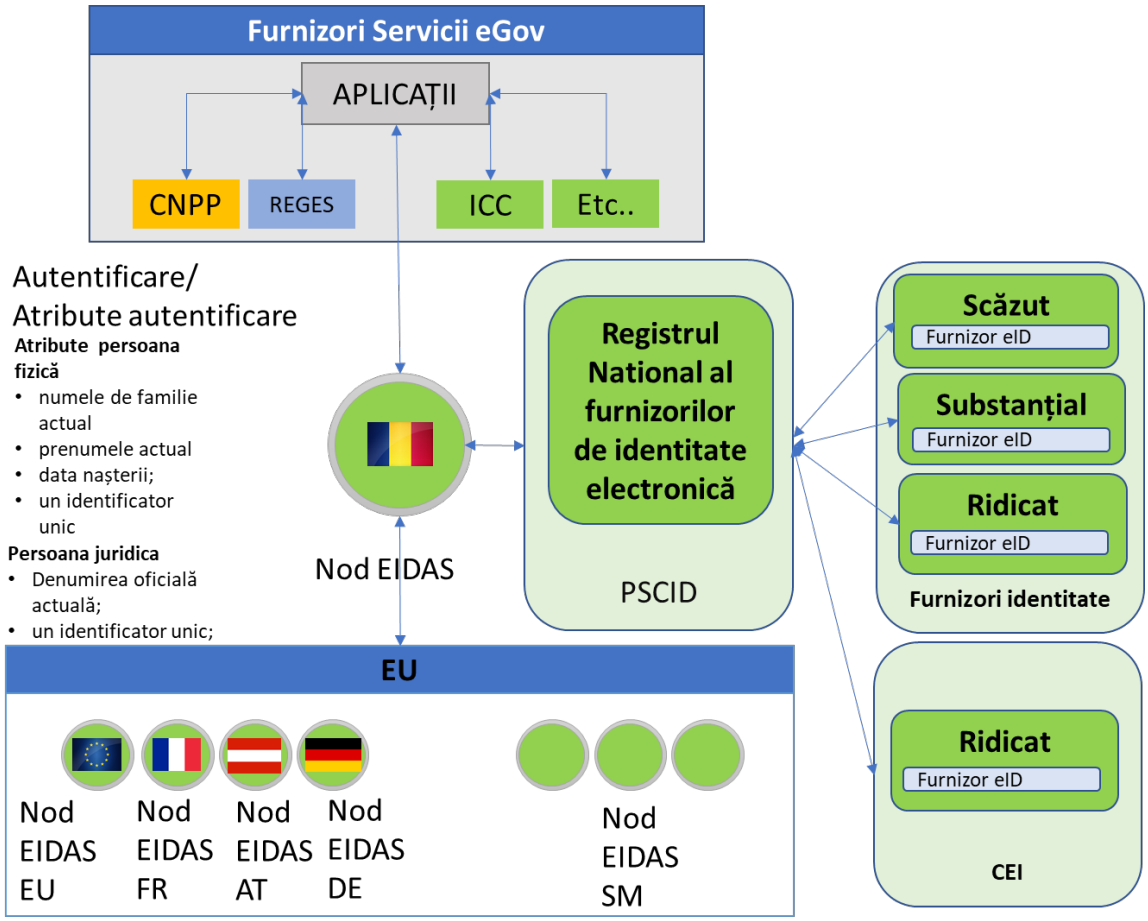
Asigurarea managementului utilizatorilor asigură în principal:

- identificarea în mod unic în sistem, a fiecărui utilizator, prin crearea unei identități electronice unice în cadrul sistemului și definirea de conturi unice și personalizate de acces;
- accesul utilizatorilor se va realiza doar prin autentificarea utilizatorilor. Vor exista informații de interes public publicate în portal care nu vor necesita autentificare; utilizarea însă a oricărui serviciu oferit prin intermediul portalului va fi asigurată doar după selectarea modalității de autentificare și prezentarea credențialelor de acces;

- gestionarea centralizată și unitară în sistem a accesului utilizatorilor prin asigurarea autorizării utilizatorilor și componentele și modulele funcționale ale acesteia conform cu drepturilor de acces definite.

Pentru asigurarea accesului cetățenilor este foarte important ca instituțiile publice să adopte modelul identităților federalizate, să accepte credențialele emise de alte instituții ale statului pentru accesarea prin intermediul PSCID. Scopul final pentru utilizatorii serviciilor electronice este acela de a avea acces la aceste servicii utilizând un număr limitat de credențiale de autentificare sau reutilizând credențialele existente și emise de alt furnizor de identități.

Schema de principiu a PSCID este ilustrată în figura de mai jos.



Caracteristicile propuse pentru PSCID sunt bazate pe profilul SAML conforme cu cerințele eIDAS ale cărui niveluri de asigurare sunt definite în Decizia de punere în aplicare a Regulamentului (UE) 2015/1502, în conformitate cu articolul 8 alineatul (3) din Regulamentul eIDAS (UE) 910/2014.

Pentru utilizatorii PDURo care nu fac obiectul PSCID – de ex. persoanele juridice – sistemul va pune la dispoziție propriul sistem de management al identităților și de control

al accesului. Sistemele de tip IAM (identity and acces management) al PDURo și PSCID vor avea o relație de trust, iar sistemul PSCID va proviziona identitățile sale către sistemul Platforma de cloud guvernamental.

Sistemul informatic propus trebuie să pună la dispoziția administratorilor o componentă pentru controlul accesului utilizatorilor interni sau externi la funcțiile aplicative ale sistemului informatic, pe baza drepturilor de acces specifice pentru fiecare categorie sau grup de utilizatori.

Este necesar ca soluția tehnică să implementeze cel puțin următoarele funcționalități:

- posibilitatea restricționării accesului utilizatorilor privilegiați la datele manipulate de aplicațiile de business, prin segregarea responsabilității;
- soluția va permite autentificarea furnizorilor de servicii medicale și a altor persoane autorizate pe baza certificatelor digitale calificate sau a sistemului nume-parola-OTP.

Sistemul va folosi următoarele nivele de încredere:

- nivelul minim de autentificare în sistem va fi: **substanțial conform Regulamentului 910/2014**

Se va introduce autentificarea cu 2 factori. Se va implementa autentificarea folosind doi factori de autentificare, respectiv nume și parolă și o modalitate suplimentară de tip one-time-password, prin mail sau folosind o aplicație mobilă. În procesul de obținere a datelor de acces se va asigura că utilizatorii sunt înscriși atât cu numele și parola dar și cu numărul de telefon mobil.

- nivel **ridicat de autentificare în sistem conform Regulamentului 910/2014**

Pentru utilizatorii care au un certificat calificat valid (și nu fac obiectul **PSCID**) se va introduce autentificarea folosind certificate digitale calificate astfel încât toți utilizatorii să acceseze sistemul în mod securizat corespunzător.
Sistemul informatic propus trebuie să pună la dispoziția administratorilor o componentă pentru realizarea funcționalităților necesare administrării sistemului precum și pentru monitorizarea funcționării acestuia în vederea urmăririi îndeplinirii obiectivelor de performanță și disponibilitate.

Această componentă trebuie să răspundă următoarelor cerințe generale:

- definirea și documentarea procedurilor și proceselor necesare pentru operarea soluției;
- minimum următoarele cerințe vor fi acoperite de aceste proceduri și definiții de procese:
    - operarea și administrarea soluției în mod proactiv și eficient;
    - monitorizarea permanenta a funcționării sistemului cu alertarea anomaliilor – erori sau avertizări legate de funcționalitate;
    - readucerea sistemului în parametrii normali de operare;
    - persoane cu nivel mediu de cunoștințe IT și a produselor soluției să poată aplica procedurile definite.
- toate componentele soluției vor înregistra principalele evenimente de succes sau de eroare în jurnale specializate care îndeplinesc următoarele cerințe:
    - pot fi securizate pentru a limita accesul la aceste informații;
    - permit consultarea lor directă de către un operator uman;
    - permit interpretarea prin metode programatice – sunt organizate într-un mod consistent și structura este documentată.

Sistemul informatic propus trebuie să pună la dispoziția administratorilor o componentă care va îndeplini atât funcțiile de audit informatic cât și funcțiile de control al accesului la informații.

Soluția de audit și control va îndeplini următoarele cerințe generale:

- va păstra un istoric de tip log al activității utilizatorilor aplicației;
- va permite includerea informațiilor despre momentul în care au fost modificate anumite seturi de date de către utilizatori.

Multitenant:

Fiecare instituție și autoritate publică este responsabilă pentru conferirea drepturilor de acces angajaților săi, luând în considerare scopul accesării datelor, protecției datelor cu caracter personal și a securității cibernetice.

*3.5.*Securitatea sistemului

Prevederi legale:

- participanții la schimbul de date sunt obligați să informeze autoritatea competentă despre vulnerabilitățile și incidentele de securitate în utilizarea platformei de interoperabilitate în termen de cel mult 24 de ore din momentul depistării acestora;
- datele transportate prin intermediul platformei sunt transportate în formă criptată;
- transferul datelor este organizat într-o manieră în care identitatea destinatarului este cunoscută în mod cert înainte de a permite destinatarului să prelucreze datele primite;
- prelucrarea datelor cu caracter personal de către instituțiile și autoritățile publice, de persoane fizice și de către entitățile de drept privat în procesul de utilizare și furnizare a serviciilor publice prin intermediul platformei de interoperabilitate se realizează cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal;
- determinarea accesului la date are loc în condițiile art. 16 (f) pentru fiecare instituție și autoritate publică în parte. Fiecare instituție va acorda angajaților și colaboratorilor săi drepturile de acces la date conform alin. (8) al prezentului articol;
- persoana vizată are dreptul să primească informațiile prevăzute la art. 13 și 14 din Regulamentul nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE în condițiile art. 12 din Regulament, la intervale rezonabile, dar nu mai mari de 1 an;
- utilizatorii de date nu trebuie să se angajeze în nicio activitate care să compromită siguranța platformei.

Sistemul va fi proiectat astfel încât să respecte Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE precum și legislația națională în domeniul prelucrării datelor cu caracter personal precum și Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

Sistemul informatic trebuie să fie protejat împotriva încercărilor deliberate sau accidentale de acces neautorizat la datele pe care aceasta le gestionează.

Designul soluției de securitate trebuie să fie astfel conceput încât să asigure securitatea și confidențialitatea atât a datelor personale ale utilizatorilor, dar și a conținutului și a anumitor funcționalități ale aplicației, astfel încât utilizatorii să acceseze doar acele secțiuni și conținut care le este permis prin apartenența la un profil sau machete de securitate.

Soluția de securitate va fi configurată astfel încât:

- Să nu permită persoanelor neautorizate modificarea sau alterarea semantică a informațiilor din sistem;
- Să asigure consistența datelor și să permită identificarea sursei datelor inițiale și a persoanelor care au accesat sau au înregistrat aceste date în sistem;
- Să asigure securizarea/protecția datelor vehiculate în sistem pe mai multe niveluri – la nivel de acces în rețea, la nivel de aplicație și la nivel de baza de date.

Prevederile de securitate vor fi implementate la următoarele niveluri ale soluției informatice propuse:

- **Controlul Accesului Logic**
    - nu **se** permite acces neautentificat la date și informații (mai puțin secțiunea publică a nodului). Orice acces în aplicație, atât la nivelul utilizatorilor cât și la nivelul altor module de aplicație, este precedat de identificarea, autentificarea și autorizarea accesului;
    - parolele de acces între modulele aplicației (de ex: la baza de date) sunt stocate criptat în fișierele de configurare;
    - credențialele de acces nu se transmit în clar prin rețea între componentele sistemului;
    - sesiunile de lucru inactive trebuie să expire după o perioadă de timp configurabilă (implicit 10 minute);
    - serviciile și porturile de comunicație folosite vor fi documentate într-o listă a serviciilor utilizate. Serviciile și porturile neutilizate vor fi dezactivate;

- sistemul informatic și componentele acestuia se vor instala și configura numai pe sisteme care au aplicate ultimele patch-uri de securitate.

- **Jurnalizare, monitorizare, auditare**

Jurnalizarea evenimentelor semnificative legate de controlul accesului

- înregistrarea în jurnal a autentificărilor cu succes (dată, oră, adresa IP);
- înregistrarea în jurnal a autentificărilor fără succes (dată, oră, adresa IP);
- aceste jurnale vor fi disponibile în aplicație pentru vizualizare de către administratorii sistemului.

- **Testare de securitate**

Aplicația va fi supusă unor verificări riguroase de securitate (auditare de securitate și test de penetrare) pentru a se identifica și elimina orice vulnerabilități înainte de a se utiliza în producție, precum și regulat, la intervale definite de timp. Testele vor respecta cel puțin metodologiile OSSTM (Open Source Security Testing Methodology) sau OWASP (Open Web Applications Security Project). Raportul final de testare de securitate va cuprinde vulnerabilitățile existente în cadrul sistemului și componentelor acestuia, și va fi structurat astfel:

- sumar executiv;
- obiectivele și scopul evaluării;
- prezentare succintă a metodologiei utilizate;
- descrierea contextului în care s-a desfășurat evaluarea;
- lista testelor de securitate efectuate;

Prezentarea individuală a vulnerabilităților descoperite după cum urmează:

- descrierea vulnerabilității;
- catalogarea vulnerabilității;
- descrierea tehnică;
- analiza severității și probabilității;
- calcularea riscului;
- contramăsuri recomandate pentru remediere;

- alte detalii și recomandări.

Scanarea de vulnerabilități informatice se va realiza prin utilizarea de aplicații dedicate și actualizate la momentul realizării scanărilor. În acest sens se vor utiliza aplicații care să conțină baze de date de vulnerabilități la nivel de rețea, sisteme de operare, aplicații/servicii, care, pe de-o parte, trebuie să permită auditarea activităților realizate astfel încât să poată fi demonstrată efectuarea acestor activități și, pe de altă parte, să conțină baze de date actualizate cu exploit-uri (coduri care demonstrează că o vulnerabilitate poate fi exploatată însă fără ca sistemul să fie propriu-zis compromis).

3.6.Confidențialitatea datelor

Confidențialitatea este o activitate de bază pentru furnizarea serviciilor publice.

În cadrul proiectului se vor respecta următoarele principii:

- că urmează abordarea **confidențialității prin concepție** pentru a asigura securitatea modulelor și a infrastructurii lor complete;
- că respectă cerințele și obligațiile juridice privind **protecția și confidențialitatea datelor** recunoscând riscurile la adresa confidențialității care reies din analiza și prelucrarea avansată a datelor.

De asemenea, trebuie să asigure respectarea de către operatori a legislației privind protecția datelor, prin:

- **„Planuri de gestionare a riscurilor”** pentru identificarea riscurilor, evaluarea potențialului impact al acestora și planificarea intervențiilor cu măsuri tehnice și organizatorice adecvate. Pe baza ultimelor evoluții tehnologice, aceste măsuri trebuie să asigure un nivel de securitate proporțional cu gradul de risc;
- **„Planuri de continuitate a activității”** și **„planuri de rezervă și de redresare”** pentru a institui procedurile necesare de asigurare a disponibilității funcțiilor în urma unui eveniment dezastruos și readucerea tuturor funcțiilor la situația normală cât mai curând posibil;
- Un **„plan de acces la date și autorizare”** care stabilește persoanele care au acces la date, datele care sunt accesibile și condițiile accesării datelor, pentru a asigura confidențialitatea. Accesul neautorizat și încălcarea normelor de securitate trebuie

monitorizat, și măsurile corespunzătoare pentru a preveni orice repetare a încălcărilor trebuie documentate și planificate;

- Dezvoltare și testare

  Avantajele dezvoltării în cloud față de dezvoltarea software tradițională:

  - Economii – Se utilizează resursele de care este nevoie;
  - Domeniu de aplicare –Numărul de scenarii diferite— mai multe browsere, mai multe sisteme de operare — pentru a vă asigura că software-ul funcționează pentru cât mai mulți utilizatori;
  - Scalabilitate – Creșterea sau reducerea fără efort a resurselor în funcție de nevoile de testare, de la testarea inițială de până la dezvoltarea de software de tip enterprise;
  - Viteză – Testarea software-ului pe diferite sisteme de operare, platforme, browsere și dispozitive simultan, reducând timpul de testare;
  - Automatizare – Folosirea cu ușurință de instrumente automate de testare a software-ului;
  - Colaborare – Dezvoltarea Agilă.

În cloud, dezvoltatorii pot lansa noi configurații sau caracteristici, iar QA poate rula teste împotriva lor imediat, făcând dezvoltarea agilă mai gestionabilă.

- Sandbox

Politica de utilizare a sandbox-ului este stabilită de echipa responsabilă de dezvoltare și echipele de securitate SRI și conformitate STS. În schimbul unor permisiuni mai deschise, dezvoltatorii vor trebui să lucreze în limitele de protecție definite de echipele de securitate și conformitate.

Zone de acoperit în politica ADR de utilizare a mediului de dezvoltare de tip „sandbox”:

- **Clasificarea datelor:** beneficiarul specifică ce clase de date sunt permise în conturile sandbox. Multe organizații interzic utilizarea datelor clienților (nume, adrese de e-mail, numere de telefon, informații de plată și așa mai departe) în mediile sandbox.

- **Conectivitate la rețea**: În cadrul contractului de dezvoltare se specifica dacă rețelelor din mediul sandbox li se permite să se conecteze la rețele din alte medii de servicii sau partajate. De obicei, aceste medii sunt izolate.
- **Controlul accesului:** specificați cine are acces la conturile sandbox ale cloudului guvernamental. Conturile pot fi fie dedicate unui singur dezvoltator, fie partajate de o echipă mică. Utilizarea conturilor individuale simplifică raportarea costurilor și facilitează identificarea proprietarilor de resurse. Conturile partajate sunt mai ușor de monitorizat și gestionat centralizat. Politica de utilizare ar trebui să specifice, de asemenea, că un rol de gestionare a identității și accesului (IAM) pe mai multe conturi trebuie implementat în fiecare cont sandbox pentru a oferi echipelor de securitate și conformitate accesul necesar pentru a monitoriza resursele și activitatea din cont.
- **Politica de etichetare:** chiar și într-un cont sandbox, etichetarea resurselor este esențială. Etichetarea ajută să identificați cine a creat resursele, cine este responsabil pentru acestea și cum ar trebui să fie alocate costurile.

- Politica ciclului de viață al resurselor: specifica cât timp pot persista resursele într-un cont sandbox. Aceasta este o modalitate bună de a le împiedica să devină medii de dezvoltare în umbră sau chiar medii de producție. Organizațiile implementează adesea politici privind ciclul de viață pentru a închide resursele după un anumit număr de zile.
- Utilizarea unor servicii calificate de asigurare a încrederii în conformitate cu regulamentul eIDAS[1] pentru a asigura integritatea, autenticitatea, confidențialitatea și nerepudierea datelor.

3.7.Componentele software

3.7.1. Componenta Portal SDG național

Portalul SDG național reprezintă componenta prin intermediul căreia se va realiza punctul unic de acces către serviciile publice electronice, pentru publicul larg, persoane fizice și juridice. Aceștia vor avea acces la sursele de informații și serviciile publice puse la dispoziție de către ADR, precum și pentru instituțiile afiliate, care vor putea accesa și aplicații interne.

Portalul va include următoarele secțiuni principale împreună cu funcționalitățile specifice asociate:

1 Regulamentul (UE) nr. 910/2014.

- Secțiune publică;
- Secțiune privată pentru persoane fizice și persoane juridice;
- Secțiune privată pentru operatorii din cadrul autorităților competente;
- Secțiune privată pentru administratorii SDG național;
- Secțiune privată pentru administratorii din cadrul autorităților competente;

Portalul va fi realizat pe o platformă flexibilă și scalabilă, capabilă să asigure un grad înalt de standardizare și reutilizare a resurselor și serviciilor, cu acces rapid la aplicații.
Portalul trebuie să permită actualizarea rapidă și facilă a conținutului, acțiune care se va realiza fără aportul specializat al unor resurse de dezvoltare, distribuirea conținutului.
Soluția Portal trebuie să asigure următoarele funcționalități minime:

- unic punct de acces către aplicațiile din sistem și către rapoartele specifice;
- include toate instrumentele necesare pentru construirea și administrarea unui portal complex, structurat pe mai multe niveluri de acces;
- interfață cu utilizatorii bogată în funcționalități care să ofere un nivel ridicat de accesibilitate, conform cu cerințele nivelului I (A) de accesibilitate WCAG;
- include funcționalități specifice de administrare de conținut pe bază de partajare, colaborare și automatizare de procese;
- permite rularea Portalului pe toate distribuțiile majore de sisteme de operare prezente pe piață: Windows, Linux și UNIX;
- asigură suport pentru apelul la distanță a portlet folosind standardul Web Services for Remote Portlets (WSRP);
- asigură autentificarea unică a utilizatorilor prin intermediul rolurilor și privilegiilor ce vor fi definite și acordate fiecărui utilizator în parte;
- interfața prezentată utilizatorului după autentificare trebuie să prezinte acces doar la informațiile/paginile web și aplicațiile la care utilizatorul are drept de utilizare conform cu rolul său în cadrul sistemului;
- conținutul accesat prin Portal trebuie să fie automat ajustat, pe baza rolurilor predefinite ale utilizatorilor în funcție de drepturile acordate;
- interfața oferită utilizatorilor de Portal va fi în limba română, cu stil de organizare unitar, indiferent de utilizator și de drepturile alocate acestuia;
- asigură efectuarea de căutări agregate folosind mai multe metode de căutare pentru interogarea și regăsirea informațiilor existente în sistem;

- asigură crearea facilă de noi pagini în Portal, pentru a menține în permanență actualizată informația din Portal;
- include mai multe stiluri predefinite de organizare și prezentare a paginilor de Portal, iar dintre aceste stiluri se va putea selecta un stil de prezentare specific Beneficiarului;
- utilizatorii trebuie să aibă posibilitatea de a particulariza paginile la care au acces la nivel de conținut, poziționare sau stil, în funcție de drepturile de personalizare acordate;
- administratorii de portal trebuie să poată controla drepturile utilizatorilor de a particulariza propriile pagini, funcție de rolul acestora, sau funcție de regulile definite;
- include un instrument dedicat pentru administrarea utilizatorilor. Acesta trebuie să realizeze definirea de utilizatori și parole, schimbare parole, gestiune a drepturilor de acces bazat pe grupuri de utilizatori/roluri astfel încât un utilizator să poată face parte din mai multe grupuri generice de drepturi de acces, etc. De asemenea, soluția trebuie să includă un mecanism de analiză de risc, care să calculeze automat un scor de risc al utilizatorului bazat pe drepturile de acces existente în sistem. Acest mecanism trebuie să poate simula în timp real modul în care scorul de risc al unui utilizator se modifică în situația în care utilizatorul respectiv solicită noi drepturi de acces, astfel încât aprobarea acestora să poată fi realizată având în vedere nivelul de risc total ce ar fi atins în cazul aprobării tuturor drepturilor de acces solicitate;
- soluția Portal trebuie să permită utilizarea profilelor de utilizatori, administratorul putând seta astfel preferințele atât la nivel de profil, grup cât și la nivel de utilizator. Aceste preferințe specifică atât accesul pe care îl vor avea la diverse porțiuni ale portalului cât și drepturile asupra acestor zone;
- utilizatorii și drepturile de acces sunt stocate și gestionate în cadrul unui sistem standard de autentificare unică. Accesul la oricare din aplicațiile componente ale soluției se va face utilizând o autentificare unică la începutul sesiunii de lucru. La autentificare, soluția de portal trebuie să analizeze permanent nivelul de risc aferent autentificării utilizatorilor utilizând factori de risc ca: locația geografică, echipamentul utilizat pentru autentificare și comportamentul utilizatorului. Pe baza acestei analize, soluția va lua decizii automate care trebuie să includă cel puțin:
    - permite / refuza accesul utilizatorului;
    - transferă informațiile și operațiunea de autentificare la un operator pentru analiza detaliată;

    - decizie privind acceptul/refuzul accesului sau solicită un element suplimentar de autentificare.
- de asemenea, soluția trebuie să permită configurarea de excepții pe baza cărora regulile specifice analizei de risc să nu fie aplicate pentru anumiți utilizatori / categorii de utilizatori;
- comunicarea utilizatorilor cu soluția portal (pentru utilizare sau administrare) trebuie să poată fi făcută în deplina siguranță din punct de vedere al comunicației și al accesului la servicii (SSL);
- soluția Portal trebuie să permită delogarea automată – să ofere un mecanism prin care un utilizator să fie delogat în cazul în care nu a mai efectuat nici o tranzacție într-o perioadă de timp (interval ce trebuie să poată fi setat de administrator);
- soluția Portal trebuie să ofere opțiuni de a defini perioade de timp în care o resursă din Portal este disponibilă. Dacă accesul se efectuează în această perioadă și utilizatorul are drepturi de acces, atunci acestuia i se va permite accesul. Dacă accesul se efectuează în afara perioadei stabilite, atunci accesul va fi blocat, chiar dacă utilizatorul are drepturi de acces pentru resursa respectivă;
- să suporte structuri ierarhice de navigare arborescentă pentru documente;
- să fie flexibil din punct de vedere al clienților de tip browser, al sistemelor de operare și al suportului pentru bazele de date;
- să asigure administrarea prin intermediul unui browser web și să suporte delegarea administrării pentru controlul accesului;
- soluția Portal trebuie să ofere o interfață de management a drepturilor de acces prin care utilizatorii interni și externi să solicite drepturi de acces la resursele sistemului – inclusiv pentru accesul de tip administrator. Cererile de drepturi de acces vor fi analizate pe baza unor fluxuri de aprobare definite în soluție iar în cazul aprobării, conturile aferente vor fi deschise automat în sistem cu informarea utilizatorului care a generat solicitarea;
- dezvoltarea portalului să se facă ușor, respectând standardele în domeniu. Pentru această soluția trebuie să ofere API-uri (Application Programming Interfaces) bine definite pentru integrarea cu aplicațiile existente, să ofere posibilitatea utilizării serviciilor web pentru a expune date și funcționalități;
- să ofere posibilitatea de a implementa portalul într-un mediu cluster, având posibilitatea de a realiza balansarea încărcării, fără componente software adiționale;

- să ofere capabilități de preluare a utilizatorilor pe un alt nod, în cazul unei căderi hardware (fail over);
- să ofere mecanisme de caching pentru paginile mai des utilizate pentru performanțe ridicate;
- soluția Portal trebuie să includă rapoarte analitice asupra acțiunilor utilizatorilor, care să ofere posibilitatea de a analiza traficul și activitatea utilizatorilor pe portal și colectarea și raportarea de metrici pentru funcționalități, incluzând accesul la pagini, elementele constitutive ale acestora (web part, widget, portlet) și documente. Prin aceste metrici portalul trebuie să permită identificarea eventualelor tipare de utilizare (usage patterns) cum ar fi durata vizitelor pe o anumita pagina sau frecvența accesului la o pagină într-o anumită perioadă de timp. Metricile colectate trebuie să poată fi corelate cu utilizatorul permițând apoi filtrarea datelor după atribute din profil cum ar fi locația utilizatorului, departamentul sau funcția (pentru utilizatorii interni – dacă este cazul);
- Platforma portal trebuie să permită colectarea următoarelor tipuri de metrici:
    - trafic la nivelul întregii componente;
    - trafic la nivel de pagina;
    - metrici referitoare la conectarea utilizatorilor;
    - metrici la nivel de elemente și performanțele acestora (frecvența utilizării, timpi de răspuns);
    - metrici referitoare la operațiile de căutare realizate prin interfața unificată;
    - metrici referitoare la documentele accesate;
    - informații de audit:
        - evenimente de acces – autentificări reușite, autentificări nereușite, autorizări reușite, autorizări nereușite;
        - operațiile specifice de administrate, cum sunt: execute, create, delete, rename, chown și chmod asupra fișierelor și directoarelor din sistem trebuie să poată fi controlate și monitorizate pentru audit;
        - rapoarte specifice de audit: număr resetări parole într-un interval de timp, utilizatori care au un anumit tip de cont de acces, conturi inactive existente în sistem etc.;
        - monitorizarea periodică a drepturilor de acces în sistem și confirmarea acestora de către persoanele abilitate;

Componenta Portal SDG național va dispune de un sistem de automatizare a comunicării cu cetățenii care trebuie să permită următoarele:

- să permită implementarea unui modul extern chatbot, bazat pe inteligență artificială și programat să desfășoare conversații într-un mod cât mai asemănător comportamentului uman, prin metodele de recunoaștere text și voce;
- să funcționeze integral on premise, fără a depinde de servicii externe;
- să ofere capabilitatea de integrare cu mai multe canale de comunicare, inclusiv: chat web, email, telefonie, sms, etc.;
    - pentru canalul de telefonie se va oferi o aplicație client ce se poate conecta la un server de SIP și purta o conversație:
        - pentru purtarea conversației se vor folosi module de transcriere a vorbirii (speech recognition) și sinteză a vorbirii (text to speech);
        - se poate configura un sunet de fundal care va fi redat pe parcursul convorbirii;
        - conversațiile se pot purta cel puțin în limbile Engleză și Română;
        - asistentul virtual va funcționa într-un mod cât mai natural și similar cu un asistent uman:
            - vocea folosită trebuie sa aibă un aspect uman, nu robotizat;
            - timpul de răspuns pentru întrebări simple trebuie sa fie de mai puțin de 1 secundă (Maxim 1 secundă între ultima vocalizare a utilizatorului și răspunsul asistentului). Pentru unele situații mai complexe timpul de răspuns poate fi prelungit, spre exemplu pentru dictarea unui număr de telefon unde utilizatorii fac pauze în vorbire;
            - asistentul poate fi configurat ca în anumite situații să permită utilizatorilor să îl întrerupă fără a aștepta terminarea mesajului. Spre exemplu dacă asistentul enumeră diferite opțiuni, utilizatorul va putea răspunde vocal cu o opțiune fără a aștepta prezentarea întregii liste.
        - asistentul telefonic poate face redirectări către alte numere de telefon;
        - asistentul telefonic permite folosirea tastaturii telefonului pentru transmiterea de informații numerice;

- Pentru canalul de chat web va fi disponibilă o aplicație web care poate fi inclusă în orice pagină html:
  - chatul web va permite comunicarea pe cale scrisă sau orală;
  - utilizatorii externi vor putea vedea o lista a tuturor conversațiilor lor istorice purtate pe chat-ul web;
  - utilizatorii externi vor putea avea mai multe conversații active în același timp;
  - utilizatorii externi vor avea posibilitatea de a închide conversația curentă;
  - utilizatorii externi pot vizualiza în chat răspunsuri pe care le-au primit în timp ce erau deconectați;
  - atunci când un utilizator extern primește un răspuns în timp ce este deconectat, acesta va fi notificat pe email;
  - utilizatorii pot cere transferul către un operator uman doar după completarea și validarea adresei de email;
  - utilizatorii ce primesc o notificare pe email au opțiunea să revină în portal pentru a continua conversația pe chat web sau pot răspunde direct pe email;
  - răspunsul trimis pe email va fi asociat cu conversația la care s-a răspuns. Utilizatorul extern va putea vedea mesajul trimis pe email și în interfața de chat web. Utilizatorul intern (operatorul) va vedea în aceeași conversație atât mesajele trimise pe chat web cât și mesajele trimise pe email ca răspuns la o notificare;
  - în timp ce utilizatorii scriu o întrebare se vor afișa posibile completări ale întrebării bazate pe conținutul configurat;
  - utilizatorii autentificați în portal (site) vor fi autentificați automat și în chat printr-o procedură securizată. Pentru autentificare site-ul va putea transmite un token către chat-ul web. Token-ul primit în web va fi folosit dintr-un server pentru a prelua datele utilizatorului în mod securizat;
  - chatul web va prezenta către utilizatorul extern identitatea și avatarul operatorului cu care discută;

        - chatul web îl va anunța pe utilizatorul extern de statusul conversației lui. Spre exemplu utilizatorul extern va fi notificat când un operator a preluat conversația lui;
        - chatul web îl va notifica pe utilizatorul extern în mod vizual și audio atunci când a primit un mesaj. Notificările audio și vizuale vor funcționa și atunci când interfața de chat este minimizată;
        - interfața de chat web va putea fi personalizată prin intermediul unei interfețe de administrare. Elementele personalizabile vor include: icon-ul de pornire al chat-ului, culoarea elementelor din chat, dimensiunea ăi poziția în pagină a ferestrei de chat, poziția în pagina a icon-ului de pornire al chat-ului;
        - chat-ul web va putea în mod proactiv sa trimită un mesaj de întâmpinare după un interval de timp configurabil. Mesajul va fi afișat deasupra icon-ului de pornire chat, fără a deschide interfața de chat;
        - la finalizarea unei conversații se va afișa un formular de feedback.
- să conțină un modul proprietar de înțelegere a limbajului natural bazat pe inteligență artificială care să îi permită recunoașterea intențiilor și entităților exprimate liber de către utilizatori, astfel:
    - să permită înțelegerea intenției utilizatorului pe baza unor exemple. Se va înțelege intenția utilizatorului chiar dacă exprimarea este puțin diferită față de exprimarea din exemple;
    - să permită extragerea de entități din frazele utilizatorilor. Entitățile pot include date, ore, localități, adrese, numere s.a.;
    - se vor putea configura tipuri noi de entități pe baza de liste de valori sau expresii regulate;
    - va avea capabilitatea de înțelegere de date și ore în diferite formate folosite în limbajul natural;
    - să funcționeze cel puțin pentru limbile Engleză și Română;
    - să învețe automat pe baza interacțiunilor cu utilizatorii. De exemplu, dacă un utilizator confirmă rezolvarea întrebării, atunci sistemul va salva exprimarea folosită de utilizator pentru extinderea automată a datelor de antrenare.
- să conțină un widget configurabil de chat care să poată fi inclus în orice pagină a unui site;

- să permită widget-ului de chat comutarea între modul scris și modul vocal;
- să permită integrarea cu soluții de e-mail și sms cu posibilitatea de extindere pentru alte canale
- să permită funcționarea omnichannel a platformei, respectiv același operator virtual configurat o singură dată să poarte conversații pe oricare dintre canalele configurate și să raporteze informația centralizat;
- să permită implementarea unui modul chatbot admin, respectiv o platformă de administrare a deciziilor care stau la baza sistemului de dialog dintre cetățean și interfața externă chatbot;
- să permită accesul utilizatorilor cu permisiuni de administrare la configurările operator-ului virtual, dar și la istoricul conversațiilor;
- să permită configurarea și administrarea conținutului asistentului în mod ușor, fără a scrie cod;
- să includă un modul de întrebări și răspunsuri prin intermediul căruia administratorii de conținut să poată configura o lista de întrebări și răspunsuri;
- conținutul de tip întrebări şi răspunsuri să poată fi exportat și importat în format xlsx. Administratorii vor avea opțiunea de a edita conținutul și direct pe documentul xlsx.
- să permită configurarea de arbori de dialog printr-o interfață vizuală similară cu o diagramă logică.
    - configurarea diagramei se va putea face fără a scrie cod;
    - configurarea va permite manipularea de date fără a scrie cod. Se vor putea extrage informații de la utilizatori, se vor putea trimite informațiile prin API, se vor putea stoca informații primite dintr-un API, se vor putea folosi datele stocate pentru generarea de mesaje dinamice și pentru configurarea de condiții în diagrama logică;
    - să permită configurarea de script-uri în interiorul diagramei prin intermediul cărora datele să poată fi prelucrate prin scrierea de cod;
    - să permită exportarea și importarea diagramelor de dialog;
    - să permită împărțirea diagramelor de dialog în subdiagrame pentru o mai bună organizare;
    - să permită configurarea conținutului în cel puțin două limbi (Română și Engleză) ;

- pentru configurarea conținutului în mai multe limbi se va putea folosi o singură diagramă. Fiecare element din diagramă va putea fi vizualizat și editat în fiecare limbă, inclusiv mesajele asistentului și exemplele de fraze pentru recunoașterea intenției;
- conținutul folosit în diagramă să poată fi accesat și în format tabelar. Sa existe o listă de mesaje, o listă de intenții utilizator, o listă de scripturi și o listă de servicii externe. Formatul tabelar va permite căutarea și editarea cu ușurință a elementelor din diagramă;
- orice modificare a diagramei, configurărilor sau conținutului chat în general întreprinsă de orice utilizator va fi înregistrată și va putea fi consultată de către administrator într-o secțiune dedicată auditului;

- să includă un modul de asistență utilizatori destinat administratorilor sistemului PDURo care:
  - să permită transferarea conversațiilor de la asistent către operatori umani în anumite situații;
  - situațiile de transfer pot include:
    - atunci când asistentul virtual nu înțelege întrebarea utilizatorului în mod repetat;
    - anumite spețe ce nu pot fi automatizate.
  - să permită utilizatorilor interni sa vizualizeze conversații și să discute cu utilizatorii externi;
  - să centralizeze conversații din diferite canale, inclusiv: chat web, email, telefonie, sms etc. ;
  - să permită transmiterea de fișiere;
  - să permită gruparea utilizatorilor interni pe departamente în funcție de competențe;
  - să permită alocarea conversațiilor transferate în mod automat către cel mai potrivit departament;
  - să permită utilizatorilor interni să identifice conversațiile alocate departamentelor din care fac parte;
  - să permită utilizatorilor interni să aloce o conversație către un departament sau către un utilizator intern;

- atunci când o conversație este alocată către un operator sistemul să notifice vizual și audio pe operatorul către care s-a alocat;
- atunci când o conversație este alocată către un departament sistemul să notifice vizual și audio pe toți operatorii ce fac parte din acel departament;
- un operator sa poată avea mai multe conversații alocate în același timp și să poată comuta între ele ușor, cu un singur click;
- operatorul să fie notificat audio și vizual atunci când primește un mesaj în una din conversațiile alocate lui;
- atunci când accesează o conversație operatorii vor putea vedea diferite metadate despre conversație și utilizatorul extern;
    - informații personale despre utilizator atunci când sunt disponibile, spre exemplu: nume, prenume, cnp, email, telefon etc. ;
    - o listă de fișiere transferate în conversație;
    - note interne despre utilizatorul extern și conversație. Notele vor putea fi accesate și editate de către utilizatorii interni ce interacționează cu conversația;
    - acțiunile întreprinse de operatori precum transferarea unei conversații sau închiderea unei conversații și data și ora la care au fost efectuate.

- să permită crearea și administrarea unei colecții de răspunsuri frecvente pe care operatorii să le poată accesa cu ușurință pentru a precompleta răspunsul pe care îl formulează. Va exista o colecție globală accesibilă tuturor operatorilor și cate o colecție personală accesibila fiecărui operator;
- să permită și să încurajeze dezvoltarea soluției de tip chatbot printr-o serie de module de analiză bazate pe nevoile recurente ale cetățenilor;
- să permită platformei moduri diferite de interacțiune pentru utilizatorii interni și externi.
- să permită fiecărui utilizator extern să creeze un cont și să asocieze o sesiune unică de interacțiune cu operatorul virtual;
- să permită fiecărui utilizator extern să creeze un cont ce poate fi atât anonim, bazat pe cookie-ul din browser, cât și pe bază de autentificare cu user și parolă proprie;
- să permită sincronizarea cu sistemul de SSO pentru a nu menține mai multe conturi utilizatorilor interni;
- să permită utilizatorilor interni acces la o serie de funcționalități pe bază de permisiuni;

- să permită funcționalitatea de creare chatbot nou (proiect nou) disponibilă administratorului principal al platformei;
- să permită administratorului să gestioneze permisiunile în cadrul proiectului, respectiv:
    - administrare de conținut (creare și editare intenții, entități, răspunsuri, scheme de dialog, etc) - include antrenarea funcționarului public virtual;
    - dezvoltare (integrează sisteme) ;
    - analizare a statisticilor și istoricului de conversații;
    - integrare cu modulul de asistenta tehnica - vede și poate răspunde la conversații escalate;
    - administrator al proiectului (poate modifica permisiunile utilizatorilor interni).
- să conțină un modul de adnotări cu ajutorul căruia administratorul de conținut poate identifica expresiile utilizatorilor care nu au putut fi recunoscute sau au fost recunoscute cu un grad mai mic de siguranță și prin care, acesta poate confirma sau corecta modul în care au fost validate intențiile și entitățile;
- să permită folosirea automată a datelor adnotate pentru o nouă antrenare a operatorului virtual;
- să conțină un set de instrumente de adnotări și rapoarte de intenții pe baza cărora se vor analiza conversațiile istorice;
- să permită administratorului platformei dreptul de vizualizare asupra listei de conturi. Fiecare cont trebuie să aibă asociate următoarele: ID, Nume, Cod direcție, Funcția, Telefon, E-mail, Tip acces;
- accesul să se realizeze pe bază de user și parolă prin intermediul LDAP;
- să permită administratorului proiectului să activeze și să configureze integrări cu alte sisteme precum canale de social media;
- să integreze module de creare și analiză de rapoarte;
- să permită listarea conversațiilor în modulul de asistenţă tehnică;
- să înregistreze data și ora conversației pentru fiecărui mesaj în parte;
- să permită listarea cronologică a conversațiilor pentru vizualizarea dialogului istoric integral;
- să permită funcționalități de gestionare a rapoartelor;
- să permită vizualizarea în formă grafică sau numerică;
- să permită exportul rapoartelor în format xlsx și csv;

- să permită gestionarea de rapoarte în funcție de următoarele criterii: total conversații pe o perioadă selectată, număr de interacțiuni pe o perioadă selectată, număr de utilizatori externi angrenați în conversații cu chatbot-ul pe o perioadă selectată, număr total de mesaje ambigue înregistrate de sistem într-o perioadă selectată;
- să includă o serie de rapoarte privind cele mai frecvente intenții și entități, dar și o serie de rapoarte care să includă cele mai frecvente intenții care au rezultat în escalări;
- să pună la dispoziție utilizatorilor o serie de instrumente pentru testarea chatboților, respectiv testarea fluxului conversațional, inclusiv al intențiilor și entităților;
- să permită configurarea unui mesaj de întâmpinare ce se va trimite automat la deschiderea ferestrei de chat;
- să permită atașarea de fișiere din fereastra de chat.

3.7.2. Server web și Reverse Proxy (DMZ)

Pentru protejarea zonei de aplicații, în zona de interfațare DMZ se vor instala punctele de intrare în sistem pentru utilizatori, prin intermediul serverelor web și reverse proxy al căror principal scop este:

- să permită, din punct de vedere tehnic, vizualizarea layout-ului și a resurselor Portal într-un browser Web;
- să se integreze cu cel puțin o soluție de tip Single-Sign On pentru autentificarea unitară a utilizatorilor;
- să permită, din punct de vedere tehnic, accesarea aplicației din browsere tradiționale (Chrome, Mozilla Firefox, Edge), cât și de pe dispozitive mobile;
- să asigure, prin componentele software ale serverului Web, funcționarea în cluster pentru a asigura balansarea încărcării și disponibilitatea maximă a sistemului;
- să ofere posibilitatea de rulare pe diverse platforme virtuale și pe sistemele de operare majore de pe piață (Windows, Linux și UNIX)

Serverele web trebuie să permită prezentarea conținutului sistemului către utilizatori și transferul de date dinspre client spre sistem (prin intermediul browserelor web). În același timp, serverele web trebuie să asigure primul nivel de securitate software din punct de vedere al accesului – configurare în mod reverse proxy, suport pentru SSL și autentificare de baza (in conjuncție cu serverele de control acces ale soluției).

Comunicațiile cu exteriorul rețelei trebuie să se realizeze atât criptat cât și în clar, în funcție de tipul informației. Serverele web trebuie să permită integrarea cu soluții de accelerare hardware a criptării/decriptării și să dispună de funcționalități de rescriere a adreselor URL.

Din motive de securitate și ușurință în utilizare, serverul web trebuie să permită implementarea unui mecanism de tip SSO în conjuncție cu soluția de control acces și, în același timp, să ofere suport pentru autentificare cu certificate digitale prin integrare cu soluția de control acces și cu o infrastructura PKI.

În plus, serverele web trebuie să ofere suport pentru IPv4 și IPv6 astfel încât să permită utilizarea în contextul noilor scheme de adresare în Internet.

Serverele web trebuie să poată rula pe toate distribuțiile majore de sisteme de operare prezente pe piață (Windows, Linux, Unix).

3.7.3. Componenta de management a proceselor (BPM)

Componenta de management a fluxurilor trebuie să conțină următoarele componente/module:

- modulul de modelare grafică a proceselor ce va permite modelarea proceselor, utilizând standardul BPMN (Business Process Modeling Notation), a interfețelor web de captură date, a tranzițiilor dintre ecrane, a indicatorilor de performanță, documentarea activităților din cadrul proceselor în mod grafic, printr-o modalitate facila de tip drag-and-drop a etichetelor standardului BPMN. Prin acest modul se vor desemna persoanele care vor interacționa cu procesele, tipul de interacțiune, regulile de atribuire sarcini de lucru, reguli de expirare, escaladare activități și calendarul specific de lucru, reguli de alertare. Standardul BPMN reprezintă o modalitate de documentare a activităților din cadrul unui proces permițând analiștilor și dezvoltatorilor să folosească un model comun de reprezentare a proceselor, facilitând o înțelegere comună a procesului, a etapelor și activităților din cadrul proceselor. Folosirea acestui standard are avantajul că procesul modelat de către analiști va putea fi transformat automat în proces executabil;
- soluția trebuie să genereze în mod automat cazuri de testare pe baza modelelor grafice ale proceselor / cerințelor de business. Soluția trebuie să includă instrumente pentru optimizarea cazurilor de testare astfel încât să utilizatorii să poată obține numărul minim de cazuri de testare care asigură gradul maxim de acoperire a condiționalităților care

necesită testare. Cazurile de testare generate trebuie să poată fi importate în mod automat în instrumente de testare automate pentru testarea proceselor de business modelate pentru a fi integrate în cadrul PDURo;

- de asemenea, soluția trebuie să asigure definirea și alocarea datelor de test necesare pentru realizarea testării cazurilor de testare astfel încât să nu existe incompatibilități între nevoile de testare și datele de testare disponibile sau datele de testare să fie utilizate de alte componente ale PDURo;
- în cazul modificării fluxurilor / proceselor, soluția trebuie să asigure regenerarea automata a cazurilor de testare conform fluxurilor actualizate, astfel încât să nu existe condiționalități sau dependințe care să rămână netestate după realizarea unei modificări;
- soluția trebuie să indice dependințele dintre fluxurile interdependente, dacă este cazul;
- soluția trebuie să asigure automatizarea testării cazurilor de testare generate prin integrarea cu instrumente de testare automată;
- modulul de interacțiune cu fluxurile ce va permite ca fiecare persoană desemnată pe un proces să își organizeze și rezolve sarcinile de lucru, iar persoanele responsabile cu managementul și monitorizarea proceselor să urmărească starea fiecărei instanțe de proces în parte;
- modulul de reguli de business va permite modelarea facilă a parametrilor de proces susceptibili de a fi modificați în viitor datorită normelor legislative, schimbări interne în cadrul organizației, astfel încât să nu fie nevoie de reproiectarea proceselor modelate, ci să ofere o modalitate facilă de modificare a comportamentului procesului în funcție de acești factori;
- modulul de spații colaborative de modelare și lucru în echipă va permite analiștilor, dezvoltatorilor și experților să colaboreze în activitatea de proiectarea a proceselor, având capacități de stocare documente legislative sau norme interne specifice organizației și de a le consulta în procesul de proiectare a fluxurilor, chat, discuții etc.;
- modulul de simulare a performantelor proceselor ce va permite identificarea rapida a factorilor care au un impact negativ în performantele proceselor, precum și identificarea numărului optim de resurse umane astfel încât procesele să se desfășoare în cele mai bune condiții și cu cele mai mici costuri interne;
- modulul de monitorizare și raportare a performan'elor proceselor va oferi responsabililor de proces capacitatea de a urmări fluxurile în lucru, erorile și incidentele apărute în infrastructura de servicii, precum și diverși indicatori prin care se măsoară

performanța oamenilor, performanța activităților efectuate, costuri interne. De asemenea, modulul va include instrumente de construire de rapoarte specifice, fără să fie nevoie de cunoștințe avansate de programare.

- modulul de integrare și interoperabilitate cu sistemele și aplicațiile interne și externe va include conectori și adaptori specifici de tehnologie și aplicație pentru a integra sisteme eterogene atât interne cat și externe organizației. Modulul va permite schimbul de informații, indiferent de tehnologia în care sistemele și aplicațiile sunt scrise. În plus, modul va asigura integritatea și consistenta datelor schimbate între organizații, oferind o imagine în timp real a fluxului de tranzacții.

Suplimentar, componenta de management a fluxurilor de business va respecta în mod obligatoriu următoarele cerințe:

- să ofere posibilitatea de a defini forme Web ce va permite utilizatorilor să interacționeze cu procesele de business. Acestea vor trebui să se bazeze pe standarde tehnologice larg utilizate, cum ar fi XHTML, CSS, JavaScript. De asemenea, va oferi un instrument de dezvoltare a formelor web de tip designer ce va permite accesul la surse de date, definirea de reguli, definirea de controale în introducerea datelor;
- va oferi un mediu de rulare a proceselor de business având suport nativ atât pentru procesele BPEL cat și procesele BPMN;
- pentru interacțiunea umană cu aplicațiile compozite, să ofere șabloane predefinite de dirijare a activităților către utilizatorii cu roluri specifice la nivelul fluxurilor;
- să ofere suport pentru comunicații sincrone și asincrone inter-aplicații;să ofere mecanisme transparente de persistenţă a stării aplicațiilor și informațiilor de audit într-o bază de date relațională;
- să permită folosirea canalelor de notificare moderne pentru informarea utilizatorilor despre evenimentele semnificative apărute în cadrul procesele de business dezvoltate;
- să se integreze cu soluții de tip Service Registry bazate pe standardul deschis Universal Description Discovery and Integration (UDDI);
- să ofere capabilități de conectare predefinite la principalele tipuri de tehnologii: baze de date relaționale, cozi de mesaje (Java JMS, Oracle Advanced Queuing (AQ), IBM MQ), sisteme de fișiere, servere FTP;
- să permită auditarea și înregistrarea fluxurilor executate sau în curs de executare precum și a datelor transportate;

- în scopul detectării problemelor de performanță, infrastructura de execuție să permită colectarea permanenta de statistici de execuție pentru fluxurile instalate;
- să includă un modul dedicat de stocare și evaluare a regulilor de business externe aplicațiilor modelate, pe care personalul non-tehnic să le poată accesa și modifica on-line prin intermediul unei console web;
- implementarea unui mecanism de export al informațiilor - variabile proces, activități, excepții -din aplicații direct în baze de date relaționale sau cozi de mesaje;
- să ofere facilități de activare a auditării în cazul terminării cu eroare a unui flux;
- să permită monitorizarea în timp real a indicatorilor de tipul Key Performance Indicators (KPI) ;
- să permită monitorizarea în timp real a SLA-urilor de business sau operaționale;
- să colecteze date utilizând diferite canale de date precum conexiuni la baze de date relaționale sau cozi de mesaje;
- definirea și prezentarea tablourilor de bord se va putea face de către personal non-tehnic utilizând un simplu browser web;
- soluția va permite definirea de alerte și planuri de acțiuni asociate nerespectării KPIurilor și SLA-urilor impuse sau altor evenimente ale sistemului;
- integrarea fluxurilor de business / aplicațiilor se va face utilizând serviciile unei componenta de tip magistrala de mesaje. Această componentă va oferi suport pentru: virtualizarea accesului la funcționalitățile de aplicații
    - conectarea la diferite tehnologii și sisteme de aplicații;
    - transformarea mesajelor schimbate între aplicații;
    - rutarea mesajelor între diferitele sisteme integrate;
    - livrarea sigura a mesajelor între sisteme.
- soluția va include funcționalități extinse de transformare a mesajelor XML utilizând standarde deschise W3C Extensible Stylesheet Language (XSL) și XQuery
- soluția va oferi funcționalități de conectare predefinite la principalele tipuri de tehnologii: baze de date relaționale, cozi de mesaje (Java JMS, Oracle Advanced Queuing (AQ), IBM MQ), sisteme de fișiere, servere FTP.

Soluția va oferi funcționalități de conectare la sisteme de aplicații de business (cel puțin 2 conectori out of the box), și de asemenea va oferi un cadru de dezvoltare pentru noi soluții de conectare la sisteme externe bazat pe standarde deschise.

3.7.4. HUB de Interconectare

Abordarea implementării serviciilor de e-guvernare prin tehnologii orientate pe servicii încurajează reutilizarea (conform Cadrului Național de Interoperabilitate). La trecerea în producție se va publica catalogul serviciilor inclusiv politica privind crearea, implementarea și administrarea serviciilor.

Conform Cadrului Național de Interoperabilitate se solicită o arhitectura de tip servicii, modulară și care să permită integrarea și interoperabilitatea cu alte sisteme și servicii.

Hub-ul de interconectare își propune să implementeze o platforma unica în schimbul de informații între diferite sisteme existente dar și viitoare la nivelul instituțiilor publice. Platforma va utiliza tehnologii moderne, standarde deschise (servicii web, JSON/XML, cozi de mesaje), va implementa schimburi de date sincrone și asincrone, asigurând un management complet al ciclului de viață al serviciilor web. Platforma nu își propune să stocheze volume mari de date, scopul fiind acela de hub de schimb de informații, dar funcție de specificul fiecărui sistem anumite seturi de date vor putea fi sincronizate la nivelul acestei platforme. Platforma își propune să fie flexibilă în modul în care componente de integrare vor fi dezvoltate și implementate, permițând asamblarea componentelor SOA sub forma de aplicații compozite. De asemenea, în vederea standardizării definirii aplicațiilor SOA, se va folosi un limbaj standard de definirea a fluxurilor de business BPEL (Business Process Execution Language) și va permite reprezentarea acestora folosind BPMN (Business Process Model and Notation).

În acest sens, această componentă va trebui să urmărească programul promovat la nivelul comunității europene și anume: ISA 2 (Interoperability Solution for European Public Administration, Business and Citizens).

Astfel, pentru a răspunde cerințelor de funcționalitate și performanță cerute, componenta HUB de interconectare trebuie să ofere următoarele capabilități minime și obligatorii:

- să fie disponibilă comercial (COTS – Commercial off the Shelf) și să ofere posibilitatea de a rula pe diverse platforme software (Windows, Linux);
- posibilitatea să fie instalată în mediu containerizat (ex: Docker) și să ruleze într-o arhitectura Kurbernetes;
- să ofere un instrument de tip CLI prin intermediul căruia să se poată asigura ciclul de viață al aplicațiilor/componentelor software de integrare dezvoltate peste platforma de SOA;

- suport pentru soluții moderne și deschise de integrare conform principiilor și conceptelor arhitecturilor Service Oriented Architecture (SOA) și Event Driven Architecture (EDA);
- să fie bazată pe standardele deschide de interoperabilitate a aplicațiilor WS-I Basic Profile, WSDL, WS¬*, XML, SOAP, UDDI, REST;
- permite comunicații sincrone și asincrone inter-aplicații;
- soluția va implementa cel puțin următoarele modele de servicii: sincron cerere/răspuns, asincron one-to-one;
- permite folosirea de canale multiple de notificare pentru informarea utilizatorilor despre evenimentele semnificative apărute în aplicații;
- se integrează cu soluții de tip Service Registry bazate pe standardul deschis Universal Description Discovery and Integration (UDDI);
- tipurile de mesajele transportate suportate de soluția de tip Service Bus vor fi cel puțin: XML, text, binar, atașament;
- capabilități extinse de transformare a mesajelor XML utilizând standarde deschise W3C Extensible Stylesheet Language (XSL) și XQuery;
- să ofere conectori la principalele tipuri de tehnologii: baze de date relaționale, cozi de mesaje (IBM MQ, Oracle AQ, JMS), sisteme de fișiere, FTP;
- posibilitatea de a crea conectori custom, particularizat pe o nevoie de integrare specifica
- să ofere conectori la principalele platforme de tip aplicații (SAP, Oracle e-Business Suite, Siebel etc);
- servicii de transport cu suport pentru persistența datelor și garantarea livrării datelor;
- capabilități extinse de transformare și dirijare a datelor bazate pe conținutul transportat;
- posibilitatea definirii, la momentul execuției, a adreselor de destinație a mesajelor, eventual prin interogarea unei soluții de tip Service Registry;
- să ofere servicii de securitate atât la nivel transport cât și la nivel de aplicație;
- gestiunea încărcării livrării mesajelor către serviciile destinație înregistrate la nivelul magistralei de interconectare folosind cozi de mesaje tampon;
- va include capabilități native de monitorizare cu suport pentru dashboard-uri ce pot afișa informații legate de alertele SLA, parametrii de operare etc.;
- soluția va asigura suport de înalta disponibilitate prin clusterizare de tip activ-activ sau activ-pasiv;

- soluția trebuie să permită stoparea temporară a unui nod din cluster pentru mentenanță și suport, sistemul în acest timp fiind disponibil pentru activități normale.
- suport complet pentru dezvoltarea, testarea, execuția, monitorizarea, optimizarea și administrarea proceselor de flux;
- modelarea declarativă a proceselor de afaceri utilizând BPEL / BPMN cu ajutorul mediului de dezvoltare integrat al sistemului;
- suport pentru standarde de larga răspândire cum ar fi: XML, web services, JMS, J2EE, SMTP, HTTPS;
- oferă șabloane predefinite de dirijare a activităților către utilizatorii cu roluri specifice la nivelul aplicațiilor precum și interfețe grafice de lucru cu fluxurile automatizate;
- trimitere automată de notificări de inițiere de activități, termene limită, stadiu de execuție, finalizare și să trateze automat acest tip de notificări primite de la sisteme externe;
- va permite colectarea permanentă de statistici de execuție - timpi de execuție, frecventă de apariției evenimente, stări fluxuri - pentru procesele instalate;
- modul integrat de stocare și evaluare a regulilor de business, externe proceselor modelate, pe care personalul non-tehnic le va putea accesa și modifica ulterior;
- modulul de reguli de business trebuie să ofere un editor de reguli precum și funcționalități avansate de discovery, guvernanță, versionare, trasabilitate și stocarea într-un mod centralizat;
- posibilitatea de a defini reguli de business în limbaj natural, descriptiv în vederea definirii unei reguli de business, fără a fi nevoie de cunoștințe de programare;
- să ofere mecanisme avansate de caching, ce asigura persistenta componentelor în memorie, pentru creșterea performanței rulării proceselor de integrare și îmbunătățire a accesului la date;
- suport pentru includerea sub-proceselor apelate dintr-un proces principal în tranzacția fluxului inițiator;
- facilități de activare a auditării fluxurilor;
- monitorizarea activității la nivelul proceselor, cu capabilități de colectare informații și raportare grafică;
- monitorizarea în timp real a indicatorilor de performantă (KPI). Definirea de alerte și acțiuni în cazul în care indicatorii de performantă nu ating anumite praguri valorice.

3.7.5. Componenta SGBD

Componenta bază de date tranzacțională trebuie să fie o bază de date de tip relațional, să fie disponibilă comercial (COTS – Commercial off the Shelf) și să ofere posibilitatea de a rula pe diverse platforme hardware virtualizate, pe sistemele de operare majore existente pe piață (Windows, Linux), precum și posibilitatea de a fi instalata într-o infrastructură Kubernetes. Baza de date tranzacțională va asigura persistenţa datelor ce vor fi manipulate la nivelul componentei de interoperabilitate, seturilor de date de tip registru precum și anumite surse de date specifice, oferind astfel capabilități de tip enterprise necesare îndeplinirii funcționalităților solicitate de către autoritatea contractantă.

Astfel, pentru a răspunde cerințelor de funcționalitate și performanță cerute, componenta de baze de date relaționale trebuie să prezinte următoarele capabilități minime și obligatorii:

Cerințe generale:

- să ofere suport pentru proceduri stocate, triggeri și tranzacții autonome;
- să permită definirea de indecși pentru acces rapid la date;
- să permită execuția paralela a operațiilor de tip SELECT, INSERT, UPDATE, DELETE, MERGE, cu blocarea doar a înregistrărilor afectate, nu a întregii tabele;
- să permită execuția de instrucțiuni INSERT în mai multe tabele simultan;
- reorganizarea, mutarea și redefinirea de tabele, indecși sau fișiere de date fără blocarea activității utilizatorilor la datele aflate în curs de modificare, indiferent de dimensiunea acestora;
- parametrii de memorie să poată fi ajustați dinamic și automat de către baza de date astfel încât zonele de memorie să fie dimensionate în concordanta cu tipul de operații ce se desfășoară la un moment dat iar pentru a face fata unui număr foarte mare de utilizatori, baza de date trebuie să ofere un mecanism de connection pooling care să optimizeze folosirea resurselor server-ului la operațiile de tip login/logout;
- să ofere mecanisme de asigurare a consistenței datelor în situația nefavorabilă a unui incident cum ar fi interogarea directa a tabelelor care să prezinte imaginea datelor exact așa cum erau acestea la un moment anterior în timp, anularea unei tranzacții care a fost comise sau restaurare rapidă a datelor, la nivel de tranzacție, tabelă sau bază de date toate acestea fără a fi necesară restaurarea dintr-un backup, efectuarea de snapshot-uri periodice sau întreținerea prin proceduri de utilizator a unor copii ale datelor

- să ofere un mecanism inclus care să permită interogarea istoricului modificărilor unei tabele, atât de tip DDL cat și DML, fără a necesita dezvoltarea de triggeri sau rutine definite de utilizator, salvarea periodica sau utilizarea funcției de audit;
- Posibilitatea de a suspenda temporar operații consumatoare de resurse (de exemplu încărcări masive de date), cu reluarea ulterioara a acestora în momentul când sistemul permite, precum și posibilitatea de a implementa scheme de prioritate în modul de accesare a bazei de date în funcție de tipul de utilizator inclusiv limitarea numărului de procesoare folosite de baza de date fără a fi necesar folosirea unei soluții de virtualizare;
- să ofere posibilitatea de izolarea din punct de vedere management și securitate a mai multor baze de date în contextul aceleași ă de baza de date;
- să ofere suport pentru date de tip multimedia;
- să ofere suport pentru tipuri de date de tip XML, JSON;
- să permită definirea tabelelor de tip „immutable” (datele din aceste tabele nu pot fi modificate, sunt permise doar operațiuni de insert), acestea putând fi utilizate la nivelul aplicației, fără a fi necesare modificări;
- să ofere un framework de dezvoltare de tip „low-code”, ce va permite dezvoltarea rapida a aplicațiilor fără a fi necesare cunoștințe avansate de dezvoltare;
- să ofere posibilitatea facila de a defini servicii de tip REST, peste obiecte sau proceduri stocate definite la nivelul bazei de date;

Înaltă disponibilitate:

- baza de date trebuie să permită funcționarea într-o arhitectură de înaltă disponibilitate de tip cluster, o singura baza de date putând fi instalata pe mai multe noduri asigurându-se toleranța la defecte hardware sau nefuncționare planificată;
- baza de date va permite balansarea încărcării între noduri, la nivelul cererilor și execuțiilor pe baza de date cluster, indiferent de natura cererilor, astfel se va permite citirea și scrierea pe oricare din nodurile clusterului de baza de date, fără impunerea niciunei limitări;
- securitate tranzacțională în cazul apariției unor erori hardware sau software în clusterul de baza de date trebuie să fie tratata de mecanismele interne ale bazei de date iar în cazul unei defecțiuni hardware și/sau software să permită reconectarea automată la nodul sau nodurile rămase disponibile;
- să ofere posibilitatea de upgradare și aplicare a patch-urilor online;

- să ofere posibilitatea adăugării de noduri suplimentare în cazul în care sistemul necesită mai multă putere de calcul (scalare pe orizontală).

Securitate și confidențialitate:

Ca și mecanisme de securitate oferite, componenta de baza de date tranzacțională trebuie să includă restricționarea accesului la nivelul obiectelor bazei de date, aplicarea simultana a mai multor politici de securitate pe un același obiect al bazei de date, precum și mecanisme native de restricționare a accesului utilizatorilor la nivel de înregistrare și coloană într-o tabelă. Baza de date trebuie să permită configurarea autentificării utilizatorilor pe baza de certificate digitale iar pentru sporirea siguranței datelor trebuie să asigure mecanisme robuste de criptare a datelor stocate cat și a celor vehiculate în timpul sesiunilor dintre utilizatori și baza de date. Toate operațiile de criptare trebuie să poată fi implementate într-un mod transparent, fără a implica modificări la nivel de aplicație de business sau client și să poată fi făcute, în funcție de nevoie, la nivel de coloană, tabelă sau chiar bază de date și să suporte cel puțin următorii algoritmi de criptare: 3DES (minim 168 bit) și AES (minim 256 bit).

Din punctul de vedere al activităților de audit, baza de date va oferi o listă cu operațiile pe care un grup sau o clasă de utilizatori le poate executa și va avea abilitatea de a se ajusta la gradul de detalii capturate de către facilitatea de audit, prin introducerea de politici de audit care să determine când un utilizator este sau nu auditat (spre exemplu situația când utilizatorul accesează doar anumite informații dintr-o tabelă sau când conectarea nu se face printr-o anumită aplicație).

De asemenea, baza de date va oferi nativ posibilitatea de a restricționa accesul utilizatorilor și administratorilor (DBA) la nivelul anumitor obiecte din baza de date și să permită impunerea de restricții inclusiv asupra comenzilor pe care aceștia le pot executa. Controlul accesului la baza de date se va asigura în mod transparent fata de aplicații prin implementarea unui mecanism de autentificare și autorizare condiționată, în funcție de parametri ca adresa de rețea, ora la care se încearcă conectarea, tip utilizator, locație de conectare. Astfel, baza de date va permite separarea atribuțiilor administratorilor la nivelul bazei de date, prin definirea de domenii de date, astfel încât administratorii bazei de date (DBA) să nu aibă acces la aceste domenii, ci doar administratorii de date desemnați explicit.

În vederea creșterii nivelului de securitate, baza de date va oferi suport pentru clasificarea datelor în cadrul tabelelor bazei de date, astfel încât un utilizator să aibă acces doar la datele care corespund nivelului său de clasificare. În ceea ce privește accesul la date, baza de date va

permite restricționare accesului utilizatorilor la anumite rânduri din tabele bazei de date pe baza de etichete și politici de securitate și va permite protejarea informației stocate în baza de date la nivel de tabela, prin oferirea accesului doar la un subset de informații (rânduri), pe baza rolului și responsabilităților acelui utilizator.

Backup:

Din punctul de vedere al operațiunilor de backup, baza de date trebuie să permită operațiuni de backup și restaurare a datelor în regim de lucru online, salvarea totală și/sau parțială a bazei de date, iar toate aceste operațiuni să fie făcute într-o formă unitară, centralizată și ușor de administrat. De asemenea, pentru optimizarea timpului alocat acestor operațiuni baza de date trebuie să ofere mai mulți algoritmi de compresie pentru datele salvate și să permită efectuarea de backup numai pentru fișierele care au suferit schimbări de la ultimul backup și pentru cele nou create (backup incremental). Operațiile de backup trebuie să permită citirea și scrierea paralelă (simultan din/în mai multe fișiere). În funcție de nevoie, baza de date trebuie să permită, pe baza datelor de backup restaurarea parțială la o imagine consistentă a acesteia de la un moment de timp specificat de cel ce realizează operația de restaurare.

Administrare și operare:

Pentru asigurarea performanţei maxime și asigurarea unui răspuns proactiv la eventualele degradări ale acesteia, baza de date trebuie să ofere mecanisme interne de monitorizare și diagnosticare continuă, automatizând colectarea parametrilor de funcționare ai bazei de date, precum și stocarea acestora pentru a putea furniza o imagine pe termen lung a modului de funcționare a bazei de date. Procesul de optimizare a instrucțiunilor SQL, trebuie să se facă automat, explorând în mod cuprinzător toate modalitățile de optimizare ale unei instrucțiuni SQL (inclusiv recomandarea de a fi creați indecși sau partiții adiționale), oferind sugestii de implementare pentru administratori, inclusiv posibilitatea de implementare fără a fi necesară modificarea codului aplicației.

Din punct de vedere al operațiunilor de administrare, soluția de baza de date trebuie să ofere o unealtă cu interfață grafică accesibilă web pentru administrarea bazei de date, care să includă următoarele facilități:

- construirea și executare scripturi SQL;
- gestionarea obiectelor bazei de date;
- efectuarea de funcții de backup și restaurare;

- administrare a utilizatorilor;
- monitorizarea bazei de date și vizualizarea fișierelor de tip log;
- vizualizarea în timp real a încărcării bazei de date, a activității utilizatorilor (inclusiv a interogărilor SQL pe care aceștia le rulează), a operațiilor mari consumatoare resurse (I /O și CPU) precum și raportarea acestor evenimente către administratori.

3.7.6. Componenta de Business Intelligence

Componenta de analiză și raportare trebuie să fie disponibilă comercial (COTS – Commercial off the Shelf), să ofere posibilitatea de a rula pe diverse platforme hardware virtualizate precum și pe sistemele de operare majore existente pe piață (Windows, Linux). Rolul acestei componente este de a defini analize detaliate și rapoartele necesare urmăririi modului de funcționare a componentelor software dezvoltate la nivelul platformei, modului în care datele sunt schimbate între diverse entități, precum și posibilitatea de unifica date din surse multiple de date. Pentru a îndeplini scopul mai sus descris, componenta de analiză și raportare trebuie să îndeplinească minimal următoarele cerințe:

- va oferi posibilitatea prezentării datelor în formate variate (de exemplu tabele, tabele pivot, grafice, texte derulante);
- va oferi funcționalități de navigare ghidată pentru utilizatorii finali, cu posibilități multiple de navigare dintr-un anumit punct, atât pentru rapoarte cât și pentru grafice;
- va permite combinarea rezultatelor obținute de pe platforme diferite la momentul interogării, astfel încât setul de date rezultat să fie unitar;
- va permite salvarea rapoartelor în formate diferite (Excel, PDF, Word, HTML);
- va oferi posibilitatea definirii de tablouri de bord și a includerii rapoartelor/graficelor în acestea, pentru toți utilizatorii finali, în funcție de drepturile fiecăruia;
- va permite tuturor utilizatorilor modificarea tablourilor de bord sau a rapoartelor, de a salva, organiza, administra și partaja rapoartele cu alți utilizatori;
- va facilita accesul la informație printr-un nivel de metadate care să ascundă utilizatorilor finali complexitatea structurilor fizice de date;
- nivelul de metadate expus utilizatorilor va fi comun la nivelul tuturor modulelor sistemului de raportare și analiză;
- utilizatorii își vor putea crea singuri propriile rapoarte (analize ad-hoc) fără să fie nevoiți să cunoască structurile fizice de date pe care le accesează;

- va permite accesarea datelor atât de pe platforme relaționale, cât și multidimensionale sau foi de calcul;
- va permite integrarea cu LDAP, oferind în același timp capabilități proprii de definire a rolurilor pentru restricționarea accesului la rapoarte;
- interacțiunea utilizatorilor finali cu aplicația se va face într-o interfață de tip web, fără a necesita instalarea de componente software suplimentare pe calculatoarele utilizatorilor;
- va expune o interfață de administrare atât a drepturilor de acces la diferite zone cât și a drepturilor de acces pe diferite tipuri de acțiuni;
- va fi scalabilă și va dispune de mecanisme de clustering a componentelor, astfel încât să poată fi adăugate ulterior resurse hardware virtuale suplimentare;
- va oferi posibilitatea prezentării simultane a aceleiași informații în formate diferite, printr-o singură execuție a interogării: de exemplu tabel + grafic;
- va permite facilități avansate de formatare a rapoartelor;
- va oferi posibilitatea de salva, organiza și partaja rapoartele cu alți utilizatori;
- va oferi capabilități de drill-down (navigare în adâncime) pe diferite nivele de agregate;
- generarea interogărilor către bazele de date va ține seama de specificul bazei de date accesate;
- va permite acces la surse de date multiple, în mod transparent pentru utilizatorul final;
- accesul utilizatorului final se va face dintr-o singură interfață web din care să aibă acces la toate componentele de analiză și raportare;
- din punctul de vedere al arhitecturii sistemului de raportare, toate componentele sale vor fi strâns integrate, vor face parte dintr-un mediu unitar de lucru și vor împărtăși un sistem de securitate comun;
- va oferi utilizatorilor posibilitatea agregărilor personalizate pe nivel, atât în baza de date, cât și în aplicația de analiza și raportare;
- va dispune de mecanisme de alertare pentru utilizatorii finali;
- va oferi utilizatorilor finali posibilitatea subscrierii la alertele definite;
- rapoartele analitice să poată fi construite pe un număr variabil de interogări analitice. Instrumentul de business intelligence nu trebuie să limiteze numărul de astfel de interogări;
- va asigura posibilitatea de writeback (scriere) în baza de date din aplicația de raportare;

- este necesar ca aplicația de raportare să poată afișa anumite valori identificate ca și critice, să semnalizeze depășirea unor praguri ale acestor valori, să semnalizeze apariția unor evenimente. Astfel, va oferi utilizatorilor posibilitatea de formatare condiționată a valorilor prin setarea unor praguri, pentru a evidenția valorile excepționale;
- să nu necesite replicarea datelor pe un server separat, ci să folosească capabilitățile bazei de date sursă;
- mediul de lucru pentru utilizatorii finali sau alți dezvoltatori de rapoarte/analize să fie în mediu web pur, interacțiunea cu sistemul să se realizeze prin operațiuni de tip „point and click" și „drag and drop" (sa nu necesite cunoștințe de programare din partea utilizatorilor) ;
- să ofere posibilitatea definirii de rapoarte înlănțuite, datele din raportul copil fiind filtrate pe baza rezultatelor din raportul părinte;
- să permită tuturor utilizatorilor crearea sau modificarea de rapoarte, analize ad-hoc și tablouri de bord, acordarea drepturilor specifice (consultare, creare de obiecte etc.) urmând a fi făcută de către administratorul platformei;
- să ofere cel puțin algoritmi analitici de tipul regresie sau clusterizare accesibili utilizatorilor din interfața platformei;
- să permită detectarea de paternuri /relații prin selectarea datelor dintr-o vizualizare , selectare care să realizeze automat evidențierea datelor corelate din toate vizualizările existente în pagină;
- să ofere posibilitatea de combina seturi de date multiple și de definire a cheilor de legătură în interfața web;
- să ofere posibilitatea de modifica manual dimensiunilor obiectelor afișate;
- să ofere posibilitatea de dimensiona automat obiectele afișate astfel încât să utilizeze tot ecranul;
- să permită folosirea datelor externe imediat ce au fost încărcate, fără a solicita activități de modelare a datelor
- posibilitatea de a efectua transformări primare la încărcarea datelor
- posibilitatea de a combina datele din fișiere externe cu date modelate în ariile de subiecte din platforma analitică;
- posibilitatea de a crea rapoarte analitice pe dispozitive mobile;

- să permită crearea de snapshoturi ale vizualizatorilor create astfel încât să permită partajarea rezultatelor analitice cu ceilalți utilizatori ai sistemului, prin parcurgerea ordonata a activităților de interpretare a datelor;
- să permită definirea de mărimi calculate prin aplicarea unor funcții matematice predefinite asupra mărimilor existente;
- să permită crearea automată a unor reprezentări sugestive pentru informațiile selectate de utilizator și să permită utilizatorului alegerea tipului de vizualizare din paleta de obiecte disponibile;
- să permită afișarea pe hartă a informațiilor, oferind suport pentru filtrarea informațiilor după criterii geospațiale prin selectarea pe hartă a ariei geografice de interes;
- să ofere posibilitatea de partajare a conținutului analizelor efectuate, într-un mod securizat, cu alți membrii ai echipei de lucru, alte departamente etc.

Numărul de utilizatori al soluției de tip BI este de 50.

3.7.7. Componenta de mascare a datelor

Sistemul propus asigură confidențialitatea informațiilor necesare pentru operare, accesul la interfața de administrare făcându-se pe bază de nume de utilizator și parolă. Totodată, sistemul asigură integritatea datelor transmise, actualizate, vizualizate sau înregistrate.

Toate informațiile despre utilizatori vor fi confidențiale în limitele stabilite prin politica de securitate. Aceste limite sunt stabilite în funcție de rolul pe care îl are fiecare utilizator în cadrul sistemului informatic propus. De asemenea, se vor respecta legislația și reglementările internaționale privind protecția intimității și a datelor personale.

Prin intermediul unei componente specializate de administrare, persoanele acreditate (administratori de sistem) vor putea restricționa accesul în anumite zone ale sistemului informatic, la anumite documente sau date, după cum va fi necesar, pentru a acorda drepturi doar anumitor utilizatori sau grupuri de utilizatori.

Cu ajutorul acestei politici, utilizatorii vor putea vizualiza, modifica sau adăuga documente/înregistrări numai în limita drepturilor de acces asociate, asigurându-se confidențialitatea datelor.

Din motive de securitate parolele utilizatorilor nu vor fi păstrate în baza de date, ci se vor păstra criptate într-un director LDAP centralizat.

Cerințe pentru componenta de mascare a datelor

În vederea îndeplinirii obiectivelor stabilite cu privire la mediul de testare/dezvoltare și totodată pentru asigurarea confidențialității informațiilor și protejării datelor cu caracter personal, sistemul informatic va include o componentă de mascare pentru transferul din bazele de date de producție în cele de testare/dezvoltare.

Existența unor date de testare consistente și suficiente reprezintă o necesitate pentru realizarea unui proces de testare eficient și concludent, fără date de testare similare condițiilor de utilizare extreme (atât din punct de vedere cantitativ cât și calitativ) orice testare realizată asupra sistemului nu va fi relevantă din punct de vedere al funcționării acestuia în producție.
Soluția trebuie să îndeplinească următoarele caracteristici tehnice minime:

- soluția trebuie să poată profila date existente pentru descoperirea automată a modelului de date și a conținutului sensibil;
- soluția trebuie să asigure generarea de date în conformitate cu următoarele formate:
    - Oracle DB Server, MySQL;
    - IBM DB2 / 400 iSeries;
    - Microsoft SQL Server;
    - PostgreSQL;
    - Sybase;
    - Fișierele XML, SQL, CSV, fișiere JSON, fișiere XLS.
- soluția trebuie să permită repetarea procesului de generare a datelor după ce modelul de date a fost definit, în scopul de a recrea datele pentru teste;
- soluția trebuie să dispună de posibilitatea creării de date invalide, bazate pe cererile utilizatorilor;
- soluția trebuie să fie capabilă să modifice date sensibile, cu un conținut alternativ. O astfel de capacitate trebui să includă următoarele funcții:
    - conservarea genului - atunci când substituie nume, nume masculine sunt substituite numai cu alte nume de sex masculin, și în mod similar de sex feminin, cu doar nume feminine;
    - conservarea integrității semantice - păstrarea constrângerilor aplicate unui set de date ca o valoare maximă sau pentru numere de card de credit;
    - valoarea cumulată - valorile totale și medii ale unei coloane mascată de date ar trebui să fie păstrate, fie strâns sau fie cu precizie.

- abilitatea de a extrage în mod condiționat seturi de date intacte referențial, în mod constant din multiple tipuri de baze de date sau fișiere;
- soluția trebuie să dispună de capacitatea de a asocia cazuri de testare cu atributele de date necesare, de a le găsi în conținutul de date existente și de a le rezerva pentru utilizatori autorizați și de a bloca înregistrările/cheile de la alte utilizări de testare;
- soluția trebuie să aibă capacitatea de a descoperi automat relațiile între date și de a oferi, de asemenea, posibilitatea administratorilor să modifice regulile de descoperire utilizate;
- soluția trebuie să furnizeze o analiză a datelor și a metadatelor bazelor de date descoperite
- urmare a procesului de descoperire, soluția trebuie să furnizeze rapoarte și documentare cu privire la datele descoperite;
- soluția trebuie să dispună de capacitatea de a înțelege modelele de date, în scopul de a menține integritatea referențială într-o bază de date. De asemenea, soluția trebuie să fie capabilă de a înțelege modelele de date, în scopul de a menține integritatea referențială între diferite baze de date;
- soluția trebuie să dispună de posibilitatea modificării datelor generate;
- soluția trebuie să fie capabilă să ruleze într-un mod de test regulile de anonimizare pentru a testa efectul pe care îl are mascarea, înainte de a aplica mascarea la datele complete existente;
- soluția trebuie să permită o mascare directă a datelor;
- soluția trebuie să permită programarea rulării funcțiilor de mascare a datelor;
- soluția trebuie să fie capabilă să lucreze și cu date care nu sunt 100% corecte, pentru a putea folosi aceste date greșite în timpul procesului de testare. Soluția trebuie să fie configurabilă astfel încât și aceste date să fie prelucrate;
- soluția trebuie să fie capabilă să genereze date invalide pentru a fi folosite în teste specifice;
- soluția trebuie să ofere posibilitatea extragerii unui subset de date care să fie mascate și să poată fi prelucrate în procesul de testare;
- soluția trebuie să suporte autentificarea folosind integrarea cu sisteme de tip LDAP;

- soluția trebuie să ofere mecanisme de control a accesului la date bazate pe utilizatori, roluri și grupuri;
- soluția trebuie să ofere suport pentru utilizatorii dintr-un director LDAP cu posibilitatea de criptare a transportului folosind TLS (LDAPS);
- soluția trebuie să ofere rapoarte care să evidențieze date vulnerabile care trebuie mascate;
- soluție trebuie să fie capabilă să identifice dimensiuni de date care există în mediul de producție și să lege aceste informații fie cu informații personale sintetice sau informații mascate pentru a crea date similare celor din producție, care să poată fi provizionate, fără să conțină date reale;

3.7.8. Securizare Acces Servicii Electronice

Datorită cerințelor de integrare ale sistemului PDURo cu sisteme externe, este necesară securizarea accesului la serviciile web expuse către aceste sisteme externe și scăderea costurilor operațiunilor administrative legate de controlul accesului la aceste servicii, prin implementarea unei componente de securizare a accesului la interfețe web în mod centralizat.

Platforma de securizare a accesului la servicii electronice va facilita schimbul de date cu acuratețe, în mod eficient și în condiții de siguranță între diferite sisteme informatice (atât din cadrul autorității contractante cât și din cadrul altor instituții cu care există sau vor exista protocoale de colaborare) conform proceselor de lucru operaționale specifice instituțiilor implicate.

Platforma trebuie să îndeplinească următoarele cerințe de bază:

- platforma trebuie să fie o aplicație software de tip COTS (Commercial Off-The-Shelf) cu licențiere perpetuă (drept de utilizare pe perioadă nedeterminată);
- platforma trebuie să fie disponibilă ca appliance software integrabil în platforma de virtualizare oferită, securizat de către producător, astfel încât să fie prevenit accesul neautorizat la funcțiile de sistem ale soluției;
- toate funcționalitățile platformei oferite de ofertant trebuie confirmate prin citate și/sau extrase din documentația producătorului disponibilă public (se include în oferă URL-ul ce prezintă informațiile relevante) sau se transmite documentația tehnică în cadrul Propunerii Tehnice. În caz de neconcordanță între documentația producătorului și ofertă primează documentația producătorului;

- să asigure capabilități de WS/API firewall și funcții de control acces pe baza de politici de acces de tip RBAC;
- soluția trebuie să realizeze conversia XML-JSON direct fără a fi nevoie de scheme separate pentru XML și JSON. Tranformarea XML-JSON trebuie să fie bidirecțională, XML-JSON și JSON-XML;
- soluția trebuie să detecteze automat atașamentele SOAP;
- soluția trebuie să permită definirea și detectarea de atașamente neașteptate sau incompatibile cu cerințele definite;
- soluția trebuie să detecteze cererile XML cu un număr foarte mare de atribute ceea ce indică un atac la nivel de conținut.

Soluția trebuie:

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

    - Security Assertion Markup Language (SAML);
    - ticket Kerberos;
    - token OAuth.
- să suporte SAML;
- să poată fi integrat cu soluții de tip directory incluzând directoare compatibile LDAP, RADIUS și Microsoft ActiveDirectory;
- să poată converti alte tipuri de tokenuri într-un token SAML;
- să aibă o funcție de Cache al tokenului pentru a oferi funcționalitatea de SSO peste mai multe backenduri care oferă servicii web;
- să poată monitoriza și alerta în cazul în care unul sau mai multe servicii API expuse nu sunt disponibile;
- să poată monitoriza și alerta în cazul în care unul sau mai multe servicii API expuse au o performanta deteriorate, sub nivelul unei limite pentru: timp de răspuns și număr de reîncercări;
- să poată prioritiza traficul pe baza clientului sau serviciului accesat;
- să dispună de un mecanism de cache pentru:
    - răspunsuri la interogări care să reducă traficul către backend-uri;
    - atribute interogate din surse externe;
    - tokenuri de securitate pentru evitarea cererilor repetate de autorizare și autentificare.
- să ofere tablouri de bord și rapoarte configurabile;
- să ofere flexibilitate pentru auditarea evenimentelor, permițând configurarea tipurilor de evenimente auditate;
- să permită logarea evenimentelor la nivel de servicii, client și tranzacții;
- să ofere următoarele opțiuni de logging:
    - fișier log local;
    - server Syslog;
    - Windows Event Log;
    - bază de date;
    - trap SNMP;

- email.

- să permită posibilitatea separării evenimentelor de securitate de cele care privesc tranzacțiile.

3.7.9. Platforma de gestiune a accesului utilizatorilor și a securității sistemului

Platforma va asigura funcționalitățile necesare pentru gestiunea utilizatorilor interni (ADR și administratorii instituțiilor publice partenere care vor face parte din sistemul PDURo) și asigurarea securității utilizării sistemului pentru:

- protejarea sistemului informatic împotriva accesului neautorizat;
- acordarea accesului la informații pe baza necesității de a cunoaște;
- segregarea rolurilor utilizatorilor și evitarea acumulării de roluri nejustificate;
- accesul facil la funcțiile sistemului pentru utilizatorii autorizați.

Pentru implementarea acestor principii, platforma trebuie să îndeplinească următoarele funcționalități minimale:

- soluție software sau suita de aplicații integrate trebuie să fie disponibile comercial (COTS – Commercial Off-The-Shelf) cu licențiere perpetuă (drept de utilizare pe perioadă nedeterminată);
- toate funcționalitățile platformei oferite de ofertant trebuie confirmate prin citate și/sau extrase din documentația producătorului disponibilă public (în acest caz se include în ofertă URL-ul ce prezintă informațiile relevante) sau transmisă atașat în cadrul Propunerii Tehnice. În caz de neconcordanță între documentația producătorului și ofertă primează documentația producătorului;
- platforma trebuie să asigure următoarele funcționalități de bază:
    - să ofere o imagine unitară a conturilor de acces asociate unui utilizator;
    - în funcție de specificul fiecărui angajat în parte și de regulile din sistem, acestuia îi vor fi alocate în mod automat resurse (conturi de acces în soluțiile din cadrul sistemului informatic);
    - orice schimbare în profilele de utilizatori, care ar putea avea impact asupra drepturilor de acces la soluțiile informatice (de exemplu schimbarea poziției,

departamentului, etc) trebuie să se reflecte în schimbarea rolurilor asociate utilizatorilor respectivi în mod automat;

- în cazul în care un angajat pleacă din organizație platforma trebuie să revoce automat toate drepturile de acces ale utilizatorului, astfel încât să se prevină tentativele de acces neautorizat;
- când un utilizator pleacă din organizație sau accesul nu mai este necesar în urma schimbării rolului, soluția trebuie să permită atât revocarea automată, cât și manuală a acestuia, conform cu politicile de acces din sistem;
- trebuie să expună o interfață web către utilizatori (self-service) care să permită vizualizarea și modificarea informațiilor din profilul propriu;
- trebuie să expună o interfață web către administratori care să permită vizualizarea și modificarea informațiilor din profilul propriu și profilele angajaților administrați
- să permită definirea drepturilor de acces ca set de bază specific poziției în organizație și definirea de roluri suplimentare, care vor putea fi alocate la cerere, pe baza de aprobare;
- Utilizatorii trebuie să poată urmări stadiul cererilor proprii – în timp real, la orice moment, folosind interfață grafică web;
- administratorii trebuie să poată urmări stadiul cererilor proprii și alocate lor – în timp real, la orice moment, folosind interfață grafica web;
- pentru depanare și verificare, administratorii trebuie să poată urmări stadiul cererilor utilizatorilor din subordine – în timp real, la orice moment, folosind interfața grafică web, dar fără a putea interveni în fluxul solicitării;
- pentru integrare ușoară cu celelalte sisteme, fluxurile de creare/modificare/revocare conturi pentru utilizatori trebuie să fie configurabile prin interfața web;
- pentru evitarea blocajelor în operarea sistemelor (de exemplu pentru situațiile în care utilizatorii sunt temporar indisponibili), platforma trebuie să permită administrarea delegată a drepturilor de acces;
- platforma trebuie să poată realiza alocarea de drepturi de acces către utilizatori pe baza de politici de acces asociate anumitor departamente, poziții sau altor atribute legate de profilul utilizatorului;

- platforma trebuie să blocheze accesul utilizatorilor neautorizați la toate funcționalitățile sistemului – cu excepția informațiilor definite ca informații publice cu acces nerestricționat. Pentru accesul la informațiile și funcționalitățile sistemului, platforma va realiza:
    - autentificarea și autorizarea utilizatorilor – pentru accesul la informațiile / funcționalitățile confidențiale platforma va solicita autentificarea cu 2 factori de autentificare. Cel de-al doilea factor de autentificare va putea fi (la alegerea beneficiarului): cod temporar transmis prin e-mail sau SMS, mesaj push într-o aplicație mobilă specifică, cod temporar generat de o aplicație mobilă compatibilă;
    - acces de tip RBAC – platforma va permite definirea de roluri specifice activității Autorității Contractante, un utilizator care are asignat unui rol va primi automat toate drepturile de acces specifice rolului respectiv. Un utilizator va putea avea asignate mai multe roluri, cumulând toate drepturile de acces aferente rolurilor respective. Totuși, pentru a evita riscurile de securitate asociate utilizatorilor cu drepturi multiple de acces, platforma trebuie să asigure realizarea automată a unei analize de risc care să calculeze pentru fiecare utilizator un scor de risc aferent drepturilor de acces ale utilizatorului respectiv. Scorul de risc trebuie actualizat automat în situația în care utilizatorului îi este asignat un nou rol în cadrul sistemului sau utilizatorul solicită noi drepturi de acces, astfel încât aprobarea drepturilor de acces (atât la acordare cât și la verificarea periodică a acestora) să fie realizată având în vedere analiza riscurilor de securitate aferente;
- platforma trebuie să ofere acces facil, printr-o interfață web, la toate funcționalitățile de administrare și configurare, și să includă funcționalități de ”auto-servire” a utilizatorilor, prin care aceștia să poată realiza majoritatea operațiunilor fără a solicita intervenția unui administrator. La inițierea unei cereri a unui utilizator, platforma trebuie să utilizeze fluxuri predefinite de aprobare iar, în cazul aprobării solicitării, operațiunea trebuie implementată în mod automat, prin funcționalități specifice ale platformei, fără a fi necesară realizare de operațiuni manuale de configurare. Astfel de operațiuni de ”auto-servire” vor include cel puțin:
    - înregistrarea în cadrul sistemului – atât pentru utilizatorii interni cât și pentru utilizatorii externi;

- acces la funcționalitățile / aplicațiile din cadrul sistemului – altele decât cele asignate automat pe baza rolului specific;
- acces de tip administrator la servere / echipamente rețea / baze de date / aplicații etc.;
- resetare parolă de acces;

- platforma trebuie să ofere utilizatorilor funcționalități pentru a urmări în timp real stadiul aprobării solicitărilor înregistrate în sistem;
- platforma trebuie să asigure protejarea documentelor confidențiale prin:
  - pentru Directoare dedicate stocării documentelor confidențiale: specificarea detaliată a drepturilor de acces la Directorul respectiv, incluzând utilizatorii care pot accesa Directorul și aplicațiile ce pot fi utilizate în acest scop. Accesul tuturor celorlalți utilizatori, inclusiv administratori de sistem, trebuie să fie refuzat;
  - pentru documente individuale: specificarea detaliată a drepturilor de acces la documentul respectiv, incluzând utilizatorii care pot accesa documentul și aplicațiile ce pot fi utilizate în acest scop. Accesul tuturor celorlalți utilizatori, inclusiv administratori de sistem, trebuie să fie refuzat;
- platforma trebuie să asigure capabilități avansate de securizare a accesului, incluzând cel puțin:
  - combinarea accesului bazat pe roluri cu atribute din profilul utilizatorului, inclusiv atribute definite specific în cadrul platformei;
  - analiza riscului asociat tentativelor de autentificare ale utilizatorilor utilizând elemente de analiză complexe – cel puțin: poziție geografică, device utilizat, comportament utilizator – analiza trebuie să aibă ca rezultat decizii automate, respectiv: acordă acces la sistem, blochează accesul la sistem, inițiază autentificarea cu doi factori de autentificare sau rutează tentativa de autentificare către o echipă de analiză în timp real care va acorda sau refuza accesul la sistem;
- platforma trebuie să asigure definirea de modalități de acces specifice pentru furnizori/colaboratori, valabilitate limitată de timp, la expirarea termenului definit în platformă accesul trebuie să fie refuzat;

- platforma trebuie să monitorizeze integritatea aplicațiilor și a fișierelor care conțin date confidențiale și să raporteze modificarea ne-autorizată a acestora cu blocarea automată a execuției fișierelor executabile;
- platforma trebuie să includă politici pentru managementul parolelor de acces: lungime parolă, sintaxă parolă, dicționar de parole interzise etc. Parolele utilizatorilor trebuie să fie stocate criptat de către platformă, utilizând algoritmi de criptare moderni. În plus, platforma trebuie să poată genera parole în mod automat la înregistrarea utilizatorilor, să poată înregistra parole pentru conturile de sistem administrate în cadrul sistemelor destinație și să asigure politici de parole multiple pentru aceeași resursă;
- platforma trebuie să colecteze automat informații de audit și să includă o gama extinsă de activități și rapoarte de audit (atât rapoarte predefinite cât și rapoarte definite de beneficiar), incluzând cel puțin:
    - rapoarte privind accesul la sistem – tentative de autentificare reușite și tentative de autentificare nereușite, tipuri de conturi de acces, utilizatori care au acces la o anumită resursă/funcționalitate, conturi inactive;
    - monitorizarea periodică a drepturilor de acces și re-aprobarea periodică a accesului de către management la nivel de resursă accesată. Conturile fără utilizator definit sau cu un utilizator inactiv trebuie să fie identificate și anulate automat de către platformă, fără a fi necesară aprobarea de către management;
    - Monitorizarea și controlul accesului la directoarele și fișierele care conțin informații cu caracter restricționat, la procesele de sistem, la operațiunile copiere sau ștergere a datelor sensibile;
- pentru a asigura accesul permanent la resursele sistemului, Platforma trebuie să includă o arhitectură High-Availability (HA) prin funcționalitățile proprii, fără a utiliza clustering la nivel de sistem de operare și/sau virtualizare.

3.7.10. Monitorizare date, sisteme și aplicații

Având în vedere complexitatea tehnică și funcțională a sistemului PDURo, precum și importanța acestuia, devine esențială necesitatea implementării unei soluții de management de aplicații care să elimine discontinuitatea serviciilor oferite de IT către zona funcțională, unificând în acest fel cele două componente.

Platforma pentru monitorizarea performanței resursei virtuale aferente sistemului PDURo va conlucra pentru detectarea și remedierea imediată, pe cât posibil automată, problemelor de funcționare care afectează utilizarea în bune condiții a sistemului informatic și îndeplinirea sarcinilor de serviciu.

Platforma trebuie să fie o aplicație software sau o suită de aplicații integrate disponibile comercial (COTS – Commercial Off-The-Shelf) cu licențiere perpetuă (drept de utilizare pe perioadă nedeterminată);

Platforma trebuie să asigure următoarele funcționalități minimale:

- monitorizarea unificată a aplicațiilor, bazelor de date, resurselor virtualizate și software;
- generare de alerte bazate pe reguli prestabilite pentru fiecare tehnologie în parte;
- integrarea cu sistemul LDAP, cu definirea de roluri tehnologice și de securitate pentru acces diferențiat.

Platforma trebuie să fie capabilă să:

- ofere tablouri de bord intuitive, asigurând astfel o învățare ușoară și rapidă a soluției;
- ofere panouri de control predefinite pentru:
    - administrarea soluției;
    - monitorizarea bazelor de date;
    - monitorizarea sistemelor de operare;
    - monitorizarea LDAP;
    - monitorizarea infrastructurilor de virtualizare și a sistemelor hibride;
    - monitorizarea containerelor.
- să ofere posibilitatea definirii de panouri de control personalizate;
- să furnizeze o paletă foarte largă de șabloane predefinite pentru monitorizarea resurselor virtualizate, pentru generarea de rapoarte, precum și posibilitatea construirii de rapoarte personalizate;
- să permită generarea automată de rapoarte la intervale predefinite și transmiterea acestora prin e-mail către utilizatori predefiniți;
- să furnizeze mecanisme de notificare prin care să transmită alerte prin email și SMS atunci când anumite praguri critice sunt depășite.

Platforma trebuie să asigure monitorizarea resurselor virtualizate și software:

- ✓ **Monitorizarea resurselor virtualizate – platforma trebuie să realizeze:**
  - monitorizarea la nivel de sistem de operare Windows/Linux/Unix;
  - analiza a proceselor active pentru a determina care dintre acestea afectează performanțele mașinilor virtuale și care mașini virtuale nu utilizează eficient resursele;
  - să includă o interfață predefinită de prezentare în timp real în format tabelar și grafic a metricilor (parametrilor de funcționare) a resurselor virtualizate care să conțină date intuitive, cu panouri de control dedicate care să prezinte o imagine de ansamblu și de detaliu a infrastructurii de virtualizare;
  - monitorizarea metricilor de performanță pentru fiecare mașină virtuală – cel puțin încărcare CPU, memorie, disc, interfață de rețea să asigure declanșarea de acțiuni automate pe baza datelor detectate astfel încât să asigure remedierea automată a problemelor de performanță;
  - monitorizarea în detaliu a soluțiilor de containerizare și clusterizare a containerelor – cel puțin Docker și să asigure declanșarea de acțiuni automate complexe, ca de exemplu: repornire/oprire container pe baza datelor detectate astfel încât să asigure remedierea automată a problemelor de performanță;
  - monitorizarea apariției unui anumit text în fișiere de jurnal (log) și să asigure declanșarea de acțiuni automate complexe pe baza datelor detectate în fișierele jurnal (log);
  - determinarea în mod automat a performanței "normală" de funcționare a componentelor de infrastructură monitorizate și să determine modele de funcționare normală bazate pe oră, zi, săptămână etc. De asemenea, soluția trebuie să asigure capacitatea de a genera alarme / evenimente în cazul depășirii valorilor normale de funcționare;
  - identificarea configurației hardware și software a mașinilor virtuale și să detecteze automat orice modificare a configurației acestora (modificare configurație hardware, instalare / dezinstalare software etc) cu generarea automată a unei alerte;

- distribuirea automată, de la distanță de patch-uri de securitate, update-uri de sisteme de operare precum și de noi aplicații sau noi versiuni ale aplicațiilor specifice de business;
- platforma trebuie să includă funcționalitatea de descoperire automată a mașinilor virtuale din rețeaua Beneficiarului și va realiza un inventar hardware și software al acestora
  - inventarul software va include cel puțin: tipul sistemului de operare, aplicațiile software instalate, service packs și update-uri de securitate instalate
  - inventarul mașinilor virtuale trebuie să includă cel puțin: procesor, memorie RAM, HDD, setări de rețea (DNS, Gateway, Subnet mask).

✓ **Monitorizarea sistemelor de operare**

- platforma trebuie să permită monitorizarea sistemelor de operare care stau la baza aplicațiilor, bazelor de date și dispozitivelor de rețea din infrastructura IT. În acest sens, va permite colectarea parametrilor de funcționare la nivel de CPU, memorie, intrări/ieșiri, tendințe de utilizare a spațiului de stocare, precum și a proceselor care rulează pe fiecare server / mașină virtuală. Toate aceste date vor fi agregate cu datele legate de diverse evenimente, date de monitorizare a bazelor de date și resurselor virtualizate pentru furnizarea unei monitorizări globale a performanței sistemului;
- platforma trebuie să ofere o perspectivă similară (model unificat) a colecțiilor de resurse monitorizate indiferent de sistemul de operare monitorizat;
- platforma trebuie să asigure capabilități de diagnosticare grafică afișând metrici în timp real și oferind posibilitatea de a naviga la metrici conexe efectuând click pe reprezentările grafice (drill-down).
- platforma trebuie să asigure:
  - monitorizarea conținutului fișierelor log și să genereze alarme atunci când identifică anumite expresii definite;
  - monitorizarea timpului de răspuns la accesarea diferitelor URL-uri;
  - identificarea blocajelor la nivelul sistemelor de operare prin monitorizarea fluctuațiilor la nivel de procese;

- prezentarea parametrilor de funcționare (CPU, memorie rețea, utilizare disc) în timp real pentru un număr configurabil de sisteme, astfel încât să ofere o imagine de ansamblu asupra stării de funcționare a infrastructurii IT la nivel de sistem de operare, cu afișarea alarmelor pe diferite niveluri de severitate.

✓ **Monitorizarea LDAP**

- platforma trebuie să detecteze, diagnosticheze și să rezolve problemele de performanță, disponibilitate și replicare la nivelul LDAP atât în medii fizice, cât și virtuale;
- platforma trebuie să dispună de un panou de control dedicat ce prezintă o imagine de ansamblu a infrastructurii LDAP (numărul de incidente de tip normal, avertisment, critic, fatal) la nivel de forest, domeniu, site, controler de domeniu;
- soluția trebuie să includă o serie de rapoarte cu informații referitoare la disponibilitatea și performanțele LDAP, printre care:
  - rapoarte referitoare la alarmele LDAP;
  - rapoarte de utilizare, precum și rapoarte de sumar și de detaliu ale resurselor hardware pentru controlerele de domeniu.
- soluția trebuie să includă o interfață de prezentare în timp real în format tabelar și grafic a metricilor (parametrilor de funcționare) la nivel de controler de domeniu – nivelul de consumare al resurselor (CPU, memorie, spațiu disc, rețea) precum și un clasament al serverelor controler de domeniu pe tip de resursă consumată (CPU, memorie, rețea, spațiu disc) la nivel de site;
- soluția trebuie să includă o interfață de administrare a regulilor ce condiționează severitatea incidentelor la nivelul LDAP cu posibilitatea sortării acestora după gradul de severitate, stare activă/inactivă.

✓ **Monitorizarea rețelei**

- platforma trebuie să monitorizeze funcționarea și disponibilitatea dispozitivelor de rețea virtuale;
- platforma trebuie să asigure următoarele funcționalități:
  - să fie capabilă să colecteze informații despre tranzacțiile echipamentelor de rețea prin intermediul ICMP (Internet Control Message Protocol) și SNMP;

- să poată afișa atât informații privind disponibilitatea dispozitivelor de rețea virtuală, cât și performanța acestora;
- să permită adăugarea/modificarea/eliminarea manuală a dispozitivelor virtuale și locațiilor de rețea și configurarea parametrilor de colectare pentru acestea;
- să permită configurarea intervalului la care se efectuează colectarea datelor;
- să permită verificarea rapidă a disponibilității unui dispozitiv virtual, fără a necesita colectarea de date despre performanța acestuia;
- să permită configurări avansate pentru colectarea de date, cum ar fi numărul și mărimea pachetelor de ping, sau timpul maxim de așteptare pentru Trace Route;
- să poată colecta și afișa date de disponibilitate, timp de răspuns și pachete pierdute referitoare la performanța echipamentelor virtuale de rețea.

✓ **Monitorizarea bazelor de date**

- platforma trebuie să poată monitoriza platforme eterogene de baze de date, ajutând astfel la reducerea costurilor administrative și la îmbunătățirea nivelului serviciilor. Trebuie să poată monitoriza cel puțin următoarele soluții de baze de date: Cassandra, DB2, MongoDB, Microsoft SQL Server, MySQL, Oracle (inclusiv RAC), PostgreSQL;

- platforma trebuie să asigure următoarele capabilități:
  - să ofere interfețe unitare pentru toate platformele de baze de date;
  - să poată monitoriza baze de date instalate fie pe medii fizice, fie pe medii virtuale;
  - să monitorizeze componentele bazelor de date pentru a asigura funcționarea acestora în limitele capacității resurselor;
  - să ofere o vizualizare de ansamblu a stării de sănătate a tuturor instanțelor bazelor de date;
  - să declanșeze alarme atunci când anumite valori de referință sunt încălcate;
  - să poată colecta date fără necesitatea instalării unui agent local, ci prin agenți la distanță, asigurând astfel un consum minim de resurse suplimentare;

- să dispună de un mecanism de eliminare a alarmelor false prin impunerea de praguri adaptive, să poată fi programate perioade de oprire și mentenanță, în care generarea de alarme va fi suprimată.

3.7.11. Componenta de securizare a mașinilor virtuale

Soluția de securizare a mașinilor virtuale trebuie să asigure următoarele funcționalități minime:

- să implementeze un sistem de autentificare bazat pe 2 factori pentru accesul administratorilor la mașinile virtuale configurate în cadrul platformei de virtualizare;
- să monitorizeze permanent accesul la mașinile virtuale configurate în cadrul platformei precum și operațiunile efectuate asupra acestora. Oprirea sau repornirea unei mașini virtuale nu va fi permisă indiferent de nivelul de acces al utilizatorului – inclusiv pentru utilizatori de tipul root sau Windows Admin;
- să monitorizeze permanent resursele de procesare ale mașinilor virtuale:
    - pentru fiecare mașină virtuală din cadrul platformei de virtualizare soluția trebuie să asigure monitorizarea resurselor de tip: procese, CPU, memorie etc.;
    - pentru fiecare mașină virtuală din cadrul platformei de virtualizare, componenta va asigura înregistrarea operațiunilor executate de utilizatorii cu drepturi de administrare (de tip root / Windows Admin etc) pentru a garanta securitatea sistemelor și pentru audit;
    - pentru fiecare mașină virtuală din cadrul platformei de virtualizare, componenta va permite stabilirea unei liste de comenzi interzise (de tip blacklist) care nu vor putea fi rulate pe mașina respectiva nici de utilizatorii cu drepturi de administrare (de tip root / Windows Admin etc);
    - soluția trebuie să permită definirea de politici de acces la mașinile virtuale pe baza de criterii multiple: interval orar, metoda de acces, metoda de logare etc.;
    - soluția trebuie să permită definirea de politici de acces individualizate pentru mașinile virtuale, în funcție de rolul acestora;
    - soluția trebuie să asigure administrarea și definirea de politici într-un mod centralizat, indiferent de sistemul de operare care rulează pe mașinile virtuale configurate în cadrul platformei;

- soluția trebuie să asigure funcționalități de management al parolelor de administrator pentru mașinile virtuale definite în cadrul platformei de virtualizare, atât în ceea ce privește sintaxa și complexitatea parolelor cât și privind modificarea automată a acestora la intervale de timp configurabile;

- soluția oferită trebuie să dețină o certificare de securitate emisă de o instituție independentă recunoscută internațional – Common Criteria sau echivalent;
- accesul administratorilor la mașinile virtuale se va realiza doar pe baza unei analize de risc, analize ce va include cel puțin analize privind locația utilizatorului, momentul inițierii cererii de acces și comportamentul anterior al respectivului utilizator;
- soluția trebuie să aibă posibilitatea de a oferi acces pe baza de roluri bine definite pentru a evita accesul neautorizat sau accesului unui utilizator cu alt rol la funcțiile critice ale mașinilor virtuale;
- soluția trebuie să permită criptarea datelor transmise prin rețea;
- soluția trebuie să permită integrarea cu un server LDAP extern, unde sunt ținute profilurile utilizatorilor;
- soluția trebuie să ofere posibilitatea de a oferi accesul la resurse pe baza unui program de timp care să poată fi definit.

3.7.12. Web Application Firewall

Se va folosi soluția de web application firewall pusă la dispoziție de către Cloud-ul Guvernamental. Configurarea acestei componente, dedicate platformei PDURo, va fi în sarcina ofertantului declarat câștigător.

3.7.13. Componenta de Backup

La nivelul sistemului ADR se vor putea configura politici de backup, recuperare și restaurare pentru sistemele de operare, fișierele de configurare, aplicații și baze de date.

Indiferent de modelul sau mediul de stocare al datelor, accesarea datelor salvate se va realiza în condiții de siguranță, cât mai facil și fără să implice costuri suplimentare.

Soluția va conține o platformă de salvare/restaurare date și orchestrare a operațiunilor de recuperare în caz de dezastru ce va îndeplini următoarele specificații tehnice minimale:

- să ofere nativ funcționalități de salvare/restaurare date, funcționalități de replicare asincrona/sincrona, respectiv funcționalități de orchestrare a operațiunilor de recuperare

în caz de dezastru (mutarea, verificarea, modificarea și repornirea tuturor mașinilor virtuale în centrul secundar de date);

- să poată scala la o arhitectură de tip multi-nod (multiple noduri independente ce sunt agregate într-un model de redundanță activ-activ);
- să permită operațiuni de salvare/restaurare a sistemelor de operare ce rulează în mașinile virtuale din platformele de virtualizare prin integrarea directa la nivelul sistemului de operare, inclusiv pentru sistemele de operare ce funcționează în topologii de tip cluster multi-nod;
- să permită operațiuni de salvare/restaurare a fișierelor și directoarelor individuale din cadrul sistemelor de operare ce rulează în mașinile virtuale din platformele de virtualizare prin integrarea directă la nivelul sistemului de operare;
- să includă posibilitatea de a efectua operațiunile de salvare date prin integrarea directa la nivelul serverelor de aplicație și a bazelor de date ce rulează în mașinile virtuale din platformele de virtualizare, astfel încât operațiunile de restaurare a datelor să aducă la o stare funcțională consistentă fiecare server de aplicație și fiecare set de baze de date;
- trebuie să fie agnostică la nivelul resurselor hardware de stocare, putând utiliza orice tip de echipament de stocare și orice tip de volum de stocare de tip SAN sau NAS;
- trebuie să includă posibilitatea de a efectua operațiunile de salvare/restaurare date prin integrarea directa la nivelul platformelor de stocare, respectiv a mecanismelor proprietare de tip snapshot folosite în aceste platforme, astfel încât procesul de salvare/restaurare date să se facă direct din snapshot-urile efectuate la nivelul volumelor de stocare;
- trebuie să permită abstractizarea a multiple resurse de stocare prin realizarea unui singur spațiu virtual de stocare, fără limitare a numărului și tipului echipamentelor de stocare folosite;
- trebuie să permită extinderea spațiului de stocare pentru salvarea seturilor de date, prin folosirea unor spatii de stocare de tip cloud, respectiv apelabile prin protocol S3, fără limitarea cantității de date stocate și/sau a localizării datelor (rezidente în sistemele de stocare locale sau în sistemele de stocare de tip cloud) și fără limitarea operațiunilor de restaurare în funcție de localizarea datelor;
- trebuie să permită operațiuni de salvare a obiectelor și datelor stocate în directoare LDAP (cel puțin Microsoft Active Directory), astfel încât să permită restaurarea la nivel

individual de utilizator/grup de utilizatori, respectiv restaurarea de obiecte individuale la orice nivel al structurii arborescente de director;

- trebuie să permită operațiuni de salvare a datelor din căsuțe de e-mail (cel puțin pentru Microsoft Exchange), astfel încât să permită restaurarea la nivel individual de utilizator/grup de utilizatori, respectiv restaurarea de mesaje e-mail individuale;
- trebuie să permită operațiuni de salvare consistenta a datelor din baze de date (cel puțin pentru Oracle, Microsoft SQL, PostgreSQL și MySQL) fără instalarea de agenți software dedicați;
- trebuie să permită operațiuni automatizate de verificare a fiecărui set de date salvate, respectiv va permite efectuarea operațiunilor de restaurare în mod test (fără a afecta funcționalitatea serviciilor și aplicațiilor ce rulează în infrastructură) pentru fiecare mașină virtuală, sistem de operare, aplicație;
- operațiunile de testare trebuie să se poată efectua atât manual cat și periodic, prin recuperarea automata în medii de test predefinite, respectiv trebuie să includă pașii de recuperare și pașii de verificare a aplicațiilor și bazelor de date. Jurnalul testelor va putea fi exportat și utilizat în scopuri de raportare și audit;
- trebuie să permită raportarea operațiunilor de salvare și restaurare, situația mașinilor protejate, capacitatea de stocare utilizata, testele de recuperare efectuate și operațiile de verificare efectuate pentru mașini și aplicații;
- trebuie să permită crearea de salvări de siguranță de tip full, incremental și sintetic, cu posibilitatea degrevării resurselor de procesare prin transferarea operațiunilor de procesare (“off-load”) a seturilor de date către platforme hardware dedicate de salvare/restaurare date;
- trebuie să permită crearea unei salvări inițiale complete, urmând ca salvările ulterioare/succesive să transmită prin rețea doar blocurile unice de date modificate;
- pentru optimizarea traficului prin rețea, trebuie să poată identifica blocurile de date unice la nivelul echipamentelor, sistemelor de operare, aplicațiilor și serviciilor ce beneficiază de mecanismele de backup implementate;
- pentru evitarea congestionării traficului prin rețea în timpul operațiunilor de salvare, trebuie să permită restricționarea cantității de date transmise prin mediul de comunicație;

- trbeuie să asigure salvarea rapidă și eficientă a datelor unice (nemodificate) cum sunt datele sistemului de operare, documentele și alte date existente în mașinile virtuale din platformele de virtualizare, respectiv în platformele de stocare;
  pPentru operațiunile de salvare trebuie să permită procesarea în paralel a mașinilor virtuale ce fac parte din politicile de salvare, respectiv procesarea în paralele a restaurărilor discurilor mașinilor virtuale;
- pentru mașinile virtuale ce fac parte din politicile de salvare, trebuie să identifice automat snapshot-urile orfane și să realizeze automat operațiunile de consolidare, fără intervenția administratorilor;
- trebuie să ofere posibilitatea de a păstra salvările realizate în scheme de retenție de tip GFS (Grandfather-Father-Son), respectiv să permită operațiuni de salvare prin protocol NDMP;
- trebuie să ofere optimizarea capacității de stocare prin mecanisme transparente de compresie și deduplicare a datelor salvate. Procesul de deduplicare trebuie să permită definirea dimensiunii blocurilor de date folosite (1 MB sau mai mici), precum și utilizarea blocurilor de date cu lungime variabila;
- la nivelul sursei de deduplicare soluția trebuie să folosească un mecanism de deduplicare ce se va integra direct cu hipervizorul platformei de virtualizare ofertate, astfel încât operațiunile de salvare date nu vor scrie decât blocurile unice de date indiferent de numărul și tipul mașinilor virtuale salvate, respectiv indiferent de tipul sistemelor de operare și a aplicațiilor ce rulează în mașinile virtuale;
- la nivelul destinației de salvare a datelor deduplicate trebuie să folosească un mecanism suplimentar de deduplicare, astfel încât operațiunile de salvare date nu vor scrie decât blocurile unice de date indiferent de cantitatea de date rezultată în urma procesului de deduplicare rulat la sursă;
- nu trebuie să folosească o bază de date centralizată pentru informațiile de tip meta-date generate de mecanismul de deduplicare, prevenind astfel potențialele pierderi de date și/sau coruperea seturilor de date salvate în eventualitatea pierderii/coruperii bazei de date dedicată metadatelor de deduplicare;
- trebuie să stocheze seturile de date salvate sub formă de fișiere ce pot fi copiate și/sau mutate ulterior fără a aduce un impact operațiunilor de restaurare a datelor din respectivele fișiere;

- trebuie să ofere posibilitatea criptării datelor stocate, respectiv criptarea fluxului de date în procesul de replicare, cel puțin prin algoritm de criptare de tip AES-256 sau superior, iar operațiunile de restaurare nu vor fi limitate de folosirea mecanismelor de criptare;
- trebuie să ofere suport pentru protecție de tip WORM (Write-Once-Read-Many);
- operațiunile de restaurare a seturilor de date trebuie să poată fi executate într-un singur flux/pas, indiferent de tipul (full, incremental, sintetic) și numărul seturilor de backup din care se execută aceste operațiuni de restaurare;
- trebuie să ofere posibilitatea efectuării operațiunilor de restaurare în regim de tip self-service, utilizatorii individuali putând astfel restaura fișiere, mașini virtuale, e-mailuri și baze de date, inclusiv restaurări punctuale în lanțul de salvări disponibile într-un set de date (restaurări de tip "point-in-time");
- trebuie să permită recuperarea granulara a fișierelor sau folderelor, prin extragerea lor din seturile de date salvate, indiferent de numărul și tipul salvărilor efectuate într-un lanț de salvări de date;
- trebuie să permită recuperări rapide de date, prin disponibilizarea imediata a acestora în mașini virtuale independente de sursele din care s-au făcut operațiunile de salvare a datelor, fără a fi necesara copierea datelor. Copierea datelor se va face după recuperarea mașinilor virtuale și se va face sub forma unor procese ce rulează în fundal;
- trebuie să ofere mecanisme de recuperare rapidă pentru baze de date Oracle și Microsoft SQL, prin disponibilizarea imediata a acestora în instanțe de baze de date, independente de sursele din care s-au făcut operațiunile de salvare a datelor, fără a fi necesară copierea datelor. Timpul de pornire al acestor baze de date (RTO) trebuie să fie sub 10 minute, indiferent de dimensiunea bazei de date salvate;
- recuperarea rapidă de date trebuie să fie disponibilă din orice set de date salvate și din orice tip de mașină fizică sau virtuală, respectiv să permită recuperarea datelor pe o altă platformă tehnologică, prin mecanisme de conversie a formatului de tip P2V (Physical-to-Virtual), V2V (Virtual-to-Virtual) și C2V (Cloud-to-Virtual);
- trebuie să permită prezentarea discurilor mașinilor virtuale direct din seturile de date salvate, către alte mașini virtuale pornite;
- trebuie să permită restaurarea integrală a mașinilor virtuale, restaurarea granulară de fișiere și/sau foldere din mașinile virtuale, respectiv restaurarea discurilor mașinilor virtuale;

- trebuie să permită restaurarea fișierelor sau folderelor către locația originală, către o mașină virtuală ce rulează, respectiv către locații terțe, independente de locațiile din care s-au efectuat salvările, fără a impune limitări referitor la dimensiunea fișierelor sau discurilor ce urmează a fi restaurate;
- trebuie să permită efectuarea operațiunilor de salvare și restaurare date pentru următoarele sisteme de fișiere: ext2, ext3, ext4, ReiserFS, JFS, XFS, Btrfs, UFS, UFS2, ZFS, HFS, HFS+, NTFS, FAT, FAT32, ReFS, inclusiv pentru sisteme de operare ce utilizează scheme de partiționare și organizare bazate pe Linux LVM și Windows Storage Spaces;
- trebuie să ofere posibilitatea de a rula scripturi, înainte sau după execuția unei operațiuni de salvare/restaurare și/sau replicare;
- trebuie să ofere posibilitatea de a urmări schimbările intervenite în configurația mediilor virtuale, respectiv identificarea utilizatorilor care au realizat aceste schimbări;
- trebuie să permită analiza obiectelor supradimensionate (mașini virtuale ce au alocate mai multe resurse decât este necesar) și va sugera o metodă de optimizare a resurselor acestora;
- trebuie să permită operațiuni automatizate, bazate pe politici, de creare și testare a scenariilor de recuperare în caz de dezastru (simularea în timp real a indisponibilității totale a centrului primar de date și a funcționării aplicațiilor și serviciilor în centrul secundar de date, respectiv a revenirii la funcționarea aplicațiilor și serviciilor în centrul primar de date), fără a afecta funcționarea aplicațiilor și serviciilor ce rulează în infrastructura;
- planurile de recuperare în caz de dezastru vor include locația de recuperare (aceeași sau alta), pașii ce se executa pentru fiecare mașină virtuală și toate acțiunile necesare pornirii în locația dorită;
- planurile de recuperare vor putea efectua operațiunile de recuperare a mașinilor virtuale din seturile de date salvate al acestor mașini, din replici ale mașinilor virtuale sau din replicarea la nivel de sistem de stocare;
- trebuie să ofere rapoarte predefinite și/sau generate în urma operațiunilor de simulare a scenariilor de recuperare în caz de dezastru în scopul documentării detaliate a pașilor necesari/efectuați în cadrul planului de recuperare, cu posibilitatea auditării planurilor de recuperare în vederea determinării datei când au fost create și modificate, respectiv în vederea determinării administratorilor care au efectuat aceste modificări;

- testarea planurilor de recuperare se va face neinvaziv, în sensul execuției testelor în medii izolate, controlate de administratori, însă va avea ca rezultat recuperări reale și pornirea în locația destinație a mașinilor virtuale din respectivele planuri de recuperare;
- planurile de testare a recuperării în caz de dezastru vor raporta parametrii RPO și RTO astfel încât aceștia vor fi determinați și respectați în cazul situațiilor de urgență;
- trebuie să permită trimiterea rapoartelor de testare și/sau execuție a planurilor de recuperare pe email, respectiv stocarea acestora în locații predefinite, astfel încât să poată fi arhivate în vederea consultărilor și auditărilor;
- trebuie să permită replicare sincronă/asincronă a datelor la distanță în mod bidirecțional, respectiv va putea folosi ca sursa de replicare mașini virtuale, grupuri de mașini virtuale, volume de stocare și seturi de date salvate. Pentru utilizarea eficientă a canalelor de comunicație dintre centrele de date, soluția de replicare va oferi suport pentru replicare doar a datelor modificate, precum și transmiterea numai a blocurilor de date unice deduplicate și comprimate;
- mecanismul de replicare va permite păstrarea mai multor replici și puncte de restaurare, configurabile pentru fiecare mașină virtuală în parte;
- mecanismul de replicare va permite monitorizarea și optimizarea lățimii de bandă, între sistemele ce participă în procesul de replicare, respectiv va permite efectuarea operațiunilor administrative dintr-o singură consolă de management;
- mecanismul de replicare va asigura integritatea datelor protejate prin verificarea zilnică a acestora;
- trebuie să asigure un sistem de management și monitorizare integrat, ce va permite monitorizarea operațiunilor, performanței și capacității, sistem apelabil inclusiv printr-un mecanism de tip REST API dedicat;
- atât în scop administrativ, cât și în vederea accesului la seturile de date, soluția va permite nativ definirea de utilizatori locali și roluri de utilizare, cu seturi diferite de permisiuni granulare aplicabile acțiunilor administrative și/sau seturilor de date. De asemenea va permite integrarea cu un sistem director de tip LDAP, pentru sincronizarea utilizatorilor și a drepturilor de acces la seturile de date partajate de sistem;
- pentru asigurarea unui nivel optim de disponibilitate operațională, soluția preconizată va permite update și upgrade al platformei fără întreruperea serviciilor;
- ca parte a funcțiilor de administrare și diagnosticare, trebuie să includă standard un mecanism de alertare pe e-mail, configurabil pentru un set specific de adrese e-mail. De

asemenea, va permite integrarea în unelte dedicate de management al infrastructurilor prin suport complet pentru protocolul SNMP versiunea 2 și 3 și prin existența în mod gratuit a descriptorilor și parametrilor platformei astfel încât integrarea se va face în mod facil în uneltele de management ce nu au implicit profile definite pentru sistemul specific preconizat;

- trebuie să permită raportarea în timp real a indicilor de performanță și capacitate, respectiv raportarea avansată asupra tuturor configurațiilor specifice și a parametrilor de funcționare, nativ prin intermediul interfeței grafice;

Oferta va conține 1 (una) platformă de salvare/restaurare date și orchestrare a operațiunilor de recuperare în caz de dezastru, dimensionată pentru minim 30 mașini virtuale, fără a impune limite asupra volumului de date salvat/replicat, respectiv fără a impune limite asupra numărului de sisteme de fișiere, aplicații și servicii salvate/replicate, conform cu specificațiile tehnice minimale de mai sus.

Toate funcționalitățile software solicitate vor include licențiere perpetuă pentru întreaga configurație a soluției ofertate, indiferent de upgrade-urile ulterioare ale acesteia.

3.7.14. Platforma de virtualizare

Se vor folosi soluțiile de virtualizare oferite de Cloudul Guvernamental.

3.7.15. Sisteme de operare

Ofertantul trebuie să includă în ofertă sistemele de operare necesare rulării sistemului în mediu virtualizat, de tip COTS și licențiate conform arhitecturii soluției propuse.

3.7.16. Platforma de tip SOC (Security Operations Center)

PDURo va trebui să se integreze cu platforma de tip SOC pusă la dispoziție de către Cloud-ul Guvernamental, aferentă componentei SaaS. Configurarea integrărilor conform specificațiilor tehnice ale platformei SOC va fi în sarcina ofertantului declarat câștigător.

3.8.Serviciile solicitate

3.8.1. Serviciile de livrare și instalare software

În cadrul proiectului se vor implementa componentele recomandate la nivel european pentru implementarea once-only și hub-ul de interconectare pentru SDG. Sistemul tehnic propus la nivelul Uniunii Europene va permite statelor membre să solicite date de la autoritățile competente din alte state membre pentru a simplifica accesul la procedurile administrative transfrontaliere inițiate de cetățeni sau întreprinderi. Procedurile acoperite de acest sistem includ tranzacții de zi cu zi, cum ar fi înregistrarea schimbării adresei și a unei mașini la mutarea în străinătate, începerea unei afaceri într-un alt stat membru sau recunoașterea academică transfrontalieră. În urma utilizării Principiului *O singură dată*, autoritatea competentă care furnizează datele acționează ca Furnizor de Date, în timp ce autoritatea competentă care primește datele acționează ca un Consumator de Date.

Conform regulamentului, sistemul tehnic OOP (once-only principle) ar trebui să devină operațional până în decembrie 2023. Acest sistem de vârf va duce în cele din urmă la o mai mare colaborare guvernamentală în UE datorită proceselor de verificare online mai rapide și mai ieftine, cu același nivel de încredere, sau chiar mai mare, decât cecurile tradiționale de zi cu zi, pe hârtie. În cadrul proiectului se va implementa infrastructura necesară pentru ca România, în calitate de stat membru, să realizeze procesele definite în cadrul OOP.

Pentru fiecare mediu în parte vor trebui să fie instalate, conform arhitecturii, produsele furnizate, în modul de disponibilitate solicitat.

Vor trebui astfel asigurate următoarele activități:

- Instalarea componentelor software;
- Configurarea sistemului software;
- Integrarea componentelor software;
- Testarea soluției.

3.8.2. Servicii de analiză a sistemului

Rolul principal al serviciilor de analiză este de a înțelege corect nevoile utilizatorilor înainte de proiectarea și implementarea unui sistem care să le îndeplinească, prin clarificarea și detalierea cerințelor formulate în prezenta documentație.

Echipa de analiză a Prestatorului trebuie să analizeze cerințele împreună cu membrii echipei de proiect din partea ADR pentru a înțelege corect cerințele utilizatorilor înainte de proiectarea și dezvoltarea software.

În cadrul fazei de analiză este foarte posibil ca anumite cerințe formulate inițial în prezentul caiet de sarcini să se transforme prin detaliere, de asemenea este posibil ca noi cerințe să fie identificate, nefiind observate inițial. În această situație, se va ține cont de rezolvarea neajunsurilor identificate și atingerea beneficiile anticipate, de obiectivele generale și specifice ale achiziției, astfel încât să se ajungă la un rezultat constructiv.

În vederea implementării platformei, Prestatorul trebuie să execute activități de analiză care să asigure premisele unei implementări eficiente. Informațiile care stau la baza procesului de analiză sunt:

- contractul, pentru termene și condiții;
- caietul de sarcini și propunerea tehnică, pentru aria de acoperire a proiectului;
- cerințele clientului colectate și evaluate în timpul acestei faze.
- Regulamentele europene menționate în cadrul caietului de sarcini.
- REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2022/1463 AL COMISIEI din 5 august 2022 de stabilire a specificațiilor tehnice și operaționale ale sistemului tehnic pentru schimbul transfrontalier automatizat de elemente justificative și aplicarea principiului „doar o singură dată” în conformitate cu Regulamentul (UE) 2018/1724 al Parlamentului European și al Consiliului
- specificații pentru blocurile arhitecturale puse la dispoziție de Uniunea Europeană: “The Once-Only Hub.” https://ec.europa.eu/digital-building-blocks/wikis/display/OOTS/OOTSHUB+Home

Beneficiarul va acorda tot sprijinul necesar pentru înțelegerea cât mai bună și completă a contextului în care va fi implementată platforma.

Analiza se va efectua la sediul Beneficiarului (sau prin ședințe ONLINE) și va avea ca finalitate un pachet de specificații tehnice agreat de comun acord cu acesta. Serviciile de analiză vor acoperi cel puțin următoarele aspecte:

- analiza contextului existent;
- înțelegerea structurii organizatorice a Beneficiarului;

- analiza situației din momentul de față din cadrul instituției Beneficiarului prin ședințe de analiză, chestionare etc. Se vor identifica și documenta procesele operaționale care vor fi impactate prin implementarea soluției în cadrul contractului;
- migrarea fluxurilor de lucru existente în PCUe în cadrul PDURo;
- definirea cerințelor informaționale pentru sistem. Se va contura astfel, imaginea sistemului informatic prin stabilirea proceselor operaționale care să precizeze succesiunea activităților, participanții și momentul intervenției acestora, locația sau contextul, modalitatea de intervenție, informația procesată și resursele utilizate. Pentru prezentarea proceselor operaționale se vor utiliza instrumente de modelare a proceselor și activităților în conformitate cu standarde de modelare și reprezentare recunoscute (UML sau echivalent);
- integrarea cu sistemele informatice identificate în cadrul etapei de analiză necesare fluxurilor descrise în cadrul caietului de sarcini;
- Stabilirea tipurilor de roluri de utilizatori care vor interacționa în viitoarea platformă;

Ofertanții trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapelor de analiză și proiectare. Descrierea trebuie să conțină cel puțin următoarele informații:

- formularul/formularele care trebuie să fie utilizate pentru fiecare livrabil;
- descrierea conținutului fiecărui livrabil;
- modul în care trebuie să fie interpretat conținutul livrabilelor.

3.8.3. Servicii de proiectare a sistemului

În vederea implementării contractului, Prestatorul va trebui să execute următoarele activități care să asigure premisele unei implementări eficiente:

- proiectarea modelului sistemului de date;
- definirea serviciilor aferente noului flux funcțional de sistem;
- definirea principalele funcționalități de sistem folosind modele entitate - asociere sau UMLsau echivalent ;
- proiectarea componentelor și arhitectura de sistem;

Proiectarea sistemului dorit, constă în detalierea la nivel tehnic a cerințelor și specificațiilor rezultate din activitatea de analiză pentru toate nivelurile și componentele sistemului care va fi realizat, astfel:

- arhitectura de sistem – va prezenta cel puțin următoarele niveluri: hardware, comunicații, componente software instalate, arhitectură logică cuprinzând descrierea componentelor de sistem, a celor dezvoltate sau personalizate și caracteristicile funcționale și non-funcționale ale acestora;
- scenarii (cazuri) de utilizare – din care să reiasă modul de utilizare a sistemului informatic adaptat din perspectiva utilizatorului final, modul în care utilizatorii interacționează cu sistemul, în corespondență directă cu activitățile menționate în cadrul proceselor operaționale ale acestor utilizatori. Scenariile de utilizare trebuie să cuprindă și interacțiunile cu sistemele externe, astfel încât să fie evidențiat exact modul în care este fructificata o integrare la nivel de sistem informatic.
- integrările la nivel de componentă software – pentru fiecare interacțiune se va specifica sistemul sursă/destinație, modalitatea de implementare, canal de comunicare, setul și structura de date transferate, reguli specifice de validare etc.;
- rapoarte ce vor fi realizate în cadrul sistemului – vor fi descrise rapoartele noi, care sunt informațiile conținute, care sunt criteriile de filtrare dacă este cazul și tipul de livrare al acestora (timp real, la cererea utilizatorului sau automatizate la un anumit moment de timp programat apriori).

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

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

3.8.4. Dezvoltare software

Pentru implementarea contractului, în urma analizei și proiectării sistemului, se va face dezvoltare software, configurare, acolo unde este cazul, și testare internă.

Toate dezvoltările trebuie să asigure compatibilitatea sistemului cu specificațiile de interfațare ale acestuia cu sistemele externe. Testarea internă se va face pentru a se asigura că funcționalitățile individuale funcționează conform documentației de analiză.

Dezvoltarea, configurarea și testarea internă se vor face folosind o metodologie de dezvoltare validată în timp bazată pe standarde/bune practici internaționale.

Prestatorul va folosi instrumente specifice de dezvoltare, configurare și testare compatibile conform cerințelor caietului de sarcini.
În cadrul propunerii tehnice ofertantul trebuie să prezinte:

- metodologia detaliată în baza căreia vor fi desfășurate activitățile de dezvoltare și testare internă, demonstrând integrarea acestor proceduri cu procedurile de analiză și proiectare;
- instrumentele utilizate în desfășurarea activităților de implementare și testare internă;
- detalierea livrabilelor aferente prestării activităților de implementare și testare internă, care să includă:
    - formularul/formularele aferente fiecărui livrabil;
    - descrierea informațiilor conținute de către fiecare livrabil;
    - modul de interpretare al conținutului fiecărui livrabil.

Componentele software ce vor fi dezvoltate în cadrul proiectului vor avea la bază principiul de CI / CD pipeline (continuous integration / continuous deployment) astfel încât să fie permise dezvoltarea continuă, testarea continuă, integrarea continuă, implementarea continuă și monitorizarea continuă a aplicațiilor pe parcursul ciclului de viață al acestora.

De asemenea, în cadrul acestei etape trebuie avute în vedere serviciile de actualizare și realizare conținut pentru **componenta de informare a cetățenilor privind legislația și obligațiile aplicabile în domeniile ce se regăsesc în Anexa I a regulamentului SDG.**

Informațiile general valabile la nivel European se vor regăsi și în portalul național. Informațiile specifice României vor fi actualizare și se vor implementa mijloace de actualizare facilă a conținutului.

În plus, se vor avea în vedere minim servicii pentru interconectarea sistemului ADR cu:

- **nodul eIDAS – proiectul SITUE;**
- **soluțiile de tip managementul identității – proiectul PSCID/ROeID;**
- **5 furnizori de servicii de e-guvernare care vor fi conectați la HUB-ul de Interconectare (ex: ONRC, MAI, MMJS, MFP, CNAS, MS etc.);**

- **Sistemul de jurnalizare și notificare ce va fi dezvoltat în cadrul Cloud-ului Guvernamental și care va asigura toate demersurile pentru prevenirea, modificarea, și distrugerea, fără drept, a înregistrărilor din jurnal, respectiv pentru protejarea autenticității și a continuității procesului de înregistrare al evenimentelor, cu excepțiile stabilite doar prin cadrul legislativ.**

Integrările se vor realiza pe baza specificațiilor de integrare ale sistemelor informatice identificate în cadrul etapei de analiză. Beneficiarul va asigura suport pentru formalizarea cadrului legal de colaborare între instituțiile partenere.

3.8.5. Migrarea fluxurilor de lucru şi a datelor din sistemul PCUe

Prestatorul va migra toate fluxurile de lucru configurate de către instituțiile partenere din cadrul actualului PCU, precum și datele aferente acestora.

3.8.6. Testarea sistemului integrat

Este necesar ca Prestatorul să planifice în detaliu, să pregătească și să efectueze o serie de teste care să confirme că sunt asigurate cerințele funcționale și non-funcționale ale sistemului, compatibilitatea sistemului cu specificațiile de interfațare ale acestuia cu sistemele externe.

Pentru nodul central, Beneficiarul se va asigura că Prestatorul a efectuat cu succes următoarele activități cu rezultatele lor, respectiv:

- toate componentele software de bază necesare au fost livrate și instalate corespunzător;
- toate elementele din nodul central sunt pe deplin funcționale;
- aplicația a fost livrată și instalată;
- sesiunile de instruire au fost livrate;
- toate documentele necesare, manuale, kit-uri de instalare și licențele solicitate în acest proiect au fost livrate;
- s-a realizat cu succes testarea proceselor interne: jurnalizare, arhivare, auditare, raportare ștergeri, managementul notificărilor;
- s-a realizat generarea de raportări statistice care au fost identificate în procesul de implementarea sistemului.

Testele non-funcționale trebuie să acopere cerințele de disponibilitate, scalabilitate, fiabilitate, robustețe, salvare și restaurare, recuperare în caz de dezastru, estimări capacitate și planificare, performanță, management configurații, extensibilitate/flexibilitate, siguranță în funcționare, securitate, management și monitorizare sistem, management căderi în sistem, contingență, operare, conectivitate și calitate servicii.

Planurile de testare trebuie să includă cel puțin următoarele elemente:

- descrierea componentei de sistem testat;
- obiectivele de testare;
- descrierea mediului de testare;
- rezultatele așteptate ale testului;
- test de abordare;
- datele de test;
- descrierea procedurilor de test;
- cazuri de testare;
- instrumente folosite de testare;
- persoanele responsabile;
- cerințe de intrare/ieșire.

Instrumente de testare

Ofertantul trebuie să precizeze în ofertă toate instrumentele de testare (aplicații, scripturi etc.), destinate a fi utilizate în timpul procedurilor de testare. Prestatorul trebuie să pună la dispoziție instrumentele de testare. Toate rezultatele testelor trebuie înregistrate și predate Beneficiarului după fiecare test.

Toate componentele HW/SW necesare testării vor fi descrise de Prestator și vor fi disponibile pentru toată perioada întregului contract (inclusiv pentru actualizări/testare pentru modificări). Același mediu de testare se va utiliza pentru a testa toate modificările cerute și derivate din modificări legislative.

Mediul de testare nu trebuie să fie reutilizat sau integrat în alt mod în mediul de producție.

Dezvoltarea și punerea în aplicare de teste

Toate testele se vor efectua/supraveghea de către Beneficiar. Pentru cazurile de testare care necesită resurse externe sau acces la alte sisteme, Beneficiarul va asigura accesul la aceste resurse. Prestatorul va oferi toate instrumentele de testare.

Coordonarea testelor

Testele vor fi coordonate de către Beneficiar/Utilizatori, care vor revizui și aproba planul și specificațiile de testare cu 10 zile înainte de execuția efectivă a testelor, vor controla că mediul de testare e conform cu cerințele, vor monitoriza efectuarea testelor și se vor asigura de aplicarea procedurilor de management al testării.

Ofertanții vor prezenta în detaliu metodologia și procedurile după care vor derula activitățile specifice de testare de acceptanță.

Metodologia propusă și procedurile care vor fi utilizate pe parcursul implementării trebuie să acopere integral tematica proiectului astfel încât să fie posibilă testarea tuturor funcționalităților identificate în etapa de analiză și proiectare.

În cadrul contractului, prestatorul va trebui să deruleze cu Autoritatea Contractantă mai multe etape de inspecții și teste în vederea recepționării și acceptării produselor și serviciilor.

3.8.7. Instruire

Un factor important în utilizarea și funcționarea corectă a sistemului este instruirea. Pentru atingerea acestui obiectiv este necesară realizarea unui număr de zile de instruire în funcție de necesitățile ADR.

Activitățile de instruire vor fi desfășurate de către Prestator la sediul ADR și trebuie să creeze competențele necesare în rândul administratorilor și operatorilor care vor acorda suport utilizatorilor finali, astfel încât, la finalul implementării, beneficiarul să nu fie dependent de prestator pentru operarea sistemului.

Instruirea va fi organizată după ce sistemul este funcțional și trebuie să permită personalului instruit să înțeleagă funcționalitățile, modul de operare a acestuia, administrarea informațiilor care trebuie să fie efectuată de către utilizator, depistarea problemelor și diagnosticarea de bază.

Prestatorul trebuie să propună orice subiect suplimentar care ar putea fi necesar pentru a se asigura că personalul este pe deplin instruit pentru a asigura utilizarea corespunzătoare a sistemului.

ADR, împreună cu prestatorul, vor stabili de comun acord modalitatea de instruire pe baza planificării proiectului și disponibilității cursanților.

Prestatorul va elabora un plan de instruire cuprinzând numărul de zile alocate pentru fiecare program de instruire din cele menționate mai jos și, eventual, programe de instruire suplimentare pe care le consideră necesare pentru implementarea și acceptanța noului sistem.

Grupul țintă este format din aproximativ 3 administratori care vor beneficia de nivelul tehnic cel mai ridicat din punct de vedere al cunoștințelor diseminate și 15 operatori care vor acorda suport utilizatorilor finali care vor beneficia de un nivel detaliat din punct de vedere al cunoștințelor diseminate pe durata instruirii. Numărul estimativ de zile de instruire este de aproximativ 5 zile pentru fiecare din grupele de utilizatori.

ADR va stabili, la nivel intern, lista participanților la cursurile de instruire și va comunica Managerului de Proiect din partea Prestatorului această listă.

Instruirea se va desfășura conform planului de instruire stabilit și agreat contractual. Instruirea se va ține în limba română, utilizând metode interactive combinate cu metode clasice, de către instructori din partea Prestatorului.

Prestatorul va prezenta înaintea fiecărei sesiuni de instruire:

- tematica cursurilor ce se vor organiza;
- durata desfășurării sesiunilor de instruire pentru fiecare categorie de utilizatori descrise mai sus;
- programa de desfășurare a cursurilor;
- suportul de curs ce urmează a fi folosit pentru fiecare grup țintă.

Instruirea se va face pe baza suportului de curs în format electronic, livrat de Prestator fiecărui participant. Acest suport de curs va conține exemple practice pentru o mai bună înțelegere a modului de funcționare și administrare a sistemului, precum și alte detalii legate de acesta.

De asemenea, Prestatorul serviciilor de instruire va pune la dispoziția utilizatorilor o documentație de instruire în limba romană sau engleză pentru administratori, atât în format fizic, cât și în format electronic:

- manuale / ghiduri de administrare pentru persoanele care vor administra sistemul;
- manuale / ghiduri de utilizare pentru utilizatorii care vor asigura operarea curentă a soluției implementate.

Ședințele de instruire constau în:

- prezentarea conceptelor de către instructor;
- ședințe practice, pentru mai bună înțelegere și utilizare a sistemului / produselor

software (sisteme de operare, sisteme de gestiune a bazelor de date etc.);

Cursuri destinate administratorilor. Vor cuprinde tematici precum administrarea sistemului, administrarea bazelor de date, monitorizarea performanțelor, asistența utilizatorilor etc. Echipa de administrare a ADR va fi instruită de către Prestator astfel încât să poată asigura funcționarea sistemului cu o asistență minimă din partea Prestatorului sau independent de acesta, începând cu perioada post-implementare.

Cursuri destinate operatorilor care vor acorda suport utilizatorilor finali. Acest tip de instruire este destinat unui grup de operatori din cadrul ADR care vor acorda suport viitorilor utilizatori ai sistemului informatic și se va derula după finalizarea testării funcționale a sistemului implementat, incluzând tematici cu privire la utilizarea noului sistem implementat. Instruirea va cuprinde și un modul cu privire la securitatea informației și a sistemului informatic, precum și la protejarea datelor cu caracter personal și la legislația aplicabilă.

La finalul activității de instruire a operatorilor și administratorilor sistemului integrat, prestatorul va prezenta beneficiarului rapoartele de instruire, listele de prezență și concluziile instruirii.

La sfârșitul programului de instruire, instructorul va cere participanților să completeze un chestionar de evaluare a cursului.

Ofertantul va prezenta un program de instruire pentru toate serviciile de instruire menționate mai jos, cu precizarea următoarelor informații:

- descrierea programului de instruire, a tematicii și a conținutului acestora;
- detalii de organizare a programului de instruire;
- descrierea rezultatelor așteptate;
- resurse puse la dispoziție de Prestator;
- resurse necesare din partea ADR.

De asemenea, ofertantul va prezenta în ofertă descrierea detaliată a procedurilor de instruire pe care le propune în cadrul proiectului. Aceasta va evidenția în mod obligatoriu următoarele:

- modalitatea de planificare a instruirii;
- modalitatea de desfășurare a instruirii;
- modalitatea de evaluare a rezultatelor instruirii;
- modalitatea de evaluare a performanțelor instructorilor.

3.8.8. Implementare (deployment)

În etapa de implementare se va realiza instalarea şi configurarea sistemului informatic și, dacă este cazul, reconfigurarea infrastructurii software de bază.

În faza de implementare a proiectului vor fi actualizate livrabilele concepute și realizate în faza de analiză și proiectare ce se referă la: arhitectura funcțională, arhitectura tehnică și modelul informațional. Documentele vor fi actualizate pe baza informațiilor obținute în urma ședințelor de prezentare a sistemului informatic Beneficiarului.

Ofertanții trebuie să descrie în detaliu metodologia după care vor derula activitățile de implementare (deployment).

Ofertanții trebuie să prezinte împreună cu oferta procedurile de implementare din cadrul propriei organizații și vor demonstra integrarea acestor proceduri cu procedurile referitoare la dezvoltare/configurare și testare internă.

Ofertanții trebuie să prezinte detaliat livrabilele care vor rezulta în urma prestării serviciilor corespunzătoare etapei de implementare.

3.8.9. Punere în producție

Ofertanții trebuie să prezinte planul care va fi utilizat la trecerea în producție a sistemului.

Planul prezentat trebuie să țină cont de legăturile logice între subsisteme astfel încât să se asigure o trecere în producție coerentă și cu impact minim în derularea activităților operaționale ale Beneficiarului.

3.8.10. Livrabile servicii

Pentru toate activitățile descrise în prezentul capitol, *3.8 – Serviciile solicitate,* se vor livra documentații în conformitate cu bunele practici în domeniu coroborate cu metodologia propusă de către Ofertantul declarat câștigător.

Livrabilele în baza cărora se vor efectua plățile sunt următoarele:

a) proces verbal de recepție a raportului (documentului) de analiză;
b) proces verbal de recepție cantitativă și calitativă, respectiv punere în funcțiune (activare) a licențelor software;
c) proces verbal de recepție a documentației tehnice aferentă activității de proiectarea a sistemului informatic;
d) proces verbal de recepție a release note-ului si raportului de testarea funcționalităților sistemului informatic, ca rezultat al activității de dezvoltare, configurare și testare software;

e) proces verbal de recepție a raportului de migrare, ca rezultat al migrării fluxurilor de lucru și a datelor din sistemul PCUe;
f) proces verbal de recepție a raportului de instruire a personalului dedicat din cadrul ADR;
g) proces verbal de recepție a raportului de punere în producție.

4. RESURSE

Atât Prestatorul, cât și Beneficiarul trebuie să asigure cadrul profesional adecvat desfășurării proiectului în bune condiții. Fiecare va pune la dispoziție toți specialiștii necesari pentru îndeplinirea scopului și obiectivelor proiectului.

În calitate de beneficiar al proiectului, ADR, înțelege că pentru bunul mers al acestuia trebuie să pună la dispoziție toate resursele necesare îndeplinirii contractului.

În acest sens, pentru buna desfășurare a fazelor proiectului, dar și pentru exploatarea curentă a acestuia după implementare, beneficiarul va asigura capacitatea operațională și administrativă necesară. Astfel, pe lângă resursele financiare, va asigura și resursele materiale necesare pentru buna implementare a proiectului. Din aceste resursele materiale deținute și utilizate pentru buna implementare a proiectului amintim:

- sediul Beneficiarului, precum și dotările necesare pentru întâlnirile echipei de proiect și desfășurării activităților acestora;
- baza logistica: mobilier (birouri, scaune, dulapuri pentru o parte din membrii echipei) și echipamente IT;
- mijloace de comunicație;
- site-ul Beneficiarului, pentru o comunicare și promovare eficientă și completă a rezultatelor proiectului.

Prestatorul are obligația de a propune spre mobilizare o echipă formată din experți calificați pentru realizarea activităților prevăzute în caietul de sarcini și va fi responsabil pentru activitatea experților și pentru obținerea rezultatelor contractului. Experții propuși vor avea calificarea și experiența profesională necesare pentru acoperirea cu succes a tuturor activităților indicate în caietul de sarcini. Astfel, Prestatorul va pune la dispoziția autorității contractante o echipă formată din personal cheie cu competențe și experiență dovedite, capabil să ducă la bun sfârșit cu succes sarcinile definite prin prezentul caiet de sarcini, astfel ca, în final, să contribuire la îndeplinirea obiectivului general și a obiectivului specific ale proiectului, în condițiile respectării cerințelor de calitate și a termenelor stabilite și încadrarea în bugetul prevăzut.

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

Nr.crt.	Tip Expert	Nr. Experți
Experți cheie		
1	Expert manager de proiect	1
2	Expert analiză și optimizare procese	1
3	Expert team leader software	1
4	Expert analiză de business	1
5	Expert arhitect sistem informatic	1
6	Expert securitate cibernetică	1
7	Expert platformă de gestiune a accesului utilizatorilor/Expert în managementul identității electronice	1
8	Expert baze de date	1
Experți non-cheie		
9	Expert dezvoltator software	3
10	Expert soluție backup și recuperare	1
11	Expert GDPR	1
12	Expert testare	1
13	Expert suport tehnic	1
14	Expert instruire	1
15	Expert portal	1
16	Expert management de procese (BPM)	1
17	Expert BI (Business Intelligence)	1

Ofertantul va îndeplini următoarele condiții minime pentru echipa de proiect:

4.1. Experți cheie

4.1.1. Expert manager de proiect - 1 persoană

Pentru expertul manager de proiect se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de manager de proiect;
- deținerea de competențe în managementul de proiect, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• este punct unic de contact în relația cu Beneficiarul și va avea între atribuțiile sale conducerea unică a echipei de proiect; • planifică activitatea echipei de proiect; • stabileşte cerințele de management al proiectului; • monitorizează implementarea proiectului; • elaborează planul revizuit de activități și urmăreşte respectarea termenelor proiectului; • elaborează rapoartele de progres lunare ce vor fi înaintate spre aprobare beneficiarului; • supraveghează îndeplinirea de către prestator a obligațiilor asumate în conformitate cu contractul semnat.

4.1.2. Expert analiză și optimizare procese– 1 persoană

Pentru expertul analiză și optimizare procese se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert analiză și optimizare procese;
- deținerea de cunoștințe în domeniul analizei și optimizării de procese de business dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/ internațional (de exemplu Lean Six Sigma sau echivalent).

Responsabilități în cadrul Contractului	• responsabil cu definirea structurii organizaționale și a structurii de management de proiect; • supraveghează desfășurarea săptămânală a proiectului și gestionează echipa proiectului desemnată de către Prestator;

	• participă la diferite ședințe și la toate evenimentele proiectului, asigurând pregătirea adecvată a acestora; • asigură o comunicare adecvată, discuții și feedback dintre diferiți participanți la acest proiect; • elaborează individual sau cu alți membrii ai echipei documentații specifice proiectului, instrumente și metodologii necesare activităților; • participă la formarea echipei din proiect în scopul verificării însușirii instrumentelor, metodologiilor și documentațiilor transferate.

4.1.3. Expert team leader software -1 persoană

Pentru expertul team leader software se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de team leader echipă dezvoltare;
- deținerea de competențe privind metodologiile de tip Scrum Agile în dezvoltare produse software, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional;
- deținerea de competențe privind administrarea infrastructurilor din centre de date, inclusiv în tehnologii cloud, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional;
- deținerea de competențe pentru abilități de realizare a arhitecturilor software, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• gestionează implementarea sistemului; • coordonează întreaga echipă tehnică, cu alocarea sarcinilor pe fiecare membru al echipei; • menține și aplică managementul riscurilor și procedurile de asigurare a calității; • asigură resurse pentru executarea serviciilor de implementare cuprinse în specificațiile tehnice; • întocmește toate rapoartele tehnice necesare conform cerințelor proiectului și/sau alte rapoarte cerute de către managerul de proiect; • validează specificațiile de business în vederea extragerii specificațiilor tehnice și gestionează relația cu clientul; • coordonează echipa în toate fazele de dezvoltare ale unei aplicații; • elaborează specificații tehnice de design și arhitectură software; • asigură managementul produselor software (roadmap dezvoltări, planificarea release-urilor, integrarea produsului în arhitectura IT a beneficiarului).

4.1.4. Expert analiză de business - 1 persoană

Pentru expertul analiză de business se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de analist de business;
- deținerea de cunoștințe privind analiza de business și modelarea proceselor de business, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• analizează, planifică și monitorizează cerințele funcționale și non-funcționale; • realizează documentele de analiză și a specificațiilor; • coordonează activitățile de analiză de business; • analizează, definește procesele de business și elaborează specificațiile detaliate ale proceselor; • analizează și interpretează cerințele; • identifică problemele din rândul proceselor, inițiază acțiuni de îmbunătățire a proceselor; • participă la definirea scenariilor de testare; • participă la structurarea procesului de instruire.

4.1.5. Expert arhitect sistem informatic- 1 persoană

Pentru expertul arhitect sistem informatic se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de arhitect sistem informatic
- deținerea de competențe în domeniul arhitecturilor complexe de tip Enterprise în contextul sistemelor informatice, dovedite prin prezentarea unei diplome/certificări recunoscută la nivel național/internațional;
- deținerea de competențe în dezvoltare de aplicații sau baze de date, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional;
- deținerea de cunoștințe în domeniul proiectării și implementării de arhitecturi software orientate pe servicii, dovedite prin prezentarea unei diplome/certificări recunoscută la nivel național/internațional;
- deținerea de cunoștințe privind metodologii de dezvoltare software bazate pe principii de dezvoltare iterativă, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• coordonează activitatea de proiectare și definire a arhitecturii sistemului respectând standardele în domeniu; • documentează și păstrează informații și/sau modele ale arhitecturii de sistem și ale structurilor de date. Se ocupă de actualizarea și modificarea acestor informații pe parcursul derulării activităților; • asigură suport pentru testare, implementare /utilizare corectă a sistemului informatic.

4.1.6. Expert securitate cibernetică – 1 persoană

Pentru expertul securitate cibernetică se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert securitate cibernetică;
- deținerea de cunoștințe privind protejarea activă a sistemelor informatice și a rețelelor și verificarea sistemelor informatice împotriva vulnerabilităților, dovedite prin prezentarea unei diplome/certificări recunoscute la nivel național/international;
- deținerea de cunoștințe privind gestiunea incidentelor de securitate prin înțelegerea mecanismelor de atac, precum și privind contracararea atacurilor cibernetice, dovedite prin prezentarea unei diplome/certificări recunoscute la nivel național/internațional;
- deținerea de cunoștințe privind implementarea componentei de securizare a mașinilor virtuale pentru soluția ofertată dovedite prin cursuri/certificări recunoscute de producător sau recunoscute la nivel național/internațional.

Responsabilități în cadrul Contractului	• realizează soluția de securitate în etapa de analiză; • este responsabil de realizarea configurarea din punct de vedere al securității a sistemelor informatice; • oferă consultanță de specialitate pentru echipa de proiect în timpul derulării proiectului;

	• realizează planul de securitate a sistemului informatic; • oferă instructaj pentru administratorii sistemului informatic și pentru utilizatorii sistemului informatic.

4.1.7. Expert platformă de gestiune a accesului utilizatorilor/ Expert în managementul identității electronice – 1 persoană

Pentru expertul platformă de gestiune a accesului utilizatorilor/ expert în managementul identității electronice se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experienţă specifică - participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert platformă de gestiune a accesului utilizatorilor/expert în managementul identității electronice;
- deținerea de cunoștințe privind managementul serviciilor IT și alinierea acestora cu nevoile de business, dovedite prin prezentarea unei diplome/certificări recunoscute la nivel național / internațional;
- deținerea de cunoștinte privind administrarea platformei de gestiune a accesului utilizatorilor și a securității sistemului pentru soluția ofertată, dovedite prin diplome / certificări recunoscute de producător sau recunoscute la nivel național / internațional;
- deținerea de cunoștințe privind monitorizarea performanței funcționării infrastructurii HW și SW (servere, baze de date, servere aplicații) utilizate pentru rularea platformei pentru prevenirea breșelor de securitate cauzate de blocarea/indisponibilitatea funcționării infrastructurii HW și SW care deservesc platforma de gestiune a accesului utilizatorilor și a securității sistemului, dovedite prin diplome / certificări recunoscute de producător sau recunoscute la nivel național / internațional.

Responsabilități în cadrul Contractului	• realizează activități specifice de implementare și configurare a platformei de gestiune a accesului utilizatorilor și a securității sistemului; • este responsabil de configurarea din punct de vedere al securității soluțiilor utilizate în cadrul platformei de gestiune a accesului utilizatorilor și a securității sistemului; • oferă consultanță de specialitate pentru echipa de proiect

	pentru activitățile și etapele de integrare cu platforma de gestiune a accesului utilizatorilor și a securității sistemului; • asigură suport tehnic în perioada de garanție; • oferă instructaj pentru administratorii sistemului informatic și pentru utilizatorii sistemului informatic.

4.1.8. Expert baze de date -1 persoană

Pentru expertul baze de date se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert baze de date;
- deținerea de competențe în tehnologia de baze de date ofertată privind administrarea, optimizarea, asigurarea înaltei disponibilități și asigurarea securității bazei de date, dovedite prin prezentarea unei diplome/certificări a producătorului în tehnologia bazei de date ofertate, recunoscut la nivel național/internațional.

Responsabilități în cadrul Contractului	• este responsabil cu proiectarea și implementarea bazelor de date; • este responsabil cu asigurarea administrării de baze de date, menținerea integrității și securității bazelor de date; • monitorizează și menține în parametrii optimi performanțele bazelor de date prin urmărirea logurilor de sistem și activității pe servere și efectuarea de operațiuni în vederea optimizării performanței; • asigură suport tehnic pentru dezvoltatori în vederea configurării și optimizării aplicațiilor dezvoltate.

Pentru demonstrarea îndeplinirii cerințelor pentru experții cheie se vor depune următoarele documente:

- CV-ul;
- copii conform cu originalul după diplomele/certificările/atestările relevante în raport cu cerințele din prezenta documentație;

- în vederea respectării principiul recunoașterii reciproce, precizăm că, pentru personalul nerezident, se permite prezentarea certificarilor/ autorizărilor corespunzatoare emise în țara de rezidență;
- documente relevante din care să reiasă îndeplinirea cerințelor de experiență profesională specifică, solicitate prin prezenta documentație - îndeplinirea cerințelor se face prin prezentarea de certificate/ documente cum ar fi: contracte, recomandări, procese verbale, documente constatatoare sau orice alte documente doveditoare;
- pentru experții care nu sunt angajați ai ofertantului, se vor prezenta declarații de disponibilitate (Formularul – Declarație de disponibilitate) datate și semnate de titular;
- prestatorul va putea utiliza în echipă și alți experți fiind responsabil de componența echipelor de experți și profilul generic al acestora ;
- prestatorul va asigura personalul administrativ și suport (backstopping) necesar echipei sale;
- fiecare dintre persoanele propuse trebuie să îndeplinească integral toate cerințele minime aferente expertului (profilului de persoană) pentru care au fost nominalizate. Nu se acceptă îndeplinirea cerințelor minime aferente unui expert prin cumul de către mai multe persoane.

4.2. Experți non-cheie

4.2.1. Expert dezvoltator software - 3 persoane

Pentru experții dezvoltator software se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de dezvoltator software;
- deținerea de competențe privind dezvoltarea de software, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional;
- deținerea de competențe privind dezvoltarea aplicațiilor cu seturi de date relaționale, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• este responsabil de dezvoltarea de aplicații software; • este responsabil de elaborarea, testarea și întreținerea aplicațiilor software; • întocmeşte documentația tehnică; • asigură suport tehnic.

Având în vedere importanța, complexitatea tehnică și funcțională a sistemului PDURo, precum și numărul entităților care vor participa în fluxul de oferire al serviciilor publice electronice prin hub sunt necesari 3 (trei) experți dezvoltator software care să asigure buna desfășurare a activităților de dezvoltare cu respectarea constrângerilor de timp de la nivelul documentației de atribuire.

4.2.2. Expert soluție backup și recuperare -1 persoană

Pentru expertul soluție back-up și recuperare se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert backup și recuperare date;
- deținerea de competențe privind configurarea și administrarea soluțiilor de backup și recuperare ofertate, dovedite prin prezentarea unei diplome/certificări a producătorului soluțiilor de backup și recuperare ofertate recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• este responsabil de instalarea și configurarea soluției de backup și recuperare date; • este responsabil de asigurarea administrării, monitorizării și disponibilității sistemelor de back-up și recuperare în parametrii normali; • planifică și participă la testarea și mentenanță componentelor sistemelor; • este responsabil de asigurarea în permanență a optimizării funcționării sistemelor; • este responsabil de documentarea instalării și configurării soluțiilor de back-up și recuperare.

4.2.3. Expert GDPR- 1 persoană

Pentru expertul GDPR se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic care a inclus servicii în domeniul protecției datelor cu caracter personal, în care a avut responsabilități specifice rolului de expert GDPR;
- deținerea de competențe în domeniul protecției datelor cu caracter personal, dovedite prin prezentarea unei diplome/certificări recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• contribuie la analiza cerințelor care derivă din GDPR; • este responsabil de verificarea și testarea, din punct de vedere funcțional și tehnic, a produsului rezultat, în conformitate cu cerințele care derivă din GDPR.

4.2.4. Expert testare - 1 persoană

Pentru expertul testare se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic, în care a avut responsabilități specifice rolului de expert testare;
- deținerea de competențe privind testarea funcționalității sistemelor informatice,

dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• este responsabil de asigurarea testării funcționalităților dezvoltate și implementate conform metodologiei de testare agreate cu Beneficiarul; • realizează documentele de testare și specificații ale scenariilor de test; • acordă suport utilizatorilor pentru testarea funcțională; • planifică activitățile de testare; • elaborează planurile, scenariile și cazurile de test; • este responsabil de întocmirea și livrarea rapoartelor de testare; • realizează testele de acceptanță specifice; • coordonează activitățile de testare la nivelul echipei de testare a Prestatorului; • este responsabil de asigurarea funcționării corecte a sistemului din punct de vedere al respectării cerințelor, consistenței datelor, al constrângerilor de timp, al validărilor de date și al gestiunii erorilor.

4.2.5. Expert suport tehnic - 1 persoană

Pentru expertul suport tehnic se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert suport tehnic;
- deținerea de competențe privind managementul sistemelor IT dovedite prin prezentarea unei diplome/certificări în domeniu recunoscute la nivel național/internațional.

Responsabilități în cadrul Contractului	• este responsabil de asigurarea analizei, planificarea, administrarea, rezolvarea, monitorizarea progresului, prioritizarea cererilor de suport; • este responsabil de asigurarea rezolvării cererilor de suport sau escaladarea acestora la un nivel superior pentru rezolvare; • identifică problemele și propune soluții pentru problemele identificate; • efectuează verificări periodice ale funcționării sistemului.

4.2.6. Expert instruire - 1 persoană

Pentru expertul instruire se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert instruire;
- deținerea de competențe în domeniul formării și dezvoltării competențelor profesionale, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• întocmește planul de instruire; • coordonează instruirea conform planului de instruire; • coordonează activitatea de instruire a administratorilor și operatorilor care vor acorda suport utilizatorilor finali.

4.2.7. Expert portal – 1 persoană

Pentru expertul portal se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert portal;
- deținerea de competențe privind soluții de tip portal dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• este responsabil de dezvoltarea și implementarea soluției de tip portal pe baza documentelor de analiză, specificații funcționale, specificații tehnice, arhitectură sistem; • este responsabil de testarea unitară a soluției de tip portal (internă); • acordă suport utilizatorilor cheie pentru testarea funcțională; • este responsabil de rezolvarea disfunctionalităților (bug-uri).

4.2.8. Expert management de procese (BPM) – 1 persoană

Pentru expertul management de procese (BPM) se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert management de procese (BPM);
- deținerea de competențe în tehnologia ofertată privind implementarea soluțiilor de management procese business (BPM), dovedite prin prezentarea unei diplome/certificări a producătorului soluțiilor de BPM ofertate, recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• este responsabil de configurarea soluției BPM pe baza documentelor de proiectare, specificații funcționale și tehnice; • realizează testarea unitară (internă); • este responsabil de crearea testelor de acceptanță; • este responsabil de rezolvarea disfuncționalităților (incidente/bug-uri).

4.2.9. Expert BI (Business Intelligence) – 1 persoană

Pentru expertul integrare aplicații și baze de date se vor prezenta documente justificative în vederea îndeplinirii următoarelor cerințe:

- experiență specifică – participarea în minim 1 proiect de implementare sistem informatic în care a avut responsabilități specifice rolului de expert BI sau care a avut responsabilități similare prezentului contract;

- deținerea de cunoștințe privind implementarea soluțiilor de business intelligence, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

Responsabilități în cadrul Contractului	• este responsabil de crearea modelelor de date/metadate pentru analiză şi raportare; • realizează activitățile de proiectare, dezvoltare și implementare a soluției de analiză şi raportare.

Pentru experții non-cheie nu se solicită documente justificative care dovedesc calificarea și experiența acestora, în cuprinsul propunerii tehnice. Aceste documente se prezintă la momentul în care vor interveni în implementarea viitorului contract.
În cuprinsul propunerii tehnice, ofertanții vor descrie momentul în care vor interveni experți non-cheie în executarea viitorului contract, precum și modul în care operatorul economic, care va îndeplini calitatea de ofertant, și-a asigurat accesul la serviciile acestora (fie prin resurse proprii, caz în care vor fi prezentate persoanele în cauză, fie prin externalizare, situație în care se vor descrie aranjamentele contractuale realizate în vederea obținerii serviciilor respective). Astfel, după intrarea în vigoare a contractului, Prestatorul, la momentul intervenției experților non-cheie, va înainta documentele suport prin care se va justifica îndeplinirea cerințelor la nivelul echipei de experți non-cheie, individual, pentru fiecare expert non-cheie în parte.

Pentru demonstrarea îndeplinirii cerințelor pentru experții non-cheie se vor depune la momentul intervenției experților următoarele documente:

- CV-ul;
- copii conform cu originalul după diplomele/certificările/atestările relevante în raport cu cerințele din prezenta documentație;
- în vederea respectării principiul recunoașterii reciproce, precizăm că, pentru personalul nerezident, se permite prezentarea certificarilor/ autorizărilor corespunzatoare emise în țara de rezidență;
- documente relevante din care să reiasă îndeplinirea cerințelor de experiență profesională specifică, solicitate prin prezenta documentație - îndeplinirea cerințelor se face prin prezentarea de certificate/ documente cum ar fi: contracte, recomandări, procese verbale, documente constatatoare sau orice alte documente doveditoare;

- pentru experții care nu sunt angajați ai ofertantului, se vor prezenta declarații de disponibilitate (Formularul – Declarație de disponibilitate) datate și semnate de titular;
- prestatorul va putea utiliza în echipă și alți experți fiind responsabil de componența echipelor de experți și profilul generic al acestora;
- prestatorul va asigura personalul administrativ și suport (backstopping) necesar echipei sale;
- fiecare dintre persoanele propuse trebuie să îndeplinească integral toate cerințele minime aferente expertului (profilului de persoană) pentru care au fost nominalizate. Nu se acceptă îndeplinirea cerințelor minime aferente unui expert prin cumul de către mai multe persoane.

Pe parcursul derulării contractului de achiziție publică, modalitatea de înlocuire a personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează conform prevederilor art. 162 din Anexa 1 (Normele metodologice) la HG nr. 395/2016.
Astfel, înlocuirea personalului de specialitate nominalizat pentru îndeplinirea contractului se realizează numai cu acceptul autorității contractante, și nu reprezintă o modificare substanțială, așa cum este aceasta definită în art. 221 din Legea 98/2016, decât în următoarele situații:

a. noul personal de specialitate nominalizat pentru îndeplinirea contractului nu îndeplinește cel puțin criteriile de calificare/selecție prevăzute în cadrul documentației de atribuire;
b. noul personal de specialitate nominalizat pentru îndeplinirea contractului nu obține cel puțin același punctaj ca personalul propus la momentul aplicării factorilor de evaluare.

În situațiile prevăzute anterior, contractantul are obligația de a 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.
Se vor avea în vedere și prevederile din Contract, anexă la prezenta documentație.

5. GARANŢIA SISTEMULUI

Pentru dezvoltările realizate în cadrul proiectului se va acorda garanție și suport tehnic pe o perioadă de 60 de luni de la data acceptanței finale, prin intermediul acestor servicii asigurându-

se funcționarea corespunzătoare a tuturor funcționalităților existente la data acceptanței finale a sistemului informatic.

Pentru componentele software de tip software standard, pe parcursul unei perioade de 36 de luni de la data acceptanței finale a sistemului informatic se vor asigura cel puțin următoarele: upgrade-uri, update-uri de securitate, instalarea de patch-uri disponibile. De asemenea, pentru aceste componente, pe lângă cele 36 de luni de garanție acordate începând cu data acceptanței finale, se va acorda suport tehnic și pe toată durata implementării proiectului.

Pe întreaga perioadă de garanție prestatorul va asigura funcționarea conform specificațiilor tehnice și funcționale agreate în documentele de analiză de business, de arhitectură, de specificații funcționale elaborate pentru dezvoltarea și implementarea sistemului, va presta servicii de suport, iar această activitate va fi monitorizată de către managerul de proiect.

Pe perioada de garanție se vor asigura prevenirea și remedierea defecțiunilor și anomaliilor apărute.

Serviciul de suport tehnic va avea scopul de a oferi utilizatorilor finali un punct unic de contact pentru toate solicitările de intervenții, pentru suport operativ și pentru semnalările unor disfuncționalități ale soluției furnizate.

Remedierea defecțiunilor pe perioada garanției se va realiza la sediul beneficiarului proiectului sau prin intervenție de la distanță (*remote maintenance*).

În perioada de garanție se vor presta cel puțin următoarele activități:

- consiliere și suport telefonic prin serviciul Help-desk;
- rezolvarea bug-urilor care nu au fost identificate în timpul implementării și/sau care apar în faza de producție; remedierea software se va face cu precădere de la distanță;
- întreținerea și buna funcționare a sistemului furnizat în parametrii agreați (funcțional, performanță, disponibilitate, integritatea datelor etc.);
- actualizări software la locația de instalare a beneficiarului sau de la distanță, inclusiv instalarea de noi versiuni ale aplicațiilor în urma efectuării corecțiilor;
- reconfigurări ale resurselor hardware virtuale și software la nivelul inițial solicitat în cazul în care erorile apărute nu sunt datorate beneficiarului;
- consiliere și suport tehnic pentru posibilități de extindere a soluției existente;
- actualizarea manualelor de utilizare și altor documente în urma efectuării corecțiilor;

- toate incidentele vor fi gestionate prin intermediul aplicației software de gestionare a tichetelor pusă la dispoziție de către prestator.

Pe timpul derulării garanției, se vor presta următoarele intervenții:

- în condițiile apariției unei erori în funcționarea resurselor hardware virtuale sau software instalate și configurate, se vor asigura verificări pentru a determina natura problemelor apărute și se va decide, de comun acord, care este cel mai potrivit mod de intervenție pentru soluționarea defecțiunii. Modalitățile de intervenție sunt: help-desk online, asistenta telefonică, realizarea, în caz de necesitate, a actualizărilor de software, remedierea în locația beneficiarului;
- actualizările de software pot face referire, dar nu limitativ, la: compilarea pe un suport magnetic sau descărcarea unor patch-uri care conțin corecții ale unor erori sau îmbunătățirea software-ului cu scopul de a crește ușurința în exploatare sau performanțele acestuia. Actualizările vor fi însoțite, dacă este cazul, de actualizări ale manualelor/ghidurilor de utilizare destinate utilizatorilor.

Controlul intervențiilor

Pentru înregistrarea tuturor tipurilor de intervenții și pentru asigurarea bunei funcționări a produselor ofertate, se va propune dacă este cazul, un model de registru pentru controlul intervențiilor, care va fi validat de comun acord în urma workshop-urilor comune avute cu beneficiarul. Beneficiarul va actualiza acest registru, pe baza documentelor elaborate de către Prestator, cu toate informațiile care descriu intervențiile respective.

Timpii de rezolvare sunt definiti în functie de gravitatea incidentului aparut:

Nivel Criticitate	Timp de răspuns	Timp soluționare temporară	Timp solutionare finala
Critic	Maxim 4 ore	12 ore	24 ore
Mediu	Maxim 4 ore	24 ore	48 ore
Minor	Maxim 4 ore	48 ore	96 ore

Tipurile incidentelor:

1. **Critic**: una sau mai multe resurse din mediul productiv sunt nefuncționale sau profund degradate, iar impactul acestui incident duce la imposibilitatea utilizării sistemului.

2. **Mediu**: impactul produs de degradarea uneia sau mai multor resurse duce la scăderea performanței sau afectarea parțială a unor funcționalități ale sistemului. Sistemul este funcțional pentru cea mai mare parte a scenariilor de utilizare.
3. **Minor**: impactul produs de degradarea uneia sau mai multor resurse este redus sau există soluție temporară.

Timpii de mai sus sunt calculați din momentul în care Prestatorul a fost înștiințat de apariția problemelor.

Datele și orele de înregistrare ce vor fi folosite pentru calcularea SLA-ului vor fi următoarele:

- În cazul utilizării telefonului:
  Data și ora de înregistrare = data și ora la care s-a încheiat convorbirea telefonică.

- În cazul utilizării e-mail-ului:
  Data și ora de înregistrare = data și ora la care se recepționează email-ul, reprezentând data și ora din server-ul de e-mail-uri (în cazul primirii de informații de către furnizor, respectiv data și ora la care furnizorul a trimis e-mail-ul, reprezentând data din server-ul de e-mail - în cazul transmiterii de informații de către furnizor.

La sfârșitul fiecărui caz deschis, Prestatorul va efectua o analiză a cauzelor care au dus la producerea deranjamentului și o va include în recomandarea finală.

Prestatorul va garanta că SLA-ul mai sus menționat se bazează pe servicii de suport pentru soluția software furnizată în cadrul acestui contract. Timpii de răspuns și timpii de remediere asigurați de către Prestator pe perioada furnizării serviciilor sunt calculați conform priorității fiecărei solicitări. Calcularea acestora se va realiza în programul de lucru de Luni până Vineri, în intervalul orar 8:30 – 17:30, cu excepția sărbătorilor legale.

Definițiile, descrise mai jos, se vor aplica la Service Level Agreement:

- **Timp de Răspuns:** Timpul scurs de la contactul inițial dintre beneficiar și HELPDESK și răspunsul primit de la echipa de suport tehnic a Prestatorului către Beneficiar. Această acțiune se va desfășura prin intermediul telefonului/e-mail;

- **Timp de Remediere:** Durata de timp până la oferirea soluției finale;

- **Remediere Temporară:** O modificare în cadrul procedurilor sau datelor care să evite erorile fără folosirea defectuoasă a produselor, dacă este posibil;

- **SLA**: Service Level Agreement identifică funcționalitățile și definește procesele care implică livrarea de către Prestator a diferitelor servicii de suport către Beneficiar;

- **Suport**: Telefonul de suport tehnic, asistență web și e-mail oferite de Prestator pentru a ajuta Beneficiarul în rezolvarea problemelor apărute;

- **HELPDESK**: Un centru de asistență tehnică ce oferă serviciul de preluare a cererilor prin telefon, web și e-mail operat de către personalul care face parte din echipa Prestatorului care oferă asistență pentru componentele soluției informatice furnizate.

6. PROCEDURA DE ACCEPTANȚĂ

- **Recepția**

Procesul prin care un produs sau un livrabil sau un serviciu este acceptat sau respins de către o comisie nominalizată a Autorității Contractante.

Acceptarea/Respingerea se va constata prin emiterea de către Autoritatea Contractantă a documentului denumit „proces verbal de recepție" din care va rezulta ce se acceptă / respinge și criteriile în baza cărora comisia a decis aprobarea/respingerea produsului său livrabilului sau serviciului sau lucrării.

În cadrul fiecărei etape/fază se va derula cel puțin o recepție sau dacă este cazul mai multe recepții aferente produselor / livrabilelor / serviciilor, iar fiecare astfel de recepție va fi documentată corespunzător.

În cazul în care Autoritatea Contractantă emite un proces verbal de recepție prin care respinge o livrare a prestatorului atunci Autoritatea Contractantă va enunța în document în clar motivul/motivele pentru care respinge livrarea. Prestatorul are obligația de a reface / înlocui pe cheltuiala proprie și de a solicita o nouă recepție. În cadrul noului proces de recepție Autoritatea Contractantă va putea emite noi observații doar la punctele la care anterior a emis observații.

- **Acceptanța Parțială (Provizorie)**

Este data (momentul în timp) la care Autoritatea Contractantă emite către Prestator documentul „proces verbal de acceptanță parțială (provizorie)”.

Procesele verbale de acceptanță parțială (provizorie) vor fi emise în baza proceselor verbale de recepție care au fost aprobate. Documentele vor atesta că prestatorul și-a îndeplinit parțial obligațiile rezultate din caietul de sarcini, respectiv că produsele au fost livrate şi serviciile au fost prestate.

Documentul “proces verbal de acceptanță parțială (provizorie)” nu va fi emis dacă un produs sau un livrabil sau un serviciu a fost respins de către Autoritatea Contractantă și ulterior nu a mai fost acceptat/aprobat printr-un nou proces verbal de recepție.

- **Acceptanța Finală**

Este data (momentul în timp) la care Autoritatea Contractantă emite către Prestator documentul „proces verbal de acceptanță finală”. Documentul va fi emis în baza proceselor verbale de acceptanță parțială (provizorie) şi reprezintă obținerea acordului final din partea beneficiarului proiectului.

7. CADRUL LEGAL CARE GUVERNEAZĂ RELAȚIA DINTRE AUTORITATEA CONTRACTANTĂ ȘI CONTRACTANT (INCLUSIV ÎN DOMENIILE MEDIULUI, SOCIAL ȘI AL RELAȚIILOR DE MUNCĂ)

Ofertantul devenit Prestator 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 *[selectați din lista de mai jos după cum este aplicabil]:*

a. Convenția nr. 87 a OIM privind libertatea de asociere şi 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.]*

Prestatorul va lua în permanență toate măsurile rezonabile de precauție necesare pentru a păstra sănătatea și securitatea personalului acestuia.

8. MANAGEMENTUL CONTRACTULUI

8.1.Aspecte organizatorice

Autoritatea contractantă

BENEFICIARUL va îndeplini rolul de Autoritate Contractantă în prezenta procedura de achiziție publică și va fi responsabil cu organizarea acestei proceduri. Totodată, **BENEFICIARUL** îndeplinește și rolul de Beneficiar al serviciilor ce urmează a fi contractate. Managementul Contractului, inclusiv implementarea administrativă și procedurală aferente Contractului, va fi asigurat de către o echipă de implementare din partea **BENEFICIARULUI** (Echipa de implementare a Proiectului), care va gestiona totodată și documentele elaborate de Prestator (analize, livrabile ale fazelor de proiect, rapoarte de progres, rapoarte, facturi, alte documente justificative etc.).

Autoritatea Contractantă este responsabilă pentru:

- punerea la dispoziția Prestatorului a tuturor informațiilor disponibile pentru obținerea rezultatelor așteptate, cum ar fi: date de intrare, raportări, situații specifice;
- punerea la dispoziția Prestatorului, dacă este cazul, a unui spațiu de lucru mobilat;
- desemnarea echipei implicate și responsabile cu interacțiunea și suportul oferit Prestatorului;
- asigurarea tuturor resurselor care sunt în sarcina să pentru buna derulare a Contractului.

Prestatorul

Prestatorul serviciilor este responsabil pentru execuția conformă și la timp a tuturor activităților și pentru furnizarea livrabilelor prevăzute în prezentul Caiet de Sarcini, corespunzătoare Proiectului.

Prestatorul va răspunde întocmai tuturor cerințelor prevăzute în prezentul Caiet de Sarcini, respectând și aplicând cele mai bune practici în domeniu.

Prestatorul este direct și integral responsabil pentru activitatea experților săi și pentru îndeplinirea scopului Contractului și obținerea rezultatelor Proiectului.

Prestatorul este pe deplin responsabil pentru:

a. asigurarea planificării resurselor în raport cu planul de lucru estimat pentru derularea contractului și prezentat în cadrul acestui Ofertei;
b. îndeplinirea obligațiilor sale, cu respectarea celor mai bune practici din domeniu, a prevederilor legale și contractuale relevante precum și cu deplina înțelegere a complexității legate de derularea cu succes a Contractului, astfel încât să se asigure îndeplinirea obiectivelor stabilite, inclusiv prin furnizarea – prin intermediul Planului de management al calității – a asigurării că activitățile și rezultatele sunt realizate la parametrii calitativi solicitați;
c. asigurarea valabilității tuturor autorizațiilor și certificatelor (atât pentru organizația sa, cât și pentru personalul/echipamentul propus pentru realizarea serviciilor) care sunt necesare (conform legislației în vigoare) pentru prestarea serviciilor;
d. prestarea serviciilor în conformitate cu cerințele Caietului de Sarcini;
e. prezentarea rezultatelor în formatul/formatele care să respecte cerințele Autorității Contractante;
f. colaborarea cu personalul Autorității Contractante alocat pentru serviciile desfășurate conform Contractului (monitorizarea progresului activităților în cadrul Contractului, coordonarea activităților în cadrul Contractului, feedback).

8.2.Asigurarea calității în cadrul contractului

Serviciile solicitate pe durata contractului trebuie să asigure obținerea rezultatelor așteptate la un nivel calitativ adecvat.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice o descriere a procedurilor de asigurare și control al calității aplicabile proceselor pe care le derulează în activitatea curentă.

Ofertantul trebuie să aloce în planul detaliat de implementare timpi suficienți de verificare și validare din punct de vedere calitativ pentru produsele livrate, serviciile prestate și pentru revizuirea livrabilelor/documentelor rezultate.
Trebuie să fie incluse în ofertă următoarele proceduri de lucru: Procedura de asistență tehnică, mentenanță și suport, Procedura de livrare, Procedura de recepție/acceptanță parțială (provizorie)/acceptanta finală, Procedura de ședințe, Procedura de control al livrărilor, Procedura de testare a livrabilelor (inclusiv cele de tip software).
Prestatorul trebuie să prezinte un plan pentru Asigurarea Calității de comun acord cu Beneficiar, ca parte a planului de lucru, în cel mult o săptămână de la ședința inițială din cadrul contractului.

Prestatorul trebuie să aloce timp suficient, în cadrul planului de lucru, pentru verificare și validare în termeni de calitate, pentru serviciile prestate în cadrul contractului și pentru livrabilele/documentele/rapoartele rezultate, în termen de 5 zile lucrătoare de la predarea acestora, dacă nu se specifică altfel.

Prestatorul va elabora procedurile standard de operare pentru toate aplicațiile livrate, cu instrucțiuni detaliate pentru sprijinirea utilizatorilor în diferite procese de lucru.

Prestatorul va pune la dispoziție manuale, documentații, proceduri complete privind concepția, implementarea și administrarea în integralitate a sistemului informatic.

Prestatorul va oferi, pe durata proiectului, trimestrial, un raport intermediar de audit intern privind modul în care au avut loc activitățile în cursul perioadei de raportare, calitatea rezultatelor obținute în cursul perioadei de raportare și propunerile de acțiuni corective și preventive menite să îmbunătățească calitatea rezultatelor. Rapoartele trimestriale vor fi transmise în primele 5 zile de la încheierea trimestrului pentru care se face raportarea și vor prezenta valorile măsurate pentru o serie de indicatori de performanță.

Monitorizarea de către autoritatea contractantă a realizării activităților de către prestator și a rezultatelor obținute în urma acestora se va efectua având la bază reperele de mai jos:

- cerințele caietului de sarcini;
- informațiile furnizate în cadrul propunerii tehnice în scopul demonstrării îndeplinirii cerințelor și pentru aplicarea criteriului de atribuire și orice alte beneficii oferite de ofertant pentru obținerea avantajului competitiv pe perioada evaluării;
- contractul semnat;

- documentele/rapoartele furnizate de prestator;
- orice alte documente relevante pentru monitorizarea rezultatelor pe perioada derulării contractului.

Pentru monitorizarea activității prestatorului, beneficiarul va avea în vedere:

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

Un instrument în derularea activității de monitorizare vor fi ședințele/întâlnirile dintre echipa prestatorului și echipa beneficiarului, ședințe care au drept scop și urmărirea progresului contractului de servicii.

Alte întâlniri/ședințe care ar putea fi desfășurate pe parcursul derulării contractului:

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

Rezultatele ședințelor vor fi documentate în minute de ședință. Ședințele se vor desfășura, în funcție de context, fie virtual (teleconferințe/videoconferințe) atunci când nu este necesară prezența fizică a prestatorului la fiecare întâlnire/ședință, fie fizic, prin prezența prestatorului la sediul beneficiarului.

Acceptarea livrabilelor obținute din derularea contractului se finalizează prin semnarea, după caz, a proceselor-verbale de recepție/acceptanță parțială (provizorie) și a unui proces-verbal de acceptanță finală. Criteriile de acceptanță de la fiecare nivel de testare vor fi stabilite în acord cu autoritatea contractantă într-un plan de testare care va fi propus de prestator, pornind de la criteriile de acceptanță propuse în ofertă, și validat de autoritatea contractantă, astfel încât să se asigure conformitatea implementării soluției cu specificațiile funcționale stabilite.

Vor avea loc recepții ale componentelor sistemului informatic (produse software, analiză, proiectare, dezvoltare, implementare, testare, intrare în producție, instruire). Recepția finală a sistemului informatic va avea loc prin testarea întregului sistem integrat pe baza unui plan de testare agreat. Acceptarea codului sursă pentru sistemul informatic (module/aplicații) se va face cu demonstrarea funcționării acestuia.

8.3.Facilități oferite de Prestator

Prestatorul va asigura experților săi sprijin administrativ, de secretariat și traducere, după caz, care să le permită experților desfășurarea în bune condiții a activităților din acest contract.
Printre altele, **Prestatorul** va fi responsabil pentru (și va suporta costurile):

- asigurarea cazării, serviciilor de masă, și transportului (local și internațional dacă este cazul) pentru personalul său;
- cheltuieli de relocare, asigurări de sănătate, după caz;
- asigurarea spațiului necesar pentru desfășurarea activităților experților (suplimentar față de cel pus la dispoziție de Autoritatea Contractantă), dotat cu mobilier și toate echipamentele și materialele necesare;
- cheltuieli de comunicare;
- serviciile de secretariat;
- orice cost legat de interpretare și traduceri, imprimarea sau multiplicarea rapoartelor;
- costurile pentru angajarea experților;
- costurile elaborării și transmiterii rapoartelor;
- orice alte cheltuieli legate de activitatea Prestatorului.

Echipamente

Prestatorul va fi responsabil și va suporta costurile pentru toate echipamentele necesare în executarea obligațiilor asumate prin Contractul de prestări servicii.
Niciun fel de echipamente nu vor fi achiziționate în numele Autorității Contractante/Beneficiar ca parte a serviciilor din cadrul Contractului sau transferate Autorității Contractante/ Beneficiarului la finalizarea Contractului.

8.4.Metodologie de lucru și raportare

Activitatea de management de proiect trebuie să se desfășoare conform unui cadru (framework) de management de proiect recunoscut internațional de către organisme profesionale specifice de Project Management.

Ofertantul trebuie să prezinte în cadrul propunerii tehnice descrierea detaliată a metodologiei proprii de management de proiect pe care o va utiliza în cadrul proiectului.

Implementarea întregului sistem trebuie să acopere următoarele:

- analiză;
- livrare, instalare și configurare;
- proiectare;
- dezvoltare software;
- implementare (deployment);
- testare și teste de acceptanță;
- instruire;
- punere în producție.

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

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

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

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

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

Ofertantul va prezenta în cadrul propunerii tehnice și modalitatea de tratare a schimbărilor în cadrul proiectului. Se va prezenta procedura de management al schimbărilor precum și formularele care vor fi utilizate în cadrul acestui proces pe durata proiectului.
Ofertantul va prezenta Planul de management al riscurilor. Această secțiune va conține cel puțin următoarele:

- identificarea, descrierea și argumentarea riscurilor care pot afecta execuția contractului;
- recomandări suplimentare de reducere/eliminare a riscurilor identificate în cuprinsul Cap. Riscuri, fără afectarea cerințelor caietului de sarcini.

8.4.1. Metodologia de lucru

Pentru buna desfășurare a activităților și atingerea rezultatelor proiectului, Prestatorul va colabora permanent cu echipa de implementare a proiectului.
În termen de 3 zile lucrătoare de la data începerii contractului, va fi organizată o întâlnire de lucru la care vor participa reprezentanți ai Beneficiarului (membrii echipei de implementare a proiectului) și ai Prestatorului (directorul de proiect și alți experți cheie a căror prezență este considerată necesară de către Prestator).
În cadrul acestei întâlniri vor fi stabilite următoarele:

- principiile de comunicare reciprocă;
- planul de lucru, prin raportare la graficul de desfășurare a activităților
- detaliile privind colaborarea;
- frecvența reuniunilor;
- modelele de procese-verbale;
- modelele de rapoarte privind progresele înregistrate;
- planurile de acțiune în cazul apariției unor probleme;
- alte detalii logistice și organizaționale.

8.4.2. Cerințe privind raportarea

Prestatorul este responsabil de elaborarea și transmiterea următoarelor rapoarte către Autoritatea Contractantă:

Raportul Inițial

Va fi întocmit în maxim 2 săptămâni de la data începerii executării Contractului. Acest document trebuie să aibă în vedere precizările din Caietul de Sarcini și Propunerea tehnică și să aducă detalierile necesare, structurări sau clarificări unde este cazul. Raportul va cuprinde

planificarea activităților, metodologia utilizată și indicatorii planificați pentru fiecare etapă. Raportul inițial va constitui principalul instrument de lucru și se va face referire la el pe toată perioada de executare a Contractului. Raportul inițial va fi înaintat spre aprobare Autorității Contractante.

Rapoarte lunare

Prestatorul va elabora un raport lunar prin care să prezinte evoluția lunară a activităților și întârzierile, dacă acestea sunt semnificative. Rapoartele lunare vor detalia:

- progresele înregistrate;
- Activități aflate în derulare cu data estimativă a finalizării acestora și cu rezultatele anticipate;
- dificultățile întâmpinate în cursul implementării proiectului și soluțiile propuse pentru a depăși respectivele dificultăți;
- rezultatele realizate în cursul perioadei de raportare, resursele utilizate, precum și recomandările sau solicitările aferente, și planificarea activităților pentru perioada următoare;
- alte documente solicitate de către AM, prevăzute în Manualul de implementare și instrucțiunile ulterioare.

Rapoartele lunare vor fi transmise până în data de 5 a următoarei luni pentru care se face raportarea (de ex. Raportul aferent activității din luna ianuarie se va transmite până pe data de 5 februarie). În cazul în care data de 5 a lunii respective este o zi nelucrătoare, Prestatorul va anticipa transmiterea raportului lunar.

Raportul final

Varianta preliminară a Raportului final trebuie să fie transmisă Echipei de implementare a Proiectului cu cel puțin o luna înainte de sfârșitul perioadei de execuție a Contractului pentru a fi analizată. Acest raport trebuie să descrie întreg procesul de execuție și va înlesni evaluarea rezultatelor obținute atât în termeni calitativi, cât și cantitativi.

Raportul va cuprinde:

- evaluarea succesului și constrângerilor majore pentru fiecare activitate;
- realizările generale ale Contractului;
- recomandări pentru acțiuni viitoare cu scopul asigurării durabilității activităților, rezultatele așteptate după finalizarea Contractului, precum și măsurile ce trebuie întreprinse de către Beneficiar în acest sens.

Varianta preliminară a acestui raport va fi revizuită cu observațiile/comentariile primite din partea Autorității Contractante, în termen de 5 zile lucrătoare de la data primirii observațiilor/comentariilor. Autoritatea Contractantă va transmite observațiile/comentariile în termen de 15 zile lucrătoare de la data primirii variantei preliminare a Raportului final.

Alte rapoarte: Autoritatea Contractantă poate cere Prestatorului să elaboreze pe parcursul derulării Contractului și alte rapoarte, în măsura în care acestea sunt legate de buna desfășurare a Contractului.

8.4.3. 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 implementare a proiectului 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, Prestatorul 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.

8.4.4. Indicatori de performanță

În scopul eficientizării modului de derulare a contractului, evitării unor întârzieri în implementare datorate elaborării incomplete și/sau superficiale a livrabilelor, precum și facilitării procesului de aprobare a acestora de către comisia de recepție stabilită la nivelul Autorității Contractante, se va avea în vedere:

Indicator privind calitatea livrabilelor proiectului

- **Categorie indicator**: Nivelul de calitate;
- **Indicator de performanță al contractului:** Livrabil adecvat pentru scopul utilizării;
- **Nivelul de performanță așteptat conform Caiet de sarcini:** Documentele elaborate sunt conforme cerințelor stabilite în Caietul de Sarcini;
- **Ce se măsoară:** Nivelul de acuratețe al livrabilelor după "peer review" (sub nivelul de calitate, agreat conform cerințelor stabilite în Caietul de Sarcini și/sau prezentat în oferta tehnică).
- **Modalitatea de evaluare:**
  - **Foarte satisfăcător (5 puncte) –** Livrabilele includ îmbunătățiri semnificative față de cerințele minime stabilite în Caietul de Sarcini și prezentate în oferta tehnică.
  - **Satisfăcător (4 puncte)** – Livrabilele includ unele îmbunătățiri și nu includ neconformități/inexactități față de nivelul agreat. Au fost necesare doar ajustări nemateriale.
  - **Acceptabil (3 puncte) -** Livrabilele nu includ neconformități/inexactități față de nivelul agreat însă nu includ nici elemente suplimentare care să aducă o valoare adăugată semnificativă proiectului. Nu au existat întârzieri semnificative ca urmare a efectuării eventualelor remedieri.
  - **Nesatisfăcător (2 puncte) -** Livrabilele prezintă neconformități / inexactități față de nivelul agreat iar aceste aspecte nu au putut fi corectate în totalitate într-o perioadă rezonabilă (ex. au cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului), dar cu toate acestea au fost remediate de către Prestator.
  - **Foarte nesatisfăcător (1 punct)** – Livrabilele prezintă neconformități / inexactități majore față de nivelul agreat, iar aceste aspecte nu au putut fi corectate de către Prestator. Autoritatea Contractantă a trebuit să mobilizeze alte resurse pentru a remedia problemele, ceea ce a condus la costuri suplimentare semnificative pentru Autoritatea Contractantă și/sau a cauzat întârzieri semnificative în realizarea activităților din calendarul general al proiectului.

Indicator privind termenele de predare a livrabilelor proiectului

- **Categorie indicator**: Nivelul de calitate
- **Indicator de performanță al contractului:** Livrabil/rezultat final predat în termenul agreat

- **Nivelul de performanță așteptat conform Caiet de sarcini:** Livrabilul/rezultatul final este predat conform termenului agreat în contract
- **Ce se măsoară:** Livrarea la timp a rezultatelor
- **Modalitatea de evaluare:**
  - **Foarte satisfăcător (5 puncte)** – livrate în termenele convenite în contract
  - **Satisfăcător (4 puncte)** – livrate imediat după încheierea termenelor convenite în Contract însă fără întârzierea activităților din calendarul general al proiectului
  - **Acceptabil (3 puncte)** – livrate după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului ce pot fi neglijate.
  - **Nesatisfăcător (2 puncte)** – livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri ale activităților din calendarul general al proiectului pentru mai mult de 60 de zile.
  - **Foarte nesatisfăcător (1 puncte)** – livrate cu mult după încheierea termenelor convenite în Contract conducând la întârzieri majore ale activităților din calendarul general al proiectului pentru mai mult de 90 de zile.

8.5.Conflictul de interese

Se aplică prevederile Legii nr. 98/2016 privind achizițiile publice, cu completările și modificările ulterioare.

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

Se vor include în propunerea tehnică informații despre strategia implementată pentru obținerea asigurării că, în legătură cu activitățile și rezultatele incluse în Contractul ce rezultă din această procedură, apariția și materializarea conflictului de interese este prevenit, prin raportare la clauzele contractuale incluse în acest sens în Documentația de atribuire.

8.6.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 Prestator (contractant sau membrii asocierii), aferente serviciilor livrate, se transferă către Autoritatea Contractantă, BENEFICIAR (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 și organele de specialitate ale administrației publice centrale au obligația de a prevedea explicit în caietele de sarcini și în contractele aferente procedurilor de achiziție publică demarate de la dat intrării în vigoare a prezentei ordonanțe de urgență, 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”***.

Înainte de plata facturii finale, Prestatorul va preda Autorității Contractante codul sursă al aplicației.

8.7.Ipoteze și riscuri

8.7.1. Ipotezele

Ipotezele avute în vedere:

- conținutul serviciilor solicitate este descris în mod explicit în cadrul Caietului de Sarcini;
- corelația dintre resursele necesare și rezultatele așteptate este realistă;
- începerea serviciilor 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 Prestatorului;
- Prestatorul va semna un acord de confidențialitate la momentul semnării Contractului și va respecta toate instrucțiunile privind utilizarea informațiilor confidențiale.

În pregătirea Ofertei, Ofertantul trebuie să aibă în vedere cel puțin riscurile și ipotezele descrise în caietul de sarcini.

8.7.2. Riscuri

Pentru a identifica și combate efectele adverse pe care contractul ar putea să le întâmpine, a fost construită o matrice de risc în vederea observării posibilelor cauze ale riscurilor și pentru a atribui o probabilitate de apariție fiecărui eveniment advers.

Autoritatea contractantă își asumă responsabilitatea pentru urmărirea și aplicarea strategiei de răspuns pentru fiecare dintre riscurile identificate pentru implementarea contractului, în sfera sa de responsabilitate.

Contractantul își asumă responsabilitatea pentru urmărirea și aplicarea strategiei de răspuns pentru fiecare dintre riscurile aferente implementării contractului ce cad în sfera sa de responsabilitate.

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
1.	Prelungirea termenelor procedurilor de achiziție publică	- realizarea și actualizarea permanentă a unui plan de achiziții - analiza permanentă a legislației referitoare la achizițiile publice - un membru al echipei de proiect are rolul de a coordona și realiza derularea achizițiilor publice
2.	Începerea activităților cu întârziere	- realizarea și actualizarea permanentă a unui plan de management - monitorizarea permanentă a respectării termenelor
3	Fluctuații de personal	- selectarea atentă a persoanelor din echipa de proiect - selectarea unei echipe de formate din persoane externe, care vor fi angajate pe toata durata proiectului
4	Modificări legislative care influențează implementarea proiectului	- monitorizarea permanentă a modificărilor legislative - respectarea Contractului de finanțare
5	Indisponibilitatea unor produse/servicii prevăzute în proiect	- plan de achiziții realist, care corespunde ofertei de pe piață - informarea prealabilă privind disponibilitatea de

Nr. crt.	Risc identificat	Măsuri de atenuare ale riscului
		oferte și livrare de servicii și bunuri
6	Calitate necorespunzătoare a produselor/serviciilor	- selecția atentă a furnizorilor de bunuri și servicii, inclusiv pe baza performanțelor dovedite anterior - întocmirea unor documentații de atribuire acoperitoare elaborarea unor clauze stricte în contracte referitor la neîndeplinirea obiectivelor la nivelul de calitate solicitat
7	Modificări în structura organizatorică a Prestatorului	- asigurarea flexibilității în planificarea și utilizarea resurselor umane incluse în proiect și posibilitatea suplimentării resurselor alocate în cazul în care riscul se materializează
8	Probleme de comunicare și coordonare între membrii echipei de proiect	- stabilirea și monitorizarea respectării unui circuit de comunicare între membrii echipei de proiect
9	Riscuri politice: - instabilitatea factorului politic poate duce la schimbări legislative și normative; - poate induce instabilitate la nivel administrativ și decizional prin schimbări în organizarea, funcționarea și/sau conducerea instituțiilor	- atenuarea efectelor acestui risc se va efectua asigurând o echipa dedicata implementării acestui proiect, astfel încât deciziile politice să nu influențeze realizarea investiției.

Riscuri care pot fi identificate la momentul elaborării Caietului de Sarcini și riscuri care pot apărea în derularea contractului sunt următoarele:

- dificultăți de colaborare și comunicare între factorii interesați implicați;
- datele și informațiile necesare desfășurării serviciilor comunicate de către Autoritatea Contractantă nu sunt suficiente pentru îndeplinirea cerințelor solicitate prin Caietul de Sarcini;
- adăugarea de activități/ solicitări de informații noi, în funcție de progresul activităților.

Aceste riscuri vor fi gestionate de către echipa de management a proiectului, din partea Autorității Contractante.

Referitor la riscurile de natură contractuală înscrise la modul general în tabelul de mai sus, identificate la nivelul ambelor părți contractante, Autoritatea contractantă a inclus în modelul de contract clauze de natură să minimizeze aceste riscuri, vizând următoarele aspecte:

- prețul va rămâne ferm și nerevizuibil pe toată perioada de valabilitate a contractului având în vedere prevederile Art. 2 din OUG 47/2022 privind ajustarea preturilor contractelor de achiziție publică/contractelor sectoriale/contractelor de concesiune/acordurilor-cadru
- contractantul se obligă prin contract că serviciile prestate respectă cel puțin calitatea prevăzută în propunerea tehnică, care va fi anexă la contract
- termenul de prestare al serviciilor care fac obiectul fiecărui contract este ferm. În situația în care din motive neimputabile Contractantului, temeinic justificate, este necesară prelungirea termenului de prestare/implementare, modificarea acestuia se va face numai cu acordul Autorității contractante, materializat printr-un act adițional la contract;

Totodată, pentru a se asigura împotriva riscului de neîndeplinire întocmai și la timp a contractului, Autoritatea contractantă va solicita constituirea de către Contractant a unei garanții de bună execuție, în cuantum de 10% din valoarea contractului, în termen de 5 zile lucrătoare de la semnare, ca o condiție de intrare în vigoare a contractului. Autoritatea contractantă va avea dreptul de a emite pretenții asupra garanției de bună execuție, în limita prejudiciului creat, în cazul în care Contractantul nu își va executa, va executa cu întârziere sau în mod necorespunzător obligațiile asumate prin contract.

9. MODALITATEA DE PLATĂ ȘI TERMENE

Plata serviciilor prestate se va realiza în mai multe tranșe, pentru livrabilele furnizate în cadrul contractului, în concordanță cu planul de lucru propus și cu oferta financiară. Plata este condiționată de semnarea proceselor-verbale de recepție a serviciilor/produselor și de emiterea proceselor verbale de acceptanță provizorie (parțială).

Modalitatea de plată și termenele aferente sunt prevăzute în Contract, anexă la prezenta documentație.

Autoritatea contractantă va considera serviciile din cadrul contractului de achiziție finalizate în momentul în care:

- toate cerințele cuprinse în caietul de sarcini au fost îndeplinite, respectiv cele asumate prin propunerea tehnică prezentată ca răspuns la acestea;
- rezultatele au fost aprobate de autoritatea contractantă, pe baza cerințelor incluse în contract.

10. LOCUL ȘI DURATA DESFĂȘURĂRII ACTIVITĂȚILOR

10.1. Locul desfășurării activităților

Contractul va fi implementat în cadrul Autorității Pentru Digitalizarea României, iar locația va fi în București. Serviciile vor fi prestate atât la sediul Beneficiarului, cât și la sediul Prestatorului, după caz.

Pentru activitățile ce vor fi realizate la sediul autorității contractante, Prestatorul trebuie să transmită datele de identificare a persoanelor care își vor desfășura activitatea la sediu și operatorul economic are obligația de a asigura instruirea personalului propriu cu privire la riscurile specifice activității pe care o vor desfășura la alt sediu decât cel al operatorului.

10.2. Durata prestării serviciilor

Perioada de implementare a contractului este de 18 de luni de la semnarea contractului, cu respectarea următoarelor termene pentru activitățile principale ale contractului:

- servicii de livrare și instalare software – maxim luna 7, finalizate cu proces verbal de recepție cantitativă și calitativă, respectiv punere în funcțiune (activare) a licențelor software;
- servicii de analiză a sistemului – maxim luna 5, finalizate cu proces verbal de recepție a raportului (documentului) de analiză;
- servicii de proiectare a sistemului – maxim luna 6, finalizate cu proces verbal de recepție a documentației tehnice aferentă activității de proiectare a sistemului informatic;
- servicii dezvoltare software – maxim luna 15, finalizate cu proces verbal de recepție a release note-ului pentru sistemul informatic, ca rezultat al activității de dezvoltare și configurare;
- servicii de migrare a fluxurilor de lucru şi a datelor din sistemul PCUe – maxim luna 15, finalizate cu proces verbal de recepție a raportului de migrare, ca rezultat al migrării fluxurilor de lucru și a datelor din sistemul PCUe;

- servicii de testare a sistemului integrat, inclusiv teste de securitate – maxim luna 17, finalizate cu proces verbal de recepție a raportului de testarea funcționalităților sistemului informatic;
- servicii de instruire – maxim luna 18, finalizate cu proces verbal de recepție a raportului de instruire a personalului dedicat din cadrul ADR;
- servicii de punere în producție – maxim luna 18, finalizate cu proces verbal de recepție a raportului de punere în producție.

Ofertanții pot propune desfășurarea activităților contractului în paralel, fără să depășească termenele limită prezentate mai sus, indicând în metodologia de implementare a contractului modul de abordare propus.

11. ANEXE

11.1. ANEXA I la REGULAMENTUL (UE) 2018/1724 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 2 octombrie 2018

Lista de informații relevante pentru cetățenii și întreprinderile
care își exercită drepturile în cadrul pieței interne menționate la art. 2 alin. (2) lit. a)

Domeniul		**INFORMAȚII PRIVIND DREPTURILE, OBLIGAȚIILE ȘI NORMELE CARE DECURG DIN DREPTUL UNIUNII ȘI DREPTUL NAȚIONAL**	
A.	Călătoriile în interiorul Uniunii	1.	documentele solicitate cetățenilor Uniunii, membrilor familiilor lor care nu sunt cetățeni ai Uniunii, minorilor care călătoresc singuri, cetățenilor din afara Uniunii atunci când călătoresc din străinătate în cadrul Uniunii (carte de identitate, pașaport, vize)
		2.	drepturile și obligațiile pasagerilor care călătoresc cu avionul, cu trenul, cu vaporul, cu autobuzul în și din Uniune, precum și ale celor care cumpără pachete de servicii de călătorie sau servicii de călătorie asociate
		3.	asistență în caz de mobilitate redusă atunci când persoanele respective călătoresc în și din Uniune
		4.	transportarea animalelor, plantelor, alcoolului, tutunului, țigărilor și a altor produse atunci când se călătorește în interiorul Uniunii
		5.	apelurile vocale și serviciile de trimitere și de primire a mesajelor electronice și de date electronice în interiorul Uniunii
B.	Munca și pensionarea în	1.	căutarea unui loc de muncă în alt stat membru
		2.	obținerea unui loc de muncă în alt stat membru
		3.	recunoașterea calificărilor profesionale pentru obținerea unui loc de muncă în alt stat membru

Domeniul		INFORMAȚII PRIVIND DREPTURILE, OBLIGAȚIILE ȘI NORMELE CARE DECURG DIN DREPTUL UNIUNII ȘI DREPTUL NAȚIONAL	
	Uniunea Europeană	4.	impozitarea în alt stat membru
		5.	normele în materie de răspundere și asigurare obligatorie legate de rezidența sau ocuparea unui loc de muncă într-un alt stat membru
		6.	condiții legate de ocuparea forței de muncă, inclusiv pentru lucrătorii detașați, prevăzute prin lege sau prin instrumente de reglementare (inclusiv informații privind programul de lucru, concedii plătite, drepturile la vacanță, drepturile și obligațiile referitoare la orele suplimentare de lucru, controalele sanitare, rezilierea contractelor, concedierile și disponibilizările)
		7.	egalitatea de tratament (normele privind combaterea discriminării la locul de muncă, privind remunerarea egală pentru femei și bărbați, și privind egalitatea de remunerare pentru angajații cu contracte de muncă cu durată nedeterminată sau determinată)
		8.	obligațiile în materie de sănătate și siguranță în ceea ce privește diferitele tipuri de activități
		9.	drepturile și obligațiile de asigurare socială în Uniune, inclusiv cele legate de stabilirea unor pensii
C.	Vehiculele în Uniune	1.	mutarea unui autovehicul temporar sau permanent într-un alt stat membru
		2.	obținerea și reînnoirea permisului de conducere
		3.	contractarea unei asigurări auto obligatorii
		4.	vânzarea și cumpărarea unui autovehicul într-un alt stat membru
		5.	normele naționale referitoare la trafic și cerințele pentru conducătorii auto, inclusiv norme generale pentru utilizarea infrastructurilor rutiere naționale: tarife în funcție de durată timp (viniete), taxe în funcție de distanța parcursă (taxe de trecere), autocolantele de emisii

Domeniul		INFORMAȚII PRIVIND DREPTURILE, OBLIGAȚIILE ȘI NORMELE CARE DECURG DIN DREPTUL UNIUNII ȘI DREPTUL NAȚIONAL	
D.	Ședereа într-un alt stat membru	1.	mutarea temporară sau permanentă într-un alt stat membru
		2.	achiziționarea și vânzarea de proprietăți imobiliare, inclusiv orice condiții și obligații referitoare la impozitare, proprietate sau utilizarea unor astfel de proprietăți, inclusiv ca reședință secundară
		3.	participarea la alegerile locale și la alegerile pentru Parlamentul European
		4.	cerințele de eliberare a permiselor de ședere pentru cetățenii Uniunii și pentru membrii familiilor lor, inclusiv pentru membrii familiei care nu sunt cetățeni ai Uniunii
		5.	condiții aplicabile pentru naturalizarea resortisanților din alte state membre
		6.	norme aplicabile în caz de deces, inclusiv norme aplicabile pentru repatrierea rămășițelor pământești în alt stat membru
E.	Studiile sau stagiile în alt stat membru	1.	sistemul de învățământ într-un alt stat membru, inclusiv educația și îngrijire timpurie, învățământul primar și secundar, învățământul superior și învățarea în rândul adulților
		2.	voluntariatul în alt stat membru
		3.	stagiile în alt stat membru
		4.	desfășurarea unor activități de cercetare în alt stat membru în cadrul unui program de învățământ
F.	Asistența medicală	1.	obținerea de îngrijiri medicale în alt stat membru
		2.	achiziționarea de produse farmaceutice prescrise în alt stat membru decât cel în care a fost eliberată rețeta, online sau în persoană
		3.	norme privind asigurările de sănătate aplicabile în cazul șederile de scurtă sau de lungă durată în alt stat membru, inclusiv procedura de solicitare a unui card european de asigurări sociale de sănătate

Domeniul		INFORMAȚII PRIVIND DREPTURILE, OBLIGAȚIILE ȘI NORMELE CARE DECURG DIN DREPTUL UNIUNII ȘI DREPTUL NAȚIONAL	
		4.	informații generale privind drepturile de acces sau obligațiile de a participa la măsurile preventive publice disponibile în materie de sănătate
		5.	serviciile furnizate prin intermediul numerelor de urgență naționale, inclusiv numerele „112” și „116”
		6.	drepturile și condițiile pentru integrarea într-un centru de îngrijire
G.	Drepturile cetățenilor și ale familiilor	1.	naștere, încredințarea copiilor minori, responsabilitățile parentale, norme privind recurgerea la o mamă purtătoare și adopția, inclusiv adopția de către al doilea părinte, obligațiile de întreținere față de copii într-o situație familială transfrontalieră
		2.	viața în cuplu cu naționalități diferite, inclusiv cupluri de același sex (căsătorii, parteneriate civile sau înregistrate, separări, divorțuri, drepturi de proprietate, drepturile coabitanților)
		3.	norme privind recunoașterea genului
		4.	drepturile și obligațiile succesorale într-un alt stat membru, inclusiv regimul fiscal
		5.	drepturi și norme aplicabile în cazul răpirii transfrontaliere a copiilor de către unul dintre părinți
H.	Drepturile consumatorilor	1.	achiziționarea de bunuri, conținut digital sau servicii (inclusiv servicii financiare) dintr-un alt stat membru, online sau în persoană
		2.	deținerea unui cont bancar în alt stat membru
		3.	racordarea la utilități (gaz, electricitate, apă, evacuarea gunoiului menajer, telecomunicații și internet)
		4.	plăți, inclusiv transferuri de credit, întârzieri în ceea ce privește plățile transfrontaliere
		5.	drepturile consumatorilor și garanțiile legate de cumpărarea de bunuri și servicii, inclusiv procedurile pentru soluționarea litigiilor în materie de consum și acordarea de despăgubiri

Domeniul		**INFORMAȚII PRIVIND DREPTURILE, OBLIGAȚIILE ȘI NORMELE CARE DECURG DIN DREPTUL UNIUNII ȘI DREPTUL NAȚIONAL**	
		6.	siguranța și securitatea produselor de consum
		7.	închirierea unui autovehicul
I.	Protecția datelor cu caracter personal	1.	exercitarea drepturilor persoanelor vizate în ceea ce privește protecția datelor cu caracter personal
Domenii de informații privind întreprinderile:			
Domeniul		**INFORMAȚII CU PRIVIRE LA DREPTURI, OBLIGAȚII ȘI NORME**	
J.	Inițierea, desfășurarea sau închiderea unei afaceri	1.	înregistrarea, schimbarea formei juridice sau închiderea unei întreprinderi (procedurile de înregistrare și formele juridice pentru desfășurarea activității)
		2.	mutarea unei întreprinderi în alt stat membru
		3.	drepturile de proprietate intelectuală (depunerea unei cereri de brevet, înregistrarea unei mărci, a unei schițe sau a unui desen, obținerea unei licențe de reproducere)
		4.	echitate și transparență în practicile comerciale, inclusiv cele privind drepturile consumatorilor și garanțiile legate de vânzarea de bunuri și servicii
		5.	oferirea de facilități online pentru plățile transfrontaliere atunci când se comercializează bunuri și servicii online
		6.	drepturile și obligațiile care decurg din dreptul contractelor, inclusiv dobânzile de penalizare
		7.	procedurile de insolvență și de lichidare a întreprinderilor

Domeniul		INFORMAȚII PRIVIND DREPTURILE, OBLIGAȚIILE ȘI NORMELE CARE DECURG DIN DREPTUL UNIUNII ȘI DREPTUL NAȚIONAL	
		8.	asigurarea de credit
		9.	fuziunile dintre companii sau vânzarea unei întreprinderi
		10.	răspunderea civilă a administratorilor unei societăți
		11.	norme și obligații privind prelucrarea datelor cu caracter personal
K.	Angajați	1.	aspecte legate de ocuparea forței de muncă prevăzute prin lege sau prin instrumente de reglementare (inclusiv programul de lucru, concedii plătite, drepturile la vacanță, drepturile și obligațiile referitoare la orele suplimentare de lucru, controalele sanitare, rezilierea contractelor, concedierile și disponibilizările)
		2.	drepturile și obligațiile de asigurare socială în Uniune (înregistrarea în calitate de angajator, înregistrarea angajaților, notificarea încetării contractului unui salariat, plata contribuțiilor de asigurări sociale, drepturile și obligațiile legate de pensii)
		3.	ocuparea forței de muncă de către lucrători din alte state membre (detașarea lucrătorilor, normele referitoare la libera prestare a serviciilor, cerințele privind reședința pentru lucrători)
		4.	egalitatea de tratament (normele privind combaterea discriminării la locul de muncă, privind remunerarea egală pentru femei și bărbați, și privind egalitatea de remunerare pentru angajații cu contracte de muncă cu durată nedeterminată sau determinată)
		5.	normele privind reprezentarea personalului
L.	Impozite	1.	TVA: informații cu privire la regulile generale, rate de impozitare și scutiri, înregistrarea și plata TVA, obținerea unei rambursări

Domeniul		INFORMAȚII PRIVIND DREPTURILE, OBLIGAȚIILE ȘI NORMELE CARE DECURG DIN DREPTUL UNIUNII ȘI DREPTUL NAȚIONAL	
		2.	accize: informații cu privire la regulile generale, rate de impozitare și scutiri, înregistrarea pentru accize și plata accizelor, obținerea unei rambursări
		3.	taxe vamale și alte impozite și taxe percepute la importuri
		4.	proceduri vamale pentru importuri și exporturi în temeiul Codului vamal al Uniunii
		5.	alte taxe: plăți, rate, declarații fiscale
M.	Bunuri	1.	obținerea marcajului CE
		2.	norme și cerințe privind produsele
		3.	identificarea standardelor aplicabile, specificațiile tehnice și obținerea certificării pentru produse
		4.	recunoașterea reciprocă a produselor care nu fac obiectul unor specificații la nivelul Uniunii
		5.	cerințe privind clasificarea, etichetarea și ambalarea substanțelor chimice periculoase
		6.	vânzarea la distanță sau în afara spațiului comercial: informațiile care urmează să fie furnizate clienților în avans, confirmarea scrisă a contractului, retragerea dintr-un contract, furnizarea de bunuri, alte obligații specifice
		7.	produsele cu defect: drepturile consumatorilor și garanții, responsabilitățile post-vânzare, căi de atac pentru partea prejudiciată
		8.	certificare, etichete (EMAS, etichetele energetice, proiectarea ecologică, eticheta ecologică a UE)
		9.	reciclarea și gestionarea deșeurilor
N.	Servicii	1.	obținerea de licențe, autorizații sau permise în vederea înființării și exploatării unei întreprinderi
		2.	informarea autorităților cu privire la activitățile transfrontaliere
		3.	recunoașterea calificărilor profesionale, inclusiv a educației și formării profesionale

Domeniul		INFORMAȚII PRIVIND DREPTURILE, OBLIGAȚIILE ȘI NORMELE CARE DECURG DIN DREPTUL UNIUNII ȘI DREPTUL NAȚIONAL	
O.	Finanțarea unei întreprinderi	1.	obținerea accesului la finanțare la nivelul Uniunii, inclusiv programele de finanțare ale Uniunii și granturile de afaceri
		2.	obținerea accesului la finanțare la nivel național
		3.	inițiative destinate antreprenorilor (schimburi organizate pentru noii antreprenori, programe de mentorat etc.)
P.	Contracte publice	1.	participarea la licitațiile publice: norme și proceduri
		2.	prezentarea unei oferte online ca răspuns la o cerere de ofertă publică
		3.	raportarea neregulilor în ceea ce privește procesul de licitație
Q.	Sănătatea și securitatea în muncă	1.	obligațiile în materie de sănătate și siguranță în ceea ce privește diferitele tipuri de activități, printre care prevenirea riscurilor, informarea și formarea profesională

11.2. Procedurile ce se regăsesc la Anexa II a Regulamentului (UE) 2018/1724

Tabel 1 – Procedurile ce se regăsesc la Anexa II a Regulamentului 2018/1724

Domenii	Procedură	Instituții responsabile	Secțiune aferentă e-guvernare	Procedură online (e-guvernare)
Naștere	Solicitarea dovezii înregistrării nașterii	Ministerul Afacerilor Interne	Familie – Naștere/ Adopție	Nu
Reședința	▪ Solicitarea dovezii de reședință	▪ Inspectoratul General pentru Imigrări ▪ Ministerul Afacerilor Interne (Direcția Generală de Evidența Persoanelor)	Stabilirea într-un stat membru	Da (parțial) – I.G.I
Studii	▪ Solicitarea finanțării studiilor în învățământul superior cum ar fi granturile de studiu și împrumuturile acordate de un organism public sau o instituție publică	▪ Ministerul Educației ▪ Universități	Studiile sau stagiile într-un alt stat membru	Nu cu excepția solicitărilor recunoașterii diplomelor și certificărilor – Centrul Național de Recunoaștere și Echivalare a Diplomelor

Domenii	Procedură	Instituții responsabile	Secțiune aferentă e-guvernare	Procedură online (e-guvernare)
	▪ Depunerea unei cereri inițiale de acces în instituții publice de învățământ superior ▪ Solicitarea recunoașterii academice a diplomelor, a certificatelor sau a altor dovezi ale studiilor sau cursurilor			
Aspecte legate de muncă	▪ Cerere de stabilire a legislației aplicabile cu titlul II din Regulamentul (CE) nr. 883/2004 ▪ Notificarea modificărilor privind circumstanțele personale sau profesionale ale persoanei care primește prestații de securitate socială, relevante pentru prestațiile respective ▪ Cerere pentru acordarea unui card european de asigurări sociale de sănătate (CEASS) ▪ Depunerea unei declarații privind impozitul pe venit	▪ Inspecția Muncii ▪ Ministerul Muncii si Solidaritatii Sociale	Munca și pensionarea în Uniunea Europeană	Nu

Domenii	Procedură	Instituții responsabile	Secțiune aferentă e-guvernare	Procedură online (e-guvernare)
Mutarea	▪ Înregistrarea unei modificări de adresă ▪ Înmatricularea unui vehicul care provine dintr-un stat membru al UE sau care a fost deja înmatriculat într-un stat membru al UE, prin proceduri standard ▪ Obținerea unor autocolante pentru utilizarea infrastructurilor rutiere naționale: tarife în funcție de durată timp (viniete), taxe în funcție de distanța parcursă (taxa de trecere) emise de un organism sau o instituție publică ▪ Obținerea unui autocolant pentru emisii emise de un organism sau o instituție publică	▪ Inspectoratul General pentru Imigrări ▪ Direcția Evidența Populației (Ministerul Afacerilor Interne) ▪ Registrul Auto Român – Direcția Regim Permise de Conducere și Înmatriculare a Vehiculelor ▪ Compania Națională de Administrare a Infrastructurii Rutiere	▪ Înregistrarea unei modificări de adresă – secțiunea Mutare în alt stat membru ▪ Înmatricularea unui vehicul – Secțiunea Vehiculele în Uniune	▪ Modificări adresa: Da - Portal IGI ▪ Înmatriculare vehicul: Nu ▪ Obținerea unor autocolante (viniete): Da - Sistem informatic de emitere, gestiune, monitorizare și control a rovinietei (SIEGMCR)
Pensionarea	▪ Solicitarea pensiei și a prestațiilor de prepensionare din sistemele obligatorii	▪ Casa Națională de Pensii Publice	Rubrica Munca și pensionarea în UE -	▪ Nu

Domenii	Procedură	Instituții responsabile	Secțiune aferentă e-guvernare	Procedură online (e-guvernare)
	▪ Solicitarea de informații privind datele legate de sistemele obligatorii de pensii		Secțiunea pensionare lipsește însă	
Demararea, desfășurarea și închiderea unei activități comerciale	▪ Notificarea activității comerciale, autorizațiile de desfășurare a activității, modificări ale activităților economice și încetarea unei activități economice care nu implică proceduri de insolvență sau lichidare, excluzând înregistrarea inițială a unei activități comerciale la registrul comerțului și cu excepția procedurilor privind constituirea sau a oricăror alte cereri ulterioare depuse de către societăți sau firme în sensul articolului 54 al doilea paragraf din TFUE ▪ Înregistrarea unui angajator (a unei persoane fizice) în sistemele obligatorii de pensii și de asigurare	▪ Agenția Națională pentru Ocuparea Forței de Muncă ▪ Agenția Națională de Administrare Fiscală ▪ Casa Națională de Asigurări de Sănătate ▪ Casa Națională de Pensii Publice ▪ Agenția Națională pentru Plăți și Inspecție Socială	▪ Inițierea, desfășurarea sau închiderea unei afaceri ▪ Angajați ▪ Impozite – Platforma nu oferă informații privind impozitul pe societăți	▪ Inițierea, desfășurarea sau închiderea unei afaceri: Da – portal.onrc.ro ▪ Înregistrare angajator/ angajat – Nu ▪ Plata impozite – Da - Ghiseul.ro

Domenii	Procedură	Instituții responsabile	Secțiune aferentă e-guvernare	Procedură online (e-guvernare)
	▪ Înregistrarea angajaților în sistemele obligatorii de pensii și de asigurare ▪ Depunerea unei declarații privind impozitul pe societăți ▪ Notificarea către sistemele de securitate socială a încetării contractului cu un angajat cu excepția procedurilor de încetare colectivă a contractelor angajaților ▪ Plata contribuțiilor sociale pentru angajați			

Sursa: Anexa II a Regulamentului (UE) 2018/1724, analiza Autorității pentru Digitalizarea României

11.3. Tabel 4 – Efortul de analiză al procedurilor administrative românești pentru a permite implementarea Regulamentului Single Digital Gateway (Anexa II)

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
MAI SPCLEP	Naștere	Solicitarea dovezii înregistrării nașterii	Dovada înregistrării nașterii sau certificatul de naștere	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională (engleza)
MAI SPCLEP	Reședința	Solicitarea dovezii de reședință	Confirmarea înregistrării la adresa curentă	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
				4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională (engleza)
MAI SPCLEP	Mutarea	Înregistrarea unei modificări a adresei	Confirmarea radierii adresei anterioare și a înregistrării noii adrese	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
				7. Traducerea oficială a documentelor într-o limbă de circulație internațională
MAI DRPCIV	Mutarea	Înmatricularea unui autovehicul care provine dintr-un stat membru al UE sau care a fost deja înmatriculat într-un stat membru al UE ([2])	Dovada înmatriculării unui vehicul	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
Ministerul Transporturilor și Infrastructurii	Mutarea	Obținerea de autocolante pentru utilizarea infrastructurilor rutiere	Primirea unui autocolant pentru taxa rutieră, a unei viniete sau a	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă

[2] Include următoarele vehicule: (a) orice autovehicul sau remorcă, astfel cum este menționat(ă) la articolul 3 din Directiva 2007/46/CE a Parlamentului European și a Consiliului (JO L 263, 9.10.2007, p.1) și (b) orice autovehicul cu două sau trei roți, cu roți jumelate sau nu, destinate transportului rutier, astfel cum este menționat la articolul 1 din Regulamentul (UE) nr. 168/2013 al Parlamentului European și al Consiliului (JO L 60, 2.3. 2013, p.5)

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
CNAIR		naționale: tarife în funcție de durată timp (viniete), taxe în funcție de distanța parcursă (taxe trecere) emise de un organism sau de o instituție publică	altei dovezi de plată	4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
Ministerul Transporturilor și Infrastructurii CNAIR	Mutarea	Obținerea unui autocolant pentru emisii emise de un organism sau o instituție publică	Primirea unui autocolant pentru emisii sau a altei dovezi de plată	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc.

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
				5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
Ministerul Educației Naționale	Studii	Solicitarea finanțării studiilor în învățământul superior, cum ar fi granturile de studiu și împrumuturile acordate de un organism public sau o instituție publică	Decizia privind cererea de finanțare sau confirmarea de primire	8. Identificarea procedurii la nivel național 9. Identificarea actelor necesare îndeplinirii procedurii 10. Procedura eliberării documentului final – legislația aplicabilă 11. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 12. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 13. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 14. Traducerea oficială a documentelor într-o limbă de circulație internațională

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
Ministerul Educației Naționale	Studii	Depunerea unei cereri inițiale de acces în instituții publice de învățământ superior	Confirmarea de primire a notificării	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
Ministerul Educației Naționale CNRED	Studii	Solicitarea recunoașterii academice a diplomelor, a certificatelor sau a altor dovezi ale	Decizia privind cererea de recunoaștere	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
		studiilor sau cursurilor		6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
Ministerul Muncii și Solidarității Sociale	Aspecte legate de muncă	Notificarea modificărilor privind circumstanțele personale sau profesionale ale persoanei care primește prestații de securitate socială, relevante pentru prestațiile respective	Confirmarea de primire a notificării acestor modificări	1. Identificarea tuturor procedurilor la nivel național care ar putea cădea sub incidența acestui eveniment de viață precum: I. Beneficii de asistență socială pentru prevenirea și combaterea sărăciei și riscului de excluziune socială: • **Ajutorul social** • **Ajutorul social pentru încălzirea locuinței** • **Ajutorul pentru susținerea familiei** **II.** Beneficii pentru susținerea copilului și a familiei care au în vedere nașterea, educația și întreținerea copiilor: • **Alocația de stat pentru copii** • **Alocația de plasament** • **Indemnizația pentru creșterea copilului** • **Stimulentul de inserție** • **Indemnizația lunară aferentă concediului de acomodare** III. Beneficii de asistență socială pentru sprijinirea persoanelor cu nevoi speciale:

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
				• **<u>Drepturi acordate persoanelor cu handicap</u>** • **<u>Indemnizația lunară acordată persoanelor cu handicap grav și accentuat</u>** 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
Ministerul Muncii și Solidarității Sociale ANOFM	Aspecte legate de muncă	Notificarea modificărilor privind circumstanțele personale sau profesionale ale	Confirmarea de primire a notificării acestor notificări	1. Identificarea tuturor procedurilor la nivel național care ar putea cădea sub incidența acestui eveniment de viață precum: • **Indemnizația de șomaj** 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
		persoanei care primește prestații de securitate socială, relevante pentru prestațiile respective		4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
Ministerul Sănătății CNAS	Aspecte legate de muncă	Notificarea modificărilor privind circumstanțele personale sau profesionale ale persoanei care primește prestații de securitate socială,	Confirmarea de primire a notificării acestor modificări	1. Identificarea tuturor procedurilor la nivel național care ar putea cădea sub incidența acestui eveniment de viață precum: • **Concedii medicale și indemnizații pentru incapacitate temporară de muncă, cauzată de boli obișnuite sau de accidente în afara muncii** • **Concedii medicale și indemnizații pentru prevenirea îmbolnăvirilor și recuperarea capacității de muncă, exclusiv pentru situațiile rezultate ca urmare a unor accidente de muncă sau boli profesionale** • **Concedii medicale și indemnizații pentru maternitate** • **Concedii medicale pentru îngrijirea copilului bolnav**

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
		relevante pentru prestațiile respective		• **<u>Indemnizație de risc maternal</u>** • **<u>Concediu medical pentru îngrijirea copilului bolnav oncologic cod 17</u>** 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
CNAS	Aspecte legate de muncă	Cerere pentru acordarea unui card european de asigurări sociale de	Cardul european de asigurări sociale de sănătate (CEASS)	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc.

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
		sănătate (CEASS)		5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
CNPP	Aspecte legate de muncă	Notificarea modificărilor privind circumstanțele personale sau profesionale ale persoanei care primește prestații de securitate socială, relevante pentru prestațiile respective	Confirmarea de primire a notificării acestor modificări	1. Identificarea tuturor procedurilor la nivel național care ar putea cădea sub incidența acestui eveniment de viață precum: • **Pensie de invaliditate** • **Pensie de urmaș** 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
CNPP	Aspecte legate de muncă	Cerere stabilire a legislației aplicabile în conformitate cu titlul II din Regulamentul (CE) nr. 883/2004	Decizie privind legislația aplicabilă	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
ANAF	Aspecte legate de muncă	Depunerea unei declarații privind impozitul pe venit	Confirmarea de primire a declarației	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
				6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 8. Traducerea oficială a documentelor într-o limbă de circulație internațională
Ministerul Muncii și Solidarității Sociale ITM	Demararea, desfășurarea și închiderea unei activități comerciale	Înregistrarea unui angajator (a unei persoane fizice) în sistemele obligatorii de pensii și de asigurare	Confirmarea înregistrării sau numărul de înregistrare la asigurările sociale	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
Ministerul Muncii și Solidarității Sociale	Demararea, desfășurarea și închiderea unei	Înregistrarea angajaților în sistemele obligatorii de	Confirmarea înregistrării sau numărul de înregistrare la	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
ITM	activități comerciale	pensii și de asigurare	asigurările sociale	4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
Ministerul Muncii și Solidarității Sociale ITM	Demararea, desfășurarea și închiderea unei activități comerciale	Notificarea către sistemele de securitate socială a încetării contractului cu un angajat, cu excepția procedurilor de încetare colectivă a	Confirmarea de primire a notificării	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
		contractelor angajaților		
ONRC	Demararea, desfășurarea și închiderea unei activități comerciale	Notificarea activității comerciale, autorizațiile de desfășurare a activității, modificări ale activităților economice care nu implică proceduri de insolvență sau lichidare, excluzând înregistrarea inițială a unei activități	Confirmarea de primire a notificării sau de modificare sau cererea de autorizare a activității comerciale	1. Identificarea tuturor procedurilor la nivel național care ar putea cădea sub incidența acestui eveniment de viață precum: • **Notificarea activității comerciale** • **Obținerea autorizației de desfășurare a activității economice** • **Modificarea activității economice** 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională.

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
		comerciale la registrul comerțului și cu excepția procedurilor privind constituirea sau a oricăror alte cereri ulterioare depuse de către societăți sau firme în sensul articolului 45 al doilea paragraf din TFUE		
ANAF	Demararea, desfășurarea și închiderea unei	Depunerea unei declarații privind	Confirmarea de primire a declarației	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
	activități comerciale	impozitul pe societăți		4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
ANAF	Demararea, desfășurarea și închiderea unei activități comerciale	Plata contribuțiilor sociale pentru angajați	Primirea sau altă formă de confirmare a plății contribuțiilor sociale pentru angajați	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
ANAF	Demararea, desfășurarea și închiderea unei activități comerciale	Înregistrarea unui angajator (a unei persoane fizice) în sistemele obligatorii de pensii și de asigurare	Confirmarea înregistrării sau numărul de înregistrare la asigurările sociale	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
CNPP	Pensionarea	Solicitarea pensiei și a prestațiilor de prepensionare din sistemele obligatorii	Confirmarea de primire a solicitării sau decizia referitoare la solicitarea pentru plata unei pensii sau	1. Identificarea tuturor procedurilor la nivel național care ar putea cădea sub incidența acestui eveniment de viață precum: • **Solicitarea pensiei pentru limită de vârstă** • **Prestații prepensionare** 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
			prestațiile de prepensionare	4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională
CNPP	Pensionarea	Solicitarea de informații privind datele legate de sistemele obligatorii de pensii	Declarația privind datele cu caracter personal referitoare la pensie	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională

Autoritate	Eveniment de viață	Procedură	Rezultat al procedurii	Efort din partea prestatorului
CNPP	Aspecte legate de muncă	Cerere stabilire a legislației aplicabile în conformitate cu titlul II din Regulamentul (CE) nr. 883/2004	Decizie privind legislația aplicabilă	1. Identificarea procedurii la nivel național 2. Identificarea actelor necesare îndeplinirii procedurii 3. Procedura eliberării documentului final – legislația aplicabilă 4. Este această procedură disponibilă online sau ar putea aceasta fi începută online? Ex: formular disponibil online, posibilitatea de a transmite documentele prin intermediul unei adrese de e-mail etc. 5. Elementele pe care le cuprinde documentul final – în vederea înregistrării în Brokerul de dovezi 6. Identificarea autorității/ autorităților (dacă acestea sunt autorități locale) care sunt competente pentru eliberarea acestor documente 7. Traducerea oficială a documentelor într-o limbă de circulație internațională

11.4. Domeniile de informații privind cetățenii ce se regăsesc la Anexa I a Regulamentului (UE) 2018/1724

Tabel 2 – Domenii de informații privind cetățenii ce se regăsesc la Anexa I a Regulamentului 2018/1724

Domenii	Instituții responsabile	Secțiune E-guvernare
Călătoriile în interiorul Uniunii	Ministerul Afacerilor Interne	Călătoriile în interiorul Uniunii
Munca și pensionarea în Uniunea Europeană	▪ Ministerul Muncii ▪ Agenția Națională pentru Ocuparea Forței de Muncă ▪ Casa Națională de Asigurări de Sănătate ▪ Agenția Națională de Administrare Fiscală ▪ Casa Națională de Pensii	Munca și pensionarea în Uniunea Europeană
Vehiculele în Uniune	▪ Registrul Auto Român ▪ Ministerul Afacerilor Interne (permise) ▪ Autoritatea de Supraveghere Financiară	Vehiculele în Uniune
Ședereа într-un alt stat membru	▪ Ministerul Afacerilor Interne ▪ Agenția Națională de Administrare Fiscală ▪ Casa Națională de Asigurări de Sănătate	Ședereа într-un alt stat membru
Studiile sau stagiile într-un alt stat membru	▪ Ministerul Educației (Centrul Național de Recunoaștere și Echivalare a Diplomelor)	Studiile sau stagiile într-un alt stat membru
Asistență medicală	▪ Casa Națională de Asigurări de Sănătate	Asistență medicală
Drepturile cetățenilor și ale familiilor	▪ Ministerul Afacerilor Interne	Drepturile cetățenilor și ale familiilor

Domenii	Instituții responsabile	Secțiune E-guvernare
	▪ Ministerul Muncii si Solidaritatii Sociale ▪ Ministerul Afacerilor Externe	
Drepturile consumatorilor	▪ Autoritatea pentru Protecția Consumatorilor	Drepturile consumatorilor
Protecția datelor cu caracter personal	▪ Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal	Protecția datelor cu caracter personal

Sursa: Anexa I a Regulamentului (UE) 2018/1724, analiza Autorității pentru Digitalizarea României

11.5. Domenii de informații privind întreprinderile ce se regăsesc la Anexa I a Regulamentului (UE) 2018/1724

Tabel 3 – Domenii de informații privind întreprinderile ce se regăsesc la Anexa I a Regulamentului 2018/1724

Domenii	Instituții responsabile	Secțiune E-guvernare
Inițierea, desfășurarea sau închiderea unei afaceri	Oficiul Național al Registrului Comerțului	Inițierea, desfășurarea sau închiderea unei afaceri
Angajați	▪ Inspecția Muncii ▪ Casa Națională de Asigurări de Sănătate	Angajați
Impozite	▪ Ministerul Afacerilor Interne ▪ Agenția Națională de Administrare Fiscală ▪ Casa Națională de Asigurări de Sănătate	Impozite
Bunuri	▪ Ministerul Educației (Centrul Național de Recunoaștere și Echivalare a Diplomelor)	Bunuri
Servicii (Autorizații/ licențe/ recunoașterea calificărilor profesionale)	▪ Ministerul Mediului (cu Agențiile pentru Protecția Mediului) ▪ Autoritatea Națională Sanitară Veterinară și pentru Siguranța Alimentelor ▪ Ministerul Sănătății (cu Direcțiile de sănătate publică județene, respectiv a municipiului București) ▪ Ministerul Afacerilor Interne (Inspectoratul General pentru Situații de Urgență)	Servicii (Autorizații/ licențe/ recunoașterea calificărilor profesionale)

Domenii	Instituții responsabile	Secțiune E-guvernare
	▪ Ministerul Educației (Centrul Național de Recunoaștere și Echivalare a Diplomelor)	
Finanțarea unei întreprinderi	▪ Instituții de credit ▪ Ministerul Antreprenoriatului și Turismului (punct de informare privind sursele de finanțare nerambursabilă pentru sectorul privat)	Finanțarea unei întreprinderi
Contracte publice	▪ Agentia Nationala pentru Achizitii Publice	Contracte publice
Sănătatea și securitatea în muncă	▪ Inspecția Muncii	Sănătatea și securitatea în muncă

Sursa: Anexa I a Regulamentului (UE) 2018/1724, analiza Autorității pentru Digitalizarea României

11.6. ANEXA III la REGULAMENTUL (UE) 2018/1724 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 2 octombrie 2018

Lista serviciilor de asistență și de soluționare a problemelor menționate la articolul 2 alineatul (2) litera (c)

1. Ghișeele unice (1)
2. Punctele de informare despre produse (2)
3. Punctele de informare despre produse pentru construcții (3)
4. Centrele naționale de asistență pentru calificări profesionale (4)
5. Punctele naționale de contact pentru asistența medicală transfrontalieră (5)
6. Rețeaua europeană de servicii de ocupare a forței de muncă (EURES) (6)
7. Soluționarea online a litigiilor (SOL) (7)

(1) Directiva 2006/123/CE a Parlamentului European și a Consiliului din 12 decembrie 2006 privind serviciile în cadrul pieței interne (JO L 376, 27.12.2006, p. 36).

(2) Regulamentul (CE) nr. 764/2008 al Parlamentului European și al Consiliului din 9 iulie 2008 de stabilire a unor proceduri de aplicare a anumitor norme tehnice naționale pentru produsele comercializate în mod legal în alt stat membru și de abrogare a Deciziei nr. 3052/95/CE (JO L 218, 13.8.2008, p. 21).

(3) Regulamentul (UE) nr. 305/2011 al Parlamentului European și al Consiliului din 9 martie 2011 de stabilire a unor condiții armonizate pentru comercializarea produselor pentru construcții și de abrogare a Directivei 89/106/CEE a Consiliului (JO L 88, 4.4.2011, p. 5).

(4) Directiva 2005/36/CE a Parlamentului European și a Consiliului din 7 septembrie 2005 privind recunoașterea calificărilor profesionale (JO L 255, 30.9.2005, p. 22).

(5) Directiva 2011/24/UE a Parlamentului European și a Consiliului din 9 martie 2011 privind aplicarea drepturilor pacienților în cadrul asistenței medicale transfrontaliere (JO L 88, 4.4.2011, p. 45).

(6) Regulamentul (UE) 2016/589 al Parlamentului European și al Consiliului din 13 aprilie 2016 privind o rețea europeană de servicii de ocupare a forței de muncă (EURES), accesul lucrătorilor la servicii de mobilitate și integrarea mai bună a piețelor forței de muncă și de modificare a Regulamentelor (UE) nr. 492/2011 și (UE) nr. 1296/2013 (JO L 107, 22.4.2016, p. 1).

(7) Regulamentul (UE) nr. 524/2013 al Parlamentului European și al Consiliului din 21 mai 2013 privind soluționarea online a litigiilor în materie de consum și de modificare a Regulamentului (CE) nr. 2006/2004 și a Directivei 2009/22/CE (Regulamentul privind SOL în materie de consum) (JO L 165, 18.6.2013, p. 1).

11.7. ANEXA I la Regulamentul de punere în aplicare (UE) 2020/1121 al Comisiei din 29 iulie 2020

Indicatorii pentru etichetare menționați la articolul 2 alineatul (3)

	Elemente care trebuie să facă parte din informațiile de etichetare care vor fi incluse în metadatele paginilor web care fac parte din portalul digital unic							
	Parte generală	***Cod de țară***	***Cod subnațional (după caz)***	***Tip de serviciu (*1)***	***Limba paginii***	***Domeniu vizat de anexa I la Regulamentul (UE) 2018/1724***		***Serviciu vizat de articolul 7 din Regulamentul (UE) 2018/1724 sau de anexa III la acesta***
	Portalul digital unic (PDU)	Conform codului ISO 3166 alpha-2 (EL pentru Grecia)	*Conform NUTS 1-3 sau UAL*		Conform codului ISO 639-1 alpha-2	A-Q	01-09	Titlul complet al serviciului
Pagini web cu informații privind norme, drepturi și obligații	X	x	*x*	Informații	x	x	x	Nu este cazul

	Elemente care trebuie să facă parte din informațiile de etichetare care vor fi incluse în metadatele paginilor web care fac parte din portalul digital unic							
	Parte generală	***Cod de țară***	***Cod subnațional (după caz)***	***Tip de serviciu*** (*1)	***Limba paginii***	***Domeniu vizat de anexa I la Regulamentul (UE) 2018/1724***		***Serviciu vizat de articolul 7 din Regulamentul (UE) 2018/1724 sau de anexa III la acesta***
Pagini web cu informații privind proceduri	X	x	*x*	Procedură	x	x	x	Nu este cazul
Pagini web cu informații despre serviciile de asistență sau de soluționare a problemelor	x	x	*x*	Asistență	x	Nu este cazul	Nu este cazul	x

(*1) Dacă o pagină conține informații referitoare la mai multe tipuri de servicii sau acoperă mai multe domenii de informații, toate elementele relevante trebuie să fie incluse în pagina respectivă sau asociate acesteia.

11.8. ANEXA II la Regulamentul de punere în aplicare (UE) 2020/1121 al Comisiei din 29 iulie 2020

Cerințele tehnice menționate la articolul 3 alineatul (2) și la articolul 10 alineatul (2)

Transmiterea datelor

Un portal cu interfață de programare a aplicațiilor (API) va expune o interfață API cu stilul Representational State Transfer (REST). Sistemul de colectare al fiecărui furnizor de servicii poate apela acest API:

1. în timp real – nu există nicio limitare a numărului de apeluri;
2. în mod regulat, conform unui program ales de furnizorul de servicii.

Securitatea API

Comunicarea cu portalul API va fi asigurată prin intermediul unei chei API. Fiecare furnizor de servicii va avea o cheie API. Această cheie va permite securizarea comunicării (criptarea canalului) și cunoașterea furnizorului de servicii care trimite datele (autentificare).

Cheile API vor fi disponibile pe o aplicație web specială de tip back-office. Fiecare furnizor de servicii își va genera propria cheie pe aplicația web, o va descărca și o va instala la sediul său.

Cerințe care permit transmiterea datelor

În scopul asigurării transmiterii automate, instrumentul de analiză web menționat la articolul 3 alineatul (2) și instrumentul alternativ de formulare a observațiilor din partea utilizatorilor menționat la articolul 10 alineatul (2):

(a) permit transmiterea datelor în format JSON prin intermediul API REST;

(b) susțin conexiuni securizate cu protocolul Hyper-Text Transfer Protocol (HTTP) pe Secure Sockets Layer (SSL);

(c) susțin codul ISO 8601 pentru reprezentarea datei și a orei. Data și ora sunt exprimate în timp universal coordonat (UTC);

(d) susțin un identificator unic pentru transmisii. Un furnizor de servicii transmite datele cu ajutorul unui identificator unic oferit prin intermediul API. În cazul în care un furnizor de servicii decide să modifice aceste date, acesta trebuie să transmită o corecție cu același identificator unic.

Frecvența transmiterii statisticilor nu ar trebui să modifice structura fișierului JSON. De exemplu, JSON ar putea conține o serie de obiecte (câte unul pentru fiecare set de statistici pentru perioada de referință), o serie de lungimi n.

Comisia pune la dispoziție o descriere tehnică detaliată a API pentru observațiile din partea utilizatorilor și statistici despre utilizatori.

11.9. ANEXA III la Regulamentul de punere în aplicare (UE) 2020/1121 al Comisiei din 29 iulie 2020

Întrebări privind observațiile din partea utilizatorilor în cadrul instrumentului comun de formulare a observațiilor de către utilizatori menționat la articolul 6 alineatul (1) litera (a):

1. Întrebări referitoare la informațiile de pe paginile web

• Ați găsit ce ați căutat? (opțiuni care se exclud reciproc: DA/NU/PARȚIAL) *[câmp obligatoriu]* (*1)

• Apreciați pagina (număr de stele: de la 1 la 5) *[câmp obligatoriu]*

• Ajutați-ne să ne îmbunătățim (text liber) *[câmp opțional]*

2. Întrebări referitoare la proceduri

• Apreciați ușurința cu care ați utilizat această procedură (număr de stele de la 1 la 5) *[câmp obligatoriu]*

• Ajutați-ne să ne îmbunătățim (text liber) *[câmp opțional]*

3. Întrebări legate de serviciile de asistență și de soluționare a problemelor

• Apreciați serviciul furnizat (număr de stele de la 1 la 5) *[câmp obligatoriu]*

• Ajutați-ne să ne îmbunătățim (text liber) *[câmp opțional]*

Instrumentul de formulare a observațiilor din partea utilizatorilor pentru informații și proceduri va fi dezvoltat în două versiuni: una cu caseta de text liber și alta fără caseta de text liber, furnizorii de servicii având posibilitatea de a alege versiunea pe care să o utilizeze în conformitate cu articolul 6 alineatul (2).