GUVERNUL ROMÂNIEI

HOTĂRÂRE
privind aprobarea Notei de fundamentare referitoare la necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „Implementarea infrastructurii de cloud guvernamental”

În temeiul art. 108 din Constituția României, republicată și al art. 42, alin. (1), lit. a), din Legea nr. 500/2002, privind finanțele publice, cu modificările și completările ulterioare,

Guvernul României adoptă prezenta hotărâre.

Art. 1. Se aprobă Nota de fundamentare referitoare la necesitatea și oportunitatea efectuării cheltuielilor aferente proiectului de investiții „Implementarea infrastructurii de cloud guvernamental”, prevăzută în anexa care face parte integrantă din prezenta hotărâre.

Art. 2. Finanțarea proiectului de investiții prevăzut la art. 1 se realizează din Programul Național de Redresare și Reziliență (PNRR), în limita sumelor aprobate cu această destinație.

Art. 3. Autoritatea pentru Digitalizarea României (ADR), Serviciul de Telecomunicații Speciale (STS) și Serviciul Român de Informații (SRI) răspund de modul de implementare a proiectului de investiții prevăzut la art. 1, potrivit prevederilor prezentei hotărâri.

PRIM-MINISTRU
Nicolae-Ionel CIUCĂ

Anexa la H.G. nr. /

NOTĂ DE FUNDAMENTARE
referitoare la necesitatea și oportunitatea efectuării
cheltuielilor aferente proiectului de investiții „Implementarea infrastructurii de cloud guvernamental”

Scopul investiției

La 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 și cibernetică);
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 Cloudului Guvernamental, 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 în Cloud a aplicațiilor cartografiate.

Cloudul Guvernamental sau Platforma de Cloud Guvernamental, așa cum este definit în OUG 89/2022, este constituită dintr-o componentă de cloud privat, denumită în continuare Cloudul privat guvernamental și din resurse și servicii publice certificate din alte tipuri de cloud publice sau private.

Conform PNRR „în realizarea Cloudului Guvernamental se vor avea în vedere, în mod special, soluții de cloud hibrid utilizate în funcție de nivelurile de sensibilitate și durabilitate ale datelor și de modalitățile de utilizare și ale aplicațiilor și organizarea într-o structură de încredere concentrică pe trei niveluri care evoluează progresiv din interior către exterior.

Nivelul 1. Cloudul Intern capitalizează soluțiile existente în prezent cu niveluri scăzute de virtualizare prin transformarea lor în soluții informatice cloudificate IaaS și PaaS accesibile instituțiilor din administrația publică. În funcție de opțiunile individuale, autoritățile și instituțiile publice vor putea dezvolta și livra servicii SaaS. Acest tip de cloud asigură interoperabilitatea bazelor de date și funcționarea soluțiilor digitale bazate și pe consumul datelor sensibile, clasificate și catalogate corespunzător, răspunzând totodată exigențelor de control și securitate a informațiilor.

Nivelul 2. Cloudul Dedicat se bazează pe soluțiile de Cloud disponibile în sectorul industrial/comercial și va fi dezvoltat astfel încât să asigure funcționarea integrată cu Cloudul intern. Acesta va fi personalizat pentru a răspunde cerințelor specifice administrației publice și se va baza pe infrastructuri dedicate cu asigurarea interoperabilității și securității cibernetice. Acest tip de cloud va permite centralizarea și prelucrarea acelor aplicații și date care prezintă cel mai scăzut tip de sensibilitate, dar care necesită, în același timp un anumit nivel de durabilitate.

Nivelul 3. Cloudul Extern este constituit dintr-un catalog de soluții de Cloud externe,

generice, accesibile în Internet ca SaaS, ușor accesibile și intuitive pentru facilitarea utilizării. Acest tip de Cloud stimulează participarea unui număr crescut de furnizori de soluții informatice în ecosistemul digital.”

Cloudul Privat Guvernamental acoperă: Cloud Intern si Cloud Dedicat, ce vor fi instalate și operaționalizate în centrele de date și se interconectează la nivel de servicii și asigură hibriditatea prin interconectarea cu alte instanțe de cloud public sau privat care fac parte din Platforma Cloud Guvernamentală.

Situația actuală

Infrastructura IT existentă în prezent în cadrul instituțiilor care livrează servicii publice digitale este inadecvată, fragmentată, depășită din punct de vedere tehnologic, cu nivel redus de interconectare și grad scăzut de securitate cibernetică.

Prin implementarea investiției vor fi asigurate infrastructura, tehnologiile și operarea Cloudului Guvernamental pentru viitoarele aplicații ale instituțiilor publice în cloud prin furnizarea de servicii IaaS, PaaS și SaaS într-un mod unitar, standardizat, eficient și adaptat cerințelor utilizatorilor finali, firme și/sau cetățeni.

Operațional, Cloudul Guvernamental va funcționa cu asigurarea elasticității specifice tehnologiilor de cloud computing și, respectiv, a disponibilității ridicate prin implementarea a două Centre de Date Principale și două Centre de Date Secundare, de nivel Tier III/IV by design. Realizarea celor două Centre de Date Secundare, interoperabile cu cele două Centre de Date Principale, este necesară pentru asigurarea cerințelor tehnice și legale de business continuity și disaster recovery.

Centrele de Date vor funcționa cu consum energetic scăzut, asigurat de cele mai avansate soluții low power și răcire, cu respectarea parametrilor de eficiență energetică prevăzuți de documentul “2021 Best Practice Guidelines for the EU Code of Conduct on Data Center Energy Efficiency”.

De asemenea, vor fi implementate tehnologii verzi de tipul panourilor fotovoltaice pentru asigurarea unei părți a alimentării cu energie electrică.

Este necesară dotarea acestor Centre de Date cu instalații tehnice de electroalimentare, climatizare, securitate la incendiu, redundante, cu un regim de funcționare neîntreruptă, operate de personal specializat și înalt calificat care să asigure monitorizarea continuă 24/7 și intervenția promptă în cazul unor disfuncționalități.

Astfel, pentru implementarea și operarea Centrelor de Date este necesar ca resursa

umană să fie înalt calificată, conform standardelor în domeniu care să asigure administrarea continuă pe toată perioada de funcționare a Cloudului Guvernamental.

Următoarele aspecte importante sunt avute în vedere pentru realizarea, operarea și administrarea Cloudului Privat Guvernamental (CPG) la nivelul infrastructurii de bază pentru livrarea sigură a serviciilor în modele IaaS și PaaS:

a. existența unei resurse umane bine pregătite și cu experiență în implementarea și administrarea de infrastructuri complexe și performanțe IT&C, la nivel central și la nivel național;
b. existența la nivel național de infrastructură redundantă de comunicații de bandă largă;
c. asigurarea de servicii integrate de comunicații și securitate;
d. monitorizarea funcțională a tuturor parametrilor tehnici ai serviciilor la nivel fizic, prin centre specializate de tip NOC, 24/7;
e. asigurarea de servicii de tip CERT/CSIRT proactive și reactive, ce includ monitorizare de securitate, audit de securitate, răspuns la incidente de securitate;
f. asigurarea managementului integrat al securității cibernetice și al infrastructurii IT&C aferentă CPG;
g. asigurarea periodică a auditului extern la nivel operațional și al managementului accesului și protecției datelor cu caracter personal;
h. creșterea nivelului general de securitate cibernetică și siguranță a datelor în administrația publică centrală și locală prin consolidarea capacităţii de prevenţie şi rezilienţă la atacuri şi incidente cibernetice;
i. asigurarea de copii de rezervă pentru restaurarea infrastructurii de Cloud Guvernamental.

Facilitățile propuse pentru includerea în Cloudul Guvernamental și care necesită amenajare/îmbunătățire/dotare cu infrastructură și suport tehnic (alimentare cu energie electrică, aer condiționat și sisteme de securitate) și dotare cu infrastructură TIC, sunt cele care au fost special concepute cu scopul de a funcționa ca Centre de Date (de nivelul III și nivelul IV), aflându-se în prezent în diferite etape de implementare.

Entitățile implicate

Autoritatea pentru Digitalizarea României (ADR), în calitate de lider de parteneriat al prezentei investiții, este o instituție înființată prin HG 89/2020 pentru a realiza obiectivele ale Guvernului României în sfera transformării digitale a societății românești.

ADR exercită, în domeniul său de competență, următoarele funcţii:

a) de strategie, prin care planifică strategic şi asigură elaborarea şi implementarea politicilor în domeniul transformării digitale şi societăţii informaţionale;

b) de reglementare, prin care reglementează participarea la elaborarea cadrului normativ şi instituţional în domeniul transformării digitale şi societăţii informaţionale, inclusiv cu privire la interoperabilitatea sistemelor informatice ale instituţiilor publice;

c) de avizare;

d) de reprezentare, prin care asigură, în numele Guvernului, reprezentarea în organismele şi organizaţiile naţionale, regionale, europene şi internaţionale, ca autoritate de stat, pentru domeniul său de activitate, în conformitate cu cadrul normativ în vigoare;

e) de autoritate de stat, prin care se asigură urmărirea şi controlul respectării reglementărilor în domeniul său de competenţă;

f) de administrare şi gestiune;

g) de promovare, coordonare, monitorizare, control şi evaluare a realizării politicilor în domeniul său de competenţă, precum şi a cadrului naţional de interoperabilitate;

h) de comunicare, prin care se asigură comunicarea atât cu celelalte structuri ale sectorului public, cât şi cu sectorul privat şi societatea civilă;

i) de implementare şi gestionare a proiectelor finanţate din fonduri europene, precum şi a programelor şi proiectelor finanţate din fonduri naţionale şi alte surse legal constituite;

j) de organism intermediar, prin care se asigură implementarea măsurilor din Programul operaţional sectorial pentru „Creşterea competitivităţii economice” şi Programul operaţional „Competitivitate” în condiţiile acordului de delegare încheiat cu autoritatea de management conform art. 15 din Hotărârea Guvernului nr. 398/2015 pentru stabilirea cadrului instituţional de coordonare şi gestionare a fondurilor europene structurale şi de investiţii şi pentru asigurarea continuităţii cadrului instituţional de coordonare şi gestionare a instrumentelor structurale 2007—2013, cu modificările şi completările ulterioare, inclusiv cu privire la alte programe cu finanţare europeană.

În conformitate cu prevederile OUG 89/2022 privind „înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice”, ADR asigură:

- elaborarea și punerea în aplicare a planului pentru migrarea și integrarea în Cloudul privat guvernamental a sistemelor informatice și a serviciilor publice electronice ale autorităților și instituțiilor publice aparținând administrației publice.
- implementarea, administrarea tehnică și operațională, mentenanța, precum și

dezvoltarea ulterioară pentru serviciile SaaS specifice Cloudului privat guvernamental, inclusiv asigurarea, prin acorduri-cadru, conform legislației achizițiilor publice, a licențelor specifice serviciilor necesare migrării în Cloudul privat guvernamental a sistemelor informatice și serviciilor publice electronice.

- migrarea, integrarea și interconectarea în Cloudul privat guvernamental a sistemelor informatice ale autorităților și instituțiilor publice, pe baza acordului încheiat de ADR cu fiecare autoritate și instituție publică notificată de către ADR în vederea migrării
- asigură sau achiziționează programele software, aplicațiile informatice și licențele necesare, precum și serviciile de analiză, proiectare și dezvoltare software, după caz în scopul exercitării atribuțiilor.
- gestionează componenta de marketplace care permite accesarea de către entitățile găzduite de Platformă a aplicațiilor disponibile, pe baza unei relații contractuale stabilite între furnizorii și entitățile găzduite care achiziționează aplicațiile respective.
- asigură interconectarea la nivel de SaaS la serviciile specifice Cloudului privat guvernamental pentru entitățile găzduite și conectate în cloud.

Serviciul de Telecomunicații Speciale (STS), în calitate de partener al investiției este organul central de specialitate, cu personalitate juridică, ce organizează, conduce, desfăşoară, controlează şi coordonează activităţile în domeniul telecomunicaţiilor speciale pentru autorităţile publice din România şi pentru alţi utilizatori prevăzuţi în anexa 1 din Legea nr. 92/1996 *privind organizarea şi funcţionarea Serviciului de Telecomunicaţii Speciale*, cu modificările şi completările ulterioare.

Activitatea STS este organizată și coordonată de Consiliul Suprem de Apărare a Țării. Controlul asupra activității instituției se exercită de către Parlamentul României, prin comisiile pentru apărare, ordine publică și siguranță națională ale celor două Camere. Totodată, prin planul de măsuri stabilit în Strategia 5G pentru România, aprobată prin Hotărârea Guvernului României nr. 429/2019 *pentru aprobarea Strategiei 5G pentru România*, STS este desemnată instituția responsabilă privind lansarea serviciilor BB-PPDR (Broadband – Public Protection and Disaster Relief).

De asemenea, prin Ordonanța de urgență a Guvernului nr. 73/2020 *privind desemnarea Serviciului de Telecomunicații Speciale ca integrator de servicii de comunicații critice destinate autorităților publice cu atribuții în managementul situațiilor de urgen*ță, STS a fost desemnat Integrator de servicii de comunicații critice în vederea asigurării continuităţii comunicaţiilor destinate autorităţilor publice cu atribuţii în managementul

situaţiilor de urgenţă pentru asigurarea continuităţii actului de comandă şi control atât la nivel strategic cât și la nivelul echipajelor de intervenție, în vederea gestionării situaţiilor de urgenţă cu potenţial de afectare a securităţii naţionale.

Potrivit atribuţiilor stabilite prin Legea nr. 92/1996 *privind organizarea şi funcţionarea Serviciului de Telecomunicaţii Speciale*, cu modificările şi completările ulterioare, STS garantează protecţia şi confidenţialitatea serviciilor de comunicaţii şi tehnologia informaţiei furnizate conform legii.

STS administrează o infrastructură integrată multiservicii, la nivel naţional, în scopul furnizării de servicii de telecomunicaţii speciale şi tehnologia informaţiei, cu grad ridicat de rezilienţă, autorităţilor publice din România.

STS este responsabil şi garantează parametrii tehnici de performanţă, în vederea asigurării funcţionării, continuităţii şi securităţii serviciilor TIC.

În cadrul infrastructurilor și reţelelor permanente, temporare şi mobile sunt furnizate servicii integrate de comunicaţii şi tehnologia informaţiei de tip voce-date-video şi de securitate asociate acestora.

La nivelul STS, începând cu anul 2007, serviciile de securitate cibernetică sunt asigurate printr-o entitate de tip CERT/CSIRT, respectiv Centrul Operațional de Răspuns la Incidente de Securitate (CORIS-STS), acreditată la nivel internațional începând cu anul 2011. Aceasta este desemnată să prevină și să răspundă la incidente de securitate care afectează funcționarea sistemelor informatice și de comunicații ale Serviciului de Telecomunicații Speciale și ale beneficiarilor legali ai acestuia.

Activitatea specifică în domeniul securității cibernetice se concretizează în:

- îmbunătățirea rezistenței și abilității de a răspunde rapid și eficient în fața atacurilor cibernetice prin automatizarea mijloacelor de detecție, corelare și blocare a evenimentelor de securitate;
- identificarea în timp real a evenimentelor de securitate care afectează funcționarea sistemelor informatice și de comunicațiile STS și ale beneficiarilor legali ai acestuia;
- consolidarea infrastructurii și proceselor de securitate, înainte de producerea sau detectarea oricărui incident sau eveniment prin realizarea de audituri și evaluări de securitate asupra aplicațiilor, sistemelor informatice sau rețelelor de comunicații;
- implementarea configurațiilor specifice de securitate la nivelul infrastructurii de comunicații și a resurselor tehnice utilizate pentru furnizarea de servicii;

- asigurarea de servicii privind managementul calității securității IT prin consultanță de specialitate acordată beneficiarilor și prin organizarea de cursuri de pregătire a personalului instituției în domeniul securității cibernetice;
- dezvoltarea de relații de cooperare în domeniul securității cibernetice atât pe plan național, cât și internațional.

Totodată, STS are calitatea de furnizor de servicii de INTERNET (ISP) și servicii asociate precum DNS, e-mail și găzduire web. În calitatea sa de ISP, pentru asigurarea securității cibernetice a acestor servicii utilizate de către beneficiar, STS implementează măsuri specifice de securitate, inclusiv protecție împotriva atacurilor de tip DDOS.

În conformitate cu prevederile OUG 89/2022 *privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice*, STS asigură:

- Infrastructura de bază a Cloudului privat guvernamental;
- implementarea, administrarea tehnică și operațională, securitatea cibernetică, mentenanța, precum și dezvoltarea ulterioară a serviciilor specifice Cloudului privat guvernamental, privind infrastructura de baza și furnizarea modelelor IaaS și PaaS;
- accesul securizat, conectivitatea și interconectarea la serviciile specifice Cloudului privat guvernamental pentru entitățile găzduite sau interconectate în cloud;
- securitatea cibernetică a Cloudului privat guvernamental prin prevenirea și contracararea atacurilor cibernetice, pentru infrastructura de bază, furnizarea modelelor IaaS și PaaS, inclusiv a atacurilor de tip DDoS îndreptate împotriva Cloudului privat guvernamental, în conformitate cu atribuțiile prevăzute prin actele normative în vigoare;
- securitatea cibernetică a serviciilor și sistemelor informatice proprii din Cloudul privat guvernamental, prin prevenirea și contracararea atacurilor cibernetice;

Serviciul Român de Informaţii (SRI), în calitate de partener al investiției, este serviciul organizat de stat, specializat în domeniul informaţiilor referitoare la securitatea naţională a României, parte componentă a sistemului naţional de apărare, conform Legii 14/1992 *privind organizarea şi funcţionarea Serviciului Român de Informaţii.*

Activitatea SRI este organizată şi coordonată de Consiliul Suprem de Apărare a Ţării

(CSAT) și controlată de Parlament.

În anul 2008, SRI a fost desemnat autoritate națională în domeniul cyber intelligence de către CSAT, iar în anul 2013 a fost operaționalizat Centrul Național CYBERINT (CNC).

Prin calitatea sa de autoritate națională în domeniul cyber intelligence, SRI, prin CNC, pledează și acționează pentru cunoașterea, prevenirea şi contracararea vulnerabilităților, riscurilor şi amenințărilor la adresa securității cibernetice a României:

- cunoașterea – înțelegerea și anticiparea amenințărilor cibernetice la adresa sistemelor și rețelelor informatice, a căror afectare poate avea impact la adresa securității naționale;
- prevenirea – derularea de măsuri pentru prevenirea materializării unor riscuri la adresa securității naționale;
- contracararea - aplicarea de măsuri pentru eliminarea amenințării.

Principala misiune este prevenirea, limitarea și/ sau stoparea consecințelor unui atac cibernetic asupra sistemelor de tehnologia informaţiei şi comunicaţii (TIC) care reprezintă infrastructuri cu valențe critice pentru securitatea națională.

De asemenea, conform Strategiei de Securitate Cibernetică a României, SRI/ CNC are rolul de a informa Consiliul Operativ de Securitate Cibernetică (COSC) cu privire la apariția incidentelor cibernetice care pot aduce atingere securităţii naţionale şi este punct de contact pentru relaţionarea cu organismele similare din străinătate, în cazul afectării securităţii cibernetice a României.

Serviciul Român de Informaţii susține importanța demersurilor de dezvoltare a culturii de securitate a populaţiei prin conştientizarea vulnerabilităţilor, riscurilor şi ameninţărilor provenite din spaţiul cibernetic şi necesitatea asigurării protecţiei sistemelor informatice proprii.

Pentru asigurarea securității cibernetice a Cloudului Privat Guvernamental, Serviciul Român de Informații va instala soluții tehnice specializate, care nu permit vizualizarea și accesarea datelor de conținut existente la nivelul CPG. Soluțiile respective vor genera exclusiv alerte de securitate cibernetică, în scopul detectării și prevenirii materializării unor atacuri cibernetice.

Aceste echipamente vor fi achiziționate de la producători cu renume la nivel mondial, care dețin inclusiv experiență în ceea ce privește securizarea unor infrastructuri

similare din alte state. SRI nu va avea acces la datele de conținut stocate și vehiculate la nivelul acestuia, ci doar la alertele generate de echipamentele respective.

În conformitate cu prevederile OUG 89/2022 *privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice*, SRI, prin intermediul Centrului Național CYBERINT, îndeplinește în cadrul CPG următoarele:

- asigurarea securității cibernetice a Cloudului Privat Guvernamental, prin cunoașterea, prevenirea și contracararea atacurilor, amenințărilor, riscurilor și vulnerabilităților cibernetice, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor Cloudului Privat Guvernamental, la nivelul SaaS și a entităților găzduite;
- cooperează cu STS pentru cunoașterea, prevenirea și contracararea atacurilor cibernetice complexe, de tip APT, îndreptate împotriva serviciilor specifice Cloudului Privat Guvernamental la nivelul IaaS, respectiv PaaS, prin schimbul nemijlocit și automat al informațiilor referitoare la incidentele de securitate, fără a transfera date de conținut.

SRI are statut de autoritate publică, activitățile desfășurate respectând principiul legalității, regulă esențială care impune respectarea legii fundamentale și a celorlalte acte normative existente de către organele de stat, de toate persoanele juridice de drept public sau privat și de toți cetățenii.

Obiectivul general al investiției

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

Obiective specifice ale investiției

Atingerea obiectivului general va fi posibilă prin realizarea următoarelor obiective specifice:

a. Amenajarea și dotarea centrelor de date cu un nivel de reziliență caracteristic nivelului Tier III/IV by design;
b. Echiparea centrelor de date cu infrastructură și tehnologii cloud specifice IT&C (hardware și software);
c. Asigurarea comunicațiilor securizate folosind infrastructurile de comunicații de bandă largă operate de autoritatea publică abilitată la nivel

național;

d. Asigurarea unui nivel ridicat al securității cibernetice a CPG, prin implementarea de mecanisme care să asigure confidențialitatea, integritatea și disponibilitatea datelor entităților găzduite, precum și detectarea și prevenirea atacurilor cibernetice complexe de tip Advanced Persistent Threat (APT) la nivel IaaS/PaaS/SaaS;
e. Asigurarea implementării serviciilor de tip SaaS necesare administraţiei publice;
f. Implementare hub interconectare și realizarea portalului pentru cetățean;
g. Asigurarea securității cibernetice a Cloudului Privat Guvernamental prin cunoașterea, prevenirea și contracararea atacurilor, amenințărilor, riscurilor și vulnerabilităților cibernetice, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor Cloudului Privat Guvernamental.

Beneficiile investiției

Implementarea Cloudului Privat Guvernamental va facilita sporirea calității și securității serviciilor informatice și de comunicații la nivel național, precum și creșterea disponibilității și a nivelului de securitate a serviciilor oferite instituțiilor și entităților din administrația publică centrală și locală - ecosistemul digital guvernamental.

Reziliența economică este astfel asigurată de faptul că dezvoltarea Cloudului Guvernamental va duce la o creștere a gradului de digitalizare a serviciilor oferite de autoritățile / instituțiile publice din România.

Acest lucru va asigura următoarele beneficii:

- eficientizarea furnizării acestor servicii;
- reducerea costurilor necesare asigurării acestora;
- 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 din societate (de exemplu pandemia COVID-19, cutremure, inundații);
- protejarea confidențialității, integrității și disponibilității informațiilor în cadrul CPG;
- protejarea împotriva atacurilor avansate de tip APT, realizate de către actori cibernetici ce utilizează mecanisme de compromitere sofisticate, prin

intermediul cărora pot urmări, printre altele, identificarea și exfiltrarea de date sensibile din cadrul infrastructurilor afectate;
- securizarea serviciilor utilizate de instituțiile beneficiare, din punctul de vedere al securității cibernetice, prin folosirea unor soluții specializate pentru asigurarea securității sistemelor, aplicațiilor și serviciilor accesibile din internet și analiza comportamentală, folosind tehnologii bazate pe IA.

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

Toate aceste beneficii obținute prin dezvoltarea infrastructurii guvernamentale de Cloud vor contribui la reziliența economiei prin asigurarea eficienței și continuității serviciilor publice furnizate de autoritățile / instituțiile publice cetățenilor și mediului de afaceri.

Totodată, va fi asigurată compatibilitatea funcțională (cloud native, cloud ready) a Centrelor de Date din cadrul Cloudului pentru a asigura un grad ridicat de reziliență și scalabilitate în cazul unei situații de criză de lungă durată, de tipul pandemic.

Utilizarea facilităților special concepute pentru a funcționa ca Centre de Date asigură găzduirea infrastructurii TIC la standarde industriale ridicate.

Centrele de date vor fi dotate cu infrastructură TIC care să permită oferirea de servicii de tip IaaS, PaaS și SaaS.

Implementarea Cloudului Guvernamental va presupune cel puțin următoarele etape:
- amenajarea de centre de date Tier IV by design pentru cele două centre principale și Tier III by design pentru cele două centre secundare;
- furnizarea infrastructurii de comunicații şi tehnologia informației (cabluri de fibră optică şi echipamente de comunicații de mare capacitate) specifice;
- dezvoltarea/extinderea rețelei de alimentare cu energie electrică pentru fiecare centru de date în parte în vederea asigurării redundanței și a necesarului de energie electrică;
- realizarea unei infrastructuri de climatizare scalabile şi redundante, eficientă din punct de vedere energetic;
- instalarea sistemului de detecție şi stingere incendiu cu gaz inert care să asigure protecția pentru întreaga infrastructură a fiecărui Centru de Date în parte;
- implementarea sistemului de securitate fizică (control acces, monitorizare video, antiefracție etc.) pentru infrastructura dezvoltată;

- implementarea rețelei de monitorizare și management a infrastructurii în cadrul facilității realizate;
- realizarea infrastructurii IT&C scalabilă și de înaltă disponibilitate (echipamente de procesare, stocare, comunicații, software virtualizare) în cadrul fiecărui Centru de Date în parte;
- achiziţia de licenţe şi echipamente specializate pentru securitate cibernetică perimetrală;
- asigurarea securității cibernetice a CPG în toate etapele de dezvoltare și funcționare ale acestuia, prin raportare la confidențialitatea, integritatea și disponibilitatea datelor;
- achiziţionarea de licenţe şi echipamente cu grad ridicat de complexitate tehnică, cu scopul de a asigura un nivel ridicat de securitate cibernetică prin prevenirea inclusiv a atacurilor cibernetice de tip APT;
- implementarea unor mecanisme de protejare a datelor stocate sau în tranzit împotriva activităților de exfiltrare, respectiv de alterare a acestora;
- implementarea de mecanisme pentru detectarea și prevenirea atacurilor cibernetice, prin raportare la o abordare pe niveluri, conform conceptului Defence in Depth;
- implementarea de mecanisme pentru managementul identității și al accesului;
- implementarea tehnologiilor specifice asigurării securității cibernetice
- implementarea de tehnologii specifice (de exemplu: CSPM, CASB, CWPP).
- testare funcțională și de securitate

Securitatea perimetrală a infrastructurii de bază și a furnizării modelelor de servicii IaaS și PaaS va fi asigurată de administratorul infrastructurii de CPG.

Beneficii pentru cetățean

Principalele beneficii ale operaționalizării cloudului guvernamental pentru cetățeni sunt:

- One-stop shop – acces direct la toate serviciile publice, prin folosirea formularelor electronice disponibile în cloud;
- Statul român accesibil - toate instituțiile vor fi interconectate în cloud, iar cetățeanul va putea solicita și primi documente de oriunde, oricând;
- Economie de timp – fără cozi, fără nicio deplasare fizică la instituţiile publice;
- Trasabilitate – cetățeanul va putea avea un istoric al interacțiunilor sale cu administrația;
- Siguranță – cloudul guvernamental va beneficia de cele mai avansate sisteme de securitate cibernetică disponibile.

Beneficii pentru autoritățile și instituțiile publice

Prin această investiție se va asigura o protecție de nivel ridicat și va contribui la creșterea capabilităților și calității serviciilor și securității cibernetice pentru întreaga platformă IT&C aparținând administrației publice, într-un mod unitar și standardizat.

Cloudul va aduce beneficii concrete și pentru activitatea administrativă:

- va asigura interoperabilitatea sistemelor publice;
- va reduce birocrația, prin eliminarea proceselor administrative redundante sau perimate;
- va asigura o mai bună colaborare şi o partajare rapidă a informaţiilor între toate instituţiile guvernamentale;
- va eficientiza costurile – instituțiile publice nu vor mai fi nevoite să asigure mentenanța pentru echipamentele hardware și software.
- creșterea eficienței aparatului administrativ va determina scăderea costurilor aferente unor sisteme informatice disparate şi astfel va duce la creșterea încrederii antreprenorilor în performanța statului și va genera creștere economică.
- protejarea integrată a datelor, aplicațiilor și rețelelor;
- gestionarea în mod securizat a accesului la servicii și resurse;
- diminuarea riscului de infectare cu malware, prin utilizarea de mecanisme de protecție
- prevenirea atacurilor prin identificarea breșelor de securitate înainte de a fi exploatate sau combaterea acestora din fazele incipiente;
- asigurarea managementului vulnerabilităților și aplicarea de patch-uri în vederea remedierii acestora;
- protejarea împotriva atacurilor care au ca scop limitarea serviciilor (Distributed Denial-of-Service - DDoS);
- automatizarea proceselor, notificărilor și a reacțiilor;
- minimizarea timpului de reacție în cazul atacurilor cibernetice;
- reducerea plajei de atacuri cibernetice care pot fi derulate împotriva rețelelor și sistemelor informatice ale acestora de către actori statali sau cu motivație financiară;

Grupul țintă al investiției îl reprezintă administrația publică centrală și locală, ecosistemul digital guvernamental.

Indicatorii de realizare ai investiției sunt:

DENUMIRE INDICATOR	**Unitate măsură**	Valoare la începutul implementării investiției	Valoare la finalul implementării investiției	Termen realizare
Instituții publice conectate și care utilizează pe deplin Cloudul Guvernamental, în conformitate cu dispozițiile prevăzute în CID	număr	**0**	**30**	**T4 2024**
Centre* de date Tier III (2) și 1 centru de date Tier IV de la momentul conceperii, hardware și software de Cloud (infrastructură ca serviciu - IaaS/platformă ca serviciu - PaaS/software ca serviciu - SaaS) funcționale, în conformitate cu dispozițiile prevăzute în CID	număr	**0**	**3**	**T4 2024**
Centre* de date Tier IV de la momentul conceperii, hardware și software de Cloud (infrastructură ca serviciu - IaaS/platformă ca serviciu - PaaS/software ca serviciu - SaaS) funcționale, în conformitate cu dispozițiile prevăzute în CID	număr	**0**	**1**	**T4 2025**

Caracteristicile principale ale investiției „Implementarea infrastructurii de cloud

guvernamental” sunt:

- Pe parcursul implementării componentei de Cloud Privat Guvernamental (CPG) se va avea în vedere neutralitatea tehnologică prin utilizarea unor echipamente și produse software complementare, de la producători diverși;
- Asigurarea rezilienței tehnologice a CPG prin implementarea unor soluții care să asigure adoptarea facilă și rapidă a noilor dezvoltări/inovări tehnologice în domeniu dar și pentru evitarea materializării conceptului de single-point-of-failure, inclusiv prin adoptarea unor soluții full stack;
- Se vor utiliza arhitecturi de procesare deschise de tip x86, x64 și/sau ARM;
- Implementarea unor servicii platformă care încurajează dezvoltarea aplicațiilor în tehnologii cloud native pentru a folosi la maxim beneficiile unei arhitecturi de cloud computing;
- Furnizarea capabilităților de reziliență prin facilități de redundanță geografică care implică utilizarea unor centre de date de nivel minim Tier 3, plasate în locații de pe cuprinsul țării;
- Serviciile aferente infrastructurii de bază să fie disponibile on premise pentru asigurarea independenței de factori externi, pentru a putea furniza în orice moment servicii în modelele IaaS, PaaS, SaaS;
- Complementar cu principiul anterior, se va avea în vedere capabilitatea de a funcționa în mod independent de alte infrastructuri de cloud pe o perioadă nedeterminată de timp, cu permiterea schimbului de date telemetrice în vederea asigurării funcționării resurselor;
- Transparența costurilor operaționale vor fi avute în vedere pentru toată perioada de utilizare a infrastructurii;
- Consultarea actorilor implicați în implementarea Platformei de Cloud Guvernamental;
- Elasticitate și scalabilitate pe orizontală;
- Implementarea principiului Do No Significant Harm (DNSH);
- Infrastructura de bază este administrată exclusiv de către personalul tehnic al Serviciului de Telecomunicații Speciale.
- Asigurarea unui nivel ridicat de securitate cibernetică a CPG prin implementarea și integrarea unor soluții tehnice specifice și definirea unor politici de securitate unitare
- securitatea cibernetică a CPG va fi implementată în conformitate cu cele mai bune practici în domeniu

Titular: Autoritatea pentru Digitalizarea României, Serviciul pentru Telecomunicații Speciale, Serviciul Român de Informații

Beneficiarii investiției: Autoritatea pentru Digitalizarea României, Serviciul pentru Telecomunicații Speciale, Serviciul Român de Informații.

Finalizarea implementării investiției: 31 decembrie 2025

Perioada de operare a investiției este de 10 ani de la data finalizării implementării investiției.

Finanțarea investiției: Valoarea totală a investiției este de 374.730.000 euro - finanțare PNRR, respectiv 1.866.155.400 lei (la cursul de schimb mediu pentru anul 2022, respectiv 1 euro=4,98 lei) din care:

Valoarea totală a investiției ADR este de 398.400.000,00 lei fără TVA

Valoarea totală a investiției STS este de 1.268.555.400,00 lei fără TVA

Valoarea totală a investiției SRI este de 199.200.000,00 lei fără TVA

Eșalonarea cheltuielilor		
- Anul I (2023)	mii lei	674.630,00
- Anul II (2024)	mii lei	779.300,00
- Anul III (2025)	mii lei	412.225,40