GUVERNUL ROMÂNIEI

ORDONANȚĂ DE URGENȚĂ

privind unele măsuri pentru sistemul de guvernanță al Cloud-ului Guvernamental precum si pentru stabilirea cadrului legal de organizare și funcționare a infrastructurilor informatice și a serviciilor de tip cloud în procesul de transformare digitală

Având în vedere faptul că tehnologia de Cloud Guvernamental este din ce în ce mai larg adoptată de către autoritățile publice din statele membre ale Uniunii Europene, ca urmare a avantajelor tehnice și economice care privesc procesarea și stocarea datelor, precum și disponibilitatea serviciilor, avantaje care au ca rezultat generarea de economii consistente sub aspectul investițiilor și al cheltuielilor operaționale,

Ținând cont de faptul că implementarea proiectului de Cloud Guvernamental este o prioritate asumată de către Guvernul României în Programul de guvernare și în actualul context național și internațional, determinat de pandemia COVID-19, realizarea acestui obiectiv a devenit stringentă, având în vedere că schimbul de date în format electronic în sectorul public este absolut necesar,

Având în vedere că, în jalonul nr. 153 din Planul Național de Redresare și Reziliență se specifică faptul că implementarea infrastructurii de cloud guvernamental cuprinde construcția a patru centre de date de tip Tier III și Tier IV, infrastructuri specifice găzduirii de sisteme informatice on-premise iar de construirea urgentă a acestora depinde transferul la timp a finanțării de către Comisia Europeană,

Având în vedere că realizarea obiectivului menționat anterior presupune, printre altele, asigurarea unui management unitar și eficient privind gestionarea centralizată a resurselor IT&C, fapt ce impune adoptarea cu celeritate a unor măsuri atât la nivel legislativ, cât și la nivelul gestionării resurselor în condiții de securitate sporită, scalabilitate, flexibilitate și adaptabilitate,

Deoarece Cloud-ul Guvernamental reprezintă un obiectiv imediat și urgent în considerarea faptului că implementarea sa asigură utilizarea forței de muncă într-un mod mai eficient, ca urmare a administrării suportului tehnic și asigurării mentenanței sistemelor în mod centralizat, fapt ce generează automatizarea pentru managementul elementelor software de la sistemul de operare până la nivel de aplicații,

Având în vedere situația extraordinară de creștere a volumului informațiilor din bazele de date critice administrate de statul român și necesitatea consolidării și interconectării acestora, precum și necesitatea asigurării în mod unitar a securității cibernetice a acestora,

Luând în considerare faptul că una dintre direcțiile de acțiune pentru asigurarea securității naționale prevăzute în Strategia Națională de Apărare a Țării pentru perioada 2020-2024, aprobată prin Hotărârea Parlamentului României nr. 22/2020, este reprezentată de realizarea infrastructurii necesare pentru digitalizarea României, cu scopul eficientizării aparatului administrativ și al creșterii calității serviciilor publice, pentru transpunerea în realitate a acestei direcții de acțiune fiind necesară implementarea proiectului de Cloud Guvernamental,

De asemenea, avand în vedere faptul ca transformarea digitală este un obiectiv de interes strategic național care cuprinde atât procesul de transformare digitală la nivelul serviciilor publice din România cât și la nivelul mediul de afaceri, în ecosistemul mediului de afaceri transformarea digitală se referă atât la procesele care guvernează activitatea curentă a companiilor dar mai ales la mecanismele de automatizare a proceselor de producție și robotizarea acestora cu impact asupra competitivității și calității produselor pe piața europeană,

Deoarece România are alocate fonduri prin Planul Național de Redresare și Reziliență (PNRR) pentru componenta de transformare digitală în valoare de 1,8 mld euro care în cea mai mare parte vizează digitalizarea marilor servicii publice, dar și investiții în digitalizarea mediului de afaceri iar pentru utilizarea eficientă a fondurilor publice în ceea ce privește cheltuielile cu mentenanța și infrastructura și echipamentele IT este necesar ca autoritățile și entitățile publice,

altele decât cele ale căror baze de date vor migra în Cloud-ul Guvernamental, să aibă alternativa stocării sistemelor informatice în infrastructuri de tip cloud gestionate de furnizorii de servicii de tip cloud,

Întrucât în lipsa unor reglementări specifice, imediate și efective ale pieței serviciilor de tip cloud se pot genera riscuri de securitate cibernetică a sistemelor informatice dar și riscuri de utilizare a informațiilor specifice de date de către utilizatori neautorizați iar prin aceasta se pot crea prejudicii proprietarilor de date persoane fizice și/sau juridice cu impact asupra fondurilor externe nerambursabile accesate de România atât prin mecanismul de redresare și reziliență cât și prin politica de coeziune,

Deoarece mediul de afaceri are nevoie de mecanisme de transformare digitală rapide și specifice care să-i permită să dezvolte platforme informatice în acord cu nevoile de automatizare și robotizare specifice pieței concurențiale europene pentru a gestiona eficient cheltuielile cu mentenanța dar și cu cele specifice echipamentelor IT,

Având în vedere contextul platformei de cloud care vizează modul în care vor fi implementate platformele informatice de cloud precum și modelul arhitectural pentru dezvoltarea unei infrastructuri de cloud adaptată la tehnologiile informaționale specifice și vizează aspecte precum platforme multicloud, hypercloud, cloud-ul hybrid, medii cloud publice și private, dar și interconectivitate, interoperabilitatea cu infrastructura existentă și cu centrele de date existente în ţară iar pentru aceasta este necesară stabilirea unei infrastructuri digitale coerente și integrată la nivelul administrației publice bazată pe modulul de guvernanță a datelor și a obiectivelor economice care să ofere servicii digitale de înaltă calitate care să satisfacă nevoia de acces deschis – cloud public cât și acces restricționat utilizând o formă de cloud privat,

În considerarea tuturor aspectelor menționate mai sus, dar și a faptului că implementarea Cloud-ului Guvernamental, astfel încât acesta să fie funcțional, necesită parcurgerea unor etape procedurale a căror desfășurare presupune o anumită perioadă de timp, iar orice întârziere în adoptarea de măsuri urgențe în acest sens ar crește substanțial riscul de dezangajare a fondurilor europene nerambursabile disponibile în acest moment pentru implementarea Cloud-ului Guvernamental, cu implicații negative asupra fondurilor naționale, reglementarea în regim de

urgență a cadrului legal necesar demarării etapelor pentru implementarea acestui proiect este cu atât mai justificată,

În conformitate cu Strategia Europeană pentru Cloud Computing, precum și aspectele prezentate anterior, se impune intervenția de urgență la nivel legislativ în vederea stabilirii cadrului normativ necesar realizării unei infrastructuri hibride pentru serviciile de Cloud Computing Guvernamental, si pentru stabilirea cadrului legal de organizare și funcționare a infrastructurilor informatice și a serviciilor de tip cloud în procesul de transformare digitală

În considerarea faptului că toate aceste elemente vizează un interes public, constituie o urgență și o situație extraordinară, a cărei reglementare nu poate fi amânată şi impune adoptarea de măsuri imediate pe calea ordonanţei de urgenţă

În temeiul art. 115 alin. (4) din Constituția României, republicată

Guvernul României adoptă prezenta ordonanță de urgență

Capitolul I
Dispoziții generale

Art. 1 -

(1) Prezenta ordonanță de urgență reglementează regimul juridic general privind înființarea, administrarea și dezvoltarea, la nivel național, a unei infrastructuri de tip cloud hibrid, denumită Cloud Guvernamental, care include o componentă de cloud privat, implementată și administrată de statul român, constând într-un ansamblu de resurse de tehnologia informației, comunicații și securitate cibernetică, interconectată la nivel de servicii cu cloud-uri publice sau private, utilizată în comun de entitățile găzduite, reprezentate de autoritățile și instituțiile publice centrale, precum și de structurile aflate în coordonarea, subordonarea sau sub autoritatea acestora.

(2) Instituțiile responsabile de realizarea Cloud-ului Guvernamental sunt Ministerul Cercetării, Inovării și Digitalizării, denumit în continuare MCID, și Autoritatea pentru Digitalizarea României, denumită în continuare ADR, în colaborare cu Serviciul de Telecomunicații

Speciale, denumit în continuare STS și Serviciul Român de Informații, denumit în continuare SRI, conform competențelor stabilite de prezenta ordonanță de urgență.

(3) Începând cu data intrării în vigoare a actului normativ prevăzut la art. 3 alin. (1) din prezenta ordonanță de urgență, sistemele informatice utilizate de către autoritățile și instituțiile publice centrale sunt dezvoltate astfel încât să fie pregătite pentru migrarea în Cloud-ul Guvernamental.

(4) Autoritățile administrației publice centrale au obligația de a migra serviciile publice electronice în Cloud-ul Guvernamental.

(5) Autoritățile administrației publice centrale pot migra în Cloud-ul Guvernamental, în limita resurselor disponibile ale Cloud-ului, serviciile informatice utilizate în activitatea internă.

(6) Nivelurile agreate ale serviciilor specifice Cloud-ului Guvernamental se stabilesc prin ordin comun al ministrului MCID, președintelui ADR, directorului STS și al directorului SRI, cu respectarea cerințelor prevăzute în actul normativ prevăzut la art. 3 alin. (1).

(7) Activitățile de informare publică, cu privire la acțiunile care vizează Cloud-ul Guvernamental se realizează de către MCID, după consultarea ADR, STS și SRI, dacă sunt vizate activitățile din responsabilitatea acestora.

(8) Prezenta ordonanță de urgență nu se aplică sistemelor informatice ale autorităților publice din domeniul apărării, ordinii publice și securității naționale, și nici celor ale autorităților publice prevăzute în Constituție în Titlul III, Capitolele I, II și VI, cu excepția celor care furnizează servicii publice electronice stabilite prin hotărâre a Guvernului.

Art. 2 -

În înțelesul prezentei ordonanțe de urgență, următorii termeni se definesc astfel:

a) Advanced Persistent Threat (APT) - concept utilizat pentru a defini un atac cibernetic derulat de o entitate statală sau grupare ostilă, ce vizează ținte strategice (din domeniul guvernamental, militar, al securității naționale și/sau al afacerilor), care, prin intermediul tehnicilor, tacticilor și procedurilor de nivel ridicat, reușește să fie nedetectabil o perioadă lungă de timp cu scopul de a extrage date pentru a obține avantaje strategice sau financiare;

b) amenințare cibernetică - orice act care ar putea cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane sau care poate avea un alt fel de impact negativ asupra acestora;

c) atac cibernetic - acţiune ostilă desfăşurată în spaţiul cibernetic de natură să afecteze securitatea informației și a sistemelor informatice și de comunicații care efectuează procesarea acesteia;
d) cloud first - principiu care implică luarea în considerare a cloud-ului înaintea tuturor celorlalte tehnologii, fie că este un proiect nou care implică soluții TIC sau o actualizare tehnologică a unui sistem informatic;
e) cloud guvernamental - ansamblu de resurse și servicii de tehnologia informației, comunicații și securitate cibernetică, utilizate în comun de entitățile găzduite, reprezentate de autoritățile și instituțiile publice centrale, precum și de structurile aflate în coordonarea, subordonarea sau sub autoritatea acestora;
f) cloud hibrid - modalitate de organizare a resurselor unui sistem de cloud computing care utilizează cel puțin două tipuri diferite de cloud computing;
g) date - orice reprezentare digitală a unor acte, fapte sau informații și orice compilație a unor astfel de acte, fapte sau informații, inclusiv sub forma unei înregistrări audio, video sau audiovizuale;
h) date primare – date prezumate ca fiind sursa cea mai credibilă și veridică de informație și care primează în fața celorlalte date colectate de orice altă instituție sau autoritate publică;
i) Distributed Denial of Service (DDoS) - atac cibernetic, din surse multiple, prin care se urmăreşte indisponibilizarea, blocarea sau epuizarea resurselor unui sistem informatic, reţea sau componentă a acesteia;
j) ghid de Guvernanță Cloud – standarde cloud care prevăd, pentru utilizare comună și repetată, reguli, orientări sau caracteristici pentru activități sau rezultatele acestora, care vizează atingerea gradului optim de ordine într-un anumit context, precum și reguli și obligații care sunt obligatorii de respectat în relația dintre furnizorul și utilizatorul de servicii publice;
k) infrastructura de bază a Cloud-ului Guvernamental - clădirile, instalațiile, dotările și echipamentele tehnologice aferente, echipamentele de tehnologia informației și comunicațiilor, inclusiv echipamentele necesare asigurării securității cibernetice, care funcționează în configurații de înaltă disponibilitate, precum și programele software, aplicațiile informatice și licențele asociate acestora;

l) infrastructura ca serviciu (IaaS) - model de punere la dispoziția utilizatorilor, la cererea acestora, pe baza unor drepturi de acces și în limita capacităților disponibile în cloud, într-un mod securizat, a resurselor din infrastructura de bază a Cloud-ului;

m) migrare în cloud - metodologia, procedura și acțiunile necesar a fi realizate pentru transferul unui sistem informatic în cloud sau pentru reproiectarea tehnologică în cazul sistemelor informatice perimate, fără a altera funcționalitățile existente ale sistemului informatic în cauză;

n) nivel agreat al serviciilor - set de parametri și indicatori specifici, în baza cărora este determinată disponibilitatea, performanța și calitatea serviciilor oferite;

o) platforma ca serviciu (PaaS) - model de punere la dispoziția utilizatorilor, la cererea acestora, pe baza unor drepturi de acces și în limita resurselor disponibile în cloud, a unor instrumente de dezvoltare, integrare, management, analiză, securitate și de suport pentru aplicațiile software și datele asociate acestora;

p) risc de securitate cibernetică - probabilitatea ca o amenințare să se materializeze, exploatând o vulnerabilitate specifică reţelelor şi sistemelor informatice;

q) securitatea cibernetică – stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și non-repudierea informațiilor în format electronic a resurselor și serviciilor publice sau private din spațiul cibernetic al Cloud-ului Guvernamental;

r) sistem informatic pregătit pentru migrare în Cloud - sistem informatic a cărui arhitectură și tehnologii folosite pentru realizarea sa permit migrarea și funcționarea în cloud;

s) software ca serviciu (SaaS) - model de punere la dispoziția utilizatorilor, la cererea acestora, a funcționalităților de utilizare a aplicațiilor furnizorului, care rulează pe o infrastructură cloud computing. Aplicațiile sunt accesibile pe baza unor drepturi de acces, prin diferite dispozitive de tip client, fie prin intermediul unei interfețe de tip thin-client precum browser web, fie prin intermediul unei aplicații software dedicate;

t) serviciu public electronic – serviciu public, astfel cum este definit de art. 5 lit. kk) din Ordonanța de urgență a Guvernului nr. 57/2019 privind Codul Administrativ, cu modificările și completările ulterioare, de tip e-guvernare, soluții oferite de tehnologia informației;

u) vulnerabilitate în spaţiul cibernetic - slăbiciune în proiectarea şi implementarea reţelelor şi sistemelor informatice sau a măsurilor de securitate aferente, care poate fi exploatată de către o ameninţare.

Capitolul II

Atribuții și responsabilități privind realizarea și operarea Cloud-ului Guvernamental

Art. 3 -

(1) Criteriile tehnice și operaționale privind implementarea, operarea, mentenanța și dezvoltarea ulterioară a Cloud-ului Guvernamental, regulile privind stabilirea nivelului agreat de servicii, precum și cele privind migrarea sistemelor informatice se stabilesc prin hotărâre de guvern, la propunerea MCID împreună cu ADR, STS și SRI.

(2) Cadrul de management și stocare a datelor în Cloud-ul Guvernamental sau în alte cloud-uri publice sau private, ținând cont de nivelul de senzitivitate al datelor, precum și mecanismul de achiziție a resurselor și serviciilor din cloud, se stabilesc prin hotărâre de Guvern, la propunerea MCID.

(3) Politicile și strategia privind implementarea, operarea, utilizarea, mentenanța și dezvoltarea ulterioară a Cloud-ului Guvernamental, inclusiv cele referitoare la Cloud First, sunt aprobate prin hotărâre de guvern, la propunerea MCID, împreună cu ADR.

(4) În îndeplinirea rolului prevăzut la art. 1 alin. (3), MCID are următoarele atribuții:

a) reprezintă interesele statului român în relațiile externe privind serviciile de Cloud Guvernamental;

b) stabilește serviciile care vor fi furnizate de Cloud-ul Guvernamental și le promovează în mod corespunzător;

c) stabilește categoriile tematice de seturi de date care vor fi prelucrate prin serviciile prevăzute la lit. b);

d) răspunde împreună cu entitățile găzduite în Cloud-ul Guvernamental de procesul de management al riscurilor pe baza analizelor de risc furnizate de către ADR, STS și SRI.

Art. 4 -

(1) ADR stabilește și urmărește punerea în aplicare a strategiei privind implementarea, operarea, mentenanța și dezvoltarea ulterioară a Cloud-ului Guvernamental, inclusiv migrarea și integrarea în Cloud-ul Guvernamental a sistemelor informatice și a serviciilor publice electronice ale instituțiilor și autorităților aparținând administrației publice.

(2) ADR asigură implementarea, administrarea tehnică și operațională, mentenanța, precum și dezvoltarea ulterioară pentru serviciile SaaS specifice Cloud-ului Guvernamental, inclusiv asigurarea, prin acorduri-cadru, conform legislației achizițiilor publice, a licențelor specifice serviciilor necesare migrării în Cloud-ul Guvernamental a sistemelor informatice și serviciilor publice electronice.

(3) Migrarea și integrarea în Cloud-ul Guvernamental a sistemelor informatice ale autorităților și instituțiilor publice, precum și cele ale structurilor aflate în coordonarea, subordonarea sau sub autoritatea acestora, se asigură de către ADR.

(4) În vederea îndeplinirii prevederilor alin. (1)-(3), ADR asigură programele software, aplicațiile informatice și licențele necesare, precum și serviciile de analiză, proiectare și dezvoltare software, după caz.

(5) Finanțarea cheltuielilor pentru activitățile prevăzute la prezentul articol se asigură prin Planul Național de Redresare și Reziliență, denumit în continuare PNRR, și de la bugetul de stat sau din alte surse de finanțare, prin bugetul ADR și al altor entități găzduite în Cloud-ul Guvernamental.

Art. 5 -

(1) Infrastructura de bază a Cloud-ului Guvernamental este asigurată de STS.

(2) STS asigură implementarea, administrarea tehnică și operațională, securitatea cibernetică, mentenanța, precum și dezvoltarea ulterioară a serviciilor specifice Cloud-ului Guvernamental, prevăzute la art. 2 lit. k), l) și o).

(3) STS asigură accesul securizat și conectivitatea la serviciile specifice Cloud-ului Guvernamental pentru entitățile găzduite.

(4) STS asigură securitatea cibernetică a Cloud-ului Guvernamental prin prevenirea și contracararea atacurilor cibernetice, pentru serviciile prevăzute la art. 2 lit. k), l) și o),

inclusiv a atacurilor de tip DDoS îndreptate împotriva Cloud-ului Guvernamental, în conformitate cu atribuțiile stabilite prin actele normative în vigoare.

(5) STS asigură securitatea cibernetică a serviciilor și sistemelor informatice proprii din Cloud-ul Guvernamental, prin prevenirea și contracararea atacurilor cibernetice.

(6) Pentru îndeplinirea rolului prevăzut la alin. (1), STS achiziționează serviciile de proiectare și asistență tehnică, lucrările de investiții, inclusiv instalațiile, dotările și echipamentele tehnologice aferente clădirii, precum și echipamentele hardware, programele software, aplicațiile informatice și licențele necesare realizării, dezvoltării ulterioare, mentenanței și funcționării serviciilor prevăzute la art. 2 lit. k), l) și o) din Cloud-ul Guvernamental.

Art. 6 -

(1) SRI asigură securitatea cibernetică a Cloud-ului Guvernamental prin cunoașterea, prevenirea și contracararea atacurilor, amenințărilor, riscurilor și vulnerabilităților cibernetice, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor specifice Cloud-ului Guvernamental menționate la art. 2 lit. s) și a entităților găzduite.

(2) SRI cooperează cu STS, conform competențelor fiecărei instituții, pentru cunoașterea, prevenirea și contracararea atacurilor cibernetice complexe, de tip APT, îndreptate împotriva serviciilor specifice Cloud-ului Guvernamental menționate la art. 2 lit. l) și o), prin schimbul nemijlocit și automat al tuturor evenimentelor de securitate, fără a schimba date de conținut.

(3) Măsurile prevăzute la alin. (1) și (2) nu se aplică situațiilor prevăzute la art. 5 alin. (5).

(4) SRI asigură implementarea, administrarea tehnică și operațională, mentenanța, precum și dezvoltarea ulterioară a serviciilor de securitate cibernetică ale Cloud-ului Guvernamental, prevăzute la alin. (1).

Art. 7 -

(1) În cazul sistemelor informatice interconectate cu Cloud-ul Guvernamental care aparțin sistemului național de apărare, ordine publică și securitate națională, securitatea cibernetică este asigurată și gestionată de STS și SRI, în colaborare cu autoritățile și instituțiile din acest sistem.

(2) În vederea îndeplinirii atribuțiilor prevăzute la art. 5-7, STS și SRI asigură echipamentele hardware, programele software, aplicațiile informatice și licențele necesare în acest scop, conform competențelor stabilite prin prezenta ordonanță.
(3) Finanțarea cheltuielilor pentru activitățile prevăzute de art. 5-7 se asigură prin PNRR și de la bugetul de stat, potrivit legii, prin bugetele STS și SRI.

Art. 8 -

(1) Entitățile publice ale căror aplicații și sisteme informatice urmează să migreze în Cloud-ul Guvernamental se stabilesc prin hotărâre de guvern, la propunerea Comitetului de E-guvernare.
(2) Entitățile publice își migrează aplicațiile și sistemele informatice în Cloud-ul guvernamental în baza unei Politici de Cloud First și a Cadrului de Management al Datelor.

Art. 9 -

(1) În procesul de dezvoltare, implementare, administrare și asigurarea securității cibernetice a Cloud-ului Guvernamental, instituțiile publice menționate la art. 1 alin. (2), prelucrează date cu caracter personal, în calitate de operatori asociați, în conformitate cu responsabilitățile prevăzute la art. 3 – 7 din prezenta ordonanță de urgență, cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal.
(2) Prelucrarea datelor cu caracter personal în procesul de utilizare și furnizare a serviciilor publice prin intermediul Cloud-ului Guvernamental se realizează de către entitățile găzduite, cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal.
(3) Modul și perioada de stocare a datelor cu caracter personal în Cloud-ul Guvernamental, modul de realizare a accesului la aceste date, precum și modul de punere în aplicare a prevederilor art. 12-20 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 raport cu utilizarea și furnizarea serviciilor publice prin intermediul Cloud-ului Guvernamental, se stabilesc prin hotărârea de Guvern menționată la art. 3 alin. (1).

Art. 10 -

(1) Infrastructura de bază a Cloud-ului Guvernamental, infrastructura ca serviciu (IaaS) și platforma ca serviciu (PaaS), prevăzute la art. 2. lit. k), l) și o) sunt proprietate a statului și în administrarea STS, care le achiziționează conform prevederilor legale în vigoare privind achizițiile publice.

(2) Softul dezvoltat și particularizat pentru entitățile găzduite sau care urmează a fi găzduite în Cloud, achiziționat conform prevederilor legale în vigoare privind achizițiile publice, este proprietatea publică a statului și în administrarea ADR, în condițiile art. 12 din Ordonanța de urgență a Guvernului nr. 41/2016 privind stabilirea unor măsuri de simplificare la nivelul administraţiei publice centrale şi pentru modificarea şi completarea unor acte normative, publicată în Monitorul Oficial, Partea I nr. 490 din 30 iunie 2016.

(3) Softul aferent migrării în Cloud a soluțiilor informatice și software ca serviciu (SaaS), prevăzute la art 2. lit. o) și s) sunt proprietate publică a statului și în administrarea ADR care le achiziționează conform prevederilor legale în vigoare privind achizițiile publice.

(4) Componentele aferente securității cibernetice sunt proprietate publică a statului și în administrarea STS și SRI care le achiziționează conform competențelor stabilite la art. 5 și 6 din prezenta ordonanță de urgență.

(5) Administratorii serviciilor furnizate la nivel IaaS, PaaS și SaaS, precum și administratorii de securitate cibernetică asigură jurnalizarea evenimentelor și accesului la datele entităților găzduite în Cloud-ul Guvernamental, în scopul realizării de audituri de conformitate periodice pe linia calității, securității și trasabilității datelor, în vederea asigurării transparenței utilizării acestora.

(6) MCID poate dispune efectuarea unor activități de audit de conformitate pe linia calității, securității și trasabilității pentru Cloud-ul Guvernamental în ansamblu sau, după caz, pentru anumite componente ale acestuia, finanțate prin bugetul acestuia.

(7) Entitățile găzduite în Cloud-ul Guvernamental pot solicita activități de audit de conformitate pe linia calității, securității și trasabilității pentru datele proprii, finanțate prin bugetul acestora.

(8) Activitățile de audit prevăzute la alin. (5) sunt realizate anual sau ori de câte ori este nevoie de entități externe, iar activitățile de audit prevăzute la alin. (6) sunt realizate ori de câte ori este nevoie, potrivit solicitării entităților găzduite. Rapoartele de audit se comunică

comisiilor parlamentare pentru tehnologia informației și comunicațiilor din Camera Deputaților și Senat.

(9) Normele metodologice de jurnalizare a evenimentelor și accesului la datele entităților găzduite în Cloud-ul Guvernamental se stabilesc prin hotărâre de guvern.

Capitolul III - Organizarea și funcționarea infrastructurilor informatice de tip cloud, altele decat Cloud-ul Guvernamental

Art. 11 -

(1) Autoritățile și/sau entitățile publice locale pot dezvolta infrastructuri informatice de tip cloud sau pot utiliza servicii de tip cloud furnizate de entități private, necesare funcționării serviciilor publice digitale pe care le gestionează, în condițiile în care nu sunt găzduite, respectiv dezvoltate în Cloud-ul Guvernamental.

(2) Infrastructurile informatice specifice de tip cloud menționate la alin. (1) au în structura acestora elemente tehnice componente, precum:

a) infrastructura de bază a Cloud-ului;
b) infrastructura ca serviciu (IaaS);
c) platforma ca serviciu (PaaS)
d) software ca serviciu (SaaS);

(3) Infrastructurile informatice de tip cloud mentionate la alin. (1) trebuie realizate și implementate astfel încât să asigure următoarele categorii de facilități:

a) furnizarea continuă, în limita nivelurilor agreate de către utilizatorii de servicii de tip cloud a serviciilor de accesare a bazelor de date și a sistemelor informatice aferente;
b) interoperabilitatea bazelor de date găzduite de structura informatică specifică cu alte baze de date găzduite de alte infrastructuri informatice specifice, inclusiv cu baze de date la nivel european;
c) interconectivitatea infrastructurilor informatice de tip cloud între diverși furnizori de servicii de tip cloud pentru a permite migrarea bazelor de date și a evita captivitatea utilizatorilor de servicii de tip cloud;

d) controlul confidențialității datelor prin intermediul instrumentelor specifice serviciilor de cloud ușor de utilizat și cu opțiuni precum și conformarea administrativă asupra accesului și permisiunilor la date;
e) securitatea cibernetică a datelor pentru a asigura reziliența la atacurile cibernetice.

Art. 12. -

(1) Fiecare serviciu specific de cloud este asigurat de cel puțin două noduri de date organizate ca centre de date, pentru a asigura furnizarea serviciilor de cloud în mod rezilient.
(2) Centrele de date menționate la alin. (1) pot găzdui cloud de tip privat, cloud de tip public, cloud de tip hibrid, în acord cu nevoile de dezvoltare ale investitorilor în infrastructuri informatice de tip cloud.

Art. 13. -

Între furnizorul de servicii de tip cloud și utilizatorul de servicii de tip cloud se încheie o convenție de administrare a serviciilor de tip cloud, care cuprinde drepturile și obligațiile aferente utilizării serviciilor de tip cloud.

Art. 14 -

MCID, în calitate de autoritate publică centrală cu rol în elaborarea strategiilor publice stabilește măsuri în domeniul serviciilor de tip cloud pentru infrastructurile de cloud menționate la art. 11 alin. (1).

Art. 15 -

(1) Serviciile de tip cloud menționate la art. 11 sunt asigurate pe baza unui Ghid de Guvernanță a Cloud-ului care prevede standarde, reguli, orientări sau caracteristici pentru activități sau rezultatele acestora, care vizează atingerea gradului optim de calitate, precum și reguli și obligații în relația dintre furnizorul și utilizatorul de servicii de tip cloud.
(2) Ghidul de Guvernanță al Cloud-ului prevăzut la alin. (1) se elaborează și se aprobă prin hotărâre de Guvern, la propunerea MCID, cu consultarea prealabilă a entităților de la art. 1, alin. (2).

Capitolul IV

Controlul parlamentar al Cloud-ului Guvernamental

Art. 16

(1) În scopul garantării drepturilor constituționale la viață intimă, familială și privată, libertatea de exprimare și secretul corespondenței, se instituie un control parlamentar asupra activității de realizare și administrare a Cloud-ului Guvernamental.
(2) Controlul parlamentar se exercită prin comisiile reunite ale Camerei Deputaților și Senat pentru tehnologia informaţiei şi comunicaţiilor.
(3) Controlul parlamentar privind administrarea și utilizarea Cloud-ul Guvernamental are următoarele obiective:

a) respectarea drepturilor constituționale la viață intimă, familială și privată, libertatea de exprimare și secretul corespondenței;
b) respectarea implementării și aplicării prevederilor prezenței ordonanțe de urgență privind Cloud-ul Guvernamental;
c) asigurarea interoperabilității prin Cloud-ul Guvernamental;
d) respectarea regimului juridic al informațiilor confidențiale și al celor nepublice utilizate în Cloud-ul Guvernamental.

Art. 17 -

(1) Anual, comisiile reunite ale Camerei Deputaților și Senatului pentru tehnologia informaţiei şi comunicaţiilor elaborează și prezintă un raport referitor la modul de administrare și utilizare a Cloud-ului Guvernamental de către autoritățile prevăzute la art. 1, alin. (2). Raportul se prezintă, spre aprobare, birourilor permanente ale celor două Camere în termen de 3 luni de la încheierea anului anterior.
(2) În urma aprobării prevăzute la alin. (1), raportul se prezintă plenului reunit al Camerei Deputaților și al Senatului.

(3) Organizarea și desfășurarea lucrărilor comisiilor reunite ale Camerei Deputaților și Senatului pentru tehnologia informaţiei şi comunicaţiilor se stabilesc prin regulament aprobat prin hotărâre a Parlamentului României.

(4) La cererea birourilor permanente ale celor două Camere, sau când consideră, comisiile reunite întocmesc şi prezintă acestora rapoarte cu privire la constatările şi concluziile rezultate în exercitarea atribuţiilor ce îi revin potrivit art. 16, alin. (3).

(5) Rapoartele comisiilor reunite sunt prezentate pe pagina de internet a Camerei Deputaților și Senatului.

Capitolul V
Dispoziții finale

Art. 18 –

(1) În vederea finanțării din PNRR a investițiilor aferente Cloud-ului Guvernamental, MCID încheie un acord de implementare cu Organismul Intermediar pentru Promovarea Societății Informaționale, denumit în continuare OIPSI, din cadrul ADR.

(2) În baza acordului de implementare prevăzut la alin. (1) și a rezultatului cererilor de finanțare depuse de ADR, STS și SRI, OIPSI încheie, respectiv emite, după caz, contracte de finanțare sau respectiv decizii de finanțare.

(3) OIPSI asigură monitorizarea tehnică a stadiului de realizare a investițiilor aferente Cloud-ului Guvernamental.

(4) MCID asigura verificarea și certificarea sumelor solicitate la rambursare de către ADR, STS și SRI, precum și autorizarea și plata acestora.

(5) Evaluarea, selecția și contractarea investițiilor va avea în vedere respectarea etapelor prevăzute în PNRR.

(6) Competența de certificare a îndeplinirii corespunzătoare a condițiilor specifice investițiilor aferente Cloud-ului Guvernamental, prevăzute în PNRR, integrate în cadrul Studiului de Fezabilitate și al Proiectului Tehnic și ulterior al caietelor de sarcini aferente achizițiilor publice aparține Comitetului Tehnico - Economic pentru Societatea Informațională, conform Hotărârii Guvernului nr. 941/2013, precum si Comitetului pentru e-guvernare şi

reducerea birocrației, înființat prin Decizia prim-ministrului nr. 331/2021, în funcție de nivelul de competențe.

(7) În scopul analizei și preavizării Studiului de fezabilitate și Proiectului tehnic prevăzute la alin. (5), la nivelul MCID, prin ordin al ministrului cercetării, inovării și digitalizării, se constituie un grup de experți externi.

(8) Pentru realizarea componentelor Cloud-ului Guvernamental respectiv pentru realizarea IaaS, PaaS, SaaS, securitate cibernetică și migrare a bazelor de date, ADR, STS și SRI organizează după caz proceduri de achiziție publică, în conformitate cu legislația în vigoare în domeniul achizițiilor publice .

(9) Prevederile art. 1, alin. (4) se implementează în termen de 2 ani de la data notificării de către ADR în acest sens. Migrarea autorităților se realizează pe baza încheierii unui protocol cu ADR.

Art. 19 -

Autoritățile și instituțiile publice centrale, precum și structurile aflate în coordonarea, subordonarea sau sub autoritatea acestora care furnizează un serviciu public electronic, cu excepția celor prevăzute la art 1. alin (9), au obligația ca în termen de 30 zile de la data solicitării ADR să transmită informațiile de detaliu relevante pentru sistemul/sistemele informatice ce vor fi migrate în Cloud-ul Guvernamental.

Art. 20 -

Prevederile art. 6 din Ordonanța de urgență a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului Național de Redresare și Reziliență al României necesare României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de Redresare și Reziliență, cu modificările și completările ulterioare, se aplică instituțiilor responsabile de realizarea Cloud-ului Guvernamental începând cu data intrării în vigoare a prezentei ordonanțe de urgență.

Art. 21 -

În termen de 60 de zile de la intrarea în vigoare a prezentei ordonanțe de urgență, MCID împreună cu ADR, STS și SRI, inițiază hotărârea de guvern prevăzută la art. 3.

Art. 22 -

Prevederile Capitolului III nu se aplică infrastructurilor de tip cloud dezvoltate de instituțiile din sistemul național de apărare, ordine publică și securitate națională.

PRIM-MINISTRU

NICOLAE-IONEL CIUCĂ