GUVERNUL ROMÂNIEI
ORDONANȚĂ DE URGENȚĂ
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

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 pentru îmbunătățirea serviciilor publice dedicate cetățenilor și pentru eficientizarea cheltuielilor aferente sistemelor și rețelelor informatice,

Având în vedere situația extraordinară generată de conflictul armat de pe teritoriul Ucrainei și nevoia urgentă de creștere a rezilienței capabilităților sistemelor și rețelelor informatice ale statului român, inclusiv prin prisma necesității asigurării securității datelor personale ale cetățenilor români,

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 și sporirea rezilienței sistemelor și rețelelor informatice ale statului român, având în vedere situația fiscal-bugetară care reclamă accesarea fără întârzieri a finanțărilor disponibile prin PNRR și ținând de cont de faptul că termenul limită asumat de România prin PNRR pentru îndeplinirea jalonului este 30 iunie a.c.;

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 Privat 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 Privat Guvernamental,

De asemenea, având 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, denumit în continuare 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 Privat 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 țară 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 Platformei de Cloud Guvernamental, astfel încât aceasta să fie funcțională, 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 Privat 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, Strategia Europeană privind Datele, Declarația Comună a Statelor Membre UE privind Noua Generație de Cloud în Europa, Cadrul European de Interoperabilitate, precum și aspectele prezentate anterior, se impune reglementarea 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 - Dispoziții generale privind Platforma de Cloud Guvernamental

(1) Prezenta ordonanță de urgență reglementează regimul juridic general privind înființarea, administrarea și dezvoltarea, la nivel național, a unei infrastructuri de tip cloud hibrid, Platforma de Cloud Guvernamental, denumită în continuare „Platforma”.

(2) În vederea utilizării serviciilor de tip cloud de către entitățile găzduite, reprezentate de autoritățile și instituțiile publice centrale și locale, se înființează Platforma, constituită dintr-o componentă de cloud privat, denumită în continuare „Cloud-ul Privat Guvernamental”, și din resurse și servicii publice certificate din alte tipuri de cloud publice sau private.

(3) Modul de utilizare a Platformei și modul de realizare a interconectării la nivel de servicii între componentele prevăzute la alin. (2) sunt stabilite într-un Ghid de Guvernanță a Platformei, 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.

(4) Ghidul prevăzut la alin. (3) se elaborează și se aprobă prin hotărâre de Guvern, la propunerea Ministerului Cercetării, Inovării și Digitalizării, denumit în continuare MCID, cu consultarea prealabilă a Autorității pentru Digitalizarea României, denumită în continuare ADR, a Serviciului de Telecomunicații Speciale, denumit în continuare STS și a Serviciului Român de Informații, denumit în continuare SRI.

(5) Cloud-ul Privat Guvernamental este administrat operațional de statul român prin ADR și constă într-un ansamblu de resurse de tehnologia informației, comunicații și securitate cibernetică, aparținând statului român, interconectat la nivel de servicii cu infrastructuri de tip cloud public sau privat.

(6) Autoritățile responsabile de realizarea Cloud-ului Privat Guvernamental sunt MCID și ADR, în colaborare cu STS și SRI, conform competențelor stabilite de prezenta ordonanță de urgență.

(7) 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 apte pentru migrarea în Cloud-ul Privat Guvernamental sau interconectate cu acesta.

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

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

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

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

(12) Prevederile prezentei ordonanțe 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 acelor sisteme care asigură servicii publice electronice, care se vor interconecta cu Cloud-ul Privat Guvernamental, respectiv a sistemelor informatice pentru care autoritățile respective doresc în mod expres să utilizeze resursele și serviciile de Cloud Privat Guvernamental.

Art. 2 – Definiții

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 şi/sau al afacerilor), care, prin intermediul tehnicilor, tacticilor şi 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 reţelelor şi al sistemelor informatice, precum şi la nivelul utilizatorilor unor astfel de sisteme şi al altor persoane sau care poate avea un alt fel de impact negativ asupra acestora;
c) atac cibernetic - acțiune ostilă desfășurată în spațiul 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 existent;
e) cloud privat – modalitate de organizare a resurselor unui sistem de cloud computing în care serviciile sunt folosite de un singur client al cloud-ului, iar resursele sunt controlate de acel client;
f) cloud public – modalitate de organizare a resurselor unui sistem de cloud computing în care serviciile sunt posibil disponibile oricărui client al cloud-ului, iar resursele sunt controlate de furnizorul de servicii cloud;
g) cloud hibrid - modalitate de organizare a resurselor unui sistem de cloud, care utilizează cel puțin două tipuri diferite de cloud computing;
h) 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;
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 Privat 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) interconectare cu Cloud-ul Privat Guvernamental – 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 Cloud-ul Privat Guvernamental.
n) marketplace – catalog de aplicații și servicii de tip cloud, disponibile în Platformă, dezvoltate inclusiv de mediul privat, ce pot fi accesate de entitățile găzduite;
o) migrare în cloud - metodologia, procedura și acțiunile necesar a fi realizate pentru pregătirea și realizarea transferului unui sistem informatic în cloud sau pentru reproiectarea tehnologică în cazul sistemelor informatice perimate, fără a altera funcționalitățile existente ale sistemului informatic în cauză;
p) nivel agreat al serviciilor - set de parametri și indicatori specifici, în baza cărora este determinată disponibilitatea, performanța și calitatea serviciilor oferite;
q) 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;
r) risc de securitate cibernetică - probabilitatea ca o amenințare să se materializeze, exploatând o vulnerabilitate specifică rețelelor și sistemelor informatice;
s) 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 Privat Guvernamental;
t) sistem informatic apt pentru migrare - sistem informatic ale cărui arhitectură și tehnologii folosite pentru realizarea sa permit migrarea și funcționarea în infrastructuri de tip cloud;
u) 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;
v) 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;
w) 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 amenințare.

Capitolul II
Atribuții și responsabilități privind realizarea și operarea Platformei de Cloud Guvernamental

Art. 3 – Atribuțiile MCID

(1) Politicile, strategia, standardele și criteriile de implementare, operare, utilizare, întreținere și dezvoltare ulterioară a Platformei se stabilesc prin hotărârea Guvernului prevăzută la art. 1 alin. (4).

(2) Cadrul de management și stocare a datelor în Platformă, inclusiv stabilirea categoriilor de date prelucrate în Platformă și găzduite de Cloud-ul Privat Guvernamental, cloud privat, cloud public, după caz, se realizează prin hotărâre de Guvern, la propunerea MCID.

(3) Politica, strategia, criteriile tehnice și operaționale privind implementarea, operarea, mentenanța și dezvoltarea ulterioară a Cloud-ului Privat Guvernamental, regulile privind stabilirea nivelului agreat de servicii, precum și cele privind migrarea sau, după caz, interconectarea sistemelor informatice se stabilesc prin hotărâre de Guvern, la propunerea MCID, împreună cu ADR, STS și SRI.

(4) Planul pentru migrarea și integrarea în Cloud-ul Privat Guvernamental a sistemelor informatice și a serviciilor publice electronice ale instituțiilor și autorităților aparținând administrației publice, precum și lista entităților publice ale căror aplicații și sisteme informatice migrează în Cloud-ul Privat Guvernamental se stabilesc prin hotărâre de guvern promovată de MCID, la propunerea ADR.

(5) MCID reprezintă interesele statului român în relațiile externe privind serviciile de Cloud Privat Guvernamental.

(6) MCID stabilește tipurile de servicii care sunt furnizate prin Platformă, respectiv stabilește și promovează tipurile de servicii furnizate prin Cloud-ul Privat Guvernamental.

(7) MCID sprijină entitățile găzduite în Cloud-ul Privat Guvernamental la procesul de management al riscurilor, pe baza analizelor de risc furnizate de către ADR, STS și SRI.

(8) MCID, la propunerea ADR, cu sprijinul STS și SRI, stabilește criteriile generale de asigurare a confidențialității, securității, interoperabilității, standardizării tehnice și semantice, respectiv performanței aplicațiilor de tip SaaS găzduite în Platformă, prin intermediul unui marketplace, inclusiv a aplicațiilor dezvoltate de mediul privat.

(9) Modul de administrare a aplicațiilor listate în marketplace este stabilit prin ordin al ministrului cercetării, inovării și digitalizării.

Art. 4 - Atribuțiile ADR

(1) ADR contribuie la elaborarea și punerea în aplicare a strategiei privind implementarea, operarea, mentenanța și dezvoltarea ulterioară a Platformei, inclusiv la elaborarea unui set de cerințe și măsuri tehnice de performanță și securitate cibernetică, realizat cu sprijinul STS și SRI.

(2) ADR elaborează și pune în aplicare planul pentru migrarea și integrarea în Cloud-ul Privat Guvernamental a sistemelor informatice și a serviciilor publice electronice ale instituțiilor și autorităților aparținând administrației publice.

(3) ADR asigură implementarea, administrarea tehnică și operațională, mentenanța, precum și dezvoltarea ulterioară pentru serviciile SaaS specifice Cloud-ului Privat Guvernamental, inclusiv asigurarea, prin acorduri-cadru, conform legislației achizițiilor

publice, a licențelor specifice serviciilor necesare migrării în Cloud-ul Privat Guvernamental a sistemelor informatice și serviciilor publice electronice.

(4) Migrarea, integrarea și interconectarea în Cloud-ul Privat Guvernamental a sistemelor informatice ale autorităților și instituțiilor publice se asigură de către ADR, în conformitate cu hotărârea de Guvern menționată la art. 3 alin. (4), pe baza acordului încheiat de ADR cu fiecare autoritate și instituție publică notificată de către ADR în vederea migrării, inclusiv cele prevăzute la art. 1 alin. (12).

(5) În cazul în care o autoritate publică consideră că un anumit sistem informatic sau o anumită aplicație nu trebuie să utilizeze o soluție de tip cloud, aceasta formulează o solicitare motivată în acest sens către Comitetul Tehnico-Economic pentru Societate Informațională.

(6) Comitetul Tehnico-Economic pentru Societatea Informațională analizează solicitarea menționată la alin. (5) și emite un aviz conform privind exceptarea de la migrare sau refuză avizarea.

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

(8) ADR gestionează marketplace-ul menționat la art. 3, alin. (8), 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.

(9) ADR asigură interconectarea la nivel de SaaS la serviciile specifice Cloud-ului Privat Guvernamental pentru entitățile găzduite și conectate în cloud.

Art. 5 – Atribuțiile STS

(1) Infrastructura de bază a Cloud-ului Privat 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 Privat Guvernamental, prevăzute la art. 2 lit. k), l) și q).

(3) STS asigură accesul securizat, conectivitatea și interconectarea la serviciile specifice Cloud-ului Privat Guvernamental pentru entitățile găzduite sau interconectate în cloud.

(4) STS asigură securitatea cibernetică a Cloud-ului Privat Guvernamental prin prevenirea și contracararea atacurilor cibernetice, pentru serviciile prevăzute la art. 2 lit. k), l) și q), inclusiv a atacurilor de tip DDoS îndreptate împotriva Cloud-ului Privat 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 Privat 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 q) din Cloud-ul Privat Guvernamental.

Art. 6 – Atribuțiile SRI

(1) SRI asigură securitatea cibernetică a Cloud-ului Privat Guvernamental prin cunoașterea, prevenirea și contracararea atacurilor, amenințărilor, riscurilor și vulnerabilităților cibernetice, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor Cloud-ului Privat Guvernamental menționate la art. 2 lit. u) 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 Privat Guvernamental menționate la art. 2 lit. l) și q), 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 Privat Guvernamental, prevăzute la alin. (1).

Art. 7 - Securitatea cibernetică a Cloud-ului Privat Guvernamental

(1) În cazul sistemelor informatice interconectate cu Cloud-ul Privat 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 - Politica de Cloud First

(1) MCID, împreună cu ADR, după consultarea mediului privat, propune politica de cloud first, în vederea adoptării acesteia prin hotărârea de Guvern prevăzută la art. 3 alin. (4).
(2) Entitățile publice migrează aplicațiile și sistemele informatice, sau, după caz, interconectează sistemele informatice în Platformă, în conformitate cu prevederile hotărârilor de Guvern menționate la art. 3 alin. (2) și (4).

Art. 9 - Prelucrarea datelor cu caracter personal

În procesul de dezvoltare, implementare, administrare și asigurarea securității cibernetice a Cloud-ului Guvernamental Privat, instituțiile publice menționate la art. 1 alin. (6) prelucrează date cu caracter personal, în calitate de persoane împuternicite de către entitățile găzduite sau interconectate, 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.

Art. 10 – Proprietatea, jurnalizarea și auditul Cloud-ului Privat Guvernamental

(1) Infrastructura de bază a Cloud-ului Privat Guvernamental, infrastructura ca serviciu (IaaS) și platforma ca serviciu (PaaS), prevăzute la art. 2. lit. k), l) și q) sunt proprietate privată 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 privată 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 administrației 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 u) sunt proprietate privată a statului și în administrarea ADR, care le achiziționează conform prevederilor legale în vigoare privind achizițiile publice.
(4) Componentele aferente securității cibernetice sunt proprietate privată a statului și sunt achiziționate și administrate de STS și SRI, potrivit competențelor stabilite la art. 5-7 din prezenta ordonanță de urgență.
(5) Privitor la dispozițiile alin. (1)-(4), în situația în care achiziționarea drepturilor de proprietate nu este posibilă, se asigură cel puțin achiziționarea drepturilor de utilizare.
(6) Administratorii serviciilor furnizate la nivel de IaaS, PaaS și SaaS, precum și administratorii de securitate cibernetică asigură jurnalizarea evenimentelor și accesului la datele entităților găzduite în Cloud-ul Privat Guvernamental, în scopul realizării de audituri de conformitate periodice pe linia protecției, calității, securității și trasabilității datelor, în vederea asigurării transparenței utilizării acestora.
(7) ADR asigură dezvoltarea unei aplicații de jurnalizare și notificare a activității de prelucrare a datelor cu caracter personal ale persoanelor vizate, destinată utilizatorilor finali ai serviciilor publice furnizate de entitățile publice găzduite în Cloud-ul Privat Guvernamental.
(8) Normele metodologice de jurnalizare a evenimentelor și accesului la datele entităților găzduite în Cloud-ul Privat Guvernamental se stabilesc prin hotărâre de guvern menționată la art. 3 alin. (2).
(9) MCID dispune, cel puțin anual sau ori de câte ori este nevoie, efectuarea unor activități de audit de conformitate pe linia protecției, calității, securității și trasabilității pentru Platformă sau, după caz, pentru anumite componente ale acesteia, finanțate prin bugetul acestuia.
(10) Autoritățile menționate la art. 1 alin. (6) întocmesc până la finalul primului trimestru al anului în curs un raport comun cu privire la activitatea de realizare și administrare a Cloud-ului Privat Guvernamental pentru anul precedent, pe care îl comunică comisiilor pentru tehnologia informației și comunicațiilor ale Camerei Deputaților și Senatului.

Capitolul III – Principalele drepturi și obligații ale entităților găzduite în Cloud-ul Privat Guvernamental

Art. 11 – Drepturile entităților găzduite

(1) Solicită sau eliberează resurse din Cloud-ul Privat Guvernamental, în conformitate cu necesitățile proprii.
(2) Achiziționează servicii de analiză de procese informaționale, dezvoltare software și suport în vederea testării sistemelor informatice din Cloud-ul Privat Guvernamental.
(3) Beneficiază de consiliere tehnică de specialitate din partea instituțiilor participante la implementarea Cloud-ului Privat Guvernamental în organizarea utilizării eficiente a serviciilor Cloud-ului Privat Guvernamental și a prestării serviciilor sale către persoane fizice și juridice.
(4) Pot solicita activități de audit de conformitate pe linia calității, securității și trasabilității pentru datele proprii, finanțate prin bugetul acestora.

Art. 12 – Obligațiile entitățile găzduite

(1) Prelucrează datele cu caracter personal în procesul de utilizare și furnizare a serviciilor publice prin intermediul Cloud-ului Privat Guvernamental cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal.

(2) Stabilesc modul și perioada de prelucrare a datelor cu caracter personal, 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 Privat Guvernamental.
(3) Întreprind toate măsurile necesare de pregătire a infrastructurii propriii pentru utilizarea eficientă a serviciilor solicitate din Cloud-ul Privat Guvernamental.
(4) Desemnează persoana de contact responsabilă în relația cu administratorul operațional al Cloud-ului Privat Guvernamental.
(5) Anunță imediat administratorul operațional despre abaterile constatate de la nivelul agreat de servicii sau despre orice alt eveniment observat care poate compromite buna funcționare a serviciilor.
(6) Autoritățile și instituțiile publice centrale, care furnizează un serviciu public electronic, cu excepția celor prevăzute la art 1 alin (12), 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 Privat Guvernamental.

Capitolul IV - Organizarea și funcționarea infrastructurilor informatice de tip cloud în Platformă, altele decat Cloud-ul Privat Guvernamental

Art. 13 – Politici generale și cadru juridic

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

(1) Infrastructurile informatice de tip cloud menționate 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. 14. – Cerințe privind reziliența

(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 servicii de cloud de tip privat, servicii de cloud de tip public, servicii de cloud de tip hibrid, în acord cu nevoile de dezvoltare ale investitorilor în infrastructuri informatice de tip cloud.

Art. 15. – Reglementare cu privire la guvernanță

Între furnizorul de servicii de tip cloud și utilizatorul de servicii de tip cloud prevăzuți la art. 13 alin. (1) se încheie o convenție de administrare a serviciilor de tip cloud, care cuprinde drepturile și obligațiile aferente utilizării serviciilor de tip cloud în Platformă.

Art. 16 - Certificarea de securitate

(1) Standardele și criteriile pentru selecția, certificarea și utilizarea serviciilor de tip cloud privat, altele decât Cloud-ul Privat Guvernamental, și ale serviciilor de tip cloud public furnizate în regim comercial se stabilesc prin ordin al ministrului cercetării, inovării și digitalizării, cu consultarea prealabilă a ADR, STS și SRI.

(2) Procedurile de certificare a securității serviciilor de tip cloud public pentru utilizare de către autoritățile publice se stabilesc prin ordin al ministrului cercetării, inovării și digitalizării, cu consultarea prealabilă a SRI și a Directoratului Național de Securitate Cibernetică, denumit în continuare DNSC, cu respectarea prevederilor Legii nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G.

Capitolul V
Dispoziții finale

Art. 17 – Dispoziții finale privind implementarea Cloud-ului Privat Guvernamental

(1) Finanțarea cheltuielilor pentru implementarea Cloud-ului Privat Guvernamental se asigură prin PNRR și de la bugetul de stat sau din alte surse de finanțare.

(2) 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 privind organizarea și funcționarea Comitetului Tehnico-Economic pentru Societatea Informațională.

(3) Pentru realizarea componentelor Cloud-ului Privat 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.

(4) ADR, STS și SRI evaluează periodic resursele necesare Cloud-ului Privat Guvernamental pentru a satisface nevoile entităților găzduite și comunică MCID planificarea capacității, în colaborare cu entitățile găzduite, pentru a estima nivelul cererii și pentru a pune în aplicare investițiile sau măsurile suplimentare necesare, pe domeniile de competență.

(5) Prevederile Capitolului IV 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