ORDONANŢĂ DE URGENŢĂ Nr. 89/2022 din 27 iunie 2022

*privind înfiinţarea, administrarea şi dezvoltarea infrastructurilor şi serviciilor informatice de tip cloud utilizate de autorităţile şi instituţiile publice*

*Text în vigoare începând cu data de 30 iunie 2023*

*REALIZATOR: COMPANIA DE INFORMATICĂ NEAMŢ*

*Text actualizat prin produsul informatic legislativ LEX EXPERT în baza actelor normative modificatoare, publicate în Monitorul Oficial al României, Partea I, până la 27 iunie 2023.*

*Formă la zi recentă*

***Act de bază***

**#B**: *Ordonanţa de urgenţă a Guvernului nr. 89/2022, publicată în Monitorul Oficial al României, Partea I, nr. 638 din 28 iunie 2022*

***Acte modificatoare***

**#M2**: *Legea nr. 180/2023*

**#M1**: *Rectificarea publicată în Monitorul Oficial al României, Partea I, nr. 680 din 7 iulie 2022*

*Modificările şi completările efectuate prin actele normative enumerate mai sus sunt scrise cu font italic. În faţa fiecărei modificări sau completări este indicat actul normativ care a efectuat modificarea sau completarea respectivă, în forma* ***#M1****,* ***#M2*** *etc.*

**#CIN**

***NOTE:***

*1. Titlul actului normativ a fost corectat conform Rectificării publicate în Monitorul Oficial al României, Partea I, nr. 680 din 7 iulie 2022 (****#M1****).*

*2. Ordonanţa de urgenţă a Guvernului nr. 89/2022 a fost aprobată cu modificări prin Legea nr. 180/2023 (****#M2****).*

**#B**

Având în vedere faptul că tehnologia de tip cloud este din ce în ce mai utilizată de către autorităţile şi instituţiile publice din statele membre ale Uniunii Europene, ca urmare a avantajelor tehnice şi economice care privesc procesarea şi stocarea datelor, precum şi disponibilitatea serviciilor, avantaje care au ca rezultat generarea de economii consistente sub aspectul investiţiilor şi al cheltuielilor operaţionale,

ţinând cont de faptul că implementarea unei infrastructuri de tip cloud în sectorul public este o prioritate asumată de către Guvernul României în Programul de guvernare şi în actualul context naţional şi internaţional, determinat de pandemia de COVID-19, iar realizarea acestui obiectiv a devenit stringentă, având în vedere că schimbul de date în format electronic în sectorul public este absolut necesar pentru îmbunătăţirea serviciilor publice dedicate cetăţenilor şi pentru eficientizarea cheltuielilor aferente sistemelor şi reţelelor informatice,

având în vedere situaţia extraordinară generată de conflictul armat de pe teritoriul Ucrainei şi nevoia urgentă de creştere a rezilienţei capabilităţilor sistemelor şi reţelelor informatice ale statului român, inclusiv prin prisma necesităţii asigurării securităţii datelor personale ale cetăţenilor români,

în considerarea faptului că obiectivul menţionat anterior presupune, printre altele, asigurarea unui management unitar şi eficient privind gestionarea centralizată a resurselor informatice şi de comunicaţii, fapt ce impune adoptarea cu celeritate a unor măsuri atât la nivel legislativ, cât şi la nivelul gestionării resurselor în condiţii de securitate sporită, scalabilitate, flexibilitate şi adaptabilitate,

deoarece realizarea unei infrastructuri de tip cloud în sectorul public reprezintă un obiectiv imediat şi urgent în considerarea faptului că implementarea sa asigură utilizarea forţei de muncă într-un mod mai eficient, ca urmare a administrării suportului tehnic şi asigurării mentenanţei sistemelor în mod centralizat, fapt ce generează automatizarea managementului componentelor software de la nivelul sistemului de operare până la cel al aplicaţiilor informatice,

având în vedere situaţia extraordinară generată de creşterea volumului informaţiilor din bazele de date critice administrate de statul român şi necesitatea consolidării şi interconectării acestora, precum şi necesitatea asigurării în mod unitar a securităţii cibernetice a acestora,

deoarece România are alocate fonduri prin Planul naţional de redresare şi rezilienţă al României, 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 şi investiţii în digitalizarea mediului de afaceri, iar pentru utilizarea eficientă a fondurilor publice în ceea ce priveşte cheltuielile cu mentenanţa şi cu infrastructura şi echipamentele informatice este necesar ca autorităţile şi instituţiile publice, altele decât cele ale căror sisteme informatice vor migra în cloudul guvernamental, să aibă alternativa stocării acestora în infrastructuri de tip cloud gestionate de furnizorii unor astfel de servicii,

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

deoarece mediul de afaceri are nevoie de mecanisme de transformare digitală rapide şi specifice care să îi permită să dezvolte platforme informatice în acord cu nevoile de automatizare şi robotizare specifice pieţei concurenţiale europene pentru a gestiona eficient cheltuielile cu mentenanţa, dar şi cu cele specifice echipamentelor informatice,

având în vedere contextul platformei de cloud, care vizează modul în care vor fi implementate platformele informatice de cloud, precum şi modelul arhitectural pentru dezvoltarea unei infrastructuri de cloud adaptate la tehnologiile informaţionale specifice, este necesară stabilirea unei infrastructuri digitale coerente şi integrate la nivelul administraţiei publice bazată pe modulul de guvernanţă a datelor şi a obiectivelor economice care să ofere servicii digitale de înaltă calitate şi care să satisfacă nevoia de acces deschis, respectiv cloud public, cât şi acces restricţionat, utilizând o formă de cloud privat,

în considerarea aspectelor menţionate mai sus, dar şi a faptului că implementarea unei infrastructuri de tip cloud în sectorul public, astfel încât aceasta să fie funcţională, necesită parcurgerea unor etape procedurale a căror desfăşurare presupune o anumită perioadă de timp, iar orice întârziere în adoptarea de măsuri urgente în acest sens ar creşte substanţial riscul de dezangajare a fondurilor europene nerambursabile disponibile în acest scop, cu implicaţii negative asupra fondurilor naţionale, reglementarea în regim de urgenţă a cadrului legal necesar demarării etapelor pentru implementarea acestui proiect este cu atât mai justificată,

ţinând cont de situaţia extraordinară generată de conflictul armat de pe teritoriul Ucrainei şi nevoia urgentă de creştere a rezilienţei capabilităţilor sistemelor şi reţelelor informatice ale statului român, inclusiv prin prisma necesităţii asigurării securităţii datelor personale ale cetăţenilor români,

reţinând că situaţia extraordinară este cauzată şi de creşterea volumului informaţiilor din bazele de date critice administrate de statul român, precum şi necesitatea consolidării, interconectării şi asigurării în mod unitar a securităţii cibernetice a acestora, în contextul conflictelor convenţionale şi neconvenţionale din vecinătatea României şi al revoluţiei digitale care acaparează toate statele lumii,

având în vedere criza conductorilor electrici, intensificarea ameninţărilor cibernetice venite dinspre spaţiul estic şi riscul real de pierdere şi alterare a datelor guvernamentale generate de astfel de atacuri ce reprezintă abateri semnificative de la obişnuit şi impun recurgerea la această cale de reglementare pentru evitarea aducerii atingerii interesului public,

reţinând faptul că una dintre direcţiile de acţiune pentru asigurarea securităţii naţionale prevăzute în Strategia naţională de apărare a ţării 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 şi al creşterii calităţii serviciilor publice, pentru transpunerea în realitate a acestei direcţii de acţiune fiind necesară implementarea unei infrastructuri de tip cloud în sectorul public,

având în vedere că reglementarea care nu poate fi amânată este cauzată de faptul că, în jalonul nr. 153 din Planul naţional de redresare şi rezilienţă, se specifică faptul că implementarea unei infrastructuri de tip cloud în sectorul public cuprinde construcţia de centre de date Tier IV de la momentul conceperii pentru cele două centre principale, Tier III de la momentul conceperii pentru cele secundare, infrastructuri specifice găzduirii de sisteme informatice on-premise, iar de construirea urgentă a acestora depind transferul la timp al finanţării de către Comisia Europeană şi sporirea rezilienţei sistemelor şi reţelelor informatice ale statului român. În acest context, situaţia fiscal-bugetară reclamă accesarea fără întârzieri a finanţărilor disponibile prin PNRR cu respectarea termenului-limită de 30 iunie a.c. asumat de România prin PNRR pentru îndeplinirea jalonului.

Întrucât lipsa reglementării, la nivel primar, generează imposibilitatea implementării pe altă cale a soluţiilor prevăzute în ordonanţa de urgenţă, fiind domenii care capacitează întreaga administraţie publică centrală, managementul informaţiilor la nivelul serviciilor publice, dinamica serviciilor publice, adaptarea acestora la noile realităţi tehnologice şi digitale, precum şi reacţia de răspuns a statului la noile provocări în domeniul conceptului de securitate extinsă,

deoarece neadoptarea prezentei ordonanţe de urgenţă poate avea drept consecinţe pierderea a peste 500 milioane de euro, pierderea credibilităţii României în faţa Comisiei Europene şi a partenerilor occidentali şi afectarea şansei României de a se adapta digital la noile realităţi privind guvernarea electronică, interoperabilitatea sistemelor informatice, regimul administrării virtuale a datelor din sectorul public şi relevanţa acestora pentru buna funcţionare a statului român,

de asemenea, având în vedere că transformarea digitală este un obiectiv de interes strategic naţional, care cuprinde procesul de transformare digitală atât la nivelul serviciilor publice din România, cât şi la nivelul mediului de afaceri, în cazul căruia acest proces se referă la mecanismele de automatizare a proceselor de producţie şi robotizarea acestora, cu impact asupra competitivităţii şi calităţii produselor şi serviciilor pe piaţa europeană,

în conformitate cu Strategia europeană pentru cloud computing, Strategia europeană privind datele, Declaraţia comună a statelor membre ale Uniunii Europene privind Noua generaţie de cloud în Europa, Cadrul european de interoperabilitate, precum şi aspectele prezentate anterior, se impune reglementarea de urgenţă a cadrului legal necesar realizării unei infrastructuri de tip cloud în sectorul public şi a cadrului legal de organizare şi funcţionare a infrastructurilor informatice şi a serviciilor de tip cloud în procesul de transformare digitală.

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

în temeiul art. 115 alin. (4) din Constituţia României, republicată,

**Guvernul României** adoptă prezenta ordonanţă de urgenţă.

**#CIN**

***\*)*** *În Monitorul Oficial al României, Partea I, nr. 638 din 28 iunie 2022, anul acestei hotărâri era indicat, în mod eronat, ca fiind "2022".*

**#B**

CAPITOLUL I

**Dispoziţii generale**

ART. 1

**Dispoziţii generale privind Platforma de cloud guvernamental**

(1) Prezenta ordonanţă de urgenţă reglementează regimul juridic general privind înfiinţarea, administrarea şi dezvoltarea, la nivel naţional, 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 autorităţile şi instituţiile publice centrale şi locale se înfiinţează Platforma, constituită dintr-o componentă de cloud privat, denumită în continuare Cloudul privat guvernamental, şi din resurse şi servicii publice certificate din alte tipuri de cloud publice sau private, în condiţiile prevăzute la art. 16.

(3) Modul de utilizare a Platformei şi modul de realizare a interconectării la nivel de servicii între componentele prevăzute la alin. (2) sunt prevăzute în Ghidul de guvernanţă a platformei\*).

(4) În termen de maximum 90 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă, prin hotărâre a Guvernului\*), la propunerea Ministerului Cercetării, Inovării şi Digitalizării, denumit în continuare MCID, cu consultarea prealabilă a Autorităţii pentru Digitalizarea României, denumită în continuare ADR, a Serviciului de Telecomunicaţii Speciale, denumit în continuare STS, şi a Serviciului Român de Informaţii, denumit în continuare SRI, se aprobă Ghidul de guvernanţă a platformei de cloud guvernamental.

(5) Cloudul privat guvernamental este administrat operaţional de ADR şi constă într-un ansamblu de resurse informatice, de comunicaţii şi de securitate cibernetică, aflate în proprietatea statului român, interconectat la nivel de servicii cu clouduri publice şi/sau cu clouduri private.

(6) Autorităţile responsabile de realizarea Cloudului privat guvernamental sunt MCID şi ADR, în colaborare cu STS şi SRI, conform competenţelor prevăzute de prezenta ordonanţă de urgenţă.

**#M2**

*(7) Începând cu data intrării în vigoare a hotărârii prevăzute la alin. (4), sistemele informatice utilizate de către autorităţile şi instituţiile publice centrale sunt dezvoltate astfel încât să fie apte pentru migrarea în Platformă sau interconectate cu aceasta.*

**#B**

(8) Autorităţile administraţiei publice centrale au obligaţia de a migra serviciile publice electronice în Cloudul privat guvernamental.

(9) Autorităţile administraţiei publice centrale pot migra în Cloudul privat guvernamental, în limita resurselor disponibile ale acestuia, serviciile informatice utilizate pentru operaţiunile administrative proprii.

**#M2**

*(9^1) Autorităţile administraţiei publice locale pot migra, respectiv rula în Platformă serviciile publice electronice şi serviciile informatice utilizate pentru operaţiunile administrative proprii, în limita resurselor disponibile ale Platformei.*

**#B**

(10) În termen de maximum 90 de zile de la data intrării în vigoare a hotărârii prevăzute la alin. (4), nivelurile agreate ale serviciilor specifice Cloudului privat guvernamental se aprobă prin ordin comun al ministrului cercetării, inovării şi digitalizării, al preşedintelui ADR, al directorului STS şi al directorului SRI, care se publică în Monitorul Oficial al României, Partea I.

(11) Activităţile de informare publică cu privire la acţiunile care vizează Cloudul privat guvernamental se realizează de către MCID, după consultarea ADR, STS şi SRI, dacă sunt vizate activităţile din responsabilitatea acestora.

(12) Prevederile prezentei ordonanţe de urgenţă nu se aplică sistemelor informatice ale autorităţilor publice din domeniul apărării, ordinii publice şi securităţii naţionale şi nici celor ale autorităţilor publice prevăzute în Constituţie în titlul III, capitolele I, II şi VI, cu excepţia acelor sisteme care asigură servicii publice electronice, care se vor interconecta cu Cloudul privat guvernamental, respectiv a sistemelor informatice pentru care autorităţile respective doresc în mod expres să utilizeze resursele şi serviciile acestuia.

**#CIN**

*\*) A se vedea Hotărârea Guvernului nr. 112/2023 privind aprobarea Ghidului de guvernanţă a platformei de cloud guvernamental.*

**#B**

ART. 2

**Definiţii**

În sensul prezentei ordonanţe de urgenţă, termenii şi expresiile de mai jos au următoarele semnificaţii:

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

b) ameninţare 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 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 informaţiei şi a sistemelor informatice şi de comunicaţii care efectuează procesarea acesteia;

d) cloud first - principiu care implică luarea în considerare a cloudului înaintea tuturor celorlalte tehnologii, fie că este un proiect nou care implică soluţii informatice şi de comunicaţii 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 cloudului, 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 cloudului, iar resursele sunt controlate de furnizorul de servicii cloud;

g) cloud hibrid - modalitate de organizare a resurselor unui sistem de cloud, care utilizează cel puţin două tipuri diferite de cloud computing;

h) date - orice reprezentare digitală a unor acte, fapte sau informaţii şi orice compilaţie a unor astfel de acte, fapte sau informaţii, 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 guvernanţă a platformei de cloud guvernamental - standarde, reguli, orientări şi caracteristici pentru activităţi şi rezultatele acestora, care vizează atingerea gradului optim de calitate, precum şi reguli şi obligaţii în relaţia dintre furnizorul şi utilizatorul de servicii de tip cloud;

k) infrastructura de bază a Cloudului privat guvernamental - clădirile, instalaţiile, dotările şi echipamentele tehnologice aferente, echipamentele informatice şi de comunicaţii, inclusiv echipamentele necesare asigurării securităţii cibernetice, care funcţionează în configuraţii de înaltă disponibilitate, precum şi programele software, aplicaţiile informatice şi licenţele asociate acestora;

l) infrastructura ca serviciu (IaaS) - model de punere la dispoziţia utilizatorilor, la cererea acestora, pe baza unor drepturi de acces şi în limita capacităţilor disponibile în cloud, într-un mod securizat, a resurselor din infrastructura de bază a cloudului;

m) interconectare cu Cloudul privat guvernamental - proces care constă în totalitatea activităţilor operaţionale, procedurale şi tehnice necesar a fi realizate în vederea transmiterii/accesării datelor dintr-un sistem informatic, care furnizează servicii publice electronice în Cloudul privat guvernamental;

n) marketplace - catalog de aplicaţii şi servicii de tip cloud, disponibile în Platformă, dezvoltate inclusiv de mediul privat, ce pot fi accesate de autorităţile şi instituţiile publice găzduite;

o) migrare în cloud - metodologia, procedura şi acţiunile necesar a fi realizate pentru pregătirea şi realizarea transferului unui sistem informatic în cloud sau pentru reproiectarea tehnologică în cazul sistemelor informatice perimate, fără a altera funcţionalităţile existente ale sistemului informatic în cauză;

p) nivel agreat al serviciilor - set de parametri şi indicatori specifici, în baza cărora este determinată disponibilitatea, performanţa şi calitatea serviciilor oferite;

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

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

s) securitatea cibernetică a Cloudului privat guvernamental - stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic aferente resurselor şi serviciilor publice sau private din spaţiul cibernetic al Cloudului privat guvernamental;

t) sistem informatic apt pentru migrare - sistem informatic ale cărui arhitectură şi tehnologii folosite pentru realizarea sa permit migrarea şi funcţionarea în infrastructuri de tip cloud;

u) software ca serviciu (SaaS) - model de punere la dispoziţia utilizatorilor, la cererea acestora, a funcţionalităţilor de utilizare a aplicaţiilor furnizorului, care rulează pe o infrastructură de tip cloud computing. Aplicaţiile sunt accesibile pe baza unor drepturi de acces, prin intermediul unui navigator internet sau al unei aplicaţii informatice dedicate;

v) serviciu public electronic - serviciu public, astfel cum este definit de art. 5 lit. kk) din Ordonanţa de urgenţă a Guvernului nr. 57/2019 privind Codul administrativ, cu modificările şi completările ulterioare, de tip e-guvernare, ce cuprinde soluţii oferite de tehnologia informaţiei;

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 ameninţare cibernetică.

CAPITOLUL II

**Atribuţii şi responsabilităţi privind realizarea şi operarea Platformei de cloud guvernamental**

ART. 3

**Atribuţiile MCID**

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

(2) Cadrul de management şi stocare a datelor în Platformă, inclusiv stabilirea categoriilor de date prelucrate în Platformă şi găzduite de Cloudul privat guvernamental, cloud privat, cloud public, după caz, se realizează prin hotărâre de Guvern, la propunerea MCID, în termen de maximum 90 de zile de la data intrării în vigoare a hotărârii prevăzute la art. 1 alin. (4).

(3) Politica, strategia, criteriile tehnice şi operaţionale privind implementarea, operarea, mentenanţa şi dezvoltarea ulterioară a Cloudului privat guvernamental, regulile privind stabilirea nivelului agreat de servicii, precum şi cele privind migrarea sau, după caz, interconectarea sistemelor informatice se stabilesc prin hotărâre de Guvern, la propunerea MCID, cu consultarea prealabilă a ADR, STS şi SRI, în termen de maximum 90 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

(4) Planul pentru migrarea şi integrarea în Cloudul privat guvernamental a sistemelor informatice şi a serviciilor publice electronice ale instituţiilor şi autorităţilor aparţinând administraţiei publice, precum şi lista autorităţilor şi instituţiilor publice ale căror sisteme informatice şi servicii publice electronice migrează în Cloudul privat guvernamental se stabilesc prin hotărâre de guvern iniţiată de MCID, la propunerea ADR, în termen de maximum 90 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă.

(5) MCID reprezintă interesele statului român în relaţiile externe privind serviciile de Cloud privat guvernamental.

(6) MCID stabileşte, prin ordin al ministrului cercetării, inovării şi digitalizării, care se publică în Monitorul Oficial al României, Partea I, tipurile de servicii care sunt furnizate prin Platformă, respectiv stabileşte şi promovează tipurile de servicii furnizate prin Cloudul privat guvernamental.

(7) MCID sprijină entităţile găzduite în Cloudul privat guvernamental în procesul de management al riscurilor, pe baza analizelor de risc furnizate de către ADR, STS şi SRI.

(8) În termen de maximum 90 de zile de la data intrării în vigoare a prezentei ordonanţe de urgenţă, MCID, la propunerea ADR, cu sprijinul STS şi SRI, propune spre adoptare, prin hotărâre de Guvern, criteriile generale de asigurare a confidenţialităţii, securităţii, interoperabilităţii, adaptării la standarde tehnice şi semantice, respectiv a performanţei aplicaţiilor de tip SaaS găzduite în Platformă, prin intermediul unui marketplace, inclusiv a aplicaţiilor dezvoltate de mediul privat, prin intermediul catalogului definit la art. 2 lit. n).

(9) Modul de administrare a aplicaţiilor listate în marketplace este prevăzut prin ordin al ministrului cercetării, inovării şi digitalizării.

ART. 4

**Atribuţiile ADR**

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

(2) ADR elaborează şi pune în aplicare planul pentru migrarea şi integrarea în Cloudul privat guvernamental a sistemelor informatice şi a serviciilor publice electronice ale autorităţilor şi instituţiilor publice aparţinând administraţiei publice.

(3) ADR asigură implementarea, administrarea tehnică şi operaţională, mentenanţa, precum şi dezvoltarea ulterioară pentru serviciile SaaS specifice Cloudului privat guvernamental, inclusiv asigurarea, prin acorduri-cadru, conform legislaţiei achiziţiilor publice, a licenţelor specifice serviciilor necesare migrării în Cloudul privat guvernamental a sistemelor informatice şi serviciilor publice electronice.

(4) Migrarea, integrarea şi interconectarea în Cloudul privat guvernamental a sistemelor informatice ale autorităţilor şi instituţiilor publice se asigură de către ADR, în conformitate cu hotărârea prevăzută la art. 3 alin. (4), pe baza acordului încheiat de ADR cu fiecare autoritate şi instituţie publică notificată de către ADR în vederea migrării, inclusiv cele prevăzute la art. 1 alin. (12).

(5) Prin excepţie de la prevederile art. 1 alin. (8), în cazul în care o autoritate sau instituţie publică consideră că un anumit sistem informatic sau o anumită aplicaţie informatică nu trebuie să utilizeze o soluţie de tip cloud, aceasta formulează o solicitare motivată în acest sens către Comitetul tehnico-economic pentru societatea informaţională.

(6) Comitetul tehnico-economic pentru societatea informaţională analizează solicitarea prevăzută la alin. (5) şi emite un aviz conform motivat privind exceptarea de la migrare sau refuză motivat avizarea.

(7) În vederea îndeplinirii prevederilor alin. (1) - (4), ADR asigură sau achiziţionează programele software, aplicaţiile informatice şi licenţele necesare, precum şi serviciile de analiză, proiectare şi dezvoltare software, după caz.

(8) ADR gestionează marketplace-ul prevăzut la art. 2 lit. n), care permite accesarea de către entităţile găzduite de Platformă a aplicaţiilor disponibile, pe baza unei relaţii contractuale stabilite între furnizorii şi entităţile găzduite care achiziţionează aplicaţiile respective.

(9) ADR asigură interconectarea la nivel de SaaS la serviciile specifice Cloudului privat guvernamental pentru entităţile găzduite şi conectate în cloud.

ART. 5

**Atribuţiile STS**

(1) Infrastructura de bază a Cloudului privat guvernamental este asigurată de STS.

(2) STS asigură implementarea, administrarea tehnică şi operaţională, securitatea cibernetică, mentenanţa, precum şi dezvoltarea ulterioară a serviciilor specifice Cloudului privat guvernamental, prevăzute la art. 2 lit. k), l) şi q).

(3) STS asigură accesul securizat, conectivitatea şi interconectarea la serviciile specifice Cloudului privat guvernamental pentru entităţile găzduite sau interconectate în cloud.

(4) STS asigură securitatea cibernetică a Cloudului privat guvernamental prin prevenirea şi contracararea atacurilor cibernetice, pentru serviciile prevăzute la art. 2 lit. k), l) şi q), inclusiv a atacurilor de tip DDoS îndreptate împotriva Cloudului privat guvernamental, în conformitate cu atribuţiile prevăzute prin actele normative în vigoare.

(5) STS asigură securitatea cibernetică a serviciilor şi sistemelor informatice proprii din Cloudul privat guvernamental, prin prevenirea şi contracararea atacurilor cibernetice.

(6) Pentru îndeplinirea rolului prevăzut la alin. (1), STS achiziţionează serviciile de proiectare şi asistenţă tehnică, lucrările de investiţii, inclusiv instalaţiile, dotările şi echipamentele tehnologice aferente clădirii, precum şi echipamentele hardware, programele software, aplicaţiile informatice şi licenţele necesare realizării, dezvoltării ulterioare, mentenanţei şi funcţionării serviciilor prevăzute la art. 2 lit. k), l) şi q) din Cloudul privat guvernamental.

ART. 6

**Atribuţiile SRI**

(1) SRI asigură securitatea cibernetică a Cloudului privat guvernamental prin cunoaşterea, prevenirea şi contracararea atacurilor, ameninţărilor, riscurilor şi vulnerabilităţilor cibernetice, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor Cloudului privat guvernamental prevăzute la art. 2 lit. u) şi a entităţilor găzduite.

(2) SRI cooperează cu STS, conform competenţelor fiecărei instituţii, pentru cunoaşterea, prevenirea şi contracararea atacurilor cibernetice complexe, de tip APT, îndreptate împotriva serviciilor specifice Cloudului privat guvernamental prevăzute la art. 2 lit. l) şi q), prin schimbul nemijlocit şi automat al informaţiilor referitoare la incidentele de securitate, fără a transfera date de conţinut.

(3) Măsurile prevăzute la alin. (1) şi (2) nu se aplică situaţiilor prevăzute la art. 5 alin. (5).

(4) SRI asigură implementarea, administrarea tehnică şi operaţională, mentenanţa, precum şi dezvoltarea ulterioară a serviciilor de securitate cibernetică ale Cloudului privat guvernamental, prevăzute la alin. (1).

ART. 7

**Securitatea cibernetică a Cloudului privat guvernamental**

(1) În cazul sistemelor informatice interconectate cu Cloudul privat guvernamental aparţinând autorităţilor din sistemul naţional de apărare, ordine publică şi securitate naţională, implementarea, administrarea tehnică şi operaţională, mentenanţa şi dezvoltarea ulterioară a serviciilor de securitate cibernetică se realizează de către structurile responsabile cu securitatea cibernetică a acestor autorităţi, precum şi în colaborare cu STS şi SRI în ceea ce priveşte interconectarea cu Cloudul privat guvernamental.

(2) În vederea îndeplinirii atribuţiilor prevăzute la art. 5 şi 6 şi la alin. (1), STS şi SRI asigură echipamentele hardware, programele software, aplicaţiile informatice şi licenţele necesare în acest scop, conform competenţelor prevăzute prin prezenta ordonanţă de urgenţă.

ART. 8

**Politica de cloud first**

(1) MCID, împreună cu ADR, după consultarea mediului privat conform legislaţiei privind dialogul social şi transparenţa în administraţia publică, propune politica de cloud first, în vederea aprobării acesteia prin hotărârea prevăzută la art. 1 alin. (4).

(2) Entităţile publice migrează aplicaţiile şi sistemele informatice sau, după caz, interconectează sistemele informatice în Platformă, în conformitate cu prevederile hotărârilor de Guvern prevăzute la art. 3 alin. (2) şi (4).

ART. 9

**Prelucrarea datelor cu caracter personal**

(1) În procesul de dezvoltare, implementare, administrare şi asigurare a securităţii cibernetice a Cloudului privat guvernamental, autorităţile şi instituţiile publice prevăzute la art. 1 alin. (6) prelucrează date cu caracter personal, în calitate de operator sau persoană împuternicită de către entităţile găzduite sau interconectate, după caz, în conformitate cu responsabilităţile prevăzute la art. 3 - 7, cu respectarea reglementărilor legale aplicabile în domeniul protecţiei datelor cu caracter personal.

(2) Prelucrarea datelor cu caracter personal prin intermediul sistemelor informatice găzduite în Platformă se realizează de către reprezentanţii autorităţilor şi instituţiilor publice, cu respectarea reglementărilor legale aplicabile în domeniul protecţiei datelor cu caracter personal.

(3) Autorităţile şi instituţiile publice prevăzute la alin. (1) şi (2) respectă regimurile de acces la date prevăzute la nivel naţional şi european şi acordă angajaţilor şi reprezentanţilor lor drepturile de acces la date prelucrate prin intermediul sistemelor informatice găzduite în Platformă, după caz, în vederea îndeplinirii prevederilor prezentei ordonanţe de urgenţă, cu respectarea prevederilor Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), cu modificările ulterioare, Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, cu modificările şi completările ulterioare, Legii nr. 363/2018 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date, precum şi ale Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor).

(4) Prevederile alin. (3) sunt aplicabile şi în ceea ce priveşte raporturile autorităţilor şi instituţiilor publice prevăzute la alin. (1) şi (2) cu părţi terţe, în vederea asigurării dezvoltării mentenanţei şi dezvoltării ulterioare a infrastructurii şi serviciilor Platformei.

(5) În aplicarea prevederilor alin. (3) şi (4), autorităţile şi instituţiile publice prevăzute la alin. (1) şi (2) au obligaţia să se asigure că datele prelucrate sunt protejate în mod adecvat împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin măsuri de asigurare a confidenţialităţii, integrităţii şi disponibilităţii acestora.

(6) Prezenta ordonanţă de urgenţă respectă drepturile fundamentale şi principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, inclusiv dreptul la respectarea vieţii private şi de familie, dreptul la protecţia datelor cu caracter personal, dreptul la proprietate şi integrarea persoanelor cu dizabilităţi, astfel încât nicio prevedere din prezentul act normativ nu trebuie să facă obiectul unei interpretări sau puneri în aplicare care nu este conformă cu Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale a Consiliului Europei.

ART. 10

**Proprietatea, jurnalizarea şi auditul Cloudului privat guvernamental**

(1) Infrastructura de bază a Cloudului privat guvernamental, infrastructura ca serviciu (IaaS) şi platforma ca serviciu (PaaS), prevăzute la art. 2 lit. k), l) şi q), sunt proprietate privată a statului şi în administrarea STS, care le achiziţionează conform prevederilor legale în vigoare privind achiziţiile publice.

(2) Softul dezvoltat şi particularizat pentru entităţile găzduite sau care urmează a fi găzduite în Cloudul privat guvernamental, achiziţionat conform prevederilor legale în vigoare privind achiziţiile publice, prin intermediul unor proceduri competitive, transparente, necondiţionate şi nediscriminatorii, este proprietatea privată a statului şi în administrarea ADR, în condiţiile prevăzute la art. 12 din Ordonanţa de urgenţă a Guvernului nr. 41/2016 privind stabilirea unor măsuri de simplificare la nivelul administraţiei publice centrale şi pentru modificarea şi completarea unor acte normative, aprobată cu modificări prin Legea nr. 179/2017, cu completările ulterioare.

(3) Softul aferent migrării în Cloudul privat guvernamental a sistemelor informatice şi software ca serviciu (SaaS), prevăzute la art. 2 lit. o) şi u), sunt proprietate privată a statului şi în administrarea ADR, care le achiziţionează conform prevederilor legale în vigoare privind achiziţiile publice, prin intermediul unor proceduri competitive, transparente, necondiţionate şi nediscriminatorii.

(4) Componentele aferente securităţii cibernetice sunt proprietate privată a statului şi sunt achiziţionate şi administrate de STS, respectiv SRI, potrivit competenţelor proprii prevăzute la art. 5 - 7, conform prevederilor legale în vigoare privind achiziţiile publice, prin intermediul unor proceduri competitive, transparente, necondiţionate şi nediscriminatorii.

(5) Privitor la dispoziţiile alin. (1) - (4), în situaţia în care achiziţionarea drepturilor de proprietate nu este posibilă, se asigură cel puţin achiziţionarea drepturilor de utilizare.

(6) Administratorii serviciilor furnizate la nivel de IaaS, PaaS şi SaaS, precum şi administratorii de securitate cibernetică asigură jurnalizarea evenimentelor şi accesului la datele entităţilor găzduite în Cloudul privat guvernamental, în scopul efectuării unor activităţi de audit de conformitate periodice pe linia protecţiei, calităţii, securităţii şi trasabilităţii datelor, în vederea asigurării transparenţei utilizării acestora.

(7) ADR asigură dezvoltarea unei aplicaţii de jurnalizare şi notificare a activităţii de prelucrare a datelor cu caracter personal ale persoanelor vizate, destinată utilizatorilor finali ai serviciilor publice furnizate de entităţile publice găzduite în Cloudul privat guvernamental.

(8) Normele metodologice privind jurnalizarea evenimentelor şi accesului la datele autorităţilor şi instituţiilor publice găzduite în Cloudul privat guvernamental se aprobă prin hotărârea prevăzută la art. 3 alin. (2).

(9) MCID dispune, cel puţin anual sau ori de câte ori este necesar, efectuarea unor activităţi de audit de conformitate pe linia protecţiei, calităţii, securităţii şi trasabilităţii pentru Platformă sau, după caz, pentru anumite componente ale acesteia, finanţate prin bugetul acestuia.

(10) Autorităţile prevăzute la art. 1 alin. (6) întocmesc până la finalul primului trimestru al anului în curs un raport comun cu privire la activitatea de realizare şi administrare a Cloudului privat guvernamental pentru anul precedent, pe care îl comunică comisiilor pentru tehnologia informaţiei şi comunicaţiilor ale Camerei Deputaţilor şi Senatului.

CAPITOLUL III

**Principalele drepturi şi obligaţii ale entităţilor găzduite în Cloudul privat guvernamental**

ART. 11

**Drepturile entităţilor găzduite în Cloudul privat guvernamental**

Autorităţile şi instituţiile publice găzduite în Cloudul privat guvernamental au următoarele drepturi:

a) solicită sau eliberează resurse din Cloudul privat guvernamental, în conformitate cu necesităţile proprii;

b) achiziţionează servicii de analiză de procese informaţionale, dezvoltare software şi suport în vederea testării sistemelor informatice din Cloudul privat guvernamental;

c) beneficiază de consiliere tehnică de specialitate din partea instituţiilor participante la implementarea Cloudului privat guvernamental în organizarea utilizării eficiente a serviciilor acestuia şi a prestării serviciilor sale către persoane fizice şi juridice;

d) pot solicita activităţi de audit de conformitate pe linia calităţii, securităţii şi trasabilităţii pentru datele proprii, finanţate prin bugetele acestora.

ART. 12

**Obligaţiile entităţilor găzduite în Cloudul privat guvernamental**

(1) Autorităţile şi instituţiile publice găzduite în Cloudul privat guvernamental au următoarele obligaţii:

a) prelucrează datele cu caracter personal în procesul de utilizare şi furnizare a serviciilor publice prin intermediul Cloudului privat guvernamental, cu respectarea reglementărilor legale aplicabile în domeniul protecţiei datelor cu caracter personal, şi se asigură de respectarea principiilor "confidenţialităţii prin concepţie" şi "securităţii prin concepţie" asupra sistemelor informatice migrate în Cloudul privat guvernamental;

b) stabilesc modul şi perioada de prelucrare a datelor cu caracter personal, modul de realizare a accesului la aceste date, precum şi modul de punere în aplicare a prevederilor art. 12 - 20 din Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE în raport cu utilizarea şi furnizarea serviciilor publice prin intermediul Cloudului privat guvernamental;

c) întreprind toate măsurile necesare de pregătire a infrastructurii proprii pentru utilizarea eficientă a serviciilor solicitate din Cloudul privat guvernamental;

d) desemnează persoana de contact responsabilă în relaţia cu ADR, în calitate de administrator operaţional al Cloudului privat guvernamental;

e) anunţă imediat administratorul operaţional despre abaterile constatate de la nivelul agreat de servicii sau despre orice alt eveniment observat care poate compromite buna funcţionare a serviciilor.

(2) În termen de 30 de zile de la data solicitării ADR, autorităţile şi instituţiile publice centrale care furnizează servicii publice electronice, cu excepţia celor prevăzute la art. 1 alin. (12), au obligaţia să transmită informaţiile relevante privind sistemele informatice ce vor fi migrate în Cloudul privat guvernamental.

CAPITOLUL IV

**Organizarea şi funcţionarea infrastructurilor informatice de tip cloud în Platformă, altele decât Cloudul privat guvernamental**

ART. 13

**Politici generale şi cadru juridic**

(1) Autorităţile şi instituţiile publice pot dezvolta infrastructuri informatice de tip cloud sau pot utiliza servicii de tip cloud furnizate de entităţi private, necesare funcţionării serviciilor publice pe care le gestionează, în condiţiile în care nu sunt găzduite, respectiv dezvoltate în Cloudul privat guvernamental.

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

a) infrastructura de bază a cloudului;

b) infrastructura ca serviciu (IaaS);

c) platforma ca serviciu (PaaS);

d) software ca serviciu (SaaS).

(3) Infrastructurile informatice de tip cloud menţionate la alin. (1) trebuie realizate şi implementate astfel încât să asigure următoarele categorii de facilităţi:

a) furnizarea continuă, în limita nivelurilor agreate de către utilizatorii de servicii de tip cloud, a serviciilor de accesare a bazelor de date şi 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 diverşi furnizori de servicii de tip cloud pentru a permite migrarea bazelor de date şi a evita captivitatea utilizatorilor de servicii de tip cloud;

d) respectarea principiilor şi prevederilor privind prelucrarea datelor cu caracter personal, precum şi asigurarea controlului confidenţialităţii, integrităţii şi disponibilităţii datelor prin intermediul instrumentelor specifice serviciilor de tip cloud;

e) securitatea cibernetică a datelor pentru a asigura rezilienţa la atacurile cibernetice.

ART. 14

**Cerinţe privind rezilienţa**

(1) Fiecare serviciu de cloud este asigurat de cel puţin două noduri de date organizate sub forma centrelor de date, pentru a asigura furnizarea serviciilor de cloud în mod rezilient.

(2) Centrele de date prevăzute la alin. (1) pot găzdui servicii de tip cloud privat, public sau hibrid, în acord cu nevoile de dezvoltare ale investitorilor în infrastructuri informatice de tip cloud.

ART. 15

**Reglementare cu privire la guvernanţă**

Între furnizorul şi utilizatorul de servicii de tip cloud şi utilizatorul de servicii de tip cloud prevăzuţi la art. 13 alin. (1) se încheie o convenţie de administrare a serviciilor de tip cloud, care cuprinde drepturile şi obligaţiile aferente utilizării acestora în Platformă.

ART. 16

**Certificarea de securitate**

(1) Standardele şi criteriile pentru selecţia, certificarea şi utilizarea serviciilor de tip cloud privat, altele decât Cloudul privat guvernamental, şi ale serviciilor de tip cloud public furnizate în regim comercial se stabilesc prin ordin al ministrului cercetării, inovării şi digitalizării, cu consultarea prealabilă a ADR, STS şi SRI, care se publică în Monitorul Oficial al României, Partea I.

(2) Procedurile de certificare a securităţii serviciilor de tip cloud public pentru utilizare de către autorităţile şi instituţiile publice se stabilesc prin ordin al ministrului cercetării, inovării şi digitalizării, cu consultarea prealabilă a SRI şi a Directoratului Naţional de Securitate Cibernetică, cu respectarea prevederilor Legii nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice şi de comunicaţii de interes naţional şi condiţiile implementării reţelelor 5G.

CAPITOLUL V

**Dispoziţii finale**

ART. 17

**Dispoziţii finale privind implementarea Cloudului privat guvernamental**

(1) Finanţarea cheltuielilor pentru activităţile ce revin ADR, STS şi SRI pentru implementarea Cloudului privat guvernamental se asigură prin PNRR şi de la bugetul de stat sau din alte surse de finanţare legal constituite.

(2) Finanţarea cheltuielilor pentru activităţile ce revin altor autorităţi în vederea îndeplinirii atribuţiilor ce le revin potrivit prezentei ordonanţe de urgenţă se asigură prin PNRR, de la bugetul de stat, prin fonduri externe nerambursabile sau din alte surse de finanţare legal constituite.

(3) Competenţa de certificare a îndeplinirii corespunzătoare a condiţiilor specifice investiţiilor aferente Cloudului guvernamental, prevăzute în PNRR, integrate în cadrul Studiului de fezabilitate şi al Proiectului tehnic şi ulterior, al caietelor de sarcini aferente achiziţiilor publice, aparţine Comitetului tehnico-economic pentru societatea informaţională, conform Hotărârii Guvernului nr. 941/2013 privind organizarea şi funcţionarea Comitetului tehnico-economic pentru societatea informaţională, cu modificările şi completările ulterioare.

(4) Pentru realizarea componentelor Cloudului privat guvernamental, respectiv IaaS, PaaS, SaaS, securitate cibernetică şi migrare a bazelor de date, ADR, STS şi SRI organizează proceduri de achiziţie publică, în conformitate cu legislaţia în vigoare în domeniul achiziţiilor publice.

(5) ADR, STS şi SRI evaluează periodic resursele necesare Cloudului privat guvernamental pentru a satisface nevoile entităţilor găzduite şi comunică MCID planificarea capacităţii, în colaborare cu entităţile găzduite, pentru a estima nivelul cererii şi pentru a pune în aplicare investiţiile sau măsurile suplimentare necesare, pe domeniile de competenţă.

(6) Prevederile capitolului IV nu se aplică infrastructurilor de tip cloud dezvoltate de instituţiile din sistemul naţional de apărare, ordine publică şi securitate naţională.

(7) În cazul sistemelor informatice dezvoltate în cadrul unor proiecte finanţate din fonduri externe nerambursabile, prevederile prezentei ordonanţe de urgenţă se aplică numai în măsura în care acestea nu aduc atingere condiţiilor prevăzute în contractele de finanţare, în special în ceea ce priveşte eligibilitatea cheltuielilor efectuate şi sustenabilitatea acestor proiecte.

---------------