INFORMARE

ACTE NORMATIVE ADOPTATE CU INCIDENȚĂ ÎN MATERIA

DREPTURILOR CETĂȚENILOR

28 iunie 2022

√ Ordonanța de urgență nr. 89/2022 privind unele măsuri pentru adoptarea sistemului de guvernanță a Platformei de cloud guvernamental, precum și pentru stabilirea cadrului legal de organizare și funcționare a infrastructurilor informatice și a serviciilor de tip cloud în procesul de transformare digitală, publicată în M.Of. nr. 638 din 28 iunie 2022

CAPITOLUL I

Dispoziții generale

ARTICOLUL 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 autoritățile și instituțiile publice centrale și locale se înființează Platforma, constituită dintr-o componentă de cloud privat, denumită în continuare Cloudul privat guvernamental, și din resurse și servicii publice certificate din alte tipuri de cloud publice sau private, în condițiile prevăzute la art. 16.

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

(4) În termen de maximum 90 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență, prin hotărâre a Guvernului, 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, se aprobă Ghidul de guvernanță a platformei de cloud guvernamental.

(5) Cloudul privat guvernamental este administrat operațional de ADR și constă într-un ansamblu de resurse informatice, de comunicații și de securitate cibernetică, aflate în

proprietatea statului român, interconectat la nivel de servicii cu clouduri publice și/sau cu clouduri private.

(6) Autoritățile responsabile de realizarea Cloudului privat guvernamental sunt MCID și ADR, în colaborare cu STS și SRI, conform competențelor prevăzute de prezenta ordonanță de urgență.

(7) Începând cu data intrării în vigoare a hotărârii prevăzute la alin. (4), sistemele informatice utilizate de către autoritățile și instituțiile publice centrale sunt dezvoltate astfel încât să fie apte pentru migrarea în Cloudul privat guvernamental sau interconectate cu acesta.

(8) Autoritățile administrației publice centrale au obligația de a migra serviciile publice electronice în Cloudul privat guvernamental.

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

(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 și digitalizării, al președintelui ADR, al directorului STS și al directorului SRI, care se publică în Monitorul Oficial al României, Partea I.

(11) Activitățile de informare publică cu privire la acțiunile care vizează Cloudul 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 Cloudul privat guvernamental, respectiv a sistemelor informatice pentru care autoritățile respective doresc în mod expres să utilizeze resursele și serviciile acestuia.

ARTICOLUL 2

Definiții

În sensul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarele semnificații:

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 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 cloudului înaintea tuturor celorlalte tehnologii, fie că este un proiect nou care implică soluții informatice și de comunicații 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 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 urmărește indisponibilizarea, blocarea sau epuizarea resurselor unui sistem informatic, rețea sau componentă a acesteia;

j) ghid de guvernanță a platformei de cloud guvernamental — standarde, reguli, orientări și caracteristici pentru activități și 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;

k) infrastructura de bază a Cloudului privat guvernamental — clădirile, instalațiile, dotările și echipamentele tehnologice aferente, echipamentele informatice și de comunicații, 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 cloudului;

m) interconectare cu Cloudul 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 Cloudul 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 autoritățile și instituțiile publice 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 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 a Cloudului privat guvernamental — stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor

în format electronic aferente resurselor și serviciilor publice sau private din spațiul cibernetic al Cloudului 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 de tip cloud computing. Aplicațiile sunt accesibile pe baza unor drepturi de acces, prin intermediul unui navigator internet sau al unei aplicații informatice 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, ce cuprinde soluții oferite de tehnologia informației;

w) vulnerabilitate în spațiul cibernetic — slăbiciune în proiectarea și implementarea rețelelor și sistemelor informatice sau a măsurilor de securitate aferente, care poate fi exploatată de către o amenințare cibernetică.

CAPITOLUL II

Atribuții și responsabilități privind realizarea și operarea Platformei de cloud guvernamental

ARTICOLUL 3

Atribuțiile MCID

(1) Politicile, strategia, standardele și criteriile de implementare, operare, utilizare, întreținere și dezvoltare ulterioară a Platformei se stabilesc prin hotărârea 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 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 și operaționale privind implementarea, operarea, mentenanța și dezvoltarea ulterioară a Cloudului 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, cu consultarea prealabilă a ADR, STS și SRI, în termen de maximum 90 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență.

(4) Planul pentru migrarea și integrarea în Cloudul privat guvernamental a sistemelor informatice și a serviciilor publice electronice ale instituțiilor și autorităților aparținând administrației publice, precum și lista autorităților și instituțiilor publice ale căror sisteme informatice și servicii publice electronice migrează în Cloudul privat guvernamental se stabilesc prin hotărâre de guvern inițiată de MCID, la propunerea ADR, în termen de maximum 90 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență.

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

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

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

(8) În termen de maximum 90 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență, MCID, la propunerea ADR, cu sprijinul STS și SRI, propune spre adoptare, prin hotărâre de Guvern, criteriile generale de asigurare a confidențialității, securității, interoperabilității, adaptării la standarde tehnice și semantice, respectiv a performanței aplicațiilor de tip SaaS găzduite în Platformă, prin intermediul unui marketplace, inclusiv a aplicațiilor dezvoltate de mediul privat, prin intermediul catalogului definit la art. 2 lit. n).

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

ARTICOLUL 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 Cloudul privat guvernamental a sistemelor informatice și a serviciilor publice electronice ale autorităților și instituțiilor publice aparținând administrației publice.

(3) ADR asigură implementarea, administrarea tehnică și operațională, mentenanța, precum și dezvoltarea ulterioară pentru serviciile SaaS specifice Cloudului privat guvernamental, inclusiv asigurarea, prin acorduri-cadru, conform legislației achizițiilor publice, a licențelor specifice serviciilor necesare migrării în Cloudul privat guvernamental a sistemelor informatice și serviciilor publice electronice.

(4) Migrarea, integrarea și interconectarea în Cloudul privat guvernamental a sistemelor informatice ale autorităților și instituțiilor 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 și instituție publică notificată de către ADR în vederea migrării, inclusiv cele prevăzute la art. 1 alin. (12).

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

(6) Comitetul tehnico-economic pentru societatea informațională analizează solicitarea prevăzută la alin. (5) și 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 achiziționează programele software, aplicațiile informatice și licențele necesare, precum și serviciile de analiză, proiectare și dezvoltare software, după caz.

(8) ADR gestionează marketplace-ul prevăzut la art. 2 lit. n), 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 Cloudului privat guvernamental pentru entitățile găzduite și conectate în cloud.

ARTICOLUL 5

Atribuțiile STS

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

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

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

(4) STS asigură securitatea cibernetică a Cloudului 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 Cloudului privat guvernamental, în conformitate cu atribuțiile prevăzute prin actele normative în vigoare.

(5) STS asigură securitatea cibernetică a serviciilor și sistemelor informatice proprii din Cloudul 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 Cloudul privat guvernamental.

ARTICOLUL 6

Atribuțiile SRI

(1) SRI asigură securitatea cibernetică a Cloudului privat guvernamental prin cunoașterea, prevenirea și contracararea atacurilor, amenințărilor, riscurilor și vulnerabilităților cibernetice, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor Cloudului privat guvernamental prevăzute 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 Cloudului privat guvernamental prevăzute la art. 2 lit. l) și q), prin schimbul nemijlocit și automat al informațiilor referitoare la incidentele de securitate, fără a transfera 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 Cloudului privat guvernamental, prevăzute la alin. (1).

ARTICOLUL 7

Securitatea cibernetică a Cloudului privat guvernamental

(1) În cazul sistemelor informatice interconectate cu Cloudul privat guvernamental aparținând autorităților din sistemul național de apărare, ordine publică și securitate națională, implementarea, administrarea tehnică și operațională, mentenanța și dezvoltarea ulterioară a serviciilor de securitate cibernetică se realizează de către structurile responsabile cu securitatea cibernetică a acestor autorități, precum și în colaborare cu STS și SRI în ceea ce privește interconectarea cu Cloudul privat guvernamental.

(2) În vederea îndeplinirii atribuțiilor prevăzute la art. 5 și 6 și la alin. (1), STS și SRI asigură echipamentele hardware, programele software, aplicațiile informatice și licențele necesare în acest scop, conform competențelor prevăzute prin prezenta ordonanță de urgență.

ARTICOLUL 8

Politica de cloud first

(1) MCID, împreună cu ADR, după consultarea mediului privat conform legislației privind dialogul social și transparența în administrația publică, propune politica de cloud first, în vederea aprobării acesteia prin hotărârea prevăzută la art. 1 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 prevăzute la art. 3 alin. (2) și (4).

ARTICOLUL 9

Prelucrarea datelor cu caracter personal

(1) În procesul de dezvoltare, implementare, administrare și asigurare a securității cibernetice a Cloudului privat guvernamental, autoritățile și instituțiile publice prevăzute la art. 1 alin. (6) prelucrează date cu caracter personal, în calitate de operator sau persoană împuternicită de către entitățile găzduite sau interconectate, după caz, în conformitate cu

responsabilitățile prevăzute la art. 3—7, cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal.

(2) Prelucrarea datelor cu caracter personal prin intermediul sistemelor informatice găzduite în Platformă se realizează de către reprezentanții autorităților și instituțiilor publice, cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal.

(3) Autoritățile și instituțiile publice prevăzute la alin. (1) și (2) respectă regimurile de acces la date prevăzute la nivel național și european și acordă angajaților și reprezentanților lor drepturile de acces la date prelucrate prin intermediul sistemelor informatice găzduite în Platformă, după caz, în vederea îndeplinirii prevederilor prezentei ordonanțe de urgență, cu respectarea prevederilor Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările ulterioare, Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare, Legii nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date, precum și ale Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

(4) Prevederile alin. (3) sunt aplicabile și în ceea ce privește raporturile autorităților și instituțiilor publice prevăzute la alin. (1) și (2) cu părți terțe, în vederea asigurării dezvoltării mentenanței și dezvoltării ulterioare a infrastructurii și serviciilor Platformei.

(5) În aplicarea prevederilor alin. (3) și (4), autoritățile și instituțiile publice prevăzute la alin. (1) și (2) au obligația să se asigure că datele prelucrate sunt protejate în mod adecvat împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a

deteriorării accidentale, prin măsuri de asigurare a confidențialității, integrității și disponibilității acestora.

(6) Prezenta ordonanță de urgență respectă drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, inclusiv dreptul la respectarea vieții private și de familie, dreptul la protecția datelor cu caracter personal, dreptul la proprietate și integrarea persoanelor cu dizabilități, astfel încât nicio prevedere din prezentul act normativ nu trebuie să facă obiectul unei interpretări sau puneri în aplicare care nu este conformă cu Convenția pentru apărarea drepturilor omului și a libertăților fundamentale a Consiliului Europei.

ARTICOLUL 10

Proprietatea, jurnalizarea

și auditul Cloudului privat guvernamental

(1) Infrastructura de bază a Cloudului 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 Cloudul privat guvernamental, achiziționat conform prevederilor legale în vigoare privind achizițiile publice, prin intermediul unor proceduri competitive, transparente, necondiționate și nediscriminatorii, este proprietatea privată a statului și în administrarea ADR, în condițiile prevăzute la art. 12 din Ordonanța de urgență a Guvernului nr. 41/2016 privind stabilirea unor măsuri de simplificare la nivelul administrației publice centrale și pentru modificarea și 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 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, prin intermediul unor proceduri competitive, transparente, necondiționate și nediscriminatorii.

(4) Componentele aferente securității cibernetice sunt proprietate privată a statului și sunt achiziționate și administrate de STS, respectiv SRI, potrivit competențelor proprii

prevăzute la art. 5—7, conform prevederilor legale în vigoare privind achizițiile publice, prin intermediul unor proceduri competitive, transparente, necondiționate și nediscriminatorii

(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 Cloudul privat guvernamental, în scopul efectuării unor activități de audit 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 Cloudul privat guvernamental.

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

(9) MCID dispune, cel puțin anual sau ori de câte ori este necesar, 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 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 și administrare a Cloudului 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 Cloudul privat guvernamental

ARTICOLUL 11

Drepturile entităților găzduite în Cloudul privat guvernamental

Autoritățile și instituțiile publice găzduite în Cloudul privat guvernamental au următoarele drepturi:

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

b) achiziționează servicii de analiză de procese informaționale, dezvoltare software și suport în vederea testării sistemelor informatice din Cloudul privat guvernamental;

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

d) pot solicita activități de audit de conformitate pe linia calității, securității și trasabilității pentru datele proprii, finanțate prin bugetele acestora.

ARTICOLUL 12

Obligațiile entităților găzduite în Cloudul privat guvernamental

(1) Autoritățile și instituțiile publice găzduite în Cloudul privat guvernamental au următoarele obligații:

a) prelucrează datele cu caracter personal în procesul de utilizare și furnizare a serviciilor publice prin intermediul Cloudului privat guvernamental, cu respectarea reglementărilor legale aplicabile în domeniul protecției datelor cu caracter personal, și se asigură de respectarea principiilor „confidențialității prin concepție” și „securității prin concepție” asupra sistemelor informatice migrate în Cloudul privat guvernamental;

b) 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 (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE în raport cu utilizarea și 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 relația cu ADR, în calitate de administrator operațional al Cloudului privat guvernamental;

e) 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.

(2) În termen de 30 de zile de la data solicitării ADR, autoritățile și instituțiile publice centrale care furnizează servicii publice electronice, cu excepția celor prevăzute la art. 1 alin.

(12), au obligația să transmită informațiile relevante privind sistemele informatice ce vor fi migrate în Cloudul privat guvernamental.

CAPITOLUL IV

Organizarea și funcționarea infrastructurilor informatice de tip cloud în Platformă, altele decât Cloudul privat guvernamental

ARTICOLUL 13

Politici generale și cadru juridic

(1) Autoritățile și instituțiile 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 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 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) respectarea principiilor și prevederilor privind prelucrarea datelor cu caracter personal, precum și asigurarea controlului confidențialității, integrității și disponibilității datelor prin intermediul instrumentelor specifice serviciilor de tip cloud;

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

ARTICOLUL 14

Cerințe privind reziliența

(1) Fiecare serviciu de cloud este asigurat de cel puțin 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.

ARTICOLUL 15

Reglementare cu privire la guvernanță

Între furnizorul și utilizatorul 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 acestora în Platformă.

ARTICOLUL 16

Certificarea de securitate

(1) Standardele și criteriile pentru selecția, certificarea și utilizarea serviciilor de tip cloud privat, altele decât Cloudul 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, care se publică în Monitorul Oficial al României, Partea I.

(2) Procedurile de certificare a securității serviciilor de tip cloud public pentru utilizare de către autoritățile și instituțiile publice se stabilesc prin ordin al ministrului cercetării, inovării și digitalizării, cu consultarea prealabilă a SRI și a Directoratului Național de Securitate Cibernetică, 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

ARTICOLUL 17

Dispoziții finale privind implementarea Cloudului privat guvernamental

(1) Finanțarea cheltuielilor pentru activitățile ce revin ADR, STS și SRI pentru implementarea Cloudului privat guvernamental se asigură prin PNRR și de la bugetul de stat sau din alte surse de finanțare legal constituite.

(2) Finanțarea cheltuielilor pentru activitățile ce revin altor autorități în vederea îndeplinirii atribuțiilor ce le revin potrivit prezentei ordonanțe de urgență se asigură prin PNRR, de la bugetul de stat, prin fonduri externe nerambursabile sau din alte surse de finanțare legal constituite.

(3) Competența de certificare a îndeplinirii corespunzătoare a condițiilor specifice investițiilor aferente Cloudului 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 tehnicoeconomic pentru societatea informațională, conform Hotărârii Guvernului nr. 941/2013 privind organizarea și funcționarea Comitetului tehnico-economic pentru societatea informațională, cu modificările și completările ulterioare.

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

(5) ADR, STS și SRI evaluează periodic resursele necesare Cloudului 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.

(6) Prevederile capitolului IV nu se aplică infrastructurilor de tip cloud dezvoltate de instituțiile din sistemul național de apărare, ordine publică și securitate națională.

(7) În cazul sistemelor informatice dezvoltate în cadrul unor proiecte finanțate din fonduri externe nerambursabile, prevederile prezentei ordonanțe de urgență se aplică numai în măsura în care acestea nu aduc atingere condițiilor prevăzute în contractele de finanțare, în special în ceea ce privește eligibilitatea cheltuielilor efectuate și sustenabilitatea acestor proiecte.