GUVERNUL ROMÂNIEI

HOTĂRÂRE
privind guvernanța Platformei de Cloud Guvernamental

În temeiul art. 108 din Constituția României, republicată, și al art. 1 alin. (4), art. 3 alin. (1) și (2), art. 3 alin. (3), (4) și (8), art. 8 alin. (1) și al art. 10 alin. (8) din Ordonanţa de urgenţă nr. 89/2022 privind înființarea, administrarea şi dezvoltarea infrastructurilor şi serviciilor informatice de tip cloud, utilizate de autorităţile şi instituţiile publice,

Guvernul României adoptă prezenta hotărâre.

Capitolul I

Dispoziții generale

Art. 1.

Prezenta hotărâre are ca obiect stabilirea unor standarde, reguli, obligații necesare activităților operaționale, procedurale și tehnice de organizare și funcționare a infrastructurilor informatice și a serviciilor de tip cloud, respectiv:

a) ghidul de guvernanță a platformei de cloud guvernamental;
b) politica, strategia, criteriile tehnice și operaționale privind implementarea, operarea, mentenanța și dezvoltarea ulterioară a Platformei Cloud Guvernamental, denumit în continuare Platforma, precum și interconectarea sistemelor informatice;
c) cadrul de management și stocare a datelor în Platformă și stabilirea categoriilor de date prelucrate și/sau găzduite în Platformă, inclusiv în componenta de cloud privat

guvernamental, denumită în continuare CPG, respectiv resursele publice sau private disponibile în Platformă;

d) planul pentru migrarea și integrarea în Platformă a aplicațiilor 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 Platformă;

e) cadrul de asigurare a confidențialității, securității, interoperabilității, adaptării la standarde tehnice și semantice, respectiv a performanței aplicațiilor de tip SaaS, Iaas, Paas găzduite în Platformă, prin intermediul unui Marketplace, inclusiv Normele metodologice de jurnalizare a evenimentelor și accesului la datele autorităților și instituțiilor publice găzduite în Platformă;

f) politica cloud first.

Art. 2.

(1) În sensul prezentei hotărâri, termenii și expresiile de mai jos au următoarele semnificații:

a) administrator - autoritate și instituție publică responsabilă de gestionarea operațională, procedurală, tehnică și/sau de securitate cibernetică, după caz, a unui set de resurse din cadrul Platformei de Cloud Guvernamental;

b) agregator de servicii de cloud - orice furnizor de servicii de cloud care cumulează și combină mai multe tipuri de servicii în unul sau mai multe pachete combinate;

c) application programming interface (API) - interfețele de programare a aplicației (API) - set de funcții, proceduri, definiții și protocoale pentru comunicarea dintre mașini și schimbul fără sincope de date.

d) catalog de servicii de cloud - lista completă a serviciilor de cloud și a aplicațiilor furnizate prin intermediul componentei marketplace, dezvoltate de ADR, autoritățile și instituțiile publice, precum și de terți;

e) centru de date - un spațiu dedicat într-o clădire specializată pentru a găzdui sisteme informatice și componente asociate, cum ar fi sistemele de telecomunicații și de tehnologia informației;

f) cloud computing - model care permite accesul prin rețea la un grup scalabil și elastic de resurse fizice sau virtuale (exemplele de resurse includ servere, sisteme de operare, rețele, software, aplicații și echipamente de stocare) care pot fi partajate cu furnizare și administrare la cerere în sistem self-service;

g) cloud ready - aplicații dezvoltate având la bază principiile de funcționare într-un cloud public sau privat, respectiv sub forma de servicii logice decuplate în instanțe de tip mașina virtuală și/sau container, putând astfel funcționa atât în infrastructurile proprii ale utilizatorilor de servicii de cloud, cât și în infrastructurile de cloud public sau privat în urma unor procese de migrare transparentă;

h) cloud nativ - aplicații dezvoltate având la bază principiile de funcționare într-un cloud public sau privat, respectiv, dar nelimitat la, sub forma de servicii logice decuplate în instanțe de tip container, bazate pe microservicii, API-uri și micro segmentare a comunicațiilor, beneficiind de resursele de procesare și comunicație flexibile, elastice, distribuite și reziliente ale infrastructurilor de cloud public sau privat;
i) date deschise - date în format prelucrabil automat ce pot fi utilizate în mod liber, reutilizate și redistribuite de către oricine în orice scop;
j) date cu valoare ridicată - sunt date a căror accesare, alterare, diseminare neautorizată sau indisponibilitate a accesului la acestea produc efecte negative în livrarea serviciilor economice, de sănătate și siguranță publică, sau a altor servicii esențiale ale statului care aduc perturbări de natură socio-economică;
k) date sensibile - sunt date a căror accesare, alterare, diseminare neautorizată sau indisponibilitate a accesului la acestea afectează îndeplinirea obiectivelor statului, pe termen mediu și lung;
l) furnizor de servicii de cloud (FSC) - entitate publică sau privată care administrează un set de resurse prin care pune la dispoziția utilizatorilor de servicii de cloud, la cererea acestora, servicii de cloud într-un model partajat de tip IaaS, PaaS sau SaaS;
m) interconectare - conectarea serviciilor, a microserviciilor, a aplicațiilor sau a bazelor de date pentru schimb de date (schimburile de date se pot face direct sau prin API-uri dedicate);
n) management al identității – metode, instrumente, tehnici și proceduri de validare a identității persoanelor atunci când acestea accesează anumite componente ale Platformei cloud guvernamental;
o) microservicii - abordare arhitecturală și organizațională în ceea ce privește dezvoltarea de aplicații informatice care sunt construite din module software independente care comunică prin intermediul unor API bine definite;
p) nivel de servicii agreat (SLA) - componenta a Acordului de furnizare, Convenție de administrare, respectiv Contractului de furnizare în care sunt incluse condițiile specifice și măsurabile legate de oferta de servicii de cloud oferite;
q) platforma API gateway – instrument care reprezintă punctul de intrare unică pentru API-uri și microservicii back-end definite atât interne, cât și externe folosit pentru interconectarea aplicațiilor și serviciilor informatice. Are rol protector, impunând securitatea și asigurând scalabilitate și disponibilitate ridicată;
r) servicii de cloud - modele de partajare securizată a resurselor din cadrul unei platforme cloud, precum IaaS, PaaS sau SaaS, către utilizatori de servicii de cloud, la cererea acestora;
s) servicii în tehnologie de cloud - furnizarea de servicii sau aplicații de tehnologia informației și comunicațiilor prin intermediul serviciilor de cloud, care includ, dar nu se limitează la, stocarea, transmiterea sau procesarea datelor;

t) utilizator de servicii de cloud (USC) - autoritate sau instituție publică centrală sau locală, din România, care utilizează servicii de cloud furnizate în cadrul Platformei de Cloud Guvernamental.

(2) Sensul termenilor și expresiilor utilizate în prezenta hotărâre au înțelesul celor identice prevăzute de Ordonanța de urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice, denumită în continuare Ordonanță.

Art. 3.

Principiile care stau la baza guvernanței Platformei de cloud guvernamental sunt:

a) realizarea accesului securizat la date;
b) alinierea cu obiectivele naționale de digitalizare prin proiectarea și furnizarea serviciilor realizate corelat cu strategiile naționale de digitalizare și securitate cibernetică;
c) conformitatea cu politicile și standardele prin proiectarea și furnizarea serviciilor se realizează cu respectarea standardelor și a criteriilor stabilite prin prezenta hotărâre;
d) interconectarea sistemelor prin accesul sigur, rapid și facil la servicii, cu accent pe trasabilitatea accesului;
e) implementarea conceptului „doar o singură dată” prin care datele minimal necesare sunt solicitate o singură dată și utilizate de toți USC, în baza accesului acordat;
f) orientarea pe USC prin proiectarea și furnizarea serviciilor pe baza nevoilor identificate;
g) asigurarea transparenței prin care proprietarii și administratorii datelor au controlul total asupra acestora și orice operațiune de prelucrare a datelor este jurnalizată în vederea auditării ulterioare de către părțile autorizate;
h) partajarea responsabilităților în cadrul Platformei între FSC și USC;
i) prelucrarea sigură a datelor în cadrul serviciilor furnizate din Platformă cu garantarea specificării și limitarea scopului aferent fiecărei prelucrări de date, iar USC trebuie să adopte măsuri tehnice și organizaționale în scopul asigurării unui nivel adecvat de protecție a datelor.
j) suveranitatea datelor - în funcție de clasificarea datelor, acestea pot fi procesate în Platformă, în infrastructuri tehnice localizate în România sau pe teritoriul statelor membre ale Uniunii Europene.

CAPITOLUL II

Politica, strategia, criteriile tehnice și operaționale privind implementarea, operarea, mentenanța și dezvoltarea ulterioară a Platformei și CPG, regulile privind stabilirea nivelului agreat de servicii, precum și cele privind migrarea și interconectarea sistemelor informatice

Art. 4.

Obiectivele de dezvoltare a Platformei sunt:

a) asigurarea instrumentelor suport pentru îmbunătățirea serviciilor oferite de autoritățile şi instituțiile publice, reformarea operaţiunilor şi a proceselor administrative interne din cadrul autorităților şi instituțiilor publice pe un fundament de transformare digitală, pentru a maximiza beneficiile procesului de e-transformare a guvernării;
b) accelerarea şi eficientizarea adoptării şi reutilizării infrastructurii de digitalizare a serviciilor electronice;
c) implementarea de către autoritățile şi instituțiile publice a politicii, standardelor tehnice şi a celor mai bune practici internaţionale în domeniul TIC;
d) elaborarea şi implementarea unui cadru de investiţii inteligente în TIC pentru a valorifica beneficiile tehnologiilor cloud computing şi a reutiliza infrastructura de digitalizare a serviciilor electronice;
e) dezvoltarea capacităţilor şi abilităților TIC în autoritățile şi instituțiile publice prin dezvoltarea continuă de platforme de colaborare şi parteneriate public-private şi preluarea practicilor inovative şi inteligente în implementarea TIC;
f) deschiderea serviciilor guvernamentale de cloud computing către mediul privat în ceea ce privește achiziționarea de bunuri şi servicii.

Art. 5.

(1) Furnizarea serviciilor oferite în cadrul Platformei se asigura de către ADR în baza contractului de furnizare încheiat cu USC.
(2) Nivelul agreat de servicii de cloud este stabilit prin acorduri de administrare încheiate de ADR cu STS şi SRI.
(3) USC conectate în CPG sunt stabilite prin acordul de administrare prevăzut la alin. (2).
(4) În vederea asigurării funcționării optime a serviciilor de cloud furnizate în Platformă, ADR, împreună cu STS, asigură funcţionalitatea modulului de raportare periodică automată, care actualizează, cu periodicitatea stabilită, datele din grila de indicatori de performanţă tehnică aprobată de către administrator şi furnizori.
(5) Rapoartele generate ca urmare a realizării activității de monitorizare, control şi evaluare a serviciilor de cloud furnizate în Platformă, potrivit alin. (2), stau la baza luării deciziilor corective pe parcursul administrării operaționale a Platformei şi a evaluării performanţei serviciilor furnizate prin resursele de cloud din cadrul Platformei.

Art. 6.

(1) Furnizarea serviciilor oferite în cadrul Platformei poate fi suspendată temporar la iniţiativa USC, printr-o cerere adresată FSC.

(2) Serviciile prevăzute la alin. (1) pot fi suspendate de către FSC, cu acordul prealabil al STS sau SRI, pentru serviciile furnizate din Platformă, și al USC, în cazul în care este compromisă buna funcţionare a serviciilor şi a sistemelor informatice ale USC.
(3) Serviciile prevăzute la alin. (1) pot fi suspendate de către FSC, la solicitarea STS sau SRI, fără consimțământul USC, cu notificarea ulterioară a acestuia:
a) în situaţii de forţă majoră,;
b) în cazul declarării stării de urgenţă, stării de asediu sau stării de război, potrivit legii.
(4) În cazurile menționate la alin. (2) și (3), furnizarea serviciilor se suspendă până la remedierea situaţiei create. Furnizarea serviciilor este reluată de îndată ce cauza suspendării a dispărut.

Art. 7.

(1) În situația în care USC stabilește faptul că serviciile solicitate sau aplicațiile utilizate nu mai corespund cerințelor operaționale, tehnice și de securitate, USC solicită FSC eliberarea resurselor.
(2) Responsabilitatea legală privind păstrarea datelor sau distrugerea acestora este a USC.

Art. 8.

(1) Dezvoltarea Platformei se realizează prin:
a) extinderea capacităţii de procesare şi stocare a datelor;
b) crearea de noi centre de date pentru creșterea gradului de reziliență și disponibilitate a sistemelor informatice în caz de accidente şi de asigurare a unui nivel înalt de disponibilitate;
c) sporirea capacității de automatizare și autoservire pentru autoritățile și instituțiile publice, pentru a beneficia mai simplu de avantajele Cloud Computing;
d) furnizarea de noi servicii și platforme de dezvoltare a aplicaţiilor software;
e) extinderea funcționalităților din contul serviciilor furnizate din clouduri publice.
(2) Pentru dezvoltarea Platformei, MCID asigură:
a) ajustarea cadrului legal pentru facilitarea dezvoltării Platformei;
b) crearea unui program de dezvoltare a abilităţilor TIC raportat la utilizarea Platformei;
c) elaborarea unui plan de integrare a noilor centre de date într-un mediu cloud distribuit în reţea;
d) dezvoltarea, prin ADR, de noi servicii în Platformă.

Art. 9. Serviciile de cloud furnizate USC din Platformă trebuie să asigure cumulativ următoarele criterii tehnice și operaționale:

a) autoservire la cererea USC - după alocare, un USC poate dispune de funcționalitățile serviciilor de cloud de procesare, stocare sau acces la rețea, după propriile nevoi, fără a fi necesară interacțiunea umană cu furnizorul de servicii de cloud;
b) acces facil la rețea - funcționalitățile serviciilor de cloud sunt accesibile prin intermediul unei rețele de comunicații standardizate;
c) punerea în comun a resurselor - utilizarea funcționalităților serviciilor de cloud se bazează pe partajarea dinamică a resurselor tehnice ale furnizorului de servicii de cloud, după criterii de disponibilitate a resurselor fizice sau virtuale;
d) alocare și eliberare rapidă și flexibilă a resurselor - disponibilitatea funcționalităților serviciilor de cloud este asigurată rapid și flexibil, proporțional cu cererea de servicii de cloud;
e) contorizarea resurselor și optimizarea serviciilor - resursele care stau la baza furnizării serviciilor de cloud pot fi monitorizate, gestionate și raportate în vederea asigurării transparenței atât pentru furnizor, cât și pentru USC. În baza măsurătorilor și raportărilor efectuate, sistemele de cloud pot optimiza, singure și în mod automat, resursele alocate.

Art.10.

În funcție de tipul și de modelul de furnizare a serviciului de cloud, procesul de evaluare de securitate la nivelul Platformei se realizează astfel:

a) pentru serviciile de cloud furnizate de către FSC pentru alte clouduri decat cloudul privat guvernamental, de către o entitate din lista auditorilor de securitate cibernetică acreditați de DNSC sau de alte autorități și instituții publice cu atribuții în domeniu;
b) pentru serviciile de cloud furnizate din CPG și de către administratorii de servicii de securitate cibernetică, conform modelului de serviciu din responsabilitate.

Art. 11.

(1) Tipurile de servicii de cloud furnizate în cadrul Platformei sunt:

a) infrastructură ca serviciu (IaaS);

b) platformă ca serviciu (PaaS);

c) software ca serviciu (SaaS).

(2) Serviciile de cloud furnizate pe modelele de punere la dispoziție a resurselor prevăzute la alin. (1) sunt furnizate cu servicii de securitate fizică și cibernetică asociate, conform prevederilor Ordonanței.

Art. 12.

La nivelul Platformei Cloud Guvernamental se stabilesc următoarele roluri:

a) Furnizor de servicii cloud (FSC);
b) Utilizator de servicii cloud (USC).

Art. 13.

(1) Din perspectiva administrării operaționale CPG conform articol 1 alin. (5) din Ordonanță, ADR:
   a) primește și analizează cerințele operaționale ale potențialilor USC pentru dezvoltarea serviciilor din Platformă;
   b) coordonează implementarea și dezvoltarea CPG;
   c) încheie acorduri cu USC cu privire la migrarea, integrarea și interconectarea în CPG, în conformitate cu prevederile art. 4 alin.(4) din Ordonanță;
   d) analizează și monitorizează gradul de adoptare a serviciilor de cloud disponibile în Platformă de către autoritățile și instituțiile publice din România;
   e) asigură listarea, administrarea și delistarea în marketplace a aplicațiilor și serviciilor disponibile în Platformă;
   f) monitorizează eficiența utilizării resurselor și propune actualizări la strategia de dezvoltare ulterioară a Platformei;
   g) întreprinde demersurile necesare pentru instruirea personalului USC în ceea ce privește utilizarea serviciilor din Platformă;
   h) colaborează cu STS și SRI pentru stabilirea nivelurilor agreate de servicii, denumit în continuare SLA și monitorizează respectarea acestuia;
   i) acordă suport USC în procesul de management al riscurilor în vederea adoptării tehnologiilor de cloud;
   j) propune actualizarea listei autorităților și instituțiilor publice ale căror sisteme informatice și servicii publice electronice migrează în CPG;
   k) asigură administrarea tehnică și operațională a serviciilor de cloud SaaS în CPG;
   l) coordonează și monitorizează rezultatele finale ale activităților de instalare, configurare, integrare, testare și trecere în producție a tehnologiilor, soluțiilor și serviciilor software;
   m) colaborează cu SRI pentru asigurarea securității cibernetice a serviciilor de cloud SaaS furnizate, în condițiile Ordonanței;
   n) administrează componenta de marketplace;
   o) monitorizează eficiența utilizării resurselor prin care se asigură furnizarea aplicațiilor listate în marketplace;
   p) furnizează, pentru USC, prin intermediul marketplace, servicii de tip cloud.

(2) Din perspectiva managementului financiar și al achizițiilor de resurse, ADR:
a) întreprinde demersuri pentru asigurarea resurselor financiare în vederea aplicării strategiei privind adoptarea, dezvoltarea și mentenanța Platformei;

b) asigură optimizarea costurilor prin adoptarea modelelor de servicii SaaS, partajate între autoritățile și instituțiile publice;
c) asigură, cu titlu gratuit, furnizarea serviciilor din CPG pentru USC, inclusiv a serviciilor de securitate cibernetică asociate.

(3) FSC are următoarele responsabilități:
a) asigură furnizarea serviciilor în CPG în baza contractelor de furnizare servicii de tip cloud încheiate cu USC;
b) SLA este parte integrantă a contractului de furnizare de servicii și definește calitatea și nivelul serviciilor. Conținutul unui SLA depinde de modelul de serviciu și de implementarea acestuia și are impact asupra responsabilităților relevante ale USC și ale FSC;
c) asigură suportul tehnic, împreună cu STS și SRI, pentru administratorul desemnat de USC prin intermediul unei componente de tip helpdesk, ticketing și callcenter pentru componentele administrate;
d) asigură prestarea serviciilor tip SaaS administrate conform nivelului agreat de servicii;
e) colaborează cu STS și SRI pentru întocmirea analizelor de risc pentru respectarea prevederilor art. 3 alin. (7) din Ordonanță;
f) informează USC cu privire la:

i) rezultatele auditurilor de securitate, sub garantarea confidențialității;

ii) incidente de securitate fizică și cibernetică și oferă suport adecvat, în limita competențelor, pentru gestionarea posibilelor riscuri de protecție a datelor prezentate de astfel de incidente, în termenii definiți în Acord în conformitate cu legea aplicabilă.

(4) Din perspectiva managementului datelor, ADR:
a) asigură, în mod partajat cu USC, respectarea politicilor, standardelor și criteriilor aplicabile serviciilor de cloud în cadrul Platformei;
b) prelucrează datele cu caracter personal încredințate de USC numai pe baza instrucțiunilor documentate ale USC;
c) sprijină USC în îndeplinirea efectivă a obligațiilor sale de operator de date cu caracter personal;
d) întocmește împreună cu STS, SRI și USC proceduri de portabilitate/recuperare/eliminare a datelor;
e) asigură ștergerea sau returnarea, la alegerea USC, a tuturor datelor cu caracter personal încredințate de aceasta din urmă după încheierea prestării serviciilor;
f) stabilește regulile minime, care trebuie implementate de către USC în cadrul politicilor, standardelor și criteriilor aplicabile serviciilor de cloud;

g) elaborează norme pentru gestionarea datelor procesate în Platforma de Cloud Guvernamental, în funcție de politicile de clasificarea datelor, inclusiv criterii tehnice și de securitate;
h) FSC asigură monitorizarea evenimentelor de prelucrare a datelor cu caracter personal prin intermediul componentei de jurnalizare și notifică USC cu privire la încălcarea protecției datelor cu caracter personal, fără întârzieri nejustificate, pentru ca USC să poată notifica, dacă este necesar, persoanele vizate afectate.
i) FSC notifică Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal în termen de 72 de ore după ce FSC ia cunoștință de încălcare. FSC furnizează USC cel puțin următoarele informații:

i) Natura încălcării datelor cu caracter personal, categoriile și numărul aproximativ de persoane vizate și categoriile și numărul aproximativ de înregistrări de date cu caracter personal în cauză;

ii) Consecințele probabile ale încălcării datelor cu caracter personal;

iii) Măsuri luate sau propuse a fi luate pentru a aborda încălcarea datelor cu caracter personal, inclusiv, după caz, măsuri pentru atenuarea posibilelor efecte adverse ale acesteia.

(5) Din perspectiva managementului soluțiilor informatice, ADR:
a) asigură implementarea sistemului care să faciliteze aplicarea principiilor europene ale sistemului tehnic „*doar o singură dată*” la nivelul autorităților și instituțiilor publice;
b) asigură analiza, proiectarea, dezvoltarea și implementarea serviciilor de tip SaaS, necesare administrației publice.

Art. 14.

(1) În baza rolului de administrator tehnic și operațional al infrastructurii de bază și al serviciilor de cloud IaaS și PaaS din cadrul CPG, STS are următoarele responsabilități:
a) asigură implementarea, administrarea tehnică și operațională, precum și disponibilitatea infrastructurii de bază;
b) proiectează împreună cu ADR, respectiv, bugetează și achiziționează produse și servicii pentru mentenanța și dezvoltarea infrastructurii de bază și a serviciilor specifice IaaS și PaaS din CPG, în conformitate cu nevoile de dezvoltare ale platformei cloud guvernamental;
c) pune la dispoziția ADR informații necesare cu privire la starea și la nivelul de utilizare a resurselor tehnice, în vederea identificării nevoilor de dezvoltare a infrastructurii de bază, potrivit prevederilor de la lit. b);

d) analizează utilizarea resurselor CPG și propune modalități de optimizare a acestora;
e) analizează, împreună cu ADR, cerințele tehnice și operaționale ale USC;
f) alocă resursele tehnice din CPG potrivit prevederilor de la lit. e) și în limita constrângerilor tehnice, operaționale și financiare;
g) alocă resurse tehnice suplimentare din CPG în urma solicitărilor ulterioare punerii în producție a serviciilor sau aplicațiilor găzduite;
h) în caz de nefuncționare sau funcționare defectuoasă a serviciilor IaaS și PaaS alocate în CPG, asigură intervenția tehnică imediată în vederea restabilirii serviciilor, cu notificarea ADR și USC și validarea funcționării serviciilor împreună cu aceștia, în conformitate cu SLA-ul agreat;
i) asigură conectarea la nivel de rețea a USC la CPG și acordă sprijin în vederea gestionării și utilizării de către acesta a resurselor alocate;
j) generează și furnizează pentru administratorii USC credențiale de acces securizat și credențiale de gestionare a serviciilor de cloud alocate;
k) asigură interconectarea CPG, la nivel de servicii, cu celelalte componente de cloud din Platformă sau cu entitățile interconectate în Platformă, cu respectarea criteriilor tehnice și de securitate stabilite în prezenta hotărâre;
l) asigură suport tehnic USC în vederea gestionării problemelor tehnice specifice furnizării serviciilor de cloud de tip IaaS și PaaS;
m) pune la dispoziția ADR documentația tehnică pentru utilizarea serviciilor IaaS și PaaS;
n) pune la dispoziție mecanisme tehnice în vederea realizării de către USC a copiilor de siguranță;
o) implementează mecanisme tehnice pentru respectarea de către USC a cerințelor de disponibilitate în centre de date multiple;
p) stabilește criteriile generale minime de performanță, precum și termenii și condițiile pentru furnizarea serviciilor IaaS și PaaS;
q) pune la dispoziția MCID, ADR sau USC, după caz, informații necesare în vedere realizării auditurilor de conformitate, la nivel IaaS și PaaS, pe linia securității și trasabilității datelor și a calității serviciilor furnizate;
r) efectuează demersurile necesare pentru instruirea personalului propriu în ceea ce privește administrarea serviciilor din CPG.

2) În calitate de administrator de securitate cibernetică al infrastructurii de bază utilizată pentru furnizarea serviciilor de cloud pe model IaaS și PaaS din cadrul CPG, STS are următoarele responsabilități:

a) asigură securitatea, inclusiv securitatea cibernetică, a infrastructurii de bază pentru furnizarea serviciilor de cloud pe model IaaS și PaaS;
b) aplică standardele și implementează măsurile tehnice și de securitate conform criteriilor stabilite prin prezenta hotărâre;

c) asigură protecția datelor aflate în tranzit, managementul identității și a drepturilor de acces, în baza listelor actualizate de către ADR, pentru administratorii resurselor alocate în CPG desemnați de USC;
d) notifică USC, cu informarea ADR, cu privire la vulnerabilitățile de securitate, la adresa disponibilității, integrității și confidențialității, identificate la nivelul serviciilor de cloud IaaS și PaaS, în vederea remedierii acestora de către USC;
e) blochează activitatea unor resurse a căror funcționare vulnerabilizează serviciile furnizate, cu obligația de a notifica ADR și USC.

(3) La solicitarea USC, prin intermediul ADR, STS asigură, cu titlu gratuit, în limita resurselor disponibile, servicii de consultanță, proiectare, dezvoltare, testare, administrare tehnică și de securitate cibernetică a serviciilor de cloud și a serviciilor în tehnologii de cloud alocate sau găzduite în CPG.

Art. 15.

(1) Din perspectiva calității de administrator de securitate cibernetică, SRI:
a) asigură securitatea cibernetică a CPG prin cunoaşterea, prevenirea şi contracararea atacurilor, ameninţărilor, riscurilor şi vulnerabilităţilor cibernetice, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor CPG de tip SaaS;
b) cooperează cu STS, conform competenţelor fiecărei instituţii, pentru cunoaşterea, prevenirea şi contracararea atacurilor cibernetice complexe, de tip APT, îndreptate împotriva serviciilor specifice CPG la nivel IaaS şi PaaS, prin schimbul nemijlocit şi automat al informaţiilor referitoare la incidentele de securitate, fără a transfera date de conţinut;
c) colaborează cu ADR și STS, conform atribuțiilor, pentru asigurarea unitară a securității cibernetice a CPG.

(2) Din perspectiva managementului financiar, SRI:
a) gestionează resursele financiare pentru achiziționarea resurselor necesare asigurării serviciilor de securitate cibernetică;
b) în raport de nivelul cererii și necesarul de resurse, gestionează fondurile financiare pentru realizarea investițiilor și măsurilor suplimentare, necesare asigurării securității cibernetice;

(3) Cu privire la managementul operațiunilor, SRI:
a) asigură alocarea serviciilor de securitate cibernetică în funcție de necesitate și de resursele disponibile;
b) colaborează cu ADR pentru stabilirea criteriilor minime de performanță pentru furnizarea serviciilor de securitate cibernetică;

c) asigură suport de specialitate, la solicitarea ADR, pentru derularea activităților de audit desfășurate în cadrul Platformei;
d) analizează lista autorităților și instituțiilor publice ale căror sisteme informatice și servicii publice electronice solicită migrare în CPG și transmite către ADR rezultatul analizei;
e) colaborează cu ADR și STS pentru întocmirea analizelor de risc, pentru respectarea prevederilor art. 3 alin. (7) din Ordonanță;
f) propune ADR blocarea activității unor resurse provizionate de USC, a căror funcționare necorespunzătoare poate afecta serviciile furnizate;
g) are dreptul de a solicita ADR estimări privind nevoia viitoare de resurse, în scopul dezvoltării serviciilor administrate;
h) are dreptul de a notifica ADR privind utilizarea improprie a unor resurse tehnice de către USC și de a solicita suspendarea accesului acestuia, cu conservarea resurselor, dacă nu răspunde în termen de 30 de zile;
i) dreptul de a notifica ADR cu privire la neîndeplinirea obligațiilor USC.

(4) Cu privire la managementul datelor, SRI:
a) implementează politicile, standardele și criteriile aplicabile serviciilor de securitate cibernetică;
b) formulează, împreună cu STS, propuneri către MCID și ADR pentru modificarea politicilor, standardelor și criteriilor aplicabile serviciilor de securitate cibernetică;

(5) Cu privire la securitate și conformitate, SRI:
a) propune MCID soluții tehnice și criterii pentru asigurarea securității cibernetice în cadrul Platformei;
b) aplică standardele și implementează măsurile de securitate cibernetică;
c) participă și asigură suport pentru evaluarea aplicațiilor încă din faza de testare, înainte de lansarea lor în producție;
d) asigură testarea din punct de vedere al securității cibernetice a aplicațiilor de tip SaaS și, la cerere, pentru cele ale USC de tip IaaS și PaaS;
e) avizează lansarea în producție a aplicațiilor în SaaS din punctul de vedere al securității cibernetice;
f) asigură izolarea USC care nu respectă standardele și criteriile pentru asigurarea securității cibernetice.

Art. 16.

Autoritățile și instituțiile publice, în calitate de USC, au următoarele responsabilități:

(1) cu privire la managementul financiar:
a) asigură resursele necesare pentru dezvoltarea și mentenanța serviciilor implementate în regie proprie;

b) asigură resursele necesare pentru implementarea măsurilor de securitate conform criteriilor stabilite, în funcție de modelul de serviciu cloud utilizat, în corelare cu standardul responsabilității partajate;
c) asigură resursele necesare pentru desfășurarea auditurilor de conformitate pe linia securității, trasabilității datelor și a calității serviciilor.

(2) cu privire la managementul operațiunilor:
a) solicită furnizarea de servicii cloud prin intermediul marketplace pus la dispoziție de administratorul operațional;
b) răspunde de procesul de management al riscurilor pentru adoptarea tehnologiilor cloud în cadrul Platformei;
c) încheie convenții de utilizare a serviciilor cloud, prestate de FSC.

(3) cu privire la managementul datelor:
a) implementează politicile, standardele şi criteriile aplicabile serviciilor de cloud în aria de competență;
b) întocmește și transmite instrucțiuni către FSC pentru prelucrarea datelor cu caracter personal;
c) întocmește împreună FSC proceduri de portabilitate/recuperare/eliminare a datelor;
d) verifică ștergerea sau returnarea tuturor datelor cu caracter personal încredințate FSC după încheierea prestării serviciilor de către acesta;
e) în calitate de proprietari/administratori sunt responsabili de prelucrarea datelor și stabilesc drepturi și criteriile de acces la datele prelucrate, pentru personalul propriu, în vederea îndeplinirii îndatoririlor de serviciu și pentru autorități și instituții terțe, în vederea îndeplinirii obligațiilor legale;
f) asigură jurnalizarea operațiunilor de acces la datele procesate în sistemele și aplicațiile implementate;
g) în calitate de proprietari/administratori sunt responsabili de implementarea strategiei copiilor de siguranță a datelor aplicațiilor și sistemelor informatice implementate;
h) împuternicește voluntar ADR și STS pentru prelucrarea de date cu caracter personal în vederea soluționării incidentelor în CPG.

(4) cu privire la securitate și conformitate:
a) aplică standardele și implementează măsurile de securitate conform criteriilor stabilite, în baza modelului de serviciu cloud alocat;
b) răspund de realizarea auditurilor de conformitate pe linia securității, trasabilității datelor și a calității serviciilor furnizate.

Art. 17.

(1) ADR încheie cu USC acord de migrare, integrare și interconectare în CPG a sistemelor informatice.
(2) ADR încheie cu USC contract de furnizare de servicii de tip cloud.
(3) FSC încheie cu USC convenție de administrare a serviciilor de tip cloud, potrivit prevederilor art. 15 din Ordonanță.
(4) În vederea contractării unui serviciu de cloud din cadrul Platformei, furnizat de un FSC public sau privat, USC se adresează ADR și stabilește cu acesta, în baza unei analize de business prealabile, tipul de serviciu cloud pe care USC poate să-l contracteze, precum și FSC selectat din marketplace.
(5) Ulterior alegerii serviciului de cloud din Platformă, USC încheie cu FSC-ul selectat de către acesta, după caz, un contract de furnizare pentru serviciile selectate din marketplace.
(6) Contractul de furnizare de servicii de cloud prevazut la alin. (5) cuprinde clauze cu privire, dar fără a se limita la, condițiile tehnice detaliate de utilizare a serviciilor de cloud, drepturile și obligațiile părților, precum și limitele împuternicirii acordate de USC în vederea prelucrării datelor cu caracter personal, precum:

a. cerințe tehnice aplicate pentru prestarea serviciilor;
b. nivelul agreat de servicii, inclusiv indicatorii de performanță ai acestora;
c. divizarea răspunderii contractuale și limitările acesteia;
d. principiile efectuării sau comandării unui audit de către părți asupra modului de implementare a acordului;
e. proceduri pentru utilizarea serviciilor potrivit alin. (2);
f. repartizarea atribuțiilor legate de utilizarea serviciilor, inclusiv obligațiile furnizorului de servicii și asigurarea nivelului de calitate a serviciilor convenit;
g. regulile de întreținere tehnică furnizate ca parte a întreținerii serviciilor;
h. obligații în domeniul drepturilor de proprietate intelectuală;
i. proceduri de securitate și reguli de răspuns la incident;
j. drepturile, obligațiile și limitele împuternicirii privind prelucrarea datelor cu caracter personal;
k. procedurile de suspendare și renunțare la utilizarea serviciilor și condițiile de încetare a contractului;
l. reguli de decontare pentru utilizarea serviciilor, acolo unde este cazul;
m. obligații de informare cu privire la prestarea serviciilor.

Art. 18.

(1) În urma încheierii contractului de furnizare, FSC asigură, la cererea USC, consultanță tehnică, precum și resurse tehnice, cu titlu gratuit, pe o perioadă prestabilită, în vederea testării serviciilor informatice ce urmează a fi folosite prin serviciile de cloud furnizate.
(2) În situația în care FSC se află în imposibilitate obiectivă de a furniza consultanță tehnică sau resurse tehnice pentru testarea serviciilor informatice, USC poate contracta servicii de consultanță tehnică sau de testare a serviciilor informatice, ce vor fi suportate din bugetul USC.
(3) Condițiile de imposibilitate obiectivă prevăzută la alin. (2) sunt:
a) o frecvență de creștere a costurilor FSC, pe cel puțin trei luni, mai mare cu cel puțin 40% față de costul inițial al consultanței tehnice evaluate și prevăzute în convenția cu USC;
b) depășirea competențelor de asigurare a consultanței tehnice, care ar reveni expres unei alte autorități publice centrale;
c) excepția de neexecutare, invocată în condițiile Legii nr. 287/2009 privind Codul civil;
d) forța majoră;
e) cazul fortuit;
(4) În etapa de testare, USC are obligația de a folosi servicii de audit tehnic și de securitate pentru evaluarea propriilor servicii livrate prin intermediul serviciilor de cloud contractate în cadrul Platformei.

Art. 19.

USC evaluează riscurile, stabilește măsurile de securitate necesare în conformitate cu standardele și criteriile aplicabile în Platformă, proiectează și implementează sistemul utilizând tehnologii de cloud și procedează la testarea acestuia privind funcționalitățile, performanța și nivelul de securitate folosind resursele tehnice de test puse la dispoziție.

Art. 20.

Pentru serviciile de tip SaaS, FSC are următoarele obligații:
a) asigură mecanismele de solicitare, alocare și disponibilizare a serviciilor furnizate;
b) asigură disponibilitatea și securitatea serviciilor furnizate, în limitele nivelului agreat de servicii;
c) asigură accesul la serviciile furnizate;
d) asigură, la cerere, suportul tehnic pentru USC în vederea folosirii mecanismelor de solicitare, alocare, utilizare și disponibilizare a serviciilor furnizate;
e) dezvoltă, instalează și gestionează componentele software necesare bunei funcționări a serviciilor furnizate;
f) asigură integrarea, la cerere, a serviciilor furnizate cu alte sisteme informatice;
g) asigură administrarea centralizată a serviciilor furnizate;
h) acordă USC drepturile de administrare pentru serviciile furnizate;

i) asigură performanţa, securitatea şi disponibilitatea serviciilor furnizate în conformitate cu nivelul agreat de servicii;
j) asigură protejarea datelor procesate în cadrul serviciilor, precum şi crearea şi stocarea copiilor de rezervă;
k) asigură, inclusiv pentru USC, documentarea serviciilor furnizate;
l) asigură suportul USC în cadrul livrării serviciilor furnizate.

(2) Pentru serviciile de tip SaaS, USC are următoarele obligații:

a) utilizează serviciile solicitate în corespundere cu acordurile sau, după caz, contractele încheiate cu furnizorul;
b) administrează serviciile alocate, în limitele responsabilităţilor specificate în convenția încheiată cu furnizorul;
c) gestionează accesul la serviciile alocate, în vederea administrării acestora, în limitele responsabilităţilor specificate în convenția încheiată cu furnizorul;
d) asigură administrarea datelor generate în cadrul utilizării serviciilor;
e) asigură, după caz, instruirea şi suportul utilizatorilor proprii.

Art. 21.

(1) În vederea administrării infrastructurii și serviciilor din Platformă și a stabilirii nivelurilor agreate de servicii de tip cloud, ADR încheie Acorduri-cadru de administrare infrastructură și servicii cloud cu STS și SRI.
(2) Responsabilitățile ADR, conform Acord-cadru, sunt:
a) primește și analizează cerințele operaționale ale potențialilor USC pentru dezvoltarea serviciilor din CPG împreună cu STS și SRI;
b) coordonează implementarea și dezvoltarea CPG;
c) analizează și monitorizează nivelul de adoptare a serviciilor de cloud disponibile în Platformă de către autoritățile și instituțiile publice din România;
d) asigură administrarea și delistarea în marketplace a aplicațiilor și serviciilor disponibile în Platformă;
e) monitorizează eficiența utilizării resurselor și propune actualizări în strategia de dezvoltare ulterioară a Platformei;
f) întreprinde demersurile necesare pentru instruirea personalului USC în ceea ce privește utilizarea serviciilor din Platformă;
g) comunică lista autorităților și instituțiilor publice ale căror sisteme informatice și servicii publice electronice solicită migrare în CPG;
h) asigură administrarea tehnică și operațională a resurselor utilizate pentru furnizarea serviciilor SaaS în CPG;
i) coordonează și monitorizează rezultatele finale ale activităților de instalare, configurare, integrare, testare și trecere în producție a tehnologiilor, soluțiilor și serviciilor software;
j) transmite spre analiză și verificare către STS și SRI toate solicitările primite din partea terților pentru listarea în componenta marketplace;

k) monitorizează eficiența utilizării resurselor prin care se asigură furnizarea aplicațiilor listate în marketplace.

(3) Responsabilitățile STS, conform acordului cadru, sunt:

a) propune ADR blocarea utilizării unor resurse provizionate către USC, a căror funcționare necorespunzătoare poate afecta serviciile furnizate;
b) solicită ADR estimări privind nevoia viitoare de resurse, în scopul dezvoltării serviciilor furnizate;
c) notifică ADR privind utilizarea ineficientă a unor resurse tehnice şi de a suspenda accesul USC, cu conservarea resurselor, dacă nu răspunde în termen de 30 de zile;
d) notifică ADR cu privire la neîndeplinirea obligațiilor USC;
e) asigură mecanismele de solicitare, alocare şi disponibilizare a resurselor de cloud furnizate;
f) asigură suport de specialitate, la solicitarea ADR şi a USC, pentru activitatea de audit;
g) asigură un set de şabloane pentru resursele de tehnologia informației pe baza cărora vor fi create şi livrate resurselor solicitate;
h) asigură securitatea fizică şi cibernetică a resurselor solicitate, în limitele nivelului agreat de servicii, în limita competențelor;
i) asigură accesul securizat la resursele alocate;
j) asigură, în caz de necesitate, la solicitarea ADR, suport tehnic USC în vederea utilizării mecanismelor de solicitare, alocare şi disponibilizare a resurselor de cloud furnizate;
k) asigură performanţa, disponibilitatea şi securitatea componentelor software de platformă solicitate, în limitele nivelului agreat de servicii;
l) asigură accesul la componentele software de platformă solicitate;
m) asigură, la cerere, suportul tehnic al USC în vederea utilizării şi integrării componentelor software de platformă în sistemele informaţionale găzduite pe resursele de cloud furnizate;
n) instalează, configurează şi gestionează componentele software de platformă;
o) asigură licenţierea pentru sistemele de operare, precum şi pentru alte componente necesare bunei funcţionări a componentelor software de platformă;
p) administrează componentele software de platformă;
q) asigură protejarea datelor procesate în cadrul componentelor software de platformă, precum şi crearea şi stocarea copiilor de rezervă;
r) asigură documentaţia tehnică a componentelor software de platformă;
s) solicită USC estimări privind nevoia viitoare de resurse, în scopul dezvoltării serviciilor furnizate;
t) transmite ADR, la solicitarea acesteia, informații cuprinzătoare cu privire la locația fizică a serverelor utilizate pentru serviciile cloud furnizate, inclusiv pentru backup, business continuitate și tranzit, precum și locații de unde se efectuează operațiunile de la distanță. Orice plan de schimbare a locației va fi furnizat către ADR înainte ca datele să fie prelucrate în noua locație, cu o înștiințare prealabilă necesară pentru ca ADR să verifice în special dacă modificarea respectă acordul;
u) analizează lista autorităților și instituțiilor publice ale căror sisteme informatice și servicii publice electronice solicită migrare în CPG și transmite către ADR rezultatul analizei.

(4) Responsabilitățile SRI, conform acordului cadru, sunt:

a) propune ADR blocarea utilizării unor resurse provizionate către USC, a căror funcționare necorespunzătoare poate afecta serviciile furnizate;
b) solicită ADR estimări privind nevoia viitoare de resurse, în scopul dezvoltării serviciilor furnizate;
c) notifică ADR privind utilizarea ineficientă a unor resurse tehnice și de a suspenda accesul USC, cu conservarea resurselor, dacă nu răspunde în termen de 30 de zile;
d) notifică ADR cu privire la neîndeplinirea obligațiilor USC;
e) asigură securitatea cibernetică la nivelul IaaS și PaaS, în condițiile art.6 alin.(2) din Ordonanță, precum și la nivel SaaS și pentru entitățile găzduite în CPG;
f) colaborează cu ADR și STS, conform atribuțiilor, pentru asigurarea unitară a securității cibernetice a CPG;
g) asigură alocarea serviciilor de securitate cibernetica în funcție de necesitate și de resursele disponibile;
h) cooperează cu ADR pentru stabilirea criteriilor minime de performanță pentru furnizarea serviciilor de securitate cibernetică;
i) asigură suport de specialitate, la solicitarea ADR, STS și a USC, pentru activitatea de audit;
j) colaborează cu ADR și STS pentru întocmirea analizelor de risc pentru respectarea prevederilor art. 3 alin. (7) din Ordonanță;
k) implementează politicile, standardele și criteriile aplicabile serviciilor de securitate cibernetică;
l) aplică standardele și implementează măsurile de securitate cibernetică, potrivit atribuțiilor prevăzute în Ordonanță;
m) participă și asigură suport pentru evaluarea aplicațiilor încă din faza de testare, înainte de lansarea lor în producție;
n) asigură testarea, din punct de vedere al securității cibernetice, a aplicațiilor USC de tip SaaS;
o) avizează lansarea în producție a aplicațiilor în SaaS din punctul de vedere al securității cibernetice;
p) asigură izolarea USC care nu respectă standardele și criteriile pentru asigurarea securității cibernetice;
q) analizează lista autorităților și instituțiilor publice ale căror sisteme informatice și servicii publice electronice solicită migrare în CPG și transmite către ADR rezultatul analizei.

Art. 22.

(1) ADR încheie acord de migrare, integrare și interconectare cu USC.
(2) ADR are următoarele obligații:
a) gestionează accesul la resursele de cloud alocate în vederea administrării acestora;
b) dezvoltă, instalează și gestionează componentele software necesare bunei funcționări a sistemelor informaționale proprii găzduite pe resursele de cloud alocate ;
c) asigură integrarea sistemelor informatice proprii găzduite pe resursele de cloud alocate cu alte sisteme informaționale;
d) asigură integrarea componentelor software de platformă în sistemele informaționale și aplicațiile migrate;

e) asigură, în mod partajat cu USC, securitatea şi disponibilitatea, la nivelul resurselor de cloud alocate;
f) asigură analiza și migrarea pentru autoritățile și instituțiile publice centrale;
g) asigură instruirea şi suportul USC sistemelor informatice găzduite pe resursele de cloud alocate pentru aplicațiile și sistemele autorităților și instituțiilor publice centrale.

(3) USC are următoarele obligații:

a) asigură licenţierea pentru sistemele de operare, precum şi pentru alte componente necesare bunei funcţionări a sistemelor informatice proprii găzduite pe resursele de cloud alocate, cu excepţia cazurilor în care FSC poate oferi licenţele necesare;
b) administrează sistemele informatice proprii găzduite pe resursele de cloud alocate, inclusiv acordă drepturile de acces la diferite componente ale sistemelor informatice;
c) asigură, în mod partajat cu FSC, performanţa, securitatea şi disponibilitatea, la nivel de sistem de operare şi aplicaţii, a sistemelor informatice proprii găzduite pe resursele de cloud alocate;
d) asigură protejarea datelor procesate în cadrul sistemelor informatice proprii găzduite în Platformă, precum şi crearea şi stocarea copiilor de rezervă;
e) asigură documentarea tehnică a sistemelor informatice proprii găzduite pe resursele de cloud alocate;
f) asigură instruirea şi suportul USC sistemelor informatice proprii găzduite pe resursele de cloud alocate.
g) asigură managementul riscurilor în abordarea tehnologiilor de cloud;
h) asigură implementarea măsurilor tehnice din aria de responsabilitate pentru gestionarea riscurilor de securitate.
i) asigură managementul riscurilor în abordarea planurilor de migrare și interconectare a sistemelor informatice;
j) administrează sistemele informatice proprii găzduite pe resursele de cloud alocate, inclusiv acordă drepturile de acces la diferite componente ale sistemelor informatice;
k) asigură, în mod partajat cu FSC, securitatea şi disponibilitatea, la nivelul resurselor de cloud alocate;
l) gestionează accesul la resursele de cloud alocate în vederea administrării acestora;
m) asigură protejarea datelor procesate în cadrul sistemelor informatice proprii găzduite pe resursele de cloud alocate;
n) asigură documentarea tehnică a sistemelor informatice proprii găzduite pe resursele de cloud alocate;
o) utilizează serviciile componentelor software de platformă conform cu acordurile de migrare și interconectare încheiate cu FSC;
p) asigură instruirea şi suportul USC pentru sistemele informatice găzduite pe resursele de cloud alocate, cu excepţia cazurilor în care USC asigură această activitate;
q) asigură managementul riscurilor în abordarea tehnologiilor de cloud;
r) asigură implementarea măsurilor tehnice din aria de responsabilitate pentru gestionarea riscurilor de securitate.

Art. 23.

(1) USC utilizează serviciile de cloud furnizate dintr-un cloud public în urma clasificării datelor utilizate în serviciile de cloud solicitate, conform politicii de clasificare a datelor.
(2) Costurile pentru realizarea conectării între Platformă și alte servicii furnizate de cloud public revin în sarcina autorității sau instituției publice solicitantă.

Art. 24.

(1) Autoritățile și instituțiile publice care optează pentru utilizarea serviciilor de cloud public solicită aviz de la ADR din care să rezulte îndeplinirea cumulativă a următoarelor condiții:
a. încadrarea datelor utilizate pentru a permite prelucrarea acestora într-un cloud public,;
b. serviciile de cloud public respectă cerințele autorităților și instituțiilor publice de confidențialitate, securitate, integritate și disponibilitate;
c. serviciile de cloud sunt găzduite și oferite pe o infrastructură de bază aflată pe teritoriul statelor membre ale UE;
d. autoritățile și instituțiile publice demonstrează capacitate de a utiliza și gestiona în mod corespunzător aceste servicii.

Art. 25.

Autoritățile și instituțiile publice includ în solicitarea pentru servicii de cloud public cel puțin următoarele informații:

a) identitatea operatorului datelor și modul în care asigură controlul acestora;
b) categoriile de angajați/reprezentanți/parteneri care au acces la date;
c) locul de stocare a datelor și mecanismele de back-up;
d) condițiile și criteriile de audit;
e) calificarea nivelului de risc;
f) standarde, certificări și garanții de funcționalitate și securitate ale produselor și serviciilor de cloud;
g) cerințele de securizare a comunicațiilor.

Secțiunea

Platforma de tip API Gateway

Art. 26.

(1) Se instituie Platforma de tip API Gateway necesară asigurării interconectării și interoperabilității sistemelor informatice publice din Platforma cloud guvernamental.

(2) Suportul tehnic al Platformei de tip API Gateway este asigurat de o infrastructură informatică dedicată, care permite schimbul de date între autoritățile și instituțiile publice în vederea asigurării interoperabilității aplicațiilor și serviciilor informatice pentru furnizarea serviciilor în Platformă.
(3) În vederea asigurării securității cibernetice a Platformei de tip API Gateway, ADR colaborează cu Directoratul Național de Securitate Cibernetică și cu SRI.
(4) În vederea asigurării securității comunicațiilor prin rețelele de transmisii de date utilizate de Platforma de tip API Gateway, ADR colaborează cu STS. ADR asigură suport pentru implementarea cerințelor de interoperabilitate și/sau interconectare a cloud-urilor private implementate de autoritățile și instituțiile publice.
(5) ADR este desemnată drept unic administrator al Platformei de tip API Gateway și are următoarele atribuții:
a) asigură interconectarea la nivel de servicii a aplicațiilor din cloudul privat guvernamental prin intermediul platformei de tip API Gateway;
b) asigură funcționarea, administrarea, mentenanța și dezvoltarea ulterioară a platformei;
c) avizează planurile de conectare a sistemelor informatice aparținând autorităților și instituțiilor publice la platformă;
d) monitorizează respectarea modului de utilizare al schimbului de date cu sistemele conectate la platformă;
e) asigură securitatea platformei și a protecției datelor cu caracter personal în relația cu instituțiile și autoritățile publice;
f) asigură jurnalizarea accesului la date;
g) asigură conectarea la platformă aplicațiilor și serviciilor informatice din surse proprii.
(6) Instituțiile și autoritățile publice conectate au următoarele obligații:
a) asigură implementarea de măsuri organizaționale și tehnice pentru schimbul de date;
b) asigură conectarea la Platformă a aplicațiilor și serviciilor informatice din surse proprii, altele decât cele de la alin. (5), lit. g);
c) implementează măsurile necesare pentru respectarea politicii referitoare la securitatea și confidențialitatea datelor;
d) ADR va fi împuternicit de către instituțiile și autoritățile publice ca și împuternicit al operatorului de date cu caracter personal;
e) ADR va publica specificatiile tehnice necesare interconectarii la nivel de aplicații și servicii în Platformă.

CAPITOLUL III

Cadrul de management şi stocare a datelor în Platformă, inclusiv stabilirea categoriilor de date prelucrate în Platformă şi găzduite de Cloudul privat guvernamental

Art. 27.

În funcție de cerințele USC, categoriile de date, precum și de arhitectura, standardizarea și nivelul de complexitate aferent sistemelor informatice utilizate de acesta, procesul de adoptare a tehnologiilor cloud se poate realiza prin:

a) migrare în Platformă, dacă sunt respectate standardele și cerințele aplicabile conform analizei aplicațiilor ce se decid a fi migrate;
b) modernizare tehnologică pentru respectarea standardelor și cerințelor aplicabile Platformă;
c) proiectare folosind tehnologii native cloud pe baza cerințelor USC și cu respectarea standardelor și cerințelor aplicabile Platformei.

Art. 28.

(1) Lista completă a aplicațiilor și serviciilor oferite în cadrul Platformei este inclusă în marketplace, aflat în administrarea ADR.
(2) Marketplace cuprinde denumirea serviciilor, descrierea acestora, modul de solicitare şi contractare, tarife pentru servicii, după caz, condiţiile ce trebuie să fie întrunite de utilizare pentru solicitarea serviciilor, condițiile de furnizare a serviciilor, precum şi alte informaţii pentru utilizarea acestora.
(3) Solicitarea serviciilor de cloud din Platformă de către USC se efectuează în baza cererii adresate ADR.

Art. 29.

(1) Serviciile publice de cloud furnizate în cadrul Platformei sunt oferite prin reţelele publice de comunicaţii.
(2) Serviciile de cloud furnizate în cadrul CPG sunt oferite prin intermediul rețelelor de comunicații aflate în administrarea STS, prin canale securizate de acces şi transport de date.

Art. 30.

USC, pentru proiectarea serviciilor, adoptând tehnologii de cloud, identifică datele pe care urmează să le utilizeze în cadrul Platformei de Cloud Guvernamental și le clasifică cu respectarea nivelului de încadrare al datelor.

Art. 31.

(1) USC, înainte de utilizarea serviciilor furnizate prin Platformă, are obligația de a încadra și gestiona datele în funcție de nivelul de risc asociat, astfel:

a) **Nivel 1 - nivel scăzut** aplicat datelor publice pentru care pierderea confidențialității, integrității sau disponibilității datelor sau a aplicațiilor nu are impact asupra activității, imaginii și siguranței autorităților și instituțiilor publice;

b) **Nivel 2 - nivel mediu** aplicat în general datelor care nu sunt destinate publicului pentru care pierderea confidențialității, integrității sau disponibilității datelor sau a aplicațiilor are un impact ușor negativ asupra activității, imaginii și siguranței autorităților și instituțiilor publice;

c) **Nivel 3 - nivel ridicat** aplicat în cazul datelor pentru care protecția este stabilită prin lege și pentru care pierderea confidențialității, integrității sau disponibilității datelor sau a aplicațiilor are un impact negativ semnificativ asupra activității, imaginii și siguranței autorităților și instituțiilor publice.

(2) FSC stabilește criteriile și cerințele minime pentru asigurarea securității și confidențialității datelor prevăzute în fiecare nivel menționat la alin (1).

(3) Auditul de securitate al FSC stabilește și actualizează o politică și proceduri pentru efectuarea evaluărilor de securitate ale sistemului informatic și ale auditurilor activelor critice, ținând cont de analiza riscurilor actualizată periodic.

Art. 32.

Încadrarea datelor într-una dintre categoriile prevăzute se realizează în baza unei analize de risc, ce are la bază următoarele aspecte de analiză:

a) impactul operațional și pierderea funcțiilor critice ale serviciului;
b) impactul financiar;
c) afectarea imaginii și reputației publice;
d) impactul asupra sănătății și siguranței publice;
e) impactul la nivel social;
f) impactul asupra activităților curente sau a atingerii obiectivelor stabilite;
g) respectarea reglementărilor.

Art. 33.

(1) În funcție de nevoia de reziliență pentru serviciile furnizate, USC care utilizează date deschise sau cu valoare ridicată, poate utiliza simultan multiple tipuri de cloud-uri din

cadrul Platformei, cu respectarea și implementarea criteriilor generale de protecție aferente.

(2) Autoritățile și instituțiile publice au obligația de a cataloga datele în funcție de categoria de date din care acestea vor face parte, în conformitate cu legislația în vigoare.

(3) Autoritățile și instituțiile publice beneficiare ale serviciilor de cloud întocmesc și actualizează lista datelor și a serviciilor digitale care cuprinde atât o descriere a relațiilor între date și serviciile digitale proprii cât și a relațiilor cu datele și serviciilor terților.

(4) Lista prevăzută la alin. (3) este pusă la dispoziția furnizorului de servicii de cloud împreună cu cererea de solicitare a serviciilor de cloud.

(5) Autoritățile și instituțiile publice au obligația actualizării informațiilor prevăzute la alin (3) odată la 2 ani sau în termen de 30 zile de la data la care s-a înregistrat o modificare.

(6) Furnizorul de servicii de cloud are obligația verificării respectării cerințelor tehnice pentru asigurarea protecției informației.

CAPITOLUL IV

Planul pentru migrarea și integrarea în CPG 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 CPG

Art. 34.

(1) ADR elaborează metodologia pentru identificarea, selectarea și prioritizarea aplicațiilor și serviciilor, care urmează a fi migrate în CPG.

(2) În metodologiile pentru migrarea aplicațiilor, ADR include o analiză a proceselor și a aplicațiilor curente din autoritatea sau instituția publică beneficiară, în vederea migrării unui ecosistem modern de aplicații, având drept scop asigurarea transformării digitale uniforme și consolidarea sistemelor la nivelul fiecărei autorități și instituții publice care se află în proces de migrare.

(3) ADR coordonează procesul de migrare a aplicațiilor și achiziționează servicii pentru migrarea aplicațiilor și serviciilor prioritare în CPG și coordonează procesul de migrare în numele autorităților și instituțiilor publice.

(4) ADR poate solicita și primi rapoarte de analiza de impact de la orice USC, cu scopul de a facilita demersurile de coordonare ale procesului de migrare și de analiză a aplicațiilor și serviciilor.

(5) ADR asigură informarea și instruirea reprezentanților autorităților și instituțiilor publice ale căror servicii sunt furnizate prin intermediul tehnologiilor din CPG.

(6) Autoritățile și instituțiile publice ale căror aplicații și servicii sunt migrate în CPG oferă acces necondiționat ADR la infrastructura curentă, documentația tehnică completă, pachete de instalare, licențe și alte active necesare migrării. Autoritățile și instituțiile publice intermediază schimburile de informații cu personalul entității care asigură mentenanța aplicațiilor/sistemelor informatice, acolo unde este cazul.

(7) Fiecare autoritate și instituție publică își dezvoltă, împreună cu ADR, planul de migrare în baza arhitecturii comune de date și a metodologiei de migrare. Arhitectura comună respectă Politica de clasificare a datelor și gestionează schimbul de date prin Platforma API Gateway.

(8) ADR, împreună cu autoritățile și instituțiile publice ale căror aplicații și servicii sunt migrate, colaborează pentru:

(a) evaluarea necesarului de resurse din CPG pentru găzduirea aplicațiilor și serviciilor informatice, acolo unde este cazul;

(b) evaluarea necesarului de resurse din cloudurile publice și cloudurile private neguvernamentale;

(c) elaborarea și aprobarea instrucțiunilor tehnice detaliate pentru migrare;

(d) evaluarea conformității aplicațiilor și serviciilor cu cerințele de cloud ready și cloud nativ, de interoperabilitate, jurnalizare, notificare și securitate;

(e) evaluarea potențialului de reutilizare a aplicațiilor și serviciilor și a posibilității de a fi provizionate ca și SaaS pentru alte autorități și instituții publice în cazul în care acestea sunt de uz general.

(9) Urmare a evaluărilor prevăzute la alin. (8), lit. (d) și (e), ADR elaborează și pune la dispoziția autorităților și instituțiilor publice planuri de mentenanță corectivă a aplicațiilor și serviciilor migrate, iar autoritățile și instituțiile publice îl implementează de îndată.

Art. 35.

(1) STS, la solicitarea ADR, oferă resursele necesare migrării aplicațiilor și serviciilor prevăzute în analiza fiecărei aplicații sau sistem informatic în parte.

(2) SRI, împreună cu STS, asigură verificarea conformității aplicațiilor și serviciilor din punct de vedere al cerințelor de securitate cibernetică a CPG, potrivit atribuțiilor prevăzute în Ordonanță.

(3) ADR stabilește, împreună cu fiecare autoritate și instituție publică în parte, planul de migrare în baza analizei tehnico-economice a serviciilor și aplicațiilor ce vor migra, precum și a evaluării resurselor și a efortului tehnico-economic.

Art. 36.

ADR asigură migrarea, găzduirea, integrarea și interconectarea în CPG a aplicațiilor și serviciilor informatice ale autorităților și instituțiilor publice centrale care funcționează în următoarele domenii, dar fără a se limita la acestea:

a. Administrație publică;
b. Agricultură;
c. Cercetare;
d. Cultură;
e. Digitalizare;
f. Economie;
g. Educație;
h. Energie;
i. Finanțe publice;
j. Fonduri europene;
k. Justiție;
l. Transporturi și infrastructură;
m. Mediu;
n. Muncă și asigurări sociale;
o. Sănătate;
p. Sport;
q. Tineret;
r. Turism.

CAPITOLUL V

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

Art. 37.

În vederea selectării tipului și modelului de serviciu din marketplace, USC împreună cu ADR face o analiză, care evaluează nivelul de pregătire și expertiză pentru adoptarea tehnologiilor cloud, din următoarele considerente:

a) suportul decizional - adoptarea tehnologiilor cloud necesită implicarea factorilor de decizie atât la nivel intern cât și în relația cu alte autorități și instituții publice pentru atingerea obiectivelor stabilite;
b) bugetul și tipul de serviciu public electronic - furnizarea serviciilor prin intermediul tehnologiilor de cloud are implicații, mai mici sau mai mari, asupra bugetului, în funcție de modelul de serviciu de cloud;

c) cadrul intern de organizare - furnizarea serviciilor prin intermediul tehnologiilor de cloud are implicații asupra modului de exploatare a resurselor TIC, atât din perspectiva resurselor umane pe care le administrează, cât și a celor pe care le utilizează, precum și a cadrului intern de reglementare;
d) arhitectura, standardizarea și nivelul de complexitate aferente sistemelor informatice - adoptarea tehnologiilor cloud are implicații semnificative în furnizarea serviciilor publice electronice, fiind un element cheie în selectarea modelului de cloud;
e) criteriile de performanță necesare pentru furnizarea serviciilor proprii;
f) cadrul național de reglementare - prevederile legislative care reglementează furnizarea serviciilor publice electronice sau organizarea și funcționarea unei autorități sau a unei autorități și instituții publice contribuie în mod semnificativ la selectarea unui anume model de serviciu cloud.

Art. 38.

(1) Ulterior încheierii acordului de furnizare, USC stabilește modelul de serviciu de cloud pe care dorește să îl utilizeze și îl comunică ADR.
(2) ADR realizează analiza de risc cu privire la serviciile solicitate de către USC.

Art. 39.

(1) Componenta marketplace cuprinde lista aplicațiilor și serviciilor de cloud, descrierea acestora, modul de solicitare și contractare, condițiile ce trebuie să fie întrunite de beneficiari pentru solicitarea serviciilor, precum și alte informații privind utilizarea acestora.
(2) În vederea exercitării funcției de administrator al marketplace, ADR are următoarele responsabilități:
a) asigură serviciile de suport și mentenanță pentru componenta marketplace;
b) se asigură de publicarea specificațiilor tehnice minimale, respectiv a cerințelor tehnice și funcționale ale aplicațiilor ce vor fi furnizate prin componenta marketplace a Platformei;
c) validează și avizează aplicațiile care vor fi publicate;
d) asigură confidențialitatea informațiilor comerciale.
(3) Criteriile de asigurare a confidențialității, securității și interoperabilității, precum și adaptarea la standardele tehnice sunt următoarele:
a) prin publicarea în componenta marketplace, dreptul de proprietate nu se transferă către ADR ci este păstrat de dezvoltator, cu excepția celor open source;
b) ADR afișează public numele dezvoltatorului, informații referitoare la oferta comercială legată de produsul listat precum și termenele și condițiile de utilizare.
c) sunt descrise clar orice limitări, condiții sau excepții de la funcționalitatea, caracteristicile aplicațiilor;
d) sunt descrise compatibilitățile cu alte aplicații;

e) aplicațiile sunt disponibile comercial, în curs de dezvoltare activă și susținute până când sunt eliminate de pe piață;
f) aplicațiile nu trebuie să instaleze sau să lanseze cod executabil în mediul USC, altul decât cel aflat în ofertă, și trebuie să fie lipsite de programe malware și vulnerabilități de securitate;
g) aplicațiile respectă regimurile de acces la date prevăzute la nivel național și european, respectă prevederile 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);
h) aplicațiile respectă funcționalitățile și caracteristicile așa cum sunt ele menționate în descriere. Dacă sunt disponibile versiuni demo, acestea oferă aceleași funcționalități cu versiunile plătite.

CAPITOLUL VI

Normele metodologice de jurnalizare a evenimentelor și accesului la datele autorităților și instituțiilor publice găzduite în CPG

Art. 40.

(1) Prin intermediul serviciilor de cloud furnizate din CPG, USC prelucrează date cu caracter personal în calitate de operatori.
(2) În vederea furnizării serviciilor de cloud, USC împuternicește FSC, în sensul Regulamentului (UE) nr. 679/2016, în vederea prelucrării datelor cu caracter personal pentru asigurarea îndeplinirii drepturilor și atribuțiilor FSC în procesul de furnizare a serviciilor de cloud. În acest sens, în acordul de furnizare a serviciilor, USC stabilește:
a) obiectul și durata prelucrării;
b) natura și scopul prelucrării;
c) tipul de date cu caracter personal prelucrate;
d) categoriile de persoane vizate;

e) obligațiile și drepturile USC și FSC.

(3) În calitate de persoană împuternicită, FSC prelucrează datele cu caracter personal numai pe baza instrucțiunilor documentate ale USC, în acord cu politica de prelucrare a datelor stabilită de acesta și cu limitele de prelucrare stabilite conform alin. (2).

(4) FSC, în calitate de persoană împuternicită, nu poate împuternici la rândul său un alt FSC sau o entitate parteneră decât cu acordul prealabil scris al USC.

Art. 41.

(1) În vederea migrării aplicațiilor sau sistemelor informatice în cloud sau pentru utilizarea unor servicii de cloud, USC are obligația de a realiza o analiză de impact asupra protecției datelor cu caracter personal, care să cuprindă analiza cel puțin a următoarelor aspecte:

a) audit informațional pentru a fi identificate toate categoriile de date ce sunt prelucrate de către USC prin serviciile de cloud ce sunt contractate;

b) identificarea și definitivarea tuturor activităților de prelucrare ce sunt efectuate prin serviciile de cloud ce sunt contractate;

c) stabilirea liniilor directoare pe care este construită politica de prelucrare a datelor;

d) identificarea perioadei optime pentru stocarea datelor cu caracter personal;

e) stabilirea operațiunilor de prelucrare ce trebuie jurnalizate, precum și perioada de stocare a jurnalizărilor;

f) stabilirea fluxurilor necesare primirii și soluționării cererilor formulate de persoanele vizate în baza Regulamentului UE nr. 679/2016;

g) stabilirea măsurilor de securitate tehnice și organizaționale ce trebuie implementate în cadrul prelucrărilor de date;

(2) În procesul de implementare a serviciilor furnizate prin CPG, USC colaborează cu FSC în vederea armonizării aspectelor menționate la alin. (1) cu resursele tehnice alocate din cadrul CPG pentru USC.

Art. 42.

(1) În scopul verificării legalității prelucrării datelor cu caracter personal, monitorizării și asigurării integrității și securității corespunzătoare a datelor cu caracter personal, USC are obligația de a stoca informații cu privire la acțiunile de prelucrare derulate prin intermediul serviciilor de cloud furnizate în cadrul CPG.

(2) Informațiile prevăzute la alin. (1) sunt stocate sub forma unor jurnale, loguri de sistem, și sunt prezentate în mod transparent și nemijlocit persoanei vizate, la cererea acesteia sau prin intermediul aplicației de notificare a prelucrărilor de date cu caracter personal, după caz.

(3) Scopul jurnalizării este de a pune la dispoziția cetățeanului sau instituțiilor autorizate, la cerere, istoricul privind acțiunile asupra datelor cu caracter personal găzduite în CPG derulate de o persoană, entitate sau sistem.
(4) Implementarea jurnalizării cuprinde dezvoltarea unor soluții tehnice astfel încât să asigure prelucrarea datelor și nerepudierea acțiunilor produse în sistemele și aplicațiile cloud de către factorul uman sau de aplicații, servicii sau interfețe de conectare.
(5) USC, cu sprijinul FSC, asigură înregistrarea, autentificarea, autorizarea, identificarea, notificarea și jurnalizarea datelor. În acest sens, ADR stabilește procedurile ce trebuie respectate în vederea realizării jurnalizării.
(6) ADR întreprinde toate demersurile pentru prevenirea, modificarea, și distrugerea, fără drept, a înregistrărilor din jurnal, respectiv pentru protejarea autenticității și a continuității procesului de înregistrare al evenimentelor, cu excepțiile stabilite doar prin cadrul legislativ.
(7) Autoritățile și instituțiile publice implementează și actualizează, periodic, instrumentele care să permită identificarea și transmiterea acțiunilor de prelucrare a datelor prevăzute la alin. (1) în vederea transmiterii acestora către serviciul de jurnalizare prevăzut la alin. (2).

Art. 43.

Jurnalele de acces la date sunt păstrate pentru o perioadă de 36 luni de la data înregistrării acțiunii privind datele respective.

Art. 44.

(1) Autoritățile și instituțiile publice, sub coordonarea ADR, dezvoltă politici și proceduri care să definească cerințele obligatorii pentru jurnalizarea acțiunilor asupra datelor cu caracter personal și comercial.
(2) Autoritățile și instituțiile publice asigură generarea înregistrărilor iar ADR asigură transmiterea și stocarea acestor evenimente de jurnalizare.
(3) ADR stabilește modalitatea de transfer a evenimentelor, frecvența evenimentelor care trebuie să fie transferate și regulile de securitate ale datelor din jurnal în tranzit, astfel încât să se asigure confidențialitatea, integritatea și disponibilitatea acestora.

Art. 45.

(1) ADR pune la dispoziție o aplicație pentru generarea de notificări în vederea informării cetățenilor cu privire la orice acțiune întreprinsă cu privire la acțiunile legate de datele cu

caracter personal sau comercial ale unei persoane, entități sau sistem și orice actualizări relevante pentru titularul datelor.

(2) Aplicația generează două tipuri de notificări:

a) Notificări declanșate datorită acțiunilor produse de factor uman

b) Notificări declanșate de aplicație, serviciu sau interfața de conectare

(3) Prin aceste notificări se asigură informarea corectă și nemijlocită a titularului datelor cu caracter personal privind acțiunile realizate la nivelul platformei care-i vizează direct datele cu caracter personal, precum și cine a fost inițiatorul acțiunii.

CAPITOLUL VII

Politica cloud first

Art. 46.

(1) Politica cloud first promovează serviciile cloud computing ca tehnologie prioritară pentru administrarea și furnizarea de servicii publice la nivel central și local.

(2) Autoritățile și instituțiile publice utilizează Platforma ca primă opțiune pentru implementarea de noi aplicații și servicii.

(3) Autoritățile și instituțiile publice, la elaborarea strategiei de investiții în domeniul TIC, vor include în criteriile de analiză care determină introducerea în programul de investiţii a obiectivelor noi de investiții TIC următoarele cerințe:

a) prioritizarea opțiunii de cloud ready sau cloud nativ;

b) respectarea prevederilor Hotărârii Guvernului nr. 941 din 27 noiembrie 2013 privind organizarea și funcționarea Comitetului Tehnico-Economic pentru Societatea Informațională, cu modificările și completările ulterioare pentru obținerea avizului conform.

(4) Începând cu data de la care este operațional CPG, autoritățile și instituțiile publice centrale, cu excepția celor prevăzute în Ordonanță, au obligația utilizării serviciilor de cloud disponibile, conform catalogului de servicii.

(5) În aplicarea prevederilor art. 1 alin. (7) din Ordonanță, toate aplicațiile informatice dezvoltate de autoritățile și instituțiile publice centrale cu finanțare din fonduri publice sunt de tip cloud ready sau cloud nativ.

(6) Autoritățile și instituțiile publice actualizează componenta TIC din strategia proprie pentru adoptarea serviciilor de cloud.

Art. 47.

(1) Prin derogare de la prevederile art. 46 alin (2), autoritățile și instituțiile publice pot implementa noi aplicații și servicii în afara Platformei, în urma obținerii unui aviz favorabil din partea Comitetului tehnico-economic pentru societatea informațională, emis în baza unor criterii tehnico-economice clare, transparente, previzibile și predictibile.
(2) Autoritățile și instituțiile publice care au calitatea de USC adoptă proceduri interne de management al serviciilor de cloud contractate.
(3) Costurile aferente interoperabilității și interconectării la nivel de servicii pentru serviciile de la alin. (1) sunt suportate de către autoritatea sau instituția publică care le solicită.

CAPITOLUL VIII
DISPOZIȚII FINALE ȘI TRANZITORII

Art. 48.

(1) Ordinul ministrului cercetării, inovării și digitalizării prevăzut la art. 32 se emite în maximum 180 de zile de la intrarea în vigoare a prezentei hotărâri.
(2) Modelul acordului de migrare, integrare și interconectare prevăzut la art. 17, alin. (1) se emite prin ordin al ministrului cercetării, inovării și digitalizării în termen de maximum 180 de zile de la intrarea în vigoare a prezentei hotărâri.
(3) Contractul de furnizare de servicii prevăzut la art. 17, alin. (2) se emite prin ordin al ministrului cercetării, inovării și digitalizării în termen de maximum 180 de zile de la intrarea în vigoare a prezentei hotărâri.
(4) Modelul acordului-cadru prevăzut la prevederile art. 21, alin. (1) se emite prin ordin al ministrului cercetării, inovării și digitalizării în termen de maximum 180 de zile de la intrarea în vigoare a prezentei hotărâri.
(5) Încadrarea datelor prevăzute la art. 32 se realizează prin ordin al ministrului cercetării, inovării și digitalizării în termen de maximum 180 de zile de la intrarea în vigoare a prezentei hotărâri.
(6) Procedurile prevăzute la art. 43 alin. (5) se stabilesc prin decizie a președintelui ADR în termen de maximum 180 de zile de la intrarea în vigoare a prezentei hotărâri.

PRIM-MINISTRU

NICOLAE-IONEL CIUCĂ