GUVERNUL ROMÂNIEI

HOTĂRÂRE

privind guvernanța Platformei de Cloud Guvernamental

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

Guvernul României adoptă prezenta hotărâre.

Capitolul I

Dispoziții generale

Art. 1.

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

a) politica, strategia, criteriile tehnice și operaționale privind implementarea, operarea, mentenanța și dezvoltarea ulterioară a Platformei de Cloud Guvernamental, denumită în continuare Platforma, precum și interconectarea sistemelor informatice;

b) 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;

c) 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;

d) cadrul de asigurare a confidențialității, securității, interoperabilității, adaptării la standarde tehnice și semantice, respectiv a performanței aplicațiilor și serviciilor de cloud de tip Iaas, Paas, SaaS 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;

e) 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;

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

c) centru de date - un spațiu dedicat, într-o clădire specializată pentru găzduirea sistemelor informatice și componentelor asociate, cum sunt sistemele tehnologice și cele de comunicații și de tehnologia informației;

d) cloud computing - model care permite accesul prin rețea la un grup scalabil și elastic de resurse fizice sau virtuale care pot fi folosite de către utilizatori, în mod partajat, la cerere, în sistem self-service, sub formă de servicii de cloud, respectiv IaaS, PaaS și SaaS;

e) cloud ready – aplicații dezvoltate pentru a fi implementate pe o infrastructură de cloud computing de tip public sau privat, sub formă de servicii logice decuplate în instanțe de tip mașină virtuală și/sau container;

f) cloud nativ - aplicații dezvoltate pentru a fi implementate pe o infrastructură de cloud computing, sub formă de servicii logice decuplate în instanțe de tip container, bazate pe microservicii, API-uri și microsegmentare a comunicațiilor, care beneficiază de funcționalitățile disponibile în infrastructură de cloud computing pentru a asigura disponibilitate și scalabilitate, fără a necesita planificarea tradițională a resurselor necesare;

g) date deschise - definiție conform prevederilor art. 2 lit. e) din Legea nr. 179/2022 privind datele deschise și reutilizarea informațiilor din sectorul public;

h) entități private - furnizorii de servicii de clouduri publice și private;

i) 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;

j) interconectare - conectarea serviciilor, a micro serviciilor, a aplicațiilor sau a bazelor de date pentru schimb de date;

k) management al identității - metode, instrumente, tehnici și proceduri de validare a identității, atunci când se accesează anumite componente ale Platformei;

l) microservicii - abordare arhitecturală care organizează aplicațiile în colecții de servicii decuplate care comunică prin intermediul unor API definite;

m) platforma API gateway - instrument de management care reprezintă punctul de intrare unic pentru API-uri și microservicii back-end definite, atât interne, cât și externe, folosit pentru interconectarea aplicațiilor și serviciilor informatice, impunând securitatea și asigurând scalabilitate și disponibilitate ridicată;

n) resurse - elemente de infrastructură formate din unități de procesare, stocare, memorie, comunicații, securitate cibernetică, licențe sau subscripții software, utilizate pentru a oferi servicii de cloud;

o) Service Level Agreement (SLA) - document care conține condițiile specifice și măsurabile legate de nivelul agreat al serviciilor.;

p) 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;

q) servicii în tehnologie de cloud - servicii sau aplicații de tehnologia informației și comunicațiilor furnizate prin intermediul serviciilor de cloud, care includ, dar nu se limitează la, stocarea, transmiterea sau procesarea datelor;

r) utilizator de servicii de cloud (USC) - autoritate și instituție publică din România care utilizează servicii de cloud furnizate în cadrul Platformei.

(2) Termenii și expresiile utilizate în prezenta hotărâre se completează cu cele prevăzute în 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 sunt:

a) realizarea accesului securizat la date;

b) alinierea cu obiectivele naționale de digitalizare, prin proiectarea și furnizarea serviciilor realizate, corelat cu legislația și strategiile naționale de digitalizare și securitate cibernetică;

c) conformitatea Platformei cu politicile și standardele din Capitolul II, prin proiectarea și furnizarea serviciilor cu respectarea prevederilor prezentei hotărâri;

d) interconectarea sistemelor prin asigurarea accesului sigur, rapid, facil și jurnalizat la servicii;

e) implementarea conceptului „*doar o singură dată*” prin care datele minimal necesare sunt solicitate de la titular o singură dată și apoi sunt utilizate de toți USC, în baza accesului acordat;

f) orientarea proiectării, dezvoltării și furnizării serviciilor de cloud în funcție de nevoile identificate ale USC;

g) dezvoltarea unor mecanisme de jurnalizare a operațiunilor de prelucrare a datelor, în vederea auditării ulterioare, în scopul asigurării transparenței prelucrării datelor cu caracter personal;

h) partajarea responsabilităților în cadrul Platformei între FSC și USC;

i) prelucrarea sigură a datelor în cadrul serviciilor furnizate în Platformă, cu garantarea specificării și limitarea scopului fiecărei prelucrări de date, prin adoptarea de către USC a unor măsuri tehnice și organizatorice în scopul asigurării unui nivel adecvat de protecție a datelor;

j) evitarea denaturării concurenței și asigurarea tratamentului egal pentru toți FSC, prin furnizarea soluțiilor complete de cloud, dezvoltate în cadrul CPG sau livrate către Platformă de către FSC;

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 și instituțiile publice, reformarea operațiunilor și a proceselor administrative din cadrul autorităților și instituțiilor publice având la bază un fundament de transformare digitală, pentru a maximiza beneficiile procesului de transformare electronică a guvernării;

b) accelerarea și eficientizarea adoptării și reutilizării infrastructurii de digitalizare a serviciilor publice electronice;

c) implementarea, de către autoritățile și instituțiile publice, a politicii, standardelor tehnice și a celor mai bune practici internaționale în domeniul tehnologiei informației și comunicațiilor, denumit în continuare TIC;

d) elaborarea și implementarea unui cadru de investiții în TIC pentru a valorifica beneficiile tuturor soluțiilor și tehnologiilor de cloud computing și a reutiliza infrastructura de digitalizare a serviciilor publice electronice;

e) formarea abilităților personalului și dezvoltarea capacităților în domeniul TIC ale autorităților și instituțiilor publice, prin dezvoltarea de platforme de colaborare și prin încheierea de parteneriate public-private, cu preluarea practicilor inovative și inteligente în implementarea TIC;

f) facilitarea, prin marketplace, a oportunităților de furnizare, de către mediul privat, de servicii de cloud, servicii de dezvoltare de software, soluții și aplicații informatice ce vor fi utilizate de instituțiile și autoritățile publice;

g) deschiderea serviciilor guvernamentale de cloud computing către mediul privat în ceea ce privește achiziționarea de bunuri și servicii.

Art. 5.

La nivelul Platformei se stabilesc următoarele roluri:

a) Furnizor de servicii cloud (FSC);

b) Utilizator de servicii cloud (USC).

Art. 6.

(1) Furnizarea serviciilor oferite în cadrul CPG se asigură de către ADR, în baza contractului de furnizare servicii încheiat cu USC.

(2) SLA este stabilit prin acorduri de administrare încheiate de ADR cu STS și SRI.

(3) SLA este stabilit prin acorduri de administrare încheiate de ADR cu FSC, pentru serviciile de cloud public din Platformă.

(4) În vederea asigurării funcționării optime a serviciilor de cloud furnizate în CPG, ADR, împreună cu STS, asigură funcționalitatea modulului de raportare periodică automată, care actualizează datele din grila de indicatori de performanță tehnică, aprobată de către administrator și FSC.

(5) Rapoartele generate în urma realizării activității de monitorizare, control și evaluare a serviciilor de cloud furnizate în CPG, potrivit prevederilor alin. (3), stau la baza luării deciziilor corective pe parcursul administrării operaționale a Platformei și a evaluării performanței serviciilor de cloud furnizate.

Art. 7.

(1) Furnizarea serviciilor de cloud oferite în cadrul Platformei poate fi suspendată temporar la inițiativa USC, printr-o cerere adresată FSC, pentru următoarele motive:

a) transformarea sau încetarea personalității juridice;

b) mutarea unui serviciu existent de la un USC la alt USC;

c) înlocuirea unui serviciu cu alt serviciu;

d) mutarea unui serviciu sau modificarea tehnică a acestuia;

e) incidente sau modificări de servicii de comunicații;

f) incidente de securitate cibernetică.

(2) Furnizarea serviciilor de cloud oferite în cadrul Platformei pentru USC poate fi suspendată temporar de către FSC, cu acordul prealabil al STS sau SRI, conform atribuțiilor prevăzute la art. 5 și 6 din Ordonanță, respectiv al USC, în cazul în care este compromisă funcționarea serviciilor și a sistemelor informatice ale USC.

(3) Furnizarea serviciilor de cloud oferite în cadrul Platformei poate fi suspendată temporar fără acordul USC, pentru o perioadă de maxim 72 ore de către FSC și la solicitarea STS sau SRI, cu notificarea USC în termen de maxim 24 ore , în următoarele cazuri:

a) în cazul în care, prin furnizarea serviciilor de cloud oferite în cadrul Platformei, se constată existența unor amenințări la adresa securității naționale a României;

b) în situații de forță majoră;

c) în cazul declarării mobilizării totale sau parțiale, a stării de urgență, stării de asediu sau stării de război, potrivit legii.

(4) În cazurile prevăzute la alin. (2) și (3), furnizarea serviciilor se suspendă până la remedierea situației create. Furnizarea serviciilor este reluată de îndată ce cauza suspendării a încetat.

Art. 8.

(1) În situația în care USC stabilește faptul că serviciile solicitate sau aplicațiile utilizate nu mai corespund cerințelor sale operaționale, tehnice și de securitate și nici nu au fost extinse sau modernizate la solicitarea sa, USC solicită FSC eliberarea, total sau parțial, a resurselor .

(2) Eliberarea resurselor informatice, astfel cum sunt definite la art. 2, alin(1), lit. n), utilizate de USC se realizează în temeiul clauzelor stabilite prin contractul de furnizare.

(3) Responsabilitatea legală privind stabilirea scopurilor și mijloacelor de prelucrare, respectarea principiilor de prelucrare, colectarea datelor, păstrarea, distrugerea, respectiv ștergerea acestora, aparține, în mod partajat, USC, FSC, ADR, SRI și STS.

Art. 9.

(1) Dezvoltarea Platformei se realizează prin:

a) extinderea capacității de procesare și stocare a datelor;
b) crearea de noi centre de date pentru creșterea gradului de disponibilitate și reziliență a sistemelor informatice;
c) sporirea capacității de automatizare și autoservire pentru USC, pentru a beneficia în mod eficient de avantajele cloud computing;
d) furnizarea de noi servicii și platforme de dezvoltare a aplicațiilor software;

e) extinderea funcționalităților resurselor și serviciilor furnizate prin intermediul cloudurilor publice;

(2) Pentru dezvoltarea Platformei, MCID asigură:

a) actualizarea cadrului legal pentru facilitarea dezvoltării Platformei;
b) crearea unui program de dezvoltare, antrenare și certificare a abilităților TIC, pentru USC și beneficiarii finali ai serviciilor de cloud, raportat la utilizarea Platformei;
c) elaborarea unui plan de integrare a noilor centre de date într-un mediu cloud distribuit în rețea;
d) elaborarea, planificarea și asigurarea bugetului necesar funcționării și dezvoltării Platformei.

Art. 10.

Serviciile de cloud furnizate pentru USC prin Platformă trebuie să asigure cumulativ următoarele criterii tehnice și operaționale:

a) acces facil al USC la rețea - funcționalitățile serviciilor de cloud sunt accesibile prin intermediul unor mecanisme standardizate;
b) autoservire la cererea USC - după alocarea resurselor în vederea furnizării serviciului, 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 FSC;
c) alocarea și eliberarea rapidă și flexibilă a resurselor;
d) criterii de performanță - fiabilitate, disponibilitate, scalabilitate, oportunitate, utilizabilitate, timp de răspuns, capacitate de transfer, gestionarea optimă a resurselor;
e) contorizarea resurselor - resursele care stau la baza furnizării serviciilor de cloud sunt monitorizate, gestionate și raportate în vederea asigurării transparenței;
f) optimizarea automată a serviciilor de cloud în baza măsurătorilor efectuate cu ajustarea resurselor alocate de către sistemele de cloud computing.
g) punerea în comun a resurselor - utilizarea funcționalităților serviciilor de cloud se bazează pe partajarea dinamică a resurselor tehnice între mai mulți USC după criterii de disponibilitate a resurselor fizice sau virtuale;

Art. 11.

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

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.

Art.12.

În funcție de tipul și de modelul de furnizare a serviciului de cloud, ADR elaborează un set de cerințe și măsuri tehnice de performanță și securitate cibernetică la nivelul Platformei, realizat cu sprijinul STS și SRI, în conformitate cu prevederile art. 4 alin. (1) din Ordonanță, aprobat prin decizia președintelui ADR.

Art. 13.

(1) În calitate de administrator operațional al CPG, la nivel de SaaS și în vederea gestionării marketplace, ADR:

a) primește și analizează cerințele operaționale ale USC pentru dezvoltarea serviciilor din CPG;
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 CPG de către autoritățile și instituțiile publice din România;
e) asigură listarea, administrarea și delistarea în/din marketplace a aplicațiilor și serviciilor disponibile;
f) monitorizează eficiența utilizării resurselor și propune actualizări la strategia de dezvoltare ulterioară a CPG;
g) întreprinde demersurile necesare pentru instruirea personalului USC în ceea ce privește utilizarea marketplace;
h) monitorizează respectarea SLA-urilor;
i) acordă suport tehnic USC în procesul de management al riscurilor, în vederea adoptării tehnologiilor de cloud;
j) stabilește, prin decizie a președintelui ADR, autoritățile și instituțiile publice ale căror sisteme informatice și servicii publice electronice se interconectează, cu acordul prealabil al autorității sau instituției publice respective, în CPG în vederea schimbului de date;
k) propune actualizarea listei autorităților și instituțiilor publice ale căror sisteme informatice și servicii publice electronice migrează în CPG;
l) asigură administrarea tehnică și operațională a serviciilor de cloud de tip SaaS în CPG;
m) coordonează activitățile de instalare, configurare, integrare, testare și trecere în producție a tehnologiilor, soluțiilor și serviciilor software și monitorizează rezultatele finale;
n) colaborează permanent cu SRI pentru asigurarea securității cibernetice a serviciilor de cloud SaaS furnizate;
o) administrează componenta de marketplace;
p) administreaza Platforma de tip API Gateway;
q) monitorizează eficiența utilizării resurselor prin care se asigură furnizarea aplicațiilor listate în marketplace;
r) pune la dispoziție procedurile și documentația necesară pentru utilizarea și administrarea marketplace;

s) asigură serviciile de suport și mentenanță pentru componenta marketplace;
t) se asigură de publicarea specificațiilor tehnice minimale, respectiv a cerințelor tehnice și funcționale ale aplicațiilor ce vor fi furnizate prin componenta marketplace a Platformei;
u) validează și avizează aplicațiile care vor fi publicate;
v) asigură confidențialitatea informațiilor comerciale;
w) asigură optimizarea costurilor prin adoptarea modelelor de servicii SaaS, partajate între autoritățile și instituțiile publice;
x) asigură, cu titlu gratuit, furnizarea serviciilor aferente CPG din marketplace pentru USC, inclusiv a serviciilor de securitate cibernetică asociate.

(2) În calitate de furnizor de servicii cloud, ADR are următoarele responsabilități:

a) primește, analizează și soluționează solicitarea serviciilor de cloud din Platformă, în baza cererii formulate de către USC;
b) asigură furnizarea serviciilor în Platformă în baza contractelor de furnizare servicii de tip cloud încheiate cu USC;
c) stabilește SLA ca parte integrantă a contractului de furnizare de servicii și definește calitatea și nivelul serviciilor;
d) asigură suportul tehnic, împreună cu STS și SRI, pentru administratorul desemnat de USC, prin intermediul unui punct de contact unic - service desk - pentru serviciile de cloud furnizate;
e) întreprinde demersuri pentru asigurarea resurselor financiare în vederea aplicării strategiei privind adoptarea, dezvoltarea și mentenanța Platformei;
f) colaborează cu STS și SRI, pentru întocmirea analizei de risc pentru respectarea prevederilor art. 3 alin. (7) din Ordonanță;
g) informează USC cu privire la rezultatele auditurilor de securitate, sub garantarea confidențialității, precum și cu privire la incidentele de securitate fizică și cibernetică, sens în care oferă suport adecvat, în limita competențelor, pentru gestionarea posibilelor riscuri de protecție a datelor prezentate de astfel de incidente;
h) asigură, în mod partajat cu USC, respectarea politicilor, standardelor și criteriilor aplicabile serviciilor de cloud în cadrul Platformei;
i) asigură implementarea principiului „*doar o singură dată*” la nivelul autorităților și instituțiilor publice.

Art. 14.

(1) În calitate 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 ulterioare;

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 și de performanță 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 credentiale 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 și propune ADR termenii și condițiile generale minime pentru furnizarea 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 și al serviciilor de cloud de tip IaaS și PaaS din cadru 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, prin intermediul 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 temporar, pe o perioadă limitată hotărâtă de comun acord cu ADR și USC, activitatea unor resurse a căror funcționare vulnerabilizează serviciile furnizate, cu obligația de a notifica ADR și USC în termen de 24 de ore.

(3) La solicitarea USC, transmisă 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) În calitate de administrator de securitate cibernetică a serviciilor de cloud de tip SaaS, din cadrul CPG, SRI are următoarele responsabilități:

a) asigură securitatea cibernetică a serviciilor de cloud de tip SaaS din CPG prin cunoașterea, prevenirea și contracararea atacurilor, amenințărilor, riscurilor și vulnerabilităților cibernetice, inclusiv a celor complexe, de tip APT, îndreptate împotriva serviciilor CPG de tip SaaS și a entităților găzduite;
b) cooperează cu STS, conform competențelor fiecărei instituții, pentru cunoașterea, prevenirea și contracararea atacurilor cibernetice complexe, de tip APT, îndreptate împotriva serviciilor specifice

CPG la nivel IaaS și PaaS, prin schimbul nemijlocit și automat al informațiilor referitoare la incidentele de securitate, fără a transfera date de conținut;

c) coopereaza cu ADR și STS, conform atribuțiilor, pentru asigurarea unitară a securității cibernetice a CPG;
d) asigură alocarea serviciilor de securitate cibernetică la nivel SaaS, în funcție de necesitate și de resursele disponibile;
e) colaborează cu ADR pentru stabilirea criteriilor minime de performanță pentru furnizarea serviciilor de securitate cibernetică la nivel SaaS;
f) asigură suport de specialitate, la solicitarea ADR, pentru derularea activităților de audit tehnic și de securitate desfășurate în cadrul Platformei;
g) analizează, din punct de vedere al securității cibernetice, lista autorităților și instituțiilor publice ale căror sisteme informatice și servicii publice electronice solicită migrare în CPG și transmite către ADR rezultatul analizei;
h) colaborează cu ADR și STS pentru întocmirea analizei de risc;
i) propune ADR blocarea activității unor resurse provizionate de USC, a căror funcționare necorespunzătoare poate afecta serviciile furnizate;
j) solicită ADR estimări privind nevoia viitoare de resurse, în scopul dezvoltării serviciilor administrate;
k) notifică ADR privind utilizarea improprie a unor resurse tehnice de către USC și solicită suspendarea accesului acestuia, cu conservarea resurselor, dacă USC nu răspunde în termen de 30 de zile;
l) notifică ADR cu privire la neîndeplinirea obligațiilor USC;
m) propune MCID și ADR, împreună cu STS și DNSC, soluții tehnice și criterii pentru asigurarea securității cibernetice în cadrul Platformei;
n) aplică standardele și implementează măsurile de securitate cibernetică pentru protecția serviciilor de cloud de tip SaaS;
o) participă și asigură suport pentru evaluarea serviciilor de tip SaaS ce urmează a fi publicate de către ADR în marketplace, în faza de testare, înainte de lansarea lor în producție;
p) asigură testarea din punct de vedere al securității cibernetice a serviciilor de tip SaaS și, la cererea USC, transmisă prin ADR, pentru celelalte USC de tip IaaS și PaaS;
q) asigură, împreună cu structurile responsabile cu securitatea cibernetică competente, testarea din punct de vedere al securității cibernetice a serviciilor de tip SaaS a autorităților și instituțiilor prevăzute în art. 7 alin. (1) din Ordonanță;
r) avizează lansarea în producție a serviciilor de tip SaaS din punct de vedere al securității cibernetice;
s) asigură izolarea USC care nu respectă standardele și criteriile pentru asigurarea securității cibernetice pentru serviciile de tip SaaS alocate în CPG,
t) implementează politicile, standardele și criteriile aplicabile serviciilor de securitate cibernetică;
u) formulează, împreună cu STS, propuneri către MCID și ADR pentru modificarea politicilor, standardelor și criteriilor aplicabile serviciilor de securitate cibernetică;
v) gestionează resursele financiare pentru achiziționarea și mentenanța resurselor necesare asigurării serviciilor de securitate cibernetică;
w) raportat la nivelul cererii și necesarul de resurse, gestionează fondurile financiare pentru realizarea investițiilor și măsurilor suplimentare, necesare asigurării securității cibernetice.

Art. 16.

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

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 și realizează auditurile de conformitate pe linia securității, trasabilității datelor și a calității serviciilor de cloud alocate,;

d) solicită, prin intermediul marketplace, furnizarea de servicii cloud puse la dispoziție de FSC;

e) răspunde de procesul de management al riscurilor pentru adoptarea tehnologiilor cloud în cadrul Platformei;

f) încheie convenții de administrare a serviciilor cloud, publicate de FSC, prin Platforma.

g) implementează politicile, standardele și criteriile aplicabile serviciilor de cloud utilizate, în aria de competență;

h) realizează copii de siguranță a datelor aplicațiilor și sistemelor informatice implementate;

i) aplică standardele și implementează măsurile de securitate conform criteriilor stabilite, în baza modelului de serviciu de cloud alocat;

j) 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 de către FSC.

Art. 17.

În aplicarea prevederilor art. 15 din Ordonanță, se stabilesc următoarele cerințe minime de încheiere a convenției de administrare a serviciilor de cloud, prevăzută la art. 16, lit. (f):

a) cerințe tehnice și de responsabilitate, privind securitatea datelor, aplicate pentru furnizarea serviciilor;

b) nivelul agreat al serviciilor, inclusiv indicatorii de performanță ai acestora;

c) răspunderea contractuală a părților și limitările acesteia;

d) principiile efectuării sau comandării unui audit de către părți asupra modului de implementare a convenției;

e) proceduri pentru utilizarea serviciilor de cloud alocate;

f) repartizarea atribuțiilor legate de utilizarea serviciilor de cloud, inclusiv obligațiile FSC și asigurarea nivelului de calitate convenit;

g) regulile de întreținere tehnică furnizate ca parte a întreținerii serviciilor;

h) obligații în domeniul drepturilor de proprietate intelectuală;

i) proceduri și reguli de răspuns la incidente de securitate;

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 convenției;

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, ADR asigură, la cererea USC, consultanță tehnică, precum și resurse tehnice, cu titlu gratuit, pe o perioadă de maximum 60 de zile, în vederea testării serviciilor în tehnologie cloud ce urmează a fi furnizate prin serviciile de cloud din CPG utilizate.

(2) În situația în care ADR 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) Situațiile de imposibilitate obiectivă prevăzută la alin. (2) sunt:

a) depășirea competențelor de asigurare a consultanței tehnice, care ar reveni expres unei alte autorități publice centrale;

b) excepția de neexecutare, invocată în condițiile art. 1556 din Legea nr. 287/2009 privind Codul civil, cu modificările și completările ulterioare;

c) forța majoră;

d) 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.

(1) 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.

(2) Pentru serviciile de tip IaaS, USC are următoarele responsabilități:

a) gestionează accesul la resursele de cloud alocate în vederea administrării acestora;

b) dezvoltă, instalează şi gestionează componentele software necesare bunei funcţionări a sistemelor informatice proprii, găzduite pe resursele de cloud alocate;

c) asigură integrarea, în caz de necesitate, a sistemelor informatice proprii, găzduite pe resursele de cloud alocate, cu alte sisteme informatice;

d) 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;

e) administrează sistemele informatice proprii, găzduite pe resursele de cloud alocate, inclusiv acordă drepturile de acces la diferite componente ale sistemelor informatice;

f) 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;

g) asigură protejarea datelor în cadrul sistemelor informatice proprii găzduite, precum şi crearea şi stocarea copiilor de rezervă;

h) asigură documentarea tehnică a sistemelor informatice proprii, găzduite pe resursele de cloud alocate;

i) asigură instruirea şi suportul utilizatorilor sistemelor informatice proprii, găzduite pe resursele de cloud alocate;

j) asigură managementul riscurilor în abordarea tehnologiilor de cloud;

k) asigură implementarea măsurilor tehnice din aria de responsabilitate pentru gestionarea riscurilor de securitate.

(3) Pentru serviciile de tip PaaS, USC are următoarele responsabilități:

a) asigură integrarea componentelor software de platformă în sistemele informatice proprii;

b) asigură licenţierea 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;

c) administrează sistemele informatice proprii, găzduite pe resursele de cloud alocate și acordă drepturile de acces la diferite componente ale sistemelor informatice;

d) asigură, în mod partajat cu FSC, securitatea şi disponibilitatea, la nivelul resurselor de cloud alocate;

e) gestionează accesul la resursele de cloud alocate în vederea administrării acestora;

f) asigură protejarea datelor în cadrul sistemelor informatice proprii, găzduite pe resursele de cloud alocate;

g) asigură documentarea tehnică a sistemelor informatice proprii, găzduite pe resursele de cloud alocate;

h) utilizează serviciile componentelor software de platformă în strictă corespondență cu convenția, sau după caz, contractul încheiate cu FSC;

i) asigură instruirea şi suportul utilizatorilor sistemelor informatice găzduite pe resursele de cloud alocate;

j) asigură managementul riscurilor în abordarea tehnologiilor de cloud;

k) asigură implementarea măsurilor tehnice din aria de responsabilitate pentru gestionarea riscurilor de securitate.

(4) Pentru serviciile de tip SaaS, USC are următoarele responsabilități:

a) utilizează serviciile solicitate în conformitate cu prevederile contractului sau, după caz, convenției încheiate cu FSC;

b) administrează serviciile alocate, în limitele responsabilităților specificate în contractul sau, după caz, convenția încheiate cu FSC;

c) gestionează accesul la serviciile alocate, în vederea administrării acestora, în limitele responsabilităților specificate în contractul sau, după caz, convenția încheiate cu FSC;

d) asigură administrarea datelor generate în cadrul utilizării serviciilor;

e) asigură, după caz, instruirea și suportul utilizatorilor proprii.

Art. 20.

Pentru serviciile de cloud din Platformă, FSC are următoarele responsabilități:

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 servicii;

g) asigură administrarea centralizată a serviciilor furnizate;

h) acordă USC drepturile de administrare pentru serviciile furnizate;

i) asigură performanța, securitatea și disponibilitatea serviciilor furnizate în conformitate cu SLA;

j) asigură protecția datelor procesate în cadrul serviciilor, precum și crearea și stocarea copiilor de rezervă;

k) asigură, inclusiv pentru USC, documentarea serviciilor furnizate;

l) asigură suportul USC în cadrul livrării serviciilor furnizate conform nivelului de servicii agreat.

Art. 21.

(1) În aplicarea prevederilor art. 13 alin (1) lit c) și în conformitate cu prevederile Capitolului V, ADR asigură migrarea, integrarea și interconectarea cu USC.

(2) ADR, în calitate de FSC, are următoarele responsabilități:

a) gestionează accesul la resursele de cloud alocate;

b) dezvoltă, instalează și gestionează componentele software necesare bunei funcționări a serviciilor proprii, găzduite pe resursele de cloud alocate ;

c) asigură integrarea serviciilor proprii, găzduite pe resursele de cloud alocate, cu alte servicii;

d) asigură integrarea componentelor software de platformă în serviciile și aplicațiile migrate;

e) asigură, în mod partajat cu USC, securitatea și disponibilitatea, la nivelul resurselor de cloud alocate;

f) asigură analiza pentru migrarea serviciilor USC.

(3) USC are următoarele responsabilități:

a) asigură licențierea pentru sistemele de operare, precum și pentru toate componentele necesare bunei funcționări a serviciilor proprii, găzduite pe resursele de cloud alocate, cu excepția cazurilor în care FSC poate oferi licențele necesare;

b) administrează serviciile proprii, găzduite pe resursele de cloud alocate, inclusiv acordă drepturile de acces la diferite componente ale serviciilor;

c) asigură, în mod partajat cu FSC, performanța, securitatea și disponibilitatea, la nivel de sistem de operare și aplicații, a serviciilor proprii, găzduite pe resursele de cloud alocate;

d) asigură protejarea datelor procesate în cadrul serviciilor proprii, găzduite în Platformă, precum și crearea și stocarea copiilor de rezervă;

e) asigură documentarea tehnică a serviciilor proprii, găzduite pe resursele de cloud alocate;

f) asigură documentarea tehnică a serviciilor proprii, în vederea migrării în cloud;

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 serviciilor, conform tehnologiilor de cloud;

j) asigură, în mod partajat cu FSC, securitatea și disponibilitatea, la nivelul resurselor de cloud alocate;

k) gestionează accesul la resursele de cloud alocate în vederea administrării acestora;

l) asigură protejarea datelor procesate în cadrul sistemelor informatice proprii, găzduite pe resursele de cloud alocate;

m) utilizează serviciile componentelor software de platformă, conform cu acordurile de migrare și interconectare încheiate cu FSC;

n) asigură analiza și migrarea în cloud, cu excepția cazurilor în care FSC asigură această activitate;

o) asigură instruirea și suportul utilizatorilor proprii pentru serviciile găzduite pe resursele de cloud alocate, cu excepția cazurilor în care FSC asigură această activitate;

p) asigură implementarea măsurilor tehnice din aria de responsabilitate pentru gestionarea riscurilor de securitate.

Art. 22.

(1) USC utilizează serviciile de cloud furnizate dintr-un cloud public cu respectarea prevederilor art. 27 și art. 29.

(2) Costurile pentru realizarea conectării între Platformă și alte servicii furnizate de cloud public revin în sarcina USC.

Art. 23.

(1) USC care optează pentru utilizarea serviciilor de cloud public are obligația îndeplinirii cumulative a următoarelor condiții:

a) de a încadra datele utilizate pentru a permite prelucrarea acestora într-un cloud public;

b) de a respecta cerințele autorităților și instituțiilor publice de confidențialitate, securitate, integritate și disponibilitate;

c) de a se asigura că serviciile de cloud public îi sunt oferite pe infrastructuri de bază aflate pe teritoriul statelor membre ale UE;

d) de a demonstra capacității de a utiliza și gestiona în mod corespunzător aceste servicii;

e) de a implementa mecanisme, proceduri tehnice și norme care garantează faptul că datele USC din cloudul public nu sunt accesate de către FSC, cu excepția situațiilor reglementate expres prin contractul de furnizare a serviciilor de cloud.

(2) În vederea îndeplinirii condițiilor prevăzute la alin. (1), la solicitarea ADR, USC prezintă următoarele date:

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.

CAPITOLUL III

Platforma de tip API Gateway

Art. 24.

(1) Se instituie Platforma de tip API Gateway în vederea asigurării interconectării sistemelor informatice ale autorităților și instituțiilor publice din Platforma de Cloud Guvernamental

(2) Suportul tehnic al Platformei de tip API Gateway este asigurat de o infrastructură informatică, care permite schimbul de date automat între autoritățile și instituțiile publice, în vederea asigurării interconectării aplicațiilor și serviciilor informatice pentru furnizarea serviciilor în Platformă.

(3) Datele cu caracter personal aflate în tranzit prin intermediul Platformei de tip API Gateway sunt criptate.

(4) În vederea asigurării securității cibernetice a Platformei de tip API Gateway, ADR colaborează cu DNSC, STS și SRI.

(5) În vederea asigurării securității comunicațiilor prin rețelele de transmisii de date utilizate de Platforma de tip API Gateway, ADR colaborează cu STS.

(6) ADR asigură suport pentru implementarea cerințelor de interconectare a Platformei cu cloud-urile private, implementate de autoritățile și instituțiile publice.

(7) ADR, în calitate de unic administrator al Platformei de tip API Gateway are următoarele atribuții:

a) asigură interconectarea la nivel de servicii a aplicațiilor din CPG prin intermediul platformei de tip API Gateway, din bugetul ADR;

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 în relația cu instituțiile și autoritățile publice;

f) asigură jurnalizarea accesului la date;

(8) ADR publică specificațiile tehnice necesare interconectării la nivel de aplicații și servicii în Platformă.

j) În ceea ce privește prelucrarea datelor cu caracter personal, ADR are rolul de persoană împuternicită de operator în relația cu autoritățile și instituțiile publice conectate, care au rol de operatori de date cu caracter personal, fiind responsabile de stabilirea scopurilor și a mijloacelor de prelucrare a datelor cu caracter personal, conform art. 4 alin (7) din Regulamentul nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulatie a acestor date şi de abrogare a Directivei 95/46/CE, denumit în continuare Regulamentul.

(9) ADR, în calitate de persoană împuternicită de operator ce oferă serviciul API Gateway, se asigură că respectă obligațiile stabilite prin art 28 alin (3) din Regulament.

(10) Autoritățile și instituțiile 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 prevăzute la alin. (7) lit. a);

c) implementează măsurile necesare pentru respectarea politicii referitoare la securitatea și confidențialitatea datelor.

CAPITOLUL IV

Cadrul de management și stocare a datelor în Platformă, inclusiv stabilirea categoriilor de date prelucrate în Platformă și găzduite de CPG

Art. 25.

În funcție de cerințele USC, de 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 în Platformă;

c) proiectare, folosind tehnologii native cloud pe baza cerințelor USC și cu respectarea standardelor și cerințelor aplicabile Platformei.

Art. 26.

Lista completă a aplicațiilor și serviciilor oferite în cadrul Platformei este publicată în marketplace și cuprinde denumirea serviciilor, descrierea acestora, modul de solicitare și contractare, tarifele pentru servicii, condițiile de utilizare serviciilor, termenii și condițiile de furnizare a serviciilor, precum și alte informații pentru utilizarea acestora.

Art. 27.

(1) Serviciile de cloud public furnizate în cadrul Platformei sunt oferite prin rețelele publice de comunicații.

(2) Serviciile de cloud furnizate în cadrul CPG sunt oferite prin intermediul rețelelor de comunicații aflate în administrarea STS.

(3) Stocarea datelor prevăzute la Art. 28 alin (1) lit c). se realizează în infrastructuri tehnice localizate în România, iar pentru datele prevăzute la Art 28 alin(1) lit a) stocarea se realizează în infrastructuri tehnice localizate pe teritoriul Uniunii Europene, fără a include teritoriile de peste mări.

Art. 28.

(1) Categoriile de date ce sunt utilizate în Platformă, sunt:

a) date cu caracter personal;

b) date fără caracter personal;

c) categorii speciale de date cu caracter personal.

(2) Contractul de furnizare servicii încheiat între FSC și USC cuprinde și obligațiile stabilite la art. 28 alin. (3) din Regulament.

(3) Persoana împuternicită, pentru acces la date în scop de mentenanță corectivă, oferă asistență tehnică asupra aplicațiilor sau sistemelor informatice ale USC, în prezența unui reprezentant al acestuia, conform prevederilor stabilite prin acordul/contractul încheiat.

Art. 29.

(1) USC, înainte de utilizarea serviciilor furnizate prin Platformă, are responsabilitatea de a încadra și gestiona datele, în funcție de nivelul de risc asociat, rezultat al evaluării de impact efectuate conform prevederilor art. 35 din Regulament.

(2) USC, prin contractul de furnizare/administrare cu fiecare FSC, stabilește criteriile și cerințele specifice pentru asigurarea securității și confidențialității datelor utilizate în Platformă.

(3) FSC nu are drept de dispoziție asupra datelor USC.

(4) USC, prin contractul de furnizare/administrare cu FSC, stabilește și actualizează politica și procedurile pentru efectuarea evaluărilor de securitate ale sistemului informatic, ținând cont de evaluarea de impact și analiza riscurilor actualizate.

(5) În funcție de încadrarea datelor potrivit prevederilor art. 28, alin. (1), USC selectează tipul de cloud ce va găzdui datele, astfel:

a) categoriile speciale de date pot fi găzduite doar în CPG sau alte clouduri private ale autorităților și instituțiilor publice interconectate în cadrul Platformei;

b) datele, altele decât cele prevăzute la lit. a), pot fi găzduite în oricare dintre cloudurile din cadrul Platformei;

Art. 30.

Suplimentar evaluării de impact prevăzute la art. 29 alin. (1), USC realizează și o evaluare care are în vedere următoarele elemente:

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;

CAPITOLUL V

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. 31.

(1) ADR, conform prevederilor art 4 alin. (2) din Ordonanță, elaborează metodologia pentru identificarea, selectarea și prioritizarea aplicațiilor și serviciilor care urmează a fi migrate în CPG .

(2) În acest scop, ADR efectuează o analiză a proceselor și a aplicațiilor curente din cadrul autorității sau instituției publice, în vederea migrării.

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

(4) ADR poate solicita și primi rapoarte de evaluare de impact de la 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 ADR la infrastructură 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, în baza acordului de migrare încheiat cu ADR, planul de migrare în baza arhitecturii comune de date și a metodologiei de migrare.

(8) ADR, împreună cu autoritățile și instituțiile publice ale căror aplicații și servicii migrează, 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 interconectare, jurnalizare, notificare și securitate;

e) evaluarea potențialului de reutilizare a aplicațiilor și serviciilor de uz general și de provizionare ca și servicii de tip SaaS, pentru alte autorități și instituții publice.

(9) Urmare evaluării prevăzute la alin. (8), ADR elaborează și pune la dispoziția autorităților și instituțiilor publice planuri de mentenanță corectivă a aplicațiilor și serviciilor migrate, în vederea aplicării acestora, în conformitate cu prevederile acordului de migrare încheiat.

Art. 32.

(1) STS, la solicitarea ADR, pune la dispoziție resurse tehnice din CPG, de tip IaaS și PaaS, 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 la art. 6 și 7 din Ordonanță.

(3) ADR stabilește, prin acordul de migrare încheiat cu USC, planul de migrare în baza analizei tehnico-economice a serviciilor și aplicațiilor ce vor migra, evaluarea resurselor și a efortului tehnico-economic.

Art. 33.

(1) ADR asigură analiza, migrarea, găzduirea, integrarea și interconectarea, în interiorul CPG, în limita bugetului alocat în acest sens, a aplicațiilor și serviciilor informatice ale autorităților și instituțiilor publice centrale prevăzute în Anexă, parte integrantă din prezenta hotărâre.

(2) Prevederile alin. (1) se aplică și autorităților și instituțiilor aflate în subordinea sau sub coordonarea celor prevăzute în Anexă.

(3) Lista autorităților și instituțiilor prevăzute la alin. (1) se actualizează periodic în funcție de solicitările entităților publice, pentru a fi găzduite în Platformă. precum și interconectarea/integrarea serviciilor publice în Platformă.

CAPITOLUL VI

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. 34.

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, ținând cont de faptul că:

a) suportul decizional pentru 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) costul și tipul de serviciu public electronic utilizat pentru furnizarea serviciilor prin intermediul tehnologiilor de cloud au implicații asupra bugetului, în funcție de modelul de serviciu de cloud;

c) cadrul intern de organizare pentru 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 pentru adoptarea tehnologiilor cloud au implicații semnificative în furnizarea serviciilor publice electronice, fiind elemente cheie în selectarea modelului de cloud;

e) criteriile de performanță necesare pentru furnizarea serviciilor proprii pot fi îndeplinite;

f) cadrul național de reglementare, reprezentat de 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. 35.

Condițiile de asigurare a confidențialității, securității și interconectării, precum și de adaptare la standardele tehnice sunt următoarele:

a) ADR afișează public numele dezvoltatorului, informații referitoare la oferta comercială legată de produsul listat, precum și termenele și condițiile de utilizare;

b) detalierea clară a oricărorlimitări, condiții sau excepții de la funcționalitatea și caracteristicile aplicațiilor;

c) descrierea compatibilității cu alte aplicații în vederea interconectării în vederea interconectării;

d) aplicațiile sunt disponibile comercial, în curs de dezvoltare activă și susținute până când sunt eliminate de pe piață;

e) 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;

f) 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, Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și

protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare;

g) 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 VII

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

Art. 36.

(1) În vederea jurnalizării evenimentelor, la nivelul serviciilor de cloud furnizate în CPG, USC prelucrează date cu caracter personal în calitate de operator.

(2) În vederea furnizării serviciilor de cloud, USC împuternicește FSC, cu respectarea prevederilor art. 28, alin. (3) din Regulament, în vederea prelucrării datelor cu caracter personal.

(3) În calitate de persoană împuternicită, FSC prelucrează datele cu caracter personal în condițiile stabilite potrivit alin. (2).

Art. 37.

(1) În vederea migrării aplicațiilor sau sistemelor informatice în cloud sau pentru utilizarea unor servicii de cloud, USC are obligația de a realiza o evaluare de impact asupra protecției datelor cu caracter personal, conform prevederilor art. 35 Secțiunea 3 din Regulamentului UE nr. 679/2016.

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

Art. 38.

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

(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 istoricul privind acțiunile asupra datelor cu caracter personal accesate prin intermediul componentei API gateway în Platformă, derulate de către USC.

(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 asigură înregistrarea, autentificarea, autorizarea, identificarea, notificarea și jurnalizarea datelor în CPG. La solicitarea USC, ADR poate recomanda bune practici în vederea realizării jurnalizării.

(6) USC întreprinde toate demersurile pentru prevenirea modificării și distrugerii, fără drept, a înregistrărilor din jurnal, respectiv pentru protejarea autenticității și a continuității procesului de înregistrare al evenimentelor, cu excepțiile stabilite de legislația în vigoare.

(7) USC implementează și actualizează, periodic, instrumente 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).

(8) ADR, STS și SRI prelucrează datele cu caracter personal, încredințate în calitate de persoană împuternicită de USC, numai pe baza instrucțiunilor documentate ale USC.

(9) ADR acordă asistență USC, la cerere, în asigurarea respectării obligațiilor legate evaluarea de impact asupra protecției datelor cu caracter personal prevăzute la art. 29 alin (1).

(10) ADR întocmește, prin decizie a președintelui, cu consultarea STS, SRI și USC, proceduri de portabilitate/recuperare/eliminare a datelor care sunt individualizate în contractul de furnizări servicii întocmit cu USC și în anexa de prelucrări a datelor cu caracter personal parte integrantă a contractului.

(11) FSC asigură ștergerea sau returnarea, la alegerea USC, a tuturor datelor cu caracter personal încredințate de acesta din urmă, după încheierea prestării serviciilor, conform clauzelor contractuale.

(12) USC verifică ștergerea sau returnarea tuturor datelor cu caracter personal încredințate FSC după încheierea prestării serviciilor de către acesta.

(13) ADR elaborează proceduri, prin decizie a președintelui, pentru gestionarea datelor procesate prin intermediul serviciilor de cloud furnizate prin CPG, în funcție de politicile de clasificare a datelor, inclusiv criterii tehnice și de securitate. Procedurile se individualizează în contractul de furnizare de servicii întocmit cu USC și în anexa de prelucrări a datelor cu caracter personal parte integrantă a respectivului contract.

(14) USC în calitate de proprietar/administrator este responsabil de prelucrarea datelor și stabilește 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.

(15) USC asigură jurnalizarea operațiunilor de acces la datele procesate în sistemele și aplicațiile implementate.

Art. 39.

(1) Jurnalele de acces la date sunt păstrate pentru o perioadă de 36 luni de la data înregistrării acțiunii privind datele respective, ca măsură tehnică necesară asigurării securității prelucrării datelor cu caracter personal, conform art. 32 din Regulament.

(2) La împlinirea termenului prevăzut la alin. (1), la solicitarea USC, datele cu caracter personal pot fi șterse în mod automat, fără posibilitatea reconstituirii, cu excepția situațiilor în care sunt utilizate în cadrul unor proceduri judiciare, caz în care acestea urmează regimul juridic al probelor, sau returnate către USC.

Art. 40.

(1) USC, dezvoltă politici și proceduri care să definească cerințele obligatorii pentru jurnalizarea acțiunilor asupra datelor cu caracter personal și comercial.

(2) USC asigură generarea înregistrărilor și mandatează ADR să asigure transmiterea și stocarea acestor evenimente de jurnalizare.

(3) ADR, în calitate de persoană împuternicită de operator, prin intermediul contractului de furnizare, oferă o modalitate de transfer a evenimentelor, stabilirea frecvenței evenimentelor care trebuie să fie transferate de către USC și opțiunile de securitate ale datelor din jurnal în tranzit, astfel încât să se asigure confidențialitatea, integritatea și disponibilitatea acestora conform art. 32 din Regulament.

Art. 41.

(1) ADR, în calitate de persoană împuternicită de operator, pune la dispoziție USC o aplicație pentru generarea de notificări în vederea informării de către aceștia a cetățenilor cu privire la orice acțiune întreprinsă în legătură cu datele cu caracter personal sau comercial ale unei persoane, entități sau sistem și orice actualizări relevante pentru persoana vizată.

(2) Aplicația poate genera două tipuri de notificări:

a) notificări declanșate datorită acțiunilor produse de factor uman;

b) notificări declanșate de aplicație, serviciu sau interfața de conectare.

(3) USC asigură informarea corectă și nemijlocită a titularului datelor cu caracter personal cu privire la acțiunile realizate la nivelul Platformei, care îi vizează direct datele cu caracter personal, precum și cu privire la inițiatorul acțiunii, prin intermediul aplicației sau prin mijloace proprii.

CAPITOLUL VIII

Politica cloud first

Art. 42.

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

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

(3) USC, la elaborarea strategiei de investiții în domeniul TIC, include în criteriile de analiză care determină introducerea în programul de investiții a obiectivelor noi de investiții TIC următoarele cerințe:

a) prioritizarea opțiunii de cloud nativ sau cloud ready;

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

(4) Începând cu data operaționalizării CPG, autoritățile și instituțiile publice centrale, cu excepția celor prevăzute în Ordonanță, au obligația utilizării serviciilor de cloud disponibile în marketplace.

(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. 43.

(1) Prin excepție de la prevederile art. 42 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 IX

PROTECȚIA DATELOR CU CARACTER PERSONAL

Art. 44

Prevederile prezentei hotărâri respectă normele și obligațiile impuse de dispozițiile în vigoare privind protecția datelor cu caracter personal.

Art. 45

(1) Datele cu caracter personal sunt prelucrate în conformitate cu prevederile Regulamentului, precum și a legislației aplicabile în domeniu.

(2) Normele europene privind protecția datelor cu caracter personal se aplică oricărui operator de date sau împuternicit, potrivit responsabilităților stabilite prin prezenta hotărâre.

Art. 46

Operatorul de date asigură respectarea deplină cel puțin a următoarelor prevederi:

a) capacitatea de a respecta drepturile persoanelor vizate privind informarea și accesul, rectificarea și ștergerea, precum și dreptul la opoziție;

b) notificarea, în caz de încălcare a securității datelor cu caracter personal, a Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal, într-un interval maximum de 72 ore de la momentul în care o astfel de încălcare a securităţii datelor a ajuns în atenția acestuia;

c) îndeplinirea tuturor îndatoririlor obligatorii privind documentarea conformării cu Regulamentul și legislația internă aplicabilă.

Art.47

(1) În aplicarea prevederilor prezentei hotărâri, în sensul legislației privind protecția datelor cu caracter personal, ADR este operator de date cu caracter personal atunci când are calitatea de USC.

(2) ADR este persoană împuternicită de către entitățile găzduite sau interconectate, după caz, atunci când are calitatea de FSC, administrator operațional al CPG, respectiv administrator operațional al marketplace, în scopul:

a) asigurării implementării, administrării tehnice și operaționale, mentenanței pentru serviciile SaaS specifice CPG;

b) dezvoltării ulterioare pentru serviciile SaaS specifice CPG;

c) migrării, integrării și interconectării în CPG a sistemelor informatice ale autorităților și instituțiilor publice;

d) jurnalizării evenimentelor, jurnalizării accesului la datele găzduite în CPG, notificării;

e) auditării.

Art. 48

STS este persoană împuternicită, pentru responsabilitățile ce decurg din calitatea de administrator tehnic și operațional al infrastructurii de bază și al serviciilor de cloud IaaS și PaaS din cadrul CPG.

Art. 49

SRI este persoană împuternicită, pentru responsabilitățile ce decurg din calitatea de administrator de securitate cibernetică a serviciilor de cloud de tip SaaS, din cadrul CPG.

Art. 50

Prevederile privind notificarea persoanei vizate prevăzute la art. 10 alin. (7) din Ordonanță se realizează în condițiile Regulamentului și ale 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, cu modificările și completările ulterioare.

Art. 51

(1) Datele cu caracter personal din cadrul Platformei sunt folosite în scopul îndeplinirii obiectivelor prevăzute la art. 4 și a al furnizării serviciilor publice electronice pentru cetățeni și aldigitalizării administrației publice, cu respectarea prevederilor legale în vigoare.

(2) Datele cu caracter personal ale persoanelor vizate, încărcate în Platformă nu pot fi prelucrate decât cu informarea prealabilă a acestora, de către USC, conform art. 13 și art. 14 din Regulament.

(3) Datele cu caracter personal sunt furnizate şi prelucrate în conformitate cu cerinţele Regulamentului, iar beneficiarii sunt informaţi cu privire la drepturile lor în calitate de persoane vizate în temeiul legislaţiei aplicabile pentru exercitarea acestor drepturi

(4) Furnizarea datelor cu caracter personal este necesară pentru migrarea și interconectarea serviciilor în Platformă, în caz contrar relaţia contractuală fiind în imposibilitate de a fi stabilită.

Art. 52.

(1) Personalul USC, FSC, ADR, SRI și STS este instruit cu privire la regulile de protecție a datelor cu caracter personal anterior validării accesului la Platformă și, ulterior, cel puțin o dată la doi ani.

(2) Instruirea personalului prevăzut la alin. (1) se referă, cel puțin, la următoarele:

a) prelucrarea datelor să fie realizată exclusiv pentru îndeplinirea atribuțiilor de serviciu;

b) datele să fie prelucrate potrivit procedurilor și prin mijloacele prevăzute de dispozițiile legale aplicabile activităților în cadrul cărora sunt utilizate datele respective;

c) prelucrarea datelor să respecte dispozițiile legale privind protecția datelor cu caracter personal aplicabile activităților în cadrul cărora sunt utilizate datele respective.

(3) Instruirea personalului cu privire la regulile de protecție a datelor cu caracter personal este realizată de către fiecare autoritate implicată, în parte, în conformitate cu prevederile Regulamentului și ale Legii nr. 363/2018 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale şi combaterii infracţiunilor sau al executării pedepselor, măsurilor educative şi de siguranţă, precum şi privind libera circulaţie a acestor date, cu modificările și completările ulterioare.

Art. 53

(1) Platforma este dezvoltată astfel încât să păstreze evidența prelucrărilor realizate și identificarea USC-ului care a realizat activitățile de prelucrare.

(2) Evidența prevăzută la alin. (1) este protejată prin măsuri corespunzătoare împotriva accesului neautorizat și poate fi utilizată numai în scopul monitorizării protecției datelor, inclusiv pentru a se verifica admisibilitatea unei solicitări de informații și legalitatea prelucrării datelor, precum și pentru asigurarea securității datelor.

(3) La solicitarea USC, informațiile conținute de evidența prevăzută la alin.(1) se pot șterge după o perioadă de 36 de luni de la introducerea acestora, cu excepția cazului în care sunt necesare pentru desfășurarea unor proceduri de monitorizare aflate în curs sau a situațiilor în care sunt utilizate în cadrul unei proceduri judiciare, caz în care acestea urmează regimul probelor, sau returnate către USC.

(4) Entitățile prevăzute la art. 52 alin. (1) stabilesc proceduri interne pentru asigurarea conformității cu dispozițiile prezentei hotărâri și a legislației din domeniul protecției datelor cu caracter personal.

(5) Procedurile prevăzute la alin. (4) includ obligativitatea ca responsabilii cu protecția datelor desemnați la nivelul autorităților prevăzute la alin.(1) să verifice semestrial, prin sondaj, prelucrările realizate de personalul propriu.

(6) Modalitatea de cooperare, măsurile necesare pentru asigurarea securității prelucrărilor, măsurile necesar a fi instituite pentru asigurarea confidențialității prelucrărilor, măsurile instituite pentru asigurarea exercitării drepturilor de către persoanele vizate și modalitatea de acces la evidența prevăzută la alin.(1) se stabilește prin acordul de migrare, contractul de furnizare de servicii, respectiv acordul de adminsitrare între părți.

Art. 54.

(1) Prevederile prezentei hotărâri nu afectează ori subminează aplicarea normelor existente în materie de protecție a datelor.

(2) Regulamentul prevalează ori de câte ori sunt prelucrate date cu caracter personal în temeiul prezentei hotărâri.

CAPITOLUL X

DISPOZIȚII FINALE ȘI TRANZITORII

Art. 55

(1) În vederea îndeplinirii atribuțiilor prevăzute la art. 4 din Ordonanță și în prezenta hotărâre, potrivit dispozițiilor art. 40 din Legea 98/2016 privind achizițiile publice, cu modificările și completările ulterioare, se desemnează ADR ca fiind unitate de achiziții centralizată pentru aplicații software și servicii software, inclusiv tehnologie de cloud, necesare Platformei, denumită în continuare UCASTC.
(2) UCASTC prevăzută la alin. (1) încheie acorduri-cadru sau utilizează sistem dinamic de achiziție în numele și pentru autoritățile și instituțiile publice, cu excepția acelor entități publice care sunt desemnate ca unități centralizate de achiziții.
(3) În baza acordurilor-cadru sau a sistemelor dinamice de achiziții încheiate de către UCASTC, în condițiile prevăzute la alin. (2), autoritățile și instituțiile publice încheie și derulează contracte subsecvente, cu avizul ADR.
(4) UCASTC devine unitate operațională în termen de 12 luni de la intrarea în vigoare a prezentei hotărâri.

Art. 56.

(1) În termen de maximum 12 luni de la data intrării în vigoare a prezentei hotărâri, toate autoritățile și instituțiile publice sunt obligate să încadreze datele pe care le operează conform 28, alin. (1).

(2) Autoritățile și instituțiile publice, în termenul prevăzut la alin. (1), notifică ADR în vederea integrării tuturor încadrărilor în Registrul Național al Registrelor administrat de către ADR.

Art. 57.

(1) Modelul contractului de furnizare de servicii prevăzute la art. 6 alin. (1) se stabilește prin ordin al ministrului cercetării, inovării și digitalizării, în termen de maximum 90 de zile de la intrarea în vigoare a prezentei hotărâri.

(2) Modelul acordului de migrare, integrare și interconectare prevăzut la art. 13 alin. (1) lit. c) și art. 21, alin. (1), precum și modalitățile de efectuare a transmiterii datelor și informațiilor cu caracter personal și a datelor sensibile se stabilește prin ordin al ministrului cercetării, inovării și digitalizării, în termen de maximum 90 de zile de la intrarea în vigoare a prezentei hotărâri. Ordinul se publică în Monitorul Oficial al României, Partea I.

(3) Procedura de încadrare a datelor prevăzute la art. 28, alin. (1) și modelul evaluării de impact prevăzute de art. 29 alin. (1) se stabilesc prin ordin al ministrului cercetării, inovării și digitalizării în termen de maximum 90 de zile de la intrarea în vigoare a prezentei hotărâri.

(4) Metodologia prevăzută la art. 31 alin. (1) se adoptă prin decizie a președintelui ADR în termen de maximum 180 de zile de la data intrării în vigoare a prezentei hotărâri.

(5) Normele privind operaționalizarea aplicației prevăzute la art. 41 se stabilesc prin decizie a președintelui ADR, în termen de maximum 180 de zile de la intrarea în vigoare a prezentei hotărâri.

(6) Procedura de listare în marketplace se stabilește prin ordin al ministrului cercetării, inovării și digitalizării în termen de maximum 180 de zile de la intrarea în vigoare a prezentei hotărâri.

(7) Procedurile interne prevăzute la art. 53 alin. (4) se stabilesc în maximum 120 de zile de la data intrării în vigoare a prezentei hotărâri.

PRIM-MINISTRU

NICOLAE-IONEL CIUCĂ

Anexa - Lista autorităților și instituțiilor publice care migrează la CPG

1. Administrația Fondului pentru Mediu
2. Administrația Națională de Meteorologie
3. Agenția de Investigare Feroviară Română
4. Agenția de Plăți și Intervenție pentru Agricultură
5. Agenția Națională a Funcționarilor Publici
6. Agenția Națională a Medicamentului și a Dispozitivelor Medicale din România
7. Agenția Națională Anti-Doping
8. Agenția Națională de Cadastru și Publicitate Imobiliară
9. Agenția Națională de Integritate
10. Agenția Națională de Presă AGERPRES
11. Agenția Națională pentru Achiziții Publice
12. Agenția Națională pentru Arii Naturale Protejate
13. Agenția Națională pentru Locuințe
14. Agenția Națională pentru Ocuparea Forței de Muncă
15. Agenția Națională pentru Plăți și Inspecție Socială
16. Agenția Națională pentru Protecția Mediului
17. Agenția Națională pentru Romi
18. Agenția pentru Finanțarea Investițiilor Rurale
19. Agenția Spațială Română
20. Autoritatea Aeronautică Civilă Română R.A.
21. Autoritatea de Audit (Curtea de Conturi a României)
22. Autoritatea de Supraveghere Financiară
23. Autoritatea Naţională de Management al Calităţii în Sănătate
24. Autoritatea Națională de Reglementare în Domeniul Energiei
25. Autoritatea Naţională de Reglementare pentru Serviciile Comunitare de Utilităţi Publice
26. Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal
27. Autoritatea Națională pentru Protecția Consumatorilor
28. Autoritatea Națională pentru Protecția Drepturilor Copilului și Adopție
29. Autoritatea Națională pentru Protecția Drepturilor Persoanelor cu Dizabilități
30. Autoritatea Națională pentru Restituirea Proprietăților
31. Autoritatea Națională Sanitară - Veterinară și pentru Siguranța Alimentelor
32. Autoritatea Navală Română
33. Autoritatea pentru Administrarea Activelor Statului
34. Autoritatea pentru Digitalizarea României
35. Avocatul Poporului
36. Banca Națională a României
37. Biblioteca Naţională a României
38. Camera Deputaților
39. Casa Națională de Asigurări de Sănătate
40. Casa Națională de Pensii Publice
41. Centrul Național de Politici și Evaluare în Educație

42. Centrul Național de Recunoaștere și Echivalare a Diplomelor
43. Comisia Națională de Strategie și Prognoză
44. Comisia Națională pentru Controlul Activităților Nucleare
45. Compania Națională Aeroporturi București S.A.
46. Compania Națională de Administrare a Infrastructurii Rutiere S.A.
47. Consiliul Concurenței
48. Consiliul Legislativ
49. Consiliul Economic și Social
50. Consiliul Național al Audiovizualului
51. Consiliul Național pentru Combaterea Discriminării
52. Consiliul Naţional pentru Studierea Arhivelor Securității
53. Consiliul Superior al Magistraturii
54. Curtea de Conturi a României
55. Departamentul pentru Luptă Antifraudă
56. Departamentul pentru Românii de Pretutindeni
57. Directoratul Național de Securitate Cibernetică
58. Garda Națională de Mediu
59. Inspectoratul de Stat în Construcții
60. Inspecția Muncii
61. Institutul Național de Cercetare-Dezvoltare pentru Fizica Pământului
62. Institutul Național de Sănătate Publică
63. Institutul Naţional de Statistică
64. Instituția Avocatul Poporului
65. Înalta Curte de Casaţie şi Justiţie
66. Ministerul Agriculturii și Dezvoltării Rurale
67. Ministerul Antreprenoriatului și Turismului
68. Ministerul Cercetării, Inovării și Digitalizării
69. Ministerul Culturii
70. Ministerul Dezvoltării, Lucrărilor Publice și Administrației
71. Ministerul Educației
72. Ministerul Energiei
73. Ministerul Finanțelor
74. Ministerul Investițiilor și Proiectelor Europene
75. Ministerul Justiției
76. Ministerul Mediului, Apelor și Pădurilor
77. Ministerul Public - Parchetul de pe lângă Înalta Curte de Casație și Justiție
78. Ministerul Sănătății
79. Ministerul Sportului
80. Ministerul Transporturilor și Infrastructurii
81. Oficiul Național pentru Jocuri de Noroc
82. Regia Autonomă Monitorul Oficial
83. Secretariatul General al Guvernului
84. Senatul României
85. Societatea Română de Radiodifuziune

86. Societatea Română de Televiziune
87. Unitatea Executivă pentru Finanțarea Învățământului Superior, a Cercetării, Dezvoltării și Inovării.