Anexa 1

Conceptul Sistemului informațional „e-CSP”

Capitolul I
DISPOZIȚII GENERALE

1. Sistemul informațional „e-CSP” *(în continuare – e-CSP)* constituie un ansamblu integrat de resurse software, hardware și organizatorice destinat formării, administrării și valorificării resursei informaționale aferente activității Consiliului Superior al Procurorilor.

2. Sistemul informațional „e-CSP” reprezintă platforma informatică instituțională unică concepută pentru digitalizarea, automatizarea și gestionarea integrată a proceselor operaționale, disciplinare și administrative aflate în competența Consiliului Superior al Procurorilor și a entităților funcționale din subordinea acestuia, prin asigurarea înregistrării, evidenței, repartizării aleatorii automate, examinării și arhivării electronice a sesizărilor și dosarelor disciplinare, gestionării documentelor electronice și a proceselor aferente carierei procurorilor, precum și prin furnizarea mecanismelor necesare monitorizării, raportării și auditării activităților desfășurate.

3. Destinația principală a e-CSP este formarea, gestionarea și utilizarea resursei informaționale instituționale care să conțină totalitatea datelor și documentelor aferente proceselor de înregistrare, repartizare, examinare și soluționare a sesizărilor disciplinare, gestionării dosarelor disciplinare și administrative, administrării documentelor electronice și gestionării proceselor aferente carierei procurorilor, asigurând evidența electronică unitară, trasabilitatea completă a acțiunilor, precum și accesul controlat la informațiile gestionate, în conformitate cu competențele legale ale utilizatorilor sistemului.

4. Sistemul informațional „e-CSP” este găzduit pe platforma tehnologică guvernamentală comună (MCloud) și este compatibil cu infrastructuri bazate pe tehnologii de tip container.

5. Implementarea e-CSP are ca obiectiv principal consolidarea capacității instituționale a Consiliului Superior al Procurorilor, prin:

a) constituirea unei resurse informaționale instituționale unice și integrate, care să asigure evidența completă și gestionarea electronică a sesizărilor disciplinare, dosarelor disciplinare, documentelor și proceselor aferente competențelor Consiliului Superior al Procurorilor și ale entităților funcționale din subordinea acestuia;

b) asigurarea repartizării aleatorii automate a sesizărilor, în conformitate cu prevederile cadrului normativ aplicabil, cu respectarea principiilor de imparțialitate, transparență și echitate în distribuirea sarcinii de muncă;

c) creșterea eficienței operaționale prin automatizarea fluxurilor de lucru, reducerea dependenței de procese manuale și optimizarea proceselor de gestionare, examinare și soluționare a sesizărilor disciplinare;

d) garantarea trasabilității complete a operațiunilor efectuate în sistem, prin jurnalizarea automată a operațiunilor și crearea mecanismelor necesare auditării tehnice și juridice;

e) consolidarea transparenței, responsabilității instituționale și capacității de monitorizare a activităților desfășurate, prin furnizarea mecanismelor de raportare, analiză și control;

f) asigurarea unui nivel înalt de securitate, integritate și confidențialitate a datelor gestionate, în conformitate cu legislația privind protecția datelor cu caracter personal și securitatea informațională;

g) facilitarea interoperabilității cu alte sisteme informaționale de stat și utilizarea serviciilor guvernamentale partajate, în vederea eficientizării schimbului de date și a proceselor administrative.

6. Principiile care stau la baza creării e-CSP sunt:

a) principiul legalității;
b) principiul veridicității datelor;
c) principiul imparțialității;
d) principiul transparenței și trasabilității;
e) principiul controlului accesului bazat pe roluri;
f) principiul plenitudinii și integrității datelor;
g) principiul controlului asupra formării și utilizării sistemului;
h) principiul modularității și scalabilității;
i) principiul securității informaționale;
j) principiul confidențialității;
k) principiul interoperabilității;
l) principiul auditabilității;
m) principiul eficienței operaționale.

Capitolul II
CADRUL NORMATIV-JURIDIC AL SISTEMULUI INFORMAȚIONAL „e-CSP”

7. Dezvoltarea, administrarea și gestionarea e-CSP este reglementată, de următoarele acte normative:

a) Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat;

b) Legea nr.71/2007 cu privire la registre;

c) Legea nr.133/2011 privind protecția datelor cu caracter personal;

d) Legea nr.148/2023 privind accesul la informațiile de interes public;

e) Legea nr. 3/2016 cu privire la Procuratură, cu modificările și completările ulterioare;

f) Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;

g) Hotărârea Guvernului nr.1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);

h) Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud);

i) Hotărârea Guvernului nr.708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);

j) Hotărârea Guvernului nr.967/2016 cu privire la mecanismul de consultare publică cu societatea civilă în procesul decizional;

k) Hotărârea Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice;

l) Hotărârea Guvernului nr.737/2017 pentru aprobarea Regulamentului cu privire la normele de creare a serviciilor de rețea și termenul de implementare a acestora;

m) Hotărârea Guvernului nr.414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat;

n) Hotărârea Guvernului nr.276/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);

o) Hotărârea Guvernului nr.386/2020 cu privire la planificarea strategică;

p) Hotărârea Guvernului nr. 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030;

q) Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design;

r) HG nr.260/2025 privind aprobarea Agendei de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025-2027;

s) HG nr.306/2025 privind aprobarea Programului Național de Aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029;

t) HG nr. 308/2025 privind aprobarea Strategiei de Transformare Digitală a Republicii Moldova 2023–2030 și Programul de implementare 2025–2027 al Strategiei de Transformare Digitală;

u) Reglementarea tehnică „Procesele ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006;

v) Regulamentul cu privire la organizarea și funcționarea Consiliului Superior al Procurorilor aprobat prin Hotărârea Consiliului Superior al Procurorilor nr.1-420/2025 din 11.12.2025.

Capitolul III
SPAȚIUL FUNCȚIONAL AL SISTEMULUI INFORMAȚIONAL „ e-CSP”

8. Sistemul informațional „e-CSP” asigură realizarea unui ansamblu de funcții de bază, orientate spre gestionarea integrată a proceselor instituționale, după cum urmează:

a) formarea și gestionarea resursei informaționale aferente activității Consiliului Superior al Procurorilor (CSP) și entităților funcționale din subordinea acestuia, prin asigurarea evidenței electronice a sesizărilor, dosarelor disciplinare, documentelor și altor obiecte informaționale relevante;

b) înregistrarea electronică a sesizărilor disciplinare și a altor documente aferente proceselor disciplinare, cu atribuirea automată a identificatorilor unici și formarea dosarului electronic;

c) asigurarea repartizării aleatorii automate a sesizărilor disciplinare către inspectori, prin intermediul mecanismului bazat pe algoritmi obiectivi, fără intervenție umană în procesul de selecție, cu respectarea principiilor de imparțialitate, echitate și transparență;

d) gestionarea dosarelor disciplinare în format electronic, inclusiv crearea, completarea, actualizarea, transmiterea și arhivarea acestora, precum și gestionarea materialelor și documentelor aferente;

e) gestionarea electronică a documentelor instituționale, inclusiv crearea, înregistrarea, stocarea, clasificarea, căutarea, accesarea și arhivarea acestora;

f) asigurarea evidenței și gestionării proceselor aferente carierei procurorilor, în conformitate cu competențele Consiliului Superior al Procurorilor;

g) asigurarea trasabilității complete a operațiunilor efectuate în sistem, prin jurnalizarea automată a acțiunilor utilizatorilor și a evenimentelor de sistem;

h) asigurarea controlului accesului la resursele informaționale, în funcție de rolurile și drepturile utilizatorilor, în conformitate cu competențele stabilite prin cadrul normativ;

i) generarea rapoartelor, statisticilor și analizelor necesare monitorizării activităților desfășurate și susținerii procesului decizional;

j) asigurarea interacțiunii cu alte sisteme informaționale de stat și asigurarea conexiunii cu platforme și servicii guvernamentale partajate;

k) asigurarea securității, integrității și protecției datelor gestionate, în conformitate cu cerințele de securitate informațională aplicabile sistemelor informaționale de stat.

9. Din punct de vedere funcțional, e-CSP este structurat pe următoarele componente:

1. Conturul *„ e-Disciplinar”*, cu următoarele funcții:

a) înregistrarea electronică a sesizărilor disciplinare și formarea automată a dosarului disciplinar electronic;

b) repartizarea aleatorie automată a sesizărilor disciplinare către inspectori, prin intermediul mecanismului informatic, în conformitate cu prevederile cadrului normativ aplicabil;

c) gestionarea dosarului disciplinar electronic, inclusiv completarea, actualizarea, transmiterea și arhivarea acestuia;

d) gestionarea documentelor, materialelor și probelor aferente procedurii disciplinare;

e) gestionarea fluxurilor de lucru aferente procedurii disciplinare, inclusiv transmiterea dosarelor către entitățile competente;

f) evidența și monitorizarea etapelor procedurale și a statutului dosarelor disciplinare;

g) asigurarea trasabilității complete a operațiunilor efectuate în cadrul procedurii disciplinare.

2. Conturul *„e-Carieră”*, cu următoarele funcții:

a) gestionarea dosarelor electronice aferente carierei procurorilor;

b) gestionarea proceselor de selecție, evaluare și promovare a procurorilor;

c) repartizarea aleatorie a dosarelor și cererilor aferente proceselor de evaluare și selecție;

d) gestionarea documentelor și informațiilor aferente proceselor de carieră;

e) generarea rapoartelor și analizelor aferente proceselor gestionate.

3. Conturul *„e-Management al documentelor”* cu următoarele funcții:

a) înregistrarea electronică a documentelor;

b) gestionarea fluxurilor documentare;

c) stocarea și arhivarea electronică a documentelor;

d) clasificarea, căutarea și accesarea documentelor;

e) gestionarea nomenclatoarelor și clasificatoarelor aferente documentelor;

f) asigurarea trasabilității documentelor și a operațiunilor efectuate asupra acestora.

4. Conturul *„ Raportare și analiză”*, cu următoarele funcții:

a) generarea rapoartelor operaționale și statistice;

b) generarea rapoartelor analitice și a indicatorilor de performanță;

c) monitorizarea activităților desfășurate în sistem;

d) exportarea datelor și rapoartelor, în conformitate cu drepturile de acces ale utilizatorilor.

5. Conturul „*Gestiunea sistemului informatic*”, cu următoarele funcții:

a) configurarea parametrilor generali ai sistemului informatic;

b) gestiunea resurselor sistemului informatic;

c) gestionarea conturilor de utilizatori și drepturilor acestora;

d) gestiunea nomenclatoarelor și clasificatoarelor (metadatelor);

e) gestiunea notificărilor;

f) jurnalizarea evenimentelor de sistem.

10. E-CSP va interacționa cu sisteme informaționale partajate și alte resurse și sisteme informaționale de stat, după cum urmează:

a) Serviciul electronic guvernamental de autentificare și control al accesului (MPass) – pentru autentificarea și controlul accesului în cadrul sistemului pe bază de roluri;

b) Platforma de interoperabilitate (MConnect) - în vederea asigurării interoperabilității și asigurării schimbului de date cu alte sisteme informaționale de stat;

c) Serviciul electronic guvernamental de jurnalizare (MLog) – mecanism securizat și flexibil de jurnalizare și audit, asigurând evidența evenimentelor în contextul utilizării sistemelor informaționale;

d) Serviciul guvernamental de notificare electronică (MNotify) - pentru notificarea utilizatorilor;

e) Serviciul guvernamental integrat de semnătură electronică (MSign) - pentru asigurarea semnării electronice a documentelor.

11. Interfața utilizator a e-CSP este proiectată astfel, încât:

a) oferă o interfață ergonomică, intuitivă și accesibilă tuturor tipurilor de utilizatori. Interfața utilizator a platformei reprezintă un design grafic echilibrat, distinct și adaptabil pentru majoritatea dispozitivelor utilizate;

b) furnizează o interfață în limbile română (implicit), engleză și rusă;

c) furnizează o interfață personalizată fiecărei categorii de utilizatori și aplicații în funcție de categoriile utilizatorilor (drepturile și rolurile acestora).

Capitolul IV
STRUCTURA ORGANIZAȚIONALĂ A SISTEMULUI INFORMAȚIONAL „e-CSP”

12. Proprietarul Sistemului informațional „e-CSP” este statul.

13. Posesorul și deținătorul sistemului e-CSP este Consiliul Superior al Procurorilor, care asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea sistemului.

14. Administratorul tehnic al e-CSP este Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, care își exercită atribuțiile în conformitate cu cadrul normativ privind administrarea tehnică și menținerea resurselor și sistemelor informaționale de stat.

15. Utilizatorii ai Sistemului informațional „e-CSP” sunt:

1. *Utilizatori interni:*

a) Administratorul de sistem – persoana responsabilă de gestiunea și menținerea operațională a sistemului informatic, efectuarea activităților de administrare;

b) Persoanele autorizate care, în exercitarea atribuțiilor de serviciu, utilizează sistemul în scopul îndeplinirii competențelor stabilite de legislația în vigoare și actele normative interne ale Consiliului Superior al Procurorilor. – membrii Consiliului Superior al Procurorilor; membrii Colegiului de disciplină și etică; inspectorii din cadrul Inspecției procurorilor; inspectorul-șef al Inspecției procurorilor; personalul subdiviziunilor structurale ale Consiliului Superior al Procurorilor; alte persoane autorizate, în conformitate cu cadrul normativ aplicabil și actele normative interne.

2. *Utilizatori externi* care includ persoanele fizice sau reprezentanții autorităților și instituțiilor care interacționează cu Consiliul Superior al Procurorilor prin intermediul sistemului, în limitele competențelor stabilite, după cum urmează: procurorii, în cazurile prevăzute de cadrul normativ aplicabil; persoanele fizice care depun sesizări sau cereri; reprezentanții autorităților publice și instituțiilor care interacționează cu Consiliul Superior al Procurorilor; alte persoane autorizate, în conformitate cu cadrul normativ aplicabil.

16. Gestionarea accesului utilizatorilor se realizează prin intermediul serviciului guvernamental MPass, în baza rolurilor și competențelor stabilite.

Capitolul V
DOCUMENTELE DE BAZĂ ALE PORTALULUI SISTEMULUI INFORMAȚIONAL „e-CSP”

17. Documentele gestionate în cadrul Sistemului informațional „e-CSP” se clasifică, în funcție de rolul și destinația acestora, în următoarele categorii:

a) documente de intrare;

b) documente de ieșire;

c) documente tehnologice.

18. Documentele de intrare reprezintă totalitatea datelor și informațiilor introduse în sistem, după cum urmează:

a) sesizările disciplinare depuse de persoane fizice sau juridice;

b) sesizările disciplinare depuse de autorități publice sau instituții;

c) sesizările disciplinare inițiate din oficiu, în conformitate cu cadrul normativ aplicabil;

d) cererile și demersurile aferente procedurilor disciplinare;

e) documentele și materialele probatorii anexate sesizărilor sau dosarelor disciplinare;

f) actele procedurale și documentele transmise de entitățile competente în cadrul procedurilor disciplinare;

g) documentele aferente proceselor de carieră a procurorilor, în conformitate cu competențele Consiliului Superior al Procurorilor;

h) datele și documentele introduse în sistem de către utilizatorii autorizați;

i) formularele electronice și datele aferente obiectelor informaționale gestionate în sistem;

j) alte documente și date necesare funcționării e-CSP, în conformitate cu cadrul normativ aplicabil.

19. Documentele de ieșire reprezintă rezultatul procesării informațiilor în cadrul sistemului, după cum urmează:

a) dosarele disciplinare electronice generate și gestionate în sistem;

b) rapoartele și actele întocmite în cadrul procedurilor disciplinare;

c) deciziile și actele procedurale generate în cadrul proceselor gestionate în sistem;

d) notificările generate automat de sistem privind statutul sesizărilor și dosarelor disciplinare;

e) rapoartele operaționale, statistice și analitice generate de sistem;

f) extrasele și informațiile furnizate utilizatorilor autorizați, în conformitate cu drepturile de acces stabilite;

g) datele și informațiile utilizate pentru monitorizarea și controlul proceselor gestionate în sistem;

h) alte documente generate de Sistemul informațional „e-CSP”, în conformitate cu cadrul normativ aplicabil.

20. Documentele tehnologice sunt acele înregistrări și resurse necesare funcționării și administrării sistemului, după cum urmează:

a) înregistrările privind utilizatorii sistemului și drepturile de acces ale acestora;

b) înregistrările jurnalului de audit și ale operațiunilor efectuate în sistem;

c) înregistrările privind repartizarea aleatorie a sesizărilor și dosarelor disciplinare;

d) nomenclatoarele, clasificatoarele și parametrii utilizați în sistem;

e) formularele electronice utilizate pentru gestionarea obiectelor informaționale;

f) configurațiile și parametrii funcționali ai sistemului;
g) ghidurile și instrucțiunile de utilizare a sistemului;
h) politicile și regulile de securitate aplicabile sistemului;
i) copiile de siguranță ale datelor și mecanismele de restaurare;
j) alte documente necesare funcționării și dezvoltării sistemului.

Capitolul VI
SPAȚIUL INFORMAȚIONAL AL SISTEMULUI INFORMAȚIONAL „e-CSP”

21. Totalitatea obiectelor informaționale de bază care reprezintă resursa informațională a e-CSP se determină în funcție de destinația acestora și include:

22. *sesizarea disciplinară* - conține informația înregistrată în sistem, prin care se solicită examinarea unor fapte ce pot constitui abateri disciplinare.

23. Identificatorul obiectului informațional *„sesizarea disciplinară”* este numărul de ordine generat de sistem, cu următoarea structură:

a) ID Sesizare – identificator unic al fiecărei sesizări disciplinare, generat automat de sistem, în format numeric sau alfanumeric;

b) Tip Sesizare – tipul sesizării disciplinare (sesizare depusă de persoană fizică, sesizare depusă de autoritate publică, autosesizare, sesizare transmisă de altă instituție, ect.);

c) Categoria sesizării – categoria sau tipologia sesizării disciplinare, conform clasificatorului stabilit în sistem;

d) ID Autor – identificatorul autorului sesizării, care poate reprezenta persoana fizică, instituția sau utilizatorul sistemului care a înregistrat sesizarea;

e) ID Procuror – identificatorul unic al procurorului vizat în sesizare, dacă este cazul;

f) Data înregistrării – data și ora la care sesizarea disciplinară a fost înregistrată în Sistemul informațional „e-CSP”;

g) Obiectul sesizării – descrierea succintă a faptelor sesizate sau a obiectului sesizării disciplinare;

h) Documente asociate – referință sau legătură către documentele electronice anexate sesizării (de exemplu: fișiere PDF, imagini, alte documente relevante);

i) Statutul sesizării – starea curentă a sesizării disciplinare în cadrul sistemului (de exemplu: „înregistrată”, „repartizată”, „în examinare”, „finalizată”, „clasată”);

j) ID Inspector – identificatorul inspectorului desemnat automat prin mecanismul de repartizare aleatorie, responsabil de examinarea sesizării disciplinare;

k) Istoric sesizare – totalitatea înregistrărilor privind acțiunile efectuate asupra sesizării disciplinare, inclusiv data, ora și utilizatorul care a efectuat acțiunea.

24. Scenarii de bază ale obiectului informațional *„sesizarea disciplinară”:*

1. Crearea și înregistrarea sesizării disciplinare, care presupune:

a) introducerea datelor aferente sesizării disciplinare în sistem de către utilizatorii autorizați sau prin intermediul mecanismelor automatizate;

b) generarea automată de către sistem a identificatorului unic al sesizării disciplinare;

c) atribuirea statutului inițial al sesizării disciplinare;

d) formarea înregistrării electronice aferente sesizării disciplinare.

2. Validarea și completarea sesizării disciplinare, care presupune:

a) verificarea datelor introduse în sistem;

b) completarea informațiilor și anexarea documentelor relevante;

c) actualizarea statutului sesizării disciplinare, după caz.

3. Repartizarea aleatorie automată a sesizării disciplinare, care presupune:

a) inițierea automată a procesului de repartizare de către sistem;

b) aplicarea algoritmului de repartizare aleatorie, în conformitate cu regulile stabilite;

c) desemnarea automată a inspectorului responsabil;

d) înregistrarea rezultatului repartizării în sistem și în jurnalul de audit;

e) actualizarea statutului sesizării disciplinare.

4. Examinarea sesizării disciplinare, care presupune:

a) accesarea sesizării disciplinare de către inspectorul desemnat;

b) analizarea informațiilor și documentelor aferente sesizării;

c) completarea dosarului disciplinar cu informații și documente relevante;

d) actualizarea statutului sesizării disciplinare, în conformitate cu evoluția procedurii.

5. Transmiterea și utilizarea sesizării disciplinare, care presupune:

a) transmiterea electronică a sesizării sau a datelor aferente către entitățile competente, după caz;

b) utilizarea datelor în cadrul procedurilor disciplinare sau administrative;

c) asigurarea accesului controlat la sesizare, în conformitate cu drepturile de acces stabilite.

6. Finalizarea sesizării disciplinare, care presupune:

a) adoptarea deciziei aferente sesizării disciplinare, după caz;

b) actualizarea statutului sesizării disciplinare cu indicarea rezultatului procedurii;

c) marcarea sesizării disciplinare ca finalizată în sistem.

7. Arhivarea sesizării disciplinare, care presupune:

a) stocarea sesizării disciplinare și a datelor aferente în sistem, în conformitate cu cerințele privind păstrarea și arhivarea datelor;

b) asigurarea integrității, securității și accesului controlat la sesizarea disciplinară arhivată.

8. Jurnalizarea operațiunilor aferente sesizării disciplinare, care presupune:

a) înregistrarea automată în jurnalul de audit a tuturor acțiunilor efectuate asupra sesizării disciplinare;

b) asigurarea trasabilității complete a ciclului de viață al sesizării disciplinare.

25. *dosarul disciplinar* - obiectul informațional care include totalitatea datelor, documentelor electronice, actelor procedurale și materialelor aferente unei proceduri disciplinare inițiate în privința unui procuror, gestionate și stocate în cadrul Sistemului informațional „e-CSP”, pe întreaga durată a ciclului de viață al procedurii disciplinare.

26. Identificatorul obiectului informațional *„dosarul disciplinar”* este numărul unic generat automat sistem, care asigură evidența, trasabilitatea și auditabilitatea

procesului de repartizare automată a sesizărilor și dosarelor disciplinare, având următoarea structură:

a) ID Repartizare– identificator unic al fiecărei operațiuni de repartizare aleatorie, generat automat de sistem, în format numeric sau alfanumeric;

b) ID Sesizare/ID Dosar – identificatorul unic al sesizării disciplinare sau al dosarului disciplinar care face obiectul repartizării;

c) Tip obiect repartizat – tipul obiectului supus repartizării (de exemplu: sesizare disciplinară, dosar disciplinar, cerere, alt tip de obiect informațional);

d) ID Inspector – identificatorul unic al inspectorului desemnat automat de sistem în urma procesului de repartizare aleatorie;

e) Lista inspectorilor eligibili – referință către lista inspectorilor eligibili pentru repartizare la momentul efectuării acesteia, conform criteriilor stabilite în sistem;

f) Algoritm de repartizare – identificatorul sau versiunea algoritmului utilizat pentru efectuarea repartizării aleatorii;

g) Valoare aleatorie generată – valoarea numerică sau alfanumerică generată automat de sistem, utilizată pentru determinarea rezultatului repartizării;

h) Data și ora repartizării – data și ora la care a fost efectuată repartizarea aleatorie în sistem;

i) Statut repartizare – starea repartizării (de exemplu: „efectuată”, „anulată”, „repetată”, „invalidată”);

j) Motiv redistribuire – motivul redistribuirii, în cazul în care repartizarea a fost anulată sau efectuată din nou (de exemplu: incompatibilitate, recuzare, eroare tehnică);

27. Scenarii de bază ale obiectului informațional *„dosarul disciplinar”*:

1. Crearea dosarului disciplinar, care presupune:

a) generarea automată a dosarului disciplinar în e-CSP, în baza unei sesizări disciplinare înregistrate sau în urma inițierii procedurii disciplinare din oficiu;

b) atribuirea automată a identificatorului unic al dosarului disciplinar;

c) asocierea dosarului disciplinar cu sesizarea disciplinară corespunzătoare;

d) atribuirea statutului inițial al dosarului disciplinar.

2. Repartizarea aleatorie automată a dosarului disciplinar, care presupune:

a) inițierea procesului de repartizare automată de către sistem, în conformitate cu regulile stabilite;

b) aplicarea algoritmului de repartizare aleatorie;

c) desemnarea automată a inspectorului responsabil de gestionarea dosarului disciplinar;

d) înregistrarea rezultatului repartizării în sistem și în jurnalul de audit;

e) actualizarea statutului dosarului disciplinar.

3. Gestionarea și completarea dosarului disciplinar, care presupune:

a) introducerea, actualizarea și gestionarea datelor aferente dosarului disciplinar;

b) anexarea documentelor, probelor și altor materiale relevante;

c) înregistrarea actelor procedurale și a acțiunilor efectuate în cadrul dosarului;

d) actualizarea statutului dosarului disciplinar, în funcție de evoluția procedurii.

4. Examinarea dosarului disciplinar, care presupune:

a) analizarea datelor și documentelor aferente dosarului disciplinar de către inspectorul desemnat;

b) efectuarea acțiunilor procedurale necesare, în conformitate cu cadrul normativ aplicabil;

c) completarea dosarului disciplinar cu actele și informațiile aferente examinării;

d) transmiterea dosarului disciplinar către entitățile competente, după caz.

5. Transmiterea și utilizarea dosarului disciplinar, care presupune:

a) transmiterea electronică a dosarului disciplinar către Colegiul de disciplină și etică sau alte entități competente, în conformitate cu cadrul normativ aplicabil;

b) utilizarea datelor și documentelor aferente dosarului disciplinar în procesul decizional;

c) asigurarea accesului controlat la dosarul disciplinar, în conformitate cu drepturile de acces stabilite.

6. Finalizarea dosarului disciplinar, care presupune:

a) înregistrarea deciziei finale aferente dosarului disciplinar;

b) actualizarea statutului dosarului disciplinar, în funcție de rezultatul procedurii;

c) marcarea dosarului disciplinar ca finalizat în sistem.

7. Arhivarea dosarului disciplinar, care presupune:

a) stocarea dosarului disciplinar și a datelor aferente în Sistemul informațional „e-CSP”, în conformitate cu cerințele privind păstrarea și arhivarea datelor;

b) asigurarea integrității, securității și accesului controlat la dosarul disciplinar arhivat.

8. Jurnalizarea operațiunilor aferente dosarului disciplinar, care presupune:

a) înregistrarea automată în jurnalul de audit a tuturor acțiunilor efectuate asupra dosarului disciplinar;

b) asigurarea trasabilității complete a ciclului de viață al dosarului disciplinar.

9. Jurnal audit repartizare – totalitatea datelor și înregistrărilor aferente procesului de repartizare, inclusiv parametrii utilizați, rezultatul repartizării și istoricul operațiunii, utilizate în scopuri de audit și control.

28. *jurnalul de audit*– include totalitatea înregistrărilor generate automat de Sistemul informațional, referitoare la acțiunile utilizatorilor, operațiunile efectuate și evenimentele de sistem, în scopul asigurării trasabilității, securității, monitorizării și auditării funcționării sistemului.

29. Identificatorul obiectului informațional „*jurnalul de audit*” este numărul unic generat automat de sistem, care asigură evidența, monitorizarea și trasabilitatea tuturor acțiunilor și evenimentelor înregistrate în sistem, având următoarea structură:

a) ID Audit – identificator unic al fiecărei înregistrări din jurnalul de audit, generat automat de sistem, în format numeric sau alfanumeric;

b) ID Utilizator – identificatorul unic al utilizatorului care a efectuat acțiunea în sistem, dacă este cazul;

c) Rol utilizator – rolul utilizatorului care a efectuat acțiunea (de exemplu: inspector, administrator, membru CSP, utilizator extern);

d) Tip acțiune – tipul acțiunii efectuate (de exemplu: autentificare, creare sesizare, repartizare aleatorie, modificare dosar, vizualizare document, semnare document);

e) ID Obiect – identificatorul unic al obiectului informațional asupra căruia a fost efectuată acțiunea (de exemplu: Sesizare ID, Dosar ID, Utilizator ID);

f) Tip obiect – tipul obiectului informațional asupra căruia a fost efectuată acțiunea (de exemplu: sesizare disciplinară, dosar disciplinar, utilizator, document);

g) Data și ora acțiunii – data și ora la care a fost efectuată acțiunea, generate automat de sistem;

h) Rezultatul acțiunii – rezultatul acțiunii efectuate (de exemplu: succes, eșec, respins, anulat);

i) Adresa IP – adresa IP a dispozitivului de la care a fost efectuată acțiunea, dacă este cazul;

j) ID Sistem – identificatorul sistemului informațional care a înregistrat acțiunea;

k) Detalii acțiune – informații suplimentare privind acțiunea efectuată, inclusiv parametrii relevanți ai operațiunii;

l) Hash integritate – cod generat automat de sistem pentru asigurarea integrității și protecției înregistrării din jurnalul de audit împotriva modificării neautorizate.

30. Scenarii de bază ale obiectului informațional „*jurnalul de audit*”:

1.Generarea automată a înregistrărilor în jurnalul de audit, care presupune:

a) crearea automată a unei înregistrări în jurnalul de audit la fiecare acțiune efectuată de utilizatori sau la producerea unui eveniment de sistem;

b) atribuirea automată a identificatorului unic al înregistrării din jurnalul de audit;

c) înregistrarea datelor privind utilizatorul, acțiunea efectuată, obiectul vizat, data și ora acțiunii și rezultatul acesteia.

2. Înregistrarea operațiunilor efectuate asupra obiectelor informaționale, care presupune:

a) înregistrarea automată a operațiunilor de creare, modificare, vizualizare, transmitere, repartizare, semnare și ștergere a obiectelor informaționale;

b) înregistrarea automată a operațiunilor de repartizare aleatorie, inclusiv parametrii utilizați și rezultatul repartizării;

c) înregistrarea automată a operațiunilor de autentificare și acces în sistem.

3. Stocarea și păstrarea înregistrărilor din jurnalul de audit, care presupune:

a) stocarea automată a înregistrărilor în condiții care asigură integritatea, securitatea și disponibilitatea acestora;

b) protejarea înregistrărilor împotriva modificării, ștergerii sau accesului neautorizat;

c) păstrarea înregistrărilor în conformitate cu cerințele cadrului normativ aplicabil.

4. Accesarea și utilizarea jurnalului de audit, care presupune:

a) accesarea înregistrărilor din jurnalul de audit de către utilizatorii autorizați, în conformitate cu drepturile de acces stabilite;

b) utilizarea jurnalului de audit în scopuri de monitorizare, control și analiză a activităților desfășurate în sistem;

c) utilizarea jurnalului de audit în cadrul procedurilor de verificare, control și audit.

5. Monitorizarea și controlul funcționării sistemului, care presupune:

a) utilizarea jurnalului de audit pentru identificarea și analiza incidentelor de securitate sau a utilizării neautorizate a sistemului;

b) utilizarea jurnalului de audit pentru verificarea corectitudinii funcționării mecanismelor sistemului, inclusiv a mecanismului de repartizare aleatorie;

c) utilizarea jurnalului de audit pentru asigurarea responsabilității utilizatorilor sistemului.

6. Asigurarea trasabilității și auditabilității, care presupune:

a) menținerea istoricului complet al acțiunilor și evenimentelor din sistem;

b) asigurarea posibilității de reconstituire a operațiunilor efectuate asupra obiectelor informaționale;

c) asigurarea suportului informațional necesar desfășurării auditului tehnic, funcțional și juridic.

31. *profilul de utilizator* - obiect informațional care cuprinde toate datele referitoare la utilizatorii autorizați. Profilul utilizatorului va conține toate informațiile legate de acesta și funcționalitățile e-CSP accesibile utilizatorului (drepturi și roluri legate de acesta);

32. *profilul de utilizator* este o entitate de sistem și conține înregistrările tuturor rolurilor de sistem pe care le poate deține utilizatorul:

a) ID Utilizator – identificatorul înregistrării;

b) Titlu – denumirea rolului;

c) Tip – descrierea rolului, nivelul de acces;

d) Data – data creării, data revocării;

e) Nume - numele și prenumele utilizatorului;

f) Funcția – funcția utilizatorului;

g) Contacte – datele de contact ale utilizatorului (telefon, adresă de email).

33. Scenarii de bază ale obiectului informațional *„profilul de utilizator”*:

1. Înregistrarea unui nou utilizator cu un rol specific în sistem;

2. Accesarea, de către administratorul de sistem, a modulului de administrare a utilizatorilor;

3. Inițierea procesului de creare prin selectarea opțiunii „Creare profil nou”;

4. Completarea formularului de profil cu următoarele date: nume, funcție, date de contact, rol atribuit, nivel de acces;

5. Validarea datelor - sistemul verifică dacă toate câmpurile obligatorii sunt completate.

a) Salvarea profilului;

b) Utilizatorul primește acces conform rolului atribuit.

6. Actualizarea datelor unui profil.

a) Accesarea, de către administratorul de sistem, a modulului de administrare a utilizatorilor;

b) Selectarea profilului care urmează a fi modificat;

c) Inițierea procesului de actualizare - se accesează formularul de editare a profilului;

d) Modificarea câmpurilor relevante;

e) Validarea datelor - sistemul validează formatul datelor;

f) Salvarea modificărilor;

g) Confirmarea modificărilor;

7. Revocarea unui utilizator.

a) Accesarea, de către administratorul de sistem, a modulului de administrare a utilizatorilor;

b) Selectarea profilului care urmează a fi revocat;

c) Inițierea procesului de revocare;

d) Confirmarea deciziei.

34. *șabloane și rapoarte* - totalitatea funcționalităților care permit generarea și salvarea în format DOCX, XLSX și PDF a rapoartelor și statisticilor în baza stocului de date al sistemului informatic, precum și identificatoare de șablon, indicatori de raportare, configurații ale formularului de raportare, statutul șablonului.

35. Obiectul informațional *„șabloane și rapoarte”* include:

a) Template ID – identificator unic intern al fiecărui șablon;

b) Denumire - numele clar și concis al șablonului;

c) Descriere – obiectivul;

d) Indicatori incluși – listă/colecție de indicatori;

e) Frecvență raport – periodicitatea raportării;

f) Unitate măsură/cantitatea;

g) Format fișier – fișier atașat;

h) Responsabil rol (utilizatori).

36. Scenarii de bază ale obiectului informațional *„șabloane și rapoarte”*:

a) Crearea șablonului nou;

b) Operatorul/proiectantul propune un șablon ce include anumite câmpuri/atribute;

c) Se atribuie Template ID, versiune și se salvează în registru, cu statutul „propus”;

d) Se realizează validarea și publicarea, schimbându-se statutul la „activ”.

e) Sistemul va crea rapoarte analitice, indicatori de performanță (set de indicatori KPI), rapoarte de monitorizare destinate utilizatorilor cu rol administrator, utilizate pentru aprecierea modalității de interacțiune a utilizatorilor autorizați cu e-CSP. Rapoartele de monitorizare vor organiza și afișa conținutul fișierelor log în baza cărora pot fi analizate și anticipate vulnerabilitățile sistemului informatic.

37. *nomenclatoare și clasificatori* - reprezintă o categorie de obiecte de informații care cuprinde toate metadatele legate de e-CSP. Componenta de gestiune a nomenclatoarelor și clasificatoarelor (metadatelor) constă dintr-un mecanism care va permite administrarea structurii și conținutului sistemului complex de nomenclatoare ale sistemului informațional, care permit referențierea informației conținute în baza de date și adaptării conținutului bazei de date.

38. Identificatorul obiectului informațional *„nomenclatoare și clasificatori”* este numărul de ordine generat de sistem, cu următoarea structură:

a) Nomenclator ID – identificator unic pentru fiecare nomenclator sau clasificator;

b) Denumire nomenclator – denumirea explicită a nomenclatorului;

c) Versiune – versiunea actuală a nomenclatorului;

d) Data validare – data aprobării/activării ultimei versiuni;

e) Statut – activ, revizuit.

39. Scenarii de bază ale obiectului informațional *„nomenclatoare și clasificatori”*:

1. Importarea sau crearea nomenclatorului.

a) Administratorul sistemului poate importa nomenclatoare în format standard (XML, JSON, CSV);

b) Fiecare cod este salvat cu metadate (versiune, sursă, descriere).

2. Sistemul validează unicitatea codurilor și consistența ierarhiei.

3. Revizuirea nomenclatoarelor.

a) Se lansează o nouă versiune a nomenclatorului;

b) Codurile noi sunt adăugate, cele învechite sunt marcate ca „expirate”;

c) Versiunile anterioare rămân disponibile pentru audit și trasabilitate.

Capitolul VII
SPAȚIUL TEHNOLOGIC AL SISTEMULUI INFORMAȚIONAL „e-CSP”

40. La dezvoltarea e-CSP se va aplica arhitectura multi-nivel (având cel puțin următoarele nivele – baza de date, subsistem de păstrare fișiere, logica de aplicație și interfața cu utilizatorul) și o metodologie secvențială de implementare. Dezvoltarea sistemului va urma etape distincte, începând cu analiza și proiectarea detaliată, urmate de implementare, testare și livrare. Această abordare va asigura o structură clară și predictibilă, cu o planificare riguroasă și o delimitare clară a fiecărei faze de dezvoltare. Arhitectura multi-nivel va permite separarea clară a responsabilităților fiecărei componente, asigurând coerență și stabilitate în implementare.

41. Spațiul informațional va utiliza standarde deschise și va fi compatibil cu sisteme care, la fel, utilizează standarde non-proprietare, cât și cu standardele deja existente.

42. Arhitectura complexului software-hardware, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale se determină de către posesor în etapele ulterioare de dezvoltare a Sistemului informațional „e-CSP”, ținând cont de:

a) implementarea unei soluții bazate pe SOA (Service-Oriented Arhitecture – arhitectură software bazată pe servicii), care oferă posibilitatea reutilizării unor funcții ale e-CSP cu noi funcționalități, fără a afecta funcționarea acestuia;

b) implementarea funcționalităților de arhivare (backup) și restabilire a datelor în caz de incidente.

43. E-CSP va putea fi ușor de scalat, prin extinderea resurselor hardware utilizate, pentru a acomoda numărul necesar de utilizatori, atât în regim normal de lucru, cât și în perioadele de vârf.

44. Sistemul de comunicații se va baza pe infrastructura și echipamentul rețelelor guvernamentale, care includ posibilitatea conectării redundante la internet. Infrastructura existentă va fi planificată în mod corespunzător, pentru a oferi nivelele adecvate de performanță și capacitate.

45. Interfețele de utilizare se vor adapta automat la diverse rezoluții de afișare și vor fi disponibile în limbile română, engleză și rusă.

46. E-CSP este construit astfel încât să fie disponibil pentru înregistrare și pentru asigurare a accesului la informație prin servicii de rețea cu un regim de disponibilitate înaltă (24 de ore, 7 zile pe săptămână).

Capitolul VIII
ASIGURAREA SECURITĂȚII INFORMAȚIONALE

47. Asigurarea securității informaționale va include totalitatea măsurilor juridice, organizatorice, economice și tehnologice, orientate spre prevenirea pericolelor securității resurselor și infrastructurii informaționale.

48. Securitatea informațională presupune protecția e-CSP, la toate etapele proceselor de creare, procesare, stocare și transmitere a datelor, de acțiuni accidentale sau intenționate cu caracter artificial sau natural, care au ca rezultat cauzarea prejudiciului posesorului și utilizatorilor resurselor informaționale și infrastructurii informaționale.

49. Asigurarea securității informației va fi realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017.

50. Principalele pericole pentru securitatea informațională a Sistemului informațional „e-CSP” sunt:

a) colectarea și utilizarea ilegală a datelor;

b) încălcarea tehnologiei de selectare și prelucrare a datelor;

c) implementarea în produsele software și hardware a componentelor care realizează funcții neprevăzute în documentația aferentă acestor produse;

d) elaborarea și distribuirea programelor care afectează funcționarea normală a sistemelor informaționale geografice de stat și de comunicații electronice, precum și a sistemelor informaționale de securitate;

e) influența asupra sistemului cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a datelor spațiale;

f) scurgerea informației prin canalele tehnice;

g) implementarea dispozitivelor electronice pentru interceptarea informației în mijloacele tehnice de prelucrare, păstrare și transmitere a datelor, utilizând sistemele de comunicații, precum și în încăperile de serviciu ale autorităților administrației publice centrale și locale;

h) nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau de alt tip;

i) interceptarea informației în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acestei informații și impunerea informației false;

j) utilizarea, la crearea și dezvoltarea infrastructurii informaționale de comunicații electronice, a tehnologiilor informaționale naționale și internaționale, a mijloacelor de protecție a informației și a mijloacelor de informatizare care nu sunt certificate;

k) accesul neautorizat la resursele informaționale din băncile și bazele de date spațiale;

l) încălcarea prevederilor Legii nr.133/2011 privind protecția datelor cu caracter personal.

51. Sistemul informațional „e-CSP” asigură următoarele obiective de securitate:

a) *autentificarea* – garantează că zonele restricționate ale e-CSP vor fi accesibile doar persoanelor autorizate, cu o identitate verificată prin serviciul electronic guvernamental de autentificare și control al accesului (MPass), inclusiv și alte

modalități de autentificare, care permit autorizarea accesului la date cu caracter public din Sistem informațional;

b) *confidențialitatea* – garantează că datele înregistrate nu pot fi accesate de o parte terță neautorizată;

c) *integritatea* – garantează că datele înregistrate în nu au fost modificate sau alterate de o parte terță neautorizată;

d) *non-repudierea* – garantează că datele înregistrate nu pot fi negate mai târziu.

52. În vederea asigurării unui nivel adecvat al securității informaționale a sistemului informatic, posesorul e-CSP elaborează și implementează politica de asigurare a securității informaționale, care detaliază totalitatea compartimentelor de securitate, rolurile, drepturile și obligațiile fiecărui actor al sistemului informatic.

53. O necesitate importantă privind securitatea este necesitatea păstrării înregistrărilor de audit pentru analiza integrității e-CSP și pentru monitorizarea activității înregistrărilor. e-CSP se va baza pe un mecanism de înregistrări de audit dublu (intern și cu utilizarea serviciului electronic guvernamental de jurnalizare (MLog)), ce urmează practicile internaționale.

Capitolul IX
ÎNCHEIERE (DISPOZIȚII FINALE)

54. Sistemul informațional „e-CSP” reprezintă soluția digitală instituțională dezvoltată pentru susținerea activității Consiliului Superior al Procurorilor și a entităților funcționale din subordinea acestuia, în vederea asigurării gestionării electronice a sesizărilor disciplinare, dosarelor disciplinare, documentelor și proceselor aferente competențelor legale ale acestora, inclusiv prin implementarea mecanismului de repartizare aleatorie automată, în conformitate cu cerințele cadrului normativ aplicabil.

55. Prezentul Concept conține descrierea elementelor principale organizaționale, funcționale, informaționale și tehnologice în baza cărora este conceput și implementat Sistemul informațional „e-CSP”, în scopul asigurării unui mecanism informatizat integrat, care să permită evidența electronică, gestionarea, repartizarea automată, examinarea și arhivarea sesizărilor disciplinare și a dosarelor aferente, precum și asigurarea trasabilității complete și auditabilității proceselor gestionate în sistem.

56. Implementarea Sistemului informațional „e-CSP” și valorificarea potențialului tehnologiilor informației și comunicațiilor vor contribui la modernizarea proceselor instituționale ale Consiliului Superior al Procurorilor, la creșterea eficienței operaționale, reducerea dependenței de procese manuale și minimizarea riscurilor asociate intervenției umane în procesele tehnice, inclusiv în procesul de repartizare a sesizărilor și dosarelor disciplinare.

57. Sistemul informațional „e-CSP” va asigura un nivel înalt de transparență, securitate, integritate și trasabilitate a datelor și operațiunilor efectuate, va facilita monitorizarea și controlul proceselor disciplinare și administrative și va contribui la consolidarea capacității instituționale a Consiliului Superior al Procurorilor, în contextul procesului de digitalizare și transformare digitală a sectorului public din Republica Moldova.

Anexa 2

REGULAMENTUL PRIVIND MODUL DE GESTIONARE A RESURSEI INFORMAȚIONALE DIN SISTEMUL INFORMAȚIONAL „E-CSP”

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul privind modul de gestionare a resursei informaționale din sistemul informațional „e-CSP” (în continuare – Regulament) este elaborat în vederea reglementării conținutului, modului de formare, organizare, administrare, funcționare și menținere a resursei informaționale aferente acestuia.

2. Sistemul informațional „e-CSP” constituie o resursă informațională oficială, creată și administrată conform prevederilor legislației Republicii Moldova, implementată și exploatată în scopul asigurării formării, păstrării, prelucrării și utilizării datelor și documentelor aferente activității Consiliului Superior al Procurorilor și entităților funcționale din subordinea acestuia, inclusiv a sesizărilor disciplinare, dosarelor disciplinare, repartizării aleatorii și altor procese instituționale gestionate în cadrul sistemului.

3. Sistemul informațional „e-CSP” este dezvoltat, administrat și gestionat în conformitate cu prevederile Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, precum și cu alte acte normative aplicabile sistemelor informaționale de stat și activității Consiliului Superior al Procurorilor.

Capitolul II
SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL EXPLOATĂRII ȘI UTILIZĂRII SISTEMULUI INFORMAȚIONAL „e-CSP”

4. Subiecții raporturilor juridice în domeniul utilizării e-CSP sunt:

a) proprietarul;
b) posesorul;
c) deținătorul;
d) registratorul;
e) destinatarul;

5. Proprietarul e-CSP este statul, care exercită dreptul de proprietate asupra sistemului în condițiile legii.

6. Posesorul și deținătorul e-CSP este Consiliul Superior al Procurorilor, care asigură administrarea, dezvoltarea și funcționarea sistemului în limitele competențelor stabilite.

7. Registratorii datelor în e-CSP sunt operatorii responsabili de înregistrarea, completarea și/sau modificarea datelor.

8. Destinatarii datelor din e-CSP sunt utilizatorii autorizați, autoritățile publice, instituțiile și persoanele fizice sau juridice care, în conformitate cu cadrul normativ aplicabil, au dreptul de a accesa sau primi datele și documentele gestionate în sistem, în limita competențelor și drepturilor de acces stabilite.

Capitolul III
DREPTURILE ȘI OBLIGAȚIILE PARTICIPANȚILOR LA UTILIZAREA SISTEMULUI INFORMAȚIONAL „e-CSP”

Secțiunea 1
Drepturile și obligațiile posesorului și a deținătorului

9. Posesorul și deținătorul e-CSP are următoarele drepturi:

a) să utilizeze informația disponibilă în cadrul e-CSP în scopul executării obligațiilor sale;

b) să elaboreze și să dezvolte, în baza competențelor, cadrul normativ cu privire la e-CSP;

c) să autorizeze suspendarea activității e-CSP în cazul unei situații excepționale stabilite în conformitate cu actele normative în domeniu, în cazul unor incidente sau în cazul existenței riscurilor semnificative de securitate pentru resursele informaționale de importanță publică;

d) să stabilească regulile de utilizare, administrare și funcționare a sistemului;

e) să solicite registratorilor de date introducerea, actualizarea sau corectarea datelor gestionate în sistem;

f) să utilizeze instrumentele de monitorizare, control și raportare oferite de sistem;

g) să dezvolte și să implementeze noi funcționalități ale sistemului, în conformitate cu necesitățile instituționale și cadrul normativ aplicabil;

h) să asigure interoperabilitatea sistemului cu alte sisteme informaționale de stat;

i) să organizeze activități de instruire și suport pentru utilizatorii sistemului;

j) să utilizeze jurnalul de audit și alte mecanisme de control pentru monitorizarea utilizării sistemului;

k) să stabilească măsurile organizatorice și funcționale necesare asigurării funcționării sistemului.

10. Posesorul și deținătorul e-CSP are următoarele obligații:

a) să asigure condițiile juridice, organizatorice și financiare pentru crearea și funcționarea e-CSP;

b) să asigure suport metodologic și operațional pentru funcționarea eficientă a e-CSP;

c) să stabilească planurile de dezvoltare ale e-CSP;

d) să asigure dezvoltarea continuă a e-CSP;

e) să asigure monitorizarea și evaluarea performanțelor e-CSP;

f) să elaboreze și să aprobe procedurile operaționale pentru operarea e-CSP;

g) să elaboreze și să aprobe regulile tehnice de conectare și accesare a e-CSP, precum și modul de utilizare a acestuia de către subiecți;

h) să asigure monitorizarea și evaluarea performanțelor e-CSP, precum și publicarea periodică a indicatorilor de performanță înregistrați de sistem;

i) să elaboreze, să aprobe și să publice pe interfața publică a e-CSP termenele și condițiile de utilizare a sistemului;

j) să asigure înregistrarea obiectelor informaționale;

k) să intervină pentru investigarea, soluționarea, înlăturarea erorilor identificate sau comunicate de subiecți;

l) să asigure securitatea și protecția datelor;

m) să asigure procesul de integrare cu sistemele informaționale externe;

n) să stabilească măsurile tehnice și organizatorice de protecție și securitate.

o) să asigure integritatea informației în cadrul e-CSP pe segmentul său de responsabilitate;

p) să monitorizeze procesul de înregistrare și prelucrare a datelor în cadrul e-CSP;

q) să asigure suportul metodologic și practic, prin elaborarea de proceduri, reguli și instrucțiuni în ceea ce privește înregistrarea, acumularea, păstrarea, completarea, corectarea, sistematizarea și utilizarea datelor;

r) să colaboreze, conform actelor normative, cu administratorul tehnic în domeniul administrării tehnice a e-CSP.

Secțiunea a 2-a
Drepturile și obligațiile registratorului

11. Registratorul are dreptul:

a) să vizualizeze și să editeze informații relevante generate din Registru, conform rolului atribuit;

b) să valideze și aprobe datele introduse de alți utilizatori, pentru a asigura corectitudinea și conformitatea acestora cu reglementările normative;

c) să acceseze spațiul informațional al e-CSP, în limitele rolului atribuit;

d) să acceseze informațiile care se conțin în Registru și care au fost prezentate de către acesta;

e) dacă sunt identificate erori sau date inexacte, registratorul are dreptul de a le modifica sau corecta, în conformitate cu reglementările și procedurile stabilite;

f) să înainteze posesorului propuneri privind modificarea actelor normative care reglementează funcționarea Registrului;

g) să solicite și să primească de la deținător susținere metodologică și practică privind funcționarea Registrului;

h) să înainteze posesorului și deținătorului propuneri privind îmbunătățirea și sporirea eficacității funcționării Registrului;

i) să acceseze datele puse la dispoziție pe e-CSP.

12. Registratorul este obligat:

a) să asigure continuitatea înregistrării datelor în Registru;

b) să asigure corectitudinea, autenticitatea și veridicitatea datelor introduse în Registru;

c) să asigure actualizarea datelor introduse în Registru;

d) să asigure revizuirea datelor înregistrate în cazul existenței solicitării din partea posesorului;

e) să întreprindă măsuri pentru evitarea accesului neautorizat al persoanelor terțe;

f) să utilizeze funcționalitățile e-CSP în exclusivitate conform destinației acestora și în strictă conformitate cu legislația;

g) să utilizeze informația obținută din Registru doar în scopurile stabilite de legislație.

Secțiunea a 3-a
Drepturile și obligațiile destinatarului

13. Destinatarul are următoarele drepturi:

a) să acceseze și să utilizeze datele și metadatele în scopurile prevăzute de cadrul normativ;

b) să vizualizeze datele și documentele aferente sesizărilor disciplinare, dosarelor disciplinare și altor obiecte informaționale, în limitele drepturilor de acces atribuite;

c) să solicite rapoarte și statistici generate de sistem;

d) să beneficieze de acces la informațiile gestionate în sistem, în conformitate cu cadrul normativ aplicabil.

e) să înainteze posesorului propuneri privind îmbunătățirea și sporirea eficacității funcționării e-CSP.

14. Destinatarul are următoarele obligații:

a) să utilizeze datele conform condițiilor de utilizare descrise de deținătorul e-CSP;

b) să respecte condițiile tehnice și organizatorice de utilizare a e-CSP;

c) să respecte cerințele privind protecția datelor și securitatea informațională;

d) să asigure confidențialitatea datelor și informațiilor la care are acces;

e) să nu utilizeze datele accesate în alte scopuri decât cele prevăzute de cadrul normativ aplicabil;

f) să respecte drepturile de acces și regulile de utilizare stabilite pentru e-CSP;

g) să utilizeze funcționalitățile sistemului exclusiv conform destinației acestora și în conformitate cu cadrul normativ aplicabil.

Capitolul IV
FUNCȚIONAREA SISTEMULUI INFORMAȚIONAL „e-CSP”

15. E-CSP funcționează în condițiile Legii nr.467/2003 cu privire la informatizare și la resursele informaționale de stat și de prezentul Regulament.

16. Interfața de utilizare a sistemului este disponibilă în limbile română, engleză și rusă.

17. Administrarea și exploatarea e-CSP sunt realizate de către posesor și deținător prin intermediul infrastructurii software și hardware, în conformitate cu prezentul Regulament.

18. Integrarea e-CSP cu alte sisteme informaționale, inclusiv cu sistemele informaționale partajate, se realizează conform Conceptului acestuia, utilizând canale de schimb de date securizate.

19. Accesul la date din e-CSP este asigurat prin intermediul aplicației informatice dedicate, utilizând mecanismele de autentificare și control al accesului, în conformitate cu cadrul normativ aplicabil.

20. Toate înregistrările și modificările operate în e-CSP se păstrează în ordine cronologică.

21. e-CSP funcționează zilnic, 24/24, cu excepția timpului rezervat pentru lucrări de mentenanță, care sunt programate.

22. Funcționarea e-CSP se suspendă de către administratorul tehnic în condițiile definite în Regulamentul privind administrarea tehnică și menținerea resurselor și sistemelor informaționale de stat, aprobat prin Hotărârea Guvernului nr.414/2018, cu informarea subiecților prin mijloacele tehnice disponibile.

23. Funcționarea e-CSP se suspendă de către administratorul tehnic, după coordonarea prealabilă cu posesorul și deținătorul, în cazul apariției uneia dintre următoarele situații:

a) efectuarea lucrărilor profilactice ale complexului de mijloace software și hardware al sistemului;

b) încălcarea cerințelor sistemului securității informației, dacă aceasta prezintă pericol pentru funcționarea sistemului;

c) apariția dificultăților tehnice în funcționarea complexului de mijloace software și hardware al sistemului;

d) la cererea scrisă a posesorului sau deținătorului.

24. Funcționarea e-CSP este asigurată de către posesor și de către deținător până la adoptarea deciziei de scoatere din exploatare a acestuia. În cazul scoaterii din exploatare, metadatele se arhivează conform cadrului normativ aplicabil.

25. În cazul scoaterii din exploatare a Sistemului informațional „e-CSP”, resursa informațională și datele gestionate în cadrul sistemului sunt arhivate și păstrate în conformitate cu cerințele cadrului normativ aplicabil.

Capitolul V
ÎNREGISTRAREA DATELOR ÎN REGISTRU

26. Registrul constituit în cadrul e-CSP, fiind integrat cu alte sisteme informaționale, asigură un mediu informațional securizat, integru, exhaustiv și transparent pentru înregistrarea, gestionarea și utilizarea datelor și documentelor electronice.

27. Evidența obiectelor informaționale se asigură conform prevederilor Conceptului e-CSP.

28. Înregistrarea datelor cu privire la obiectele informaționale în e-CSP se efectuează de către registratori;

29. Înregistrarea se efectuează în ordine cronologică, fiecărei înregistrări fiindu-i atribuită data efectuării înscrierii în e-CSP;

30. Accesul la informația bazei de date pentru înregistrare va fi limitată în funcție de drepturile și rolurile specifice utilizatorilor. Fiecare categorie de utilizatori va avea acces la o interfață personalizată pentru vizualizarea și gestionarea informației bazei de date;

31. Codul de identificare a înregistrării este unic, invariabil și nu poate fi atribuit altor înregistrări, inclusiv după radierea acestuia din e-CSP

32. Registratorii se vor autentifica în e-CSP prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass).

Capitolul VI
MODIFICAREA, COMPLETAREA ȘI RADIEREA DATELOR DIN REGISTRU

33. Modificarea, corectarea, completarea sau radierea datelor din e-CSP se efectuează cu indicarea motivului și în baza documentelor justificative, asigurându-se trasabilitatea acțiunilor.

34. e-CSP asigură accesul la istoricul complet al modificărilor, precum și vizualizarea datelor la orice etapă a prelucrării acestora.

35. Orice intervenție asupra datelor se realizează exclusiv în condițiile stabilite de legislație și pe baza documentelor justificative.

36. Modificările efectuate sunt păstrate în ordine cronologică, fără a afecta integritatea sau accesibilitatea datelor inițiale.

37. Actualizarea datelor nu constituie corectare, registratorii fiind obligați să asigure corectitudinea și actualitatea informațiilor introduse.

38. E-CSP utilizează datele până la atingerea scopului, ulterior permite arhivarea datelor și a documentelor în format electronic, în vederea eficientizării procesului de prelucrare și furnizare către utilizator a informației documentate.

39. Termenul de păstrare a documentelor electronice este echivalent cu cel prevăzut pentru documentele pe suport de hârtie.

40. Indiferent de nivelul de acces al utilizatorului, dreptul de acces nu trebuie să posede dreptul de a suprima direct înregistrările bazei de date, fiind admisă doar schimbarea statutului înregistrării ce urmează a fi eliminată. De asemenea, nu se va admite modificarea directă a datelor bazei de date fără a fi coordonate și aprobate de către instituția responsabilă.

41. Orice modificare a datelor este jurnalizată, indicând momentul efectuării și utilizatorul responsabil.

Capitolul VII
MĂSURI DE ASIGURARE A SECURITĂȚII

42. Securitatea informațională presupune protecția e-CSP în toate etapele proceselor de creare, de procesare, de stocare și de transmitere a datelor, de acțiuni accidentale sau intenționate cu caracter artificial sau natural, care au ca rezultat cauzarea prejudiciului posesorului/deținătorului și utilizatorilor resurselor informaționale și infrastructurii informaționale.

43. Elaborarea, menținerea și administrarea e-CSP este realizată în conformitate cu legislația și standardele naționale în domeniul asigurării securității informaționale și protecției informației.

44. Asigurarea securității informației se realizează în conformitate cu obligațiile de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, aprobate prin Hotărârea Guvernului nr.562/2025.

45. Executarea măsurilor de asigurare a securității informaționale și a suportului software atât împotriva accesului neautorizat la bazele de date ale e-CSP, cât și împotriva modificării neautorizate a conținutului obiectelor informaționale și a suportului software al e-CSP îi revine deținătorului.

Capitolul VIII
CONTROLUL ȘI RESPONSABILITATE INSTITUȚIONALĂ

46. Ținerea e-CSP este supusă controlului intern și extern, în conformitate cu legislația.

47. Controlul intern asupra modului de ținere a e-CSP se realizează de către posesorul sistemului informațional.

48. Controlul extern asupra respectării cerințelor privind crearea, ținerea și reorganizarea e-CSP se efectuează de către autoritățile abilitate cu atribuții în domeniul auditului informatic.

49. Responsabilitatea pentru corectitudinea și veridicitatea datelor transmise spre publicare în e-CSP aparține registratorilor, inclusiv deținătorului acestuia pentru datele proprii publicate;

50. Suspendarea activităților minime ale e-CSP se realizează la solicitarea posesorului, sau din inițiativa administratorului tehnic în condițiile Hotărârii Guvernului 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat.