

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. _____
din _____ 2025

Pentru aprobarea Conceptului Sistemului informațional „Registrul circulației bunurilor culturale mobile” și a Regulamentului resursei informaționale formate de Sistemul informațional „Registrul circulației bunurilor culturale mobile”

În temeiul art. 22 lit. d) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările ulterioare, Guvernul

HOTĂRĂȘTE:

1. Se instituie Sistemul informațional „Registrul circulației bunurilor culturale mobile”;

2. Se aprobă:

2.1 Conceptul Sistemului informațional „Registrul circulației bunurilor culturale mobile”, conform Anexei nr. 1;

2.2 Regulamentul resursei informaționale formate de Sistemul informațional „Registrul circulației bunurilor culturale mobile”, conform Anexei nr. 2

3. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Culturii.

4. Prezenta hotărâre intră în vigoare peste o lună de la data publicării în Monitorul Oficial al Republicii Moldova.

PRIM-MINISTRU

ALEXANDRU MUNTEANU

Contrasemnează:

Ministrul Culturii

Cristian Jordan

Conceptul Sistemului informațional „Registrul circulației bunurilor culturale mobile”

Capitolul I Introducere

1. În contextul adoptării de către Republica Moldova a aquis-ului european, cadrul normativ și instituțional în domeniul bunurilor culturale mobile a fost modificat: Legea nr. 280/2011 privind protejarea patrimoniului cultural mobil (în continuare Legea nr. 280/2011) a fost amendată, Codul Vamal, în speță articolele cu referire la bunurile culturale, au fost ajustate la prevederile legii menționate. Prin Hotărârea de Guvern nr. 470/2023 a fost aprobat Regulamentul de circulație a bunurilor culturale mobile, iar modificările normative au dus la crearea Serviciului de Evidență și Circulație a Bunurilor Culturale Mobile, cu scopul de a concentra sarcinile de evidență a bunurilor culturale și monitorizare a circulației acestora în cadrul unei entități distincte.

2. Scopul Legii nr. 280/2011 este ajustarea cadrului legislativ național în domeniul recuperării și restituirii patrimoniului cultural mobil, alinierea la cerințele prevăzute de legislația Uniunii Europene și încurajarea cooperării dintre Republica Moldova și statele membre UE în vederea recuperării și restituirii patrimoniului cultural mobil de importanță europeană. Având în vedere că traficul de bunuri culturale este, de obicei, o infracțiune transfrontalieră, legislația UE joacă un rol important în prevenirea și depistarea unor astfel de cazuri.

3. Sistemul informațional „Registrul circulației bunurilor culturale mobile” (în continuare SI RBCM) constituie registru de stat departamental, creat și administrat în conformitate cu Legea nr. 71/2007 cu privire la registre.

Capitolul II DISPOZIȚII GENERALE

4. Conceptul SI RBCM (în continuare – Concept) specifică cerințele de bază privind SI RBCM, destinația și scopul creării acestuia, funcțiile de bază, obiectele sistemului, structura resurselor informaționale, infrastructura informațională a sistemului, cerințele de bază privind furnizarea informațiilor și preluarea acestora de către autoritățile cu atribuții în circulația bunurilor culturale pentru a se asigura că circulația bunurilor culturale mobile este conformă cerințelor stabilite în cadrul normativ aplicabil și cerințele cu privire la securitatea și protecția informațiilor și pentru a contribui la contracararea traficului ilicit de bunuri culturale.

5. SI RBCM reprezintă o resursă informațională de stat, care cuprinde date sistematizate referitoare la domeniul evidenței și circulației interne și externe a bunurilor culturale mobile, inclusiv date despre subiecții supuși monitorizării și autoritățile de monitorizare și supraveghere a domeniului, activitățile desfășurate și măsurile luate de către acestea, cererile, notificările, certificatele și adevărurile și deciziile de interdicere a punerii bunurilor culturale în liberă circulație.

6. SI RBCM este destinat pentru a sprijini măsurile de monitorizare și supraveghere a evidenței și circulației bunurilor culturale mobile. Sistemul va asigura autoritățile de monitorizare și supraveghere a domeniului cu un instrument eficient și centralizat pentru monitorizarea activităților desfășurate și a măsurilor aplicate de acestea, în cooperare cu Serviciul Vamal, pentru a asigura că circulația bunurilor culturale se desfășoară conform cerințelor normative aplicabile sau că nu pun în pericol patrimoniul cultural mobil și nu contribuie la traficul ilicit de bunuri culturale.

7. Noțiunile utilizate în prezentul Concept au semnificațiile prevăzute în Legea nr. 71/2007 cu privire la registre, Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat.

8. Scopurile SI RBCM sunt:

8.1. asigurarea cu o soluție informatică performantă, utilizată ca suport pentru automatizarea activității în vederea implementării prevederilor cadrului normativ privind circulația bunurilor culturale;

8.2. organizarea interacțiunii eficiente și a schimbului de informații dintre Serviciul de Evidență și Circulație a Bunurilor Culturale Mobile (în continuare SECBCM) și Serviciul Vamal prin utilizarea sistemelor informaționale;

8.3. creșterea trasabilității bunurilor culturale mobile, prin urmărirea digitală a circulației acestora (export, import, transfer, împrumut, restituire), în conformitate cu legislația națională și standardele Uniunii Europene.

8.4. colectarea și prelucrarea operativă a informațiilor privind circulația bunurilor culturale;

8.5. evidența statistică și analitică privind activitățile desfășurate și măsurile aplicate de autoritățile cu competențe în domeniul circulației bunurilor culturale mobile;

8.6. asigurarea schimbului de date obligatoriu cu Serviciul Vamal al Republicii Moldova în vederea controlului circulației bunurilor culturale mobile, conform Codului vamal și HG 470/2023.

9. SI RBCM are următoarele sarcini:

9.1. asigurarea înregistrării și prelucrării informațiilor privind activitățile desfășurate de către autoritățile competente în domeniul protejării patrimoniului

cultural național mobil și circulației bunurilor culturale, inclusiv a măsurilor administrative dispuse în cazul constatării nerespectării regimului de protejare sau a procedurilor de export/import;

9.2. recepționarea notificărilor de respingere a solicitărilor de scoatere definitivă sau temporară a bunurilor culturale mobile și a datelor asociate, transmise de către Serviciul Vamal, în scopul prevenirii și neadmiterii scoaterii ilicite a bunurilor culturale din Republica Moldova;

9.3. asigurarea interacțiunii informaționale și a interoperabilității cu bazele de date gestionate de SECBCM, Serviciul Vamal și alte autorități publice relevante, în vederea schimbului de date referitoare la circulația, exportul și importul bunurilor culturale mobile;

9.4. controlul accesului la date și asigurarea securității informaționale la formarea, stocarea și exploatarea resursei informaționale a SI RBCM, în conformitate cu cerințele cadrului normativ privind securitatea cibernetică, protecția datelor cu caracter personal și utilizarea infrastructurii guvernamentale de interoperabilitate.

10. Principiile de bază ale SI RBCM sunt:

10.1. *principiul legalității*, care presupune crearea, dezvoltarea și exploatarea SI RBCM în conformitate cu legislația Republicii Moldova în vigoare;

10.2. *principiul integrității datelor*, care presupune păstrarea conținutului și interpretarea univocă a informațiilor în condițiile unor acțiuni accidentale. Integritatea se consideră păstrată dacă datele nu au fost denaturate sau distruse;

10.3. *principiul veridicității datelor*, care presupune gestionarea informațiilor privind bunurile culturale mobile în baza unor date autentice și confirmate de documentele oficiale;

10.4. *principiul plenitudinii datelor*, care are în vedere asigurarea volumului complet al informațiilor gestionate de SI RBCM, conform actelor normative aplicabile domeniului patrimoniului cultural mobil;

10.5. *principiul confidențialității informației*, care se referă la restricționarea accesului persoanelor neautorizate la informațiile cu acces limitat, inclusiv cele cu caracter personal sau sensibile;

10.6. *principiul securității informaționale*, care presupune asigurarea nivelului necesar de integritate, confidențialitate și disponibilitate a datelor, precum și protecția acestora împotriva pierderii, alterării, denaturării, deteriorării, modificării, accesului ori utilizării neautorizate. Securitatea SI RBCM implică reziliența la atacuri cibernetice și protecția datelor atât la nivel de sistem, cât și la nivel de conținut;

10.7. *principiul compatibilității*, conform căruia SI RBCM trebuie să fie compatibil cu alte sisteme informaționale publice existente în țară și cu infrastructura guvernamentală de interoperabilitate;

10.8. *principiul dezvoltării progresive*, care presupune perfecționarea continuă a SI RBCM în conformitate cu apariția unor noi obiecte, procese și cerințe normative;

10.9. *principiul modularității și al scalabilității*, care asigură posibilitatea de a extinde sau adapta funcționalitățile sistemului fără modificarea componentelor existente;

10.10. *principiul neexcesivității și pertinentei prelucrării datelor cu caracter personal*, care subliniază necesitatea limitării volumului de date prelucrate, astfel încât să fie gestionate doar informațiile relevante și necesare scopului SI RBCM.

Capitolul III

SPAȚIUL JURIDICO-NORMATIV AL FUNCȚIONĂRII SISTEMULUI

12. Dezvoltarea, administrarea și exploatarea Sistemului informațional în domeniul bunurilor culturale mobile “SI RBCM” se realizează în conformitate cu legislația Republicii Moldova și cu standardele tehnice în vigoare, după cum urmează:

12.1. Acte normative cu caracter general în domeniul tehnologiei informației:

12.1.1. Constituția Republicii Moldova;

12.1.2. Legea nr. 1069/2000 cu privire la informatică;

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

12.1.4. Legea nr. 71/2007 cu privire la registre.

12.2. Domeniul identității electronice, semnăturii electronice și infrastructurii guvernamentale:

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

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

12.2.3. Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);

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

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

12.2.6. Hotărârea Guvernului nr. 280/2020 privind serviciul guvernamental de plăți electronice (MPay);

12.2.7. Hotărârea Guvernului nr. 250/2021 privind serviciul guvernamental de notificare electronică (MNotify);

12.2.8. Hotărârea Guvernului nr. 414/2018 privind măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat.

12.3. Domeniul interoperabilității și al schimbului de date:

12.3.1. Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

12.3.2. Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect).

12.4. Domeniul protecției datelor și al accesului la informații:

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

12.4.2. Legea nr. 148/2023 privind accesul la informațiile de interes public.

12.5. Domeniul securității cibernetice și al infrastructurilor critice:

12.5.1. 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;

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

12.6. Domeniul bunurilor culturale mobile și al regimului vamal:

12.6.1. Legea nr. 280/2011 privind protejarea patrimoniului cultural național mobil;

12.6.2. Codul vamal al Republicii Moldova nr. 95/2021;

12.6.3. Hotărârea Guvernului nr. 92/2023 pentru punerea în aplicare a Codului vamal nr. 95/2021;

12.6.4. Hotărârea Guvernului nr. 470/2023 pentru punerea în aplicare a prevederilor Legii nr. 280/2011 privind protejarea patrimoniului cultural național mobil.

12.7. Alte acte relevante:

12.7.1. Legea nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității (aplicabilă în cazul recunoașterii expertizelor acreditați);

12.7.2. Legea nr. 131/2012 privind controlul de stat (aplicabilă în cazul verificărilor administrative în domeniul patrimoniului cultural);

12.7.3. Legea nr. 172/2014 privind aprobarea Nomenclurii combinate a mărfurilor (pentru corelarea codurilor tarifare vamale ale bunurilor culturale);

12.7.4. Hotărârea Guvernului nr. 683/2018 privind normele tehnice de interoperabilitate și armonizare a seturilor de date spațiale;

12.7.5. Hotărârea Guvernului nr. 412/2020 privind Portalul guvernamental al unităților de drept;

12.7.6. Hotărârea Guvernului nr. 413/2020 privind Portalul guvernamental al cetățeanului.

12.7.7. Hotărârea Guvernului nr. 677/2025 cu privire la consolidarea accesibilității serviciilor electronice și a site-urilor web oficiale (modelul unitar de design).

12.7.8. Hotărârea Guvernului nr. 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023–2030.

12.7.9. Hotărârea Guvernului nr. 305/2024 cu privire la platforma de găzduire și partajare a documentelor (MDocs).

12.7.10. Hotărârea Guvernului nr. 323/2021 pentru aprobarea Conceptului Sistemului informațional „Catalogul semantic” și a modului de ținere a Registrului format de Sistemul informațional „Catalogul semantic”.

12.8. Standardele și reglementările tehnice aplicabile. La elaborarea și implementarea SI RBCM se vor respecta următoarele standarde și reglementări tehnice:

12.8.1. SM EN ISO/IEC 27001 – Securitatea informației, securitatea cibernetică și protecția vieții private. Sisteme de management al securității informației – Cerințe;

12.8.2. SM EN ISO/IEC 27002 – Securitatea informației, securitatea cibernetică și protecția vieții private. Măsurile de control al securității informației;

12.8.3. SM EN ISO/IEC 12207 – Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului;

12.8.4. SM EN ISO/IEC 15288 – Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului;

12.8.5. SM EN ISO/IEC 15408-1 – Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea TI. Partea 1: Introducere și model general;

12.8.6. SM EN ISO/IEC 15408-2 – Partea 2: Cerințe funcționale de securitate;

12.8.7. SM EN ISO/IEC 15408-3 – Partea 3: Cerințe de asigurare a securității;

12.8.8. Reglementarea tehnică RT 38370656-002:2006 – Procesele ciclului de viață al software-ului.

Capitolul IV

SPAȚIUL FUNCȚIONAL AL SI RBCM

Secțiunea 1 Funcțiile de bază ale SI RBCM

13. Sistemul informațional în domeniul bunurilor culturale mobile (SI RBCM) asigură executarea funcțiilor sale de bază și a funcțiilor specifice, determinate de destinația acestuia, grupate în contururi funcționale specializate.

13. Funcțiile de bază ale SI RBCM sunt:

13.1. Formarea resursei informaționale a SI RBCM se realizează prin:

13.1.1. înregistrarea inițială a obiectelor și a datelor aferente, în baza deciziilor adoptate de autoritățile competente;

13.1.2. actualizarea sistematică a informațiilor la modificarea atributelor obiectelor de evidență;

13.1.3. modificarea statutului unui obiect (de exemplu: arhivare, restituire, retragere), cu păstrarea istoricului integral al modificărilor;

13.1.4. arhivarea și radierea datelor se realizează în conformitate cu termenii de păstrare prevăzuți în cadrul normativ;

13.1.5. identificarea unică și trasabilitatea atribuie fiecărui obiect un identificator unic valabil pe toată durata existenței sale în SI RBCM și asigură jurnalizarea cronologică a tuturor operațiunilor efectuate.

13.2. Organizarea suportului informațional are loc, după cum urmează:

13.2.1. administrarea a accesului de date, conform drepturilor stabilite:

13.2.2. furnizarea controlată a informațiilor asigură punerea la dispoziția utilizatorului a informațiilor din baza de date a SI RBCM, conform nivelurilor de acces stabilite;

13.2.3. asigurarea confidențialității și integrității datelor garantează utilizarea informațiilor exclusiv în scopuri legale, precum și protejarea acestora împotriva accesului neautorizat, modificării sau pierderii;

13.2.4. auditarea și trasabilitatea înregistrează și monitorizează toate operațiunile efectuate asupra datelor, în vederea asigurării responsabilității și transparenței.

13.3. Stabilirea nivelurilor de acces ale utilizatorilor se realizează prin următoarele funcții:

13.3.1 autentificare și autorizare asigură identificarea utilizatorilor și acordarea accesului la resursele SI RBCM prin intermediul platformei guvernamentale MPass, potrivit drepturilor stabilite și cadrului normativ aplicabil;

13.3.2 administrare a accesului stabilește și gestionează nivelurile de acces la informațiile din SI RBCM, conform competențelor instituționale și politicilor de securitate aprobate.

13.4. Asigurarea securității și protecției informațiilor se realizează prin următoarele funcții:

13.4.1 protecție a datelor și comunicațiilor – asigură securitatea informațiilor pe întreg ciclul de viață (colectare, stocare, procesare, transmitere și arhivare), în conformitate cu cerințele minime obligatorii de securitate cibernetică stabilite prin Hotărârea Guvernului nr. HG 562/2025 și cu standardele SM EN ISO/IEC 27001 și 27002;

13.4.2. gestionare a incidentelor de securitate – permite monitorizarea, detectarea și raportarea evenimentelor care pot afecta integritatea,

confidențialitatea sau disponibilitatea datelor, conform politicilor de securitate aprobate de administratorul sistemului.

13.5. Asigurarea calității informației se realizează prin următoarele funcții:

13.5.1 validare a datelor – efectuează verificări automate ale completitudinii și corectitudinii informațiilor introduse în SI RBCM;

13.5.2 audit și control al datelor – permite efectuarea auditului periodic și corelarea informațiilor între surse, în conformitate cu metodologia aprobată de administratorul SI RBCM.

13.6. Asigurarea interoperabilității funcționale, semantice și tehnice a SI RBCM se realizează prin următoarele funcții:

13.6.1. integrare prin platforma guvernamentală de interoperabilitate (MConnect) și componenta MConnect Events, în scopul asigurării schimbului de date în timp real și furnizării serviciilor proactive;

13.6.2. conformitate semantică și tehnică – asigură utilizarea clasificatoarelor și standardelor comune de date și respectarea cerințelor de interoperabilitate stabilite de autoritatea competentă în domeniu – Instituția publică Agenția de Guvernare Electronică (AGE).

Secțiunea a 2-a

Contururile funcționale de bază

14. Spațiul funcțional al Sistemului informațional în domeniul bunurilor culturale mobile (SI RBCM) reprezintă ansamblul funcțiilor realizate de subsistemele și modulele sale informaționale, care interacționează reciproc și asigură schimbul coerent de date între participanți prin intermediul infrastructurii guvernamentale de interoperabilitate.

15. În cadrul SI RBCM sunt definite următoarele contururi funcționale principale:

15.1 Conturul de coordonare și administrare;

15.2 Conturul de participare;

15.3 Conturul de guvernare și raportare.

Fiecare contur funcțional cuprinde totalitatea funcțiilor specifice realizate de subsistemele corespunzătoare, integrate prin platforma de interoperabilitate MConnect și găzduite pe infrastructura comună MCloud.

16. Conturul de coordonare și administrare include următoarele funcții specifice (realizate de SECBCM):

16.1. administrarea bazelor de date, clasificatoarelor și nomenclatoarelor utilizate;

16.2. gestionarea identității și a accesului utilizatorilor (autentificare MPass, control pe rol/competență);

- 16.3. semnarea și validarea documentelor prin MSign;
 - 16.4. jurnalizarea și auditarea evenimentelor prin MLog;
 - 16.5. aplicarea măsurilor de securitate conform ISO/IEC 27001–27002 și cerințelor STISC;
 - 16.6. protecția datelor cu caracter personal potrivit Legii 133/2011;
 - 16.7. mentenanța tehnică și administrarea infrastructurii găzduite în MCloud;
 - 16.8. interoperabilitatea tehnică prin MConnect și coordonarea schimburilor de date cu Serviciul Vamal și alte autorități participante;
 - 16.9. consolidarea rapoartelor statistice și operaționale pentru Ministerul Culturii și Guvern.
17. Conturul de participare include următoarele funcții specifice (realizate de Serviciul Vamal al Republicii Moldova):
- 17.1. recepționarea și validarea electronică a documentelor transmise prin SI RBCM;
 - 17.2. schimbul de date cu Sistemul Informațional Integrat Vamal (SIIV) prin MConnect;
 - 17.3. notificarea automată a rezultatelor verificărilor vamale;
 - 17.4. jurnalizarea evenimentelor prin MLog;
 - 17.5. elaborarea rapoartelor statistice privind fluxurile vamale asociate bunurilor culturale mobile;
 - 17.6. preluarea automată din SIIV a datelor declarației vamale: număr, dată, regim vamal, articol de marfă, birou vamal, statutul controlului;
 - 17.7. transmiterea automată către Serviciul Vamal a informațiilor privind actele emise de SI RBCM relevante pentru controlul circulației bunurilor culturale mobile;
 - 17.8. generarea notificărilor de recepționare, acceptare sau refuz al actului emis;
 - 17.8.1. Schimbul de date dintre SI RBCM și Serviciul Vamal se realizează prin mesaje standardizate – înștiințare de recepționare, înștiințare de acceptare și înștiințare de refuz – transmise prin platforma de interoperabilitate MConnect, semnate electronic prin MSign și jurnalizate automat prin MLog.
 - 17.9. verificarea autenticității documentelor SI RBCM prezentate la controlul vamal.
 - 17.10. corelarea operațiunilor de introducere/scoatere cu registrele interne ale SECBCM.
18. Conturul de guvernanță și raportare include următoarele funcții specifice (realizate de Ministerul Culturii):
- 18.1. aprobarea politicilor de dezvoltare și interoperabilitate;

- 18.2. analiza și utilizarea rapoartelor consolidate furnizate de SECBCM;
- 18.3. coordonarea cooperării internaționale și armonizarea cadrului normativ;
- 18.4. asigurarea conformității SI RBCM cu politicile de transformare digitală ale statului.
- 19. Arhitectura funcțională a SI RBCM este modulară și interoperabilă, concepută pentru:
 - 19.1. gestionarea completă, trasabilă și securizată a proceselor de evidență, expertizare, autorizare și circulație a bunurilor culturale mobile;
 - 19.2. integrarea cu serviciile guvernamentale comune (MConnect, MPass, MSign, MLog, MNotify, MPay, MCloud);
 - 19.3. conformitatea cu cerințele privind protecția datelor și securitatea cibernetică stabilite de cadrul normativ național și standardele internaționale aplicabile.
 - 19.4. toate înregistrările introduse în SI RBCM sunt confirmate prin semnătura electronică calificată a registratorului.

Secțiunea a 3-a

Interconexiunea cu alte sisteme

20. Pentru asigurarea funcționării eficiente, sigure și interoperabile, SI RBCM se interconectează cu platformele și serviciile guvernamentale comune. Scopul interconectării este schimbul automat și securizat de date cu alte sisteme publice, reducerea redundanței informaționale și integrarea proceselor de autorizare, evidență și raportare privind circulația bunurilor culturale mobile. Arhitectura SI RBCM se proiectează astfel încât, pe lângă realizarea schimbului de date sincron prin MConnect, să permită integrarea cu componenta MConnect Events pentru expunerea evenimentelor sistemice în timp real în contextul realizării serviciilor proactive, în conformitate cu ghidul tehnic publicat de AGE.

20.1. Platforma de interoperabilitate (MConnect) – asigură schimbul securizat de date și interoperabilitatea cu alte sisteme informaționale de stat.

20.2. Serviciul guvernamental de autentificare și control al accesului (MPass) – identificarea electronică și autentificarea utilizatorilor sistemului (mecanism SSO).

20.3. Serviciul guvernamental de semnătură electronică (MSign) – semnarea electronică a documentelor și operațiunilor efectuate în SI RBCM.

20.4. Serviciul guvernamental de jurnalizare (MLog) – înregistrarea, monitorizarea și auditarea evenimentelor din sistem, pentru asigurarea trasabilității, integrității și securității operațiunilor electronice.

20.5. Serviciul guvernamental de notificare electronică (MNotify) – transmiterea automată a notificărilor și informărilor către utilizatori.

20.6. Serviciul guvernamental de plăți electronice (MPay) – procesarea online a plăților aferente serviciilor electronice oferite prin SI RBCM (achitarea taxelor pentru eliberarea adeverințelor, certificatelor etc.).

20.7. Portalul guvernamental integrat EVO – oferă acces simplificat pentru persoanele juridice și persoanele fizice la serviciile și informațiile disponibile prin SI RBCM. Prin intermediul Portalului guvernamental integrat EVO, persoanele juridice vor putea vizualiza datele din registru și vor putea obține informațiile documentate despre persoanele fizice și unitățile de drept.

20.8. Infrastructura guvernamentală de cloud computing (MCloud) – asigură găzduirea sigură, scalabilă și redundantă a SI RBCM.

Capitolul V

STRUCTURA ORGANIZAȚIONALĂ A SI RBCM

21. Proprietar al SI RBCM este statul Republica Moldova, care stabilește posesorii, deținătorii, administratorii tehnici și utilizatorii sistemelor informaționale de stat. Resursele financiare pentru dezvoltarea, implementarea și exploatarea SI RBCM se asigură din bugetul de stat și din alte surse legale, conform cadrului normativ în vigoare.

22. Posesorul SI RBCM este Ministerul Culturii, în calitate de autoritate publică centrală responsabilă de politicile de stat în domeniul patrimoniului cultural național. Ministerul Culturii:

22.1. exercită rolul de posesor instituțional și coordonator de domeniu;

22.2. asigură condițiile juridice, organizaționale, metodologice, financiare și tehnice pentru crearea, administrarea și dezvoltarea sistemului;

22.3. coordonează și monitorizează procesele de evidență și circulație a bunurilor culturale mobile, potrivit Legii nr. 280/2011 și HG nr. 470/2023.

23. Deținătorul SI BCM este Serviciul Tehnologia Informației și Securitate Cibernetică (STISC), care asigură:

23.1. găzduirea sistemului în infrastructura guvernamentală comună (MCloud);

23.2. mentenanța tehnică la nivel de infrastructură;

23.3. aplicarea măsurilor de securitate informațională la nivel de infrastructură, realizarea copiilor de rezervă și păstrarea acestora, în conformitate cu Hotărârea Guvernului nr. 128/2014 și Hotărârea Guvernului nr. 562/2025.

24. Administratorul SI RBCM este SECBCM, autoritate administrativă subordonată Ministerului Culturii. SECBCM exercită atribuțiile de administrare tehnică și operațională a sistemului, asigurând:

24.1. administrarea bazelor de date, a fluxurilor informaționale și a componentelor funcționale;

24.2. gestionarea drepturilor de acces și atribuirea nivelurilor de acces utilizatorilor, prin intermediul serviciului guvernamental MPass;

24.3. gestionarea și actualizarea nomenclatoarelor, clasificatoarelor și a tipurilor de documente utilizate în sistem;

24.4. monitorizarea activităților și auditarea evenimentelor prin MLog;

24.5. aplicarea măsurilor de securitate cibernetică, confidențialitate și integritate a datelor, conform SM EN ISO/IEC 27001–27002, HG 201/2017 și politicilor STISC privind infrastructura guvernamentală comună;

24.6. coordonarea proceselor de interoperabilitate funcțională, semnătură electronică (MSign), notificare (MNotify) și plăți electronice (MPay) în cadrul infrastructurii MConnect și MCloud;

24.7. instruirea și suportul pentru utilizatorii autorizați;

24.8. raportarea periodică către Ministerul Culturii și către Serviciul Tehnologia Informației și Securitate Cibernetică privind performanța, securitatea și disponibilitatea sistemului.

25. Participanții instituționali și registratorii de date în cadrul SI RBCM sunt autoritățile competente în domeniul gestionării și circulației bunurilor culturale mobile, potrivit Legii nr. 280/2011 și HG nr. 470/2023, după cum urmează:

25.1. Ministerul Culturii este posesor al sistemului și autoritate responsabilă de politicile de stat în domeniu;

25.2. SECBCM – administrator al SI RBCM și coordonator funcțional al SI RBCM;

25.2.1. SECBCM are calitatea de posesor și deținător al registrului în sensul art. 11 și 12 din Legea nr. 71/2007.

25.3. Serviciul Vamal al Republicii Moldova – partener instituțional, responsabil de verificarea și monitorizarea exportului și importului bunurilor culturale mobile;

25.3.1. Serviciul Vamal al Republicii Moldova are calitatea de furnizor și destinatar de date, conform art. 14–15 din Legea nr. 71/2007.

25.4. Ministerul Dezvoltării Economice și Digitalizării – autoritate responsabilă de elaborarea și promovarea politicilor de stat în domeniul dezvoltării economice și al transformării digitale;

26. Utilizatorii datelor din SI RBCM sunt persoanele juridice și fizice de drept public sau privat care utilizează informațiile generate de sistem potrivit competențelor legale, în scopul exercitării atribuțiilor funcționale, al procesului decizional și al informării publice. Nivelurile de acces și drepturile de utilizare sunt stabilite de SECBCM, în calitate de administrator tehnic și de sistem, în

conformitate cu legislația privind protecția datelor cu caracter personal și regulamentele interne de exploatare.

Capitolul VI

DOCUMENTELE SI RBCM

27. În cadrul SI RBCM se utilizează documente electronice generate, procesate și gestionate în conformitate cu Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere și cu actele normative privind documentul și semnătura electronică. Documentele utilizate în SI RBCM se clasifică în următoarele categorii:

27.1. documente de intrare – acte, cereri și fișiere electronice introduse de utilizatori autorizați pentru inițierea, actualizarea sau completarea proceselor de evidență, autorizare, expertizare și circulație a bunurilor culturale mobile;

27.2. documente de ieșire – documente electronice generate automat de sistem ca rezultat al procesării datelor (certificate, adeverințe, notificări, decizii administrative și rapoarte statistice);

27.3. documente tehnologice – documente interne destinate administrării SI RBCM (inclusiv documentele de interoperabilitate: mesaje electronice, protocoale de schimb și documente tehnice aferente integrării cu serviciile guvernamentale conexe);

28. Documentele de intrare, de ieșire și de interoperabilitate se generează conform formularelor și modelelor stabilite de Regulamentul privind circulația bunurilor culturale mobile, aprobat prin HG nr. 470/2023, precum și potrivit cerințelor tehnice ale platformei de interoperabilitate MConnect. Toate documentele sunt semnate electronic prin serviciul MSign, marcate temporal și arhivate electronic în conformitate cu standardele SM EN ISO/IEC 27001 și 27002.

29. Documentele tehnologice ale SI RBCM includ:

29.1. documentația tehnică de descriere a structurii de date, fluxurilor informaționale și interfețelor de interoperabilitate;

29.2. nomenclatoarele, clasificatoarele și ghidurile de utilizare;

29.3. jurnalele de evenimente și rapoartele de audit generate prin MLog;

29.4. procesele de backup, restaurare și arhivare digitală efectuate conform politicilor de securitate ale infrastructurii MCloud și cerințelor STISC.

Capitolul VII

SPAȚIUL INFORMAȚIONAL AL SI RBCM

30. Spațiul informațional al SI RBCM reprezintă ansamblul datelor și obiectelor informaționale gestionate în cadrul sistemului, care se formează, se actualizează și se arhivează în procesul electronic de evidență, expertizare, autorizare și circulație a bunurilor culturale mobile. Resursa informațională a SI RBCM este compusă din totalitatea datelor create, prelucrate și schimbate între participanții autorizați, în conformitate cu Legea nr. 280/2011 și Hotărârea Guvernului nr. 470/2023, și include următoarele obiecte informaționale principale:

- 30.1. cererea de eliberare a certificatului de export (definitiv sau temporar);
- 30.2. cererea de eliberare a adeverinței de export;
- 30.3. raportul de expertiză;
- 30.4. certificatul de export și adeverința de export emise în format electronic;
- 30.5. notificarea privind circulația bunurilor culturale mobile;
- 30.6. înștiințările electronice generate automat (recepționare, validare, refuz);
- 30.7. datele referitoare la persoanele fizice și juridice participante (solicitant, expert, autoritate competentă, Serviciul Vamal);
- 30.8. evenimentele sistemice și jurnalele de acțiuni generate automat în procesul de operare și interoperabilitate.
- 30.9. fiecărui obiect informațional (bun cultural mobil, certificat, decizie) i se atribuie un identificator unic și invariabil, conform art. 20 alin. (2) din Legea nr. 71/2007.

31. Fiecare obiect informațional este identificat printr-un identificator unic de sistem (IUS), generat automat la momentul creării documentului. Identificatorul permite urmărirea ciclului de viață al obiectului informațional și asigură trasabilitatea și integritatea datelor în procesele de audit, arhivare și interoperabilitate. Structura și regulile de formare a identificatorilor sunt stabilite de Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) și SECBCM.

31.1. Pentru cererea de eliberare a certificatului (pct. 30.1), identificatorul include: prefix SI RBCM / tip obiect / an înregistrare / număr secvențial.

31.2. Pentru cererea de eliberare a adeverinței (pct. 30.2), identificatorul include: prefix SI RBCM / tip obiect / an înregistrare / număr secvențial.

31.3. Pentru raportul de expertiză (pct. 30.3), identificatorul include: prefix SI RBCM / tip obiect / an înregistrare / număr secvențial.

31.4. Pentru certificat și adeverință (pct. 30.4), identificatorul include: prefix SI RBCM / tip obiect / an emitere / număr secvențial.

31.5. Pentru notificarea privind circulația bunurilor culturale mobile (pct. 30.5), identificatorul include: prefix SI RBCM / tip obiect / an / număr secvențial.

31.6. Pentru înștiințările electronice generate automat (pct. 30.6), identificatorul include: prefix SI RBCM / tip obiect / referință la obiectul principal / marcaj temporal.

31.7. Pentru datele despre persoane fizice și juridice (pct. 30.7), identificatorul include referința la identificatorul oficial din registrul sursă, utilizat în cadrul schimbului de date.

31.8. Pentru evenimentele sistemice și jurnalele de acțiuni (pct. 30.8), identificatorul include: prefix SI RBCM / tip jurnal / marcaj temporal / număr secvențial.

32. Datele gestionate de SI RBCM se structurează în funcție de destinație și nivel de acces, fiind clasificate în:

32.1. date de identificare a bunurilor culturale mobile;

32.2. date privind expertizarea și clasificarea bunurilor;

32.3. date privind autorizarea, exportul, importul și circulația temporară;

32.4. date referitoare la titularii de drepturi și la autoritățile implicate;

32.5. date de interoperabilitate și jurnale de evenimente.

Toate datele sunt stocate și procesate în conformitate cu legislația privind protecția datelor cu caracter personal și cu standardele de securitate SM EN ISO/IEC 27001 și 27002.

33. În vederea asigurării consistenței, interoperabilității și compatibilității cu alte registre de stat, în SI RBCM se utilizează un sistem unificat de clasificatoare și nomenclatoare, elaborat în conformitate cu clasificatoarele naționale și internaționale, care sunt utilizate în forma lor oficială și reprezintă:

33.1. clasificatoare naționale – CUATM, CTP, CFOJ, CAEM-2, CCN;

33.2. clasificatoare de domeniu – tipuri de bunuri culturale mobile, categorii de circulație, statute juridice, tipuri de documente;

33.3. clasificatoare internaționale – codurile armonizate TARIC și standardele ICCD pentru obiecte de patrimoniu.

34. Clasificatoarele și nomenclatoarele specifice domeniului bunurilor culturale mobile se elaborează și se actualizează de către SECBCM, în baza competențelor sale legale de gestionare a evidenței și a registrului patrimoniului cultural mobil, cu avizul Ministerului Culturii și în coordonare cu STISC, în scopul asigurării interoperabilității și compatibilității cu alte registre de stat.

34.1. În scopul asigurării interoperabilității și a schimbului de date cu alte sisteme și resurse informaționale de stat, Serviciul de Evidență și Circulație a Bunurilor Culturale Mobile înregistrează activele semantice utilizate în Sistemul informațional „Catalogul semantic.

35. În scopul schimbului sigur, coerent și automatizat de date, SI RBCM interacționează, prin intermediul platformei de interoperabilitate MConnect, cu următoarele resurse și servicii guvernamentale comune:

35.1. Registrul de Stat al Populației (RSP) – pentru identificarea și validarea datelor despre persoanele fizice;

35.2. Registrul de Stat al Unităților de Drept (RSUD) – pentru verificarea datelor despre persoanele juridice participante;

35.3. Sistemul Informațional Integrat Vamal (SIIV) – pentru schimbul de date privind exportul, importul și reintroducerea bunurilor culturale mobile;

Capitolul VIII

SPAȚIUL TEHNOLOGIC AL SI RBCM

36. SI RBCM este proiectat ca un sistem modular, bazat pe componente integrate și compatibil cu tehnologiile de tip cloud computing. Arhitectura sistemului asigură dezvoltarea scalabilă, interoperabilitatea, securitatea informațională și implementarea modificărilor fără întreruperea funcționării registrului.

37. Dezvoltarea și modernizarea SI RBCM se realizează etapizat, în funcție de prioritățile stabilite de Ministerul Culturii (posesorul sistemului) și Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) (deținătorul infrastructural), cu respectarea cerințelor HG nr. 211/2019 privind platforma de interoperabilitate și HG 562/2025 privind securitatea cibernetică.

38. Arhitectura tehnologică a SI RBCM este organizată pe trei niveluri interdependente:

38.1. nivelul de prezentare – interfața utilizatorilor autorizați, care asigură accesul securizat și interacțiunea intuitivă cu funcționalitățile sistemului;

38.2. nivelul aplicațiilor – conține logica funcțională și mecanismele de procesare, validare și integrare a datelor;

38.3. nivelul de date – cuprinde bazele de date și resursele de stocare, administrate conform standardelor de securitate și integritate.

39. Platforma tehnologică a SI RBCM utilizează tehnologii moderne, bazate pe standarde deschise și non-proprietare, compatibile cu infrastructura guvernamentală comună și cu alte sisteme informaționale de stat. Dezvoltarea, operarea și mentenanța sistemului se efectuează în conformitate cu standardele SM EN ISO/IEC 27001, 27002 și 15408, precum și cu cerințele stabilite de STISC.

40. În procesul de dezvoltare și exploatare, SI RBCM respectă următoarele principii tehnologice:

40.1. modularitate și scalabilitate, pentru adaptarea ușoară la cerințele de extindere și integrare;

40.2. arhitectură orientată pe servicii (SOA), care permite reutilizarea componentelor și integrarea cu alte sisteme;

40.3. continuitatea operațională, asigurată prin mecanisme de redundanță, backup și restaurare;

40.4. protecția și confidențialitatea datelor, conform cadrului național de securitate cibernetică;

40.5. administrarea identității și a accesului, pe baza autentificării prin MPass și a unei matrice de drepturi configurate după roluri;

40.6. asigurarea jurnalizării complete, prin serviciul guvernamental MLog, pentru trasabilitatea acțiunilor utilizatorilor și a evenimentelor de sistem;

40.7. mentenanță și costuri optimizate, prin utilizarea infrastructurii guvernamentale comune și a resurselor partajate în MCloud.

41. Conformitatea tehnologică a SI RBCM este asigurată prin:

41.1. respectarea standardelor internaționale privind structura, calitatea și securitatea datelor (ISO/IEC 27001, 27002, 15408, 25010);

41.2. utilizarea protocoalelor și formatelor deschise de schimb de date (XML, JSON, SOAP, REST, HTTPS);

41.3. compatibilitatea cu cerințele de interoperabilitate definite prin HG nr. 211/2019;

41.4. suportul interfețelor web, accesibile securizat prin browser, conform politicilor STISC.

42. SI RBCM este găzduit pe platforma tehnologică guvernamentală comună (MCloud), în conformitate cu HG nr. 128/2014, utilizând infrastructura guvernamentală de tip cloud pentru alocarea rațională a resurselor și menținerea continuității serviciilor.

Sistemul utilizează și integrează următoarele servicii guvernamentale comune:

42.1. MConnect – pentru interoperabilitatea și schimbul securizat de date cu alte sisteme informaționale de stat;

42.2. MPass – pentru autentificarea și identificarea electronică a utilizatorilor;

42.3. MSign – pentru semnarea electronică a documentelor și a operațiunilor;

42.4. MNotify – pentru notificarea electronică a utilizatorilor;

42.5. MLog – pentru jurnalizarea evenimentelor și auditarea acțiunilor din sistem;

42.6. MPay – pentru procesarea și confirmarea plăților electronice aferente serviciilor oferite prin SI RBCM.

42.7. MDocs – pentru stocarea și partajarea documentelor din cadrul SI RBCM;

42.8. Portalul guvernamental integrat EVO – pentru afișarea datelor și accesul la serviciile aferente circulației bunurilor culturale mobile;

43. SI RBCM va fi implementat cu respectarea cerințelor aferente modelului unitar de design, în conformitate cu prevederile Hotărârii Guvernului nr. 677/2025.

43.1. Înainte de punerea în exploatare a SI RBCM, aspectele aferente designului se coordonează cu Instituția publică Agenția de Guvernare Electronică.

Capitolul IX

ASIGURAREA SECURITĂȚII INFORMAȚIONALE A SI RBCM

43. Securitatea informațională a SI RBCM are drept scop protecția datelor, proceselor și infrastructurii tehnologice împotriva acțiunilor accidentale sau intenționate, care pot afecta confidențialitatea, integritatea sau disponibilitatea informației. Securitatea este asigurată pe întreg ciclul de viață al datelor – de la colectare și procesare până la stocare, transmitere și arhivare.

44. Asigurarea securității informaționale a SI RBCM se realizează în conformitate cu:

44.1. 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;

44.2. standardele internaționale SM EN ISO/IEC 27001 și 27002 privind sistemele de management al securității informației;

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

44.4. Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere.

45. Posesorul (Ministerul Culturii), deținătorul (STISC) și administratorul SI RBCM și de sistem (SECBCM) elaborează și aplică politica internă de securitate informațională, care include:

45.1. evaluarea periodică a riscurilor și măsurile de reducere a acestora;

45.2. instruirea personalului privind securitatea cibernetică;

45.3. audituri tehnice periodice de conformitate;

45.4. proceduri de gestionare a incidentelor și notificare către autoritățile competente.

46. Principalele obiective de securitate ale SI RBCM sunt:

46.1. autentificarea – accesul la sistem este permis doar utilizatorilor autorizați, autentificați prin serviciul guvernamental MPass;

46.2. autorizarea – accesul la resursele sistemului se realizează conform rolurilor și nivelurilor de acces definite de SECBCM;

46.3. confidențialitatea – protejarea datelor împotriva accesului neautorizat;

46.4. integritatea – prevenirea modificării sau alterării neautorizate a informațiilor;

46.5. nonrepudierea – garantarea imposibilității negării acțiunilor efectuate în sistem;

46.6. disponibilitatea – asigurarea accesului continuu la serviciile și datele sistemului, inclusiv prin mecanisme de redundanță și restaurare.

47. Pentru atingerea obiectivelor de securitate, SI RBCM implementează următoarele mecanisme tehnice și organizatorice:

47.1. utilizarea semnăturii electronice calificate (MSign) pentru garantarea autenticității și integrității documentelor;

47.2. aplicarea măsurilor de protecție perimetrală și firewall, la nivel de infrastructură MCloud, conform politicilor STISC;

47.3. utilizarea soluțiilor de protecție antivirus și antimalware pe toate serverele și punctele de acces;

47.4. implementarea sistemelor de detectare și prevenire a intruziunilor (IDS/IPS);

47.5. asigurarea comunicației criptate (HTTPS, TLS) între componentele sistemului și utilizatori;

47.6. efectuarea backup-urilor periodice și a proceselor de restaurare;

47.7. monitorizarea și auditarea continuă a activităților prin serviciul guvernamental MLog.

48. Protecția datelor cu caracter personal este parte integrantă a securității informaționale a SI RBCM și se realizează prin:

48.1. prelucrarea doar a datelor strict necesare scopului legal al sistemului;

48.2. aplicarea măsurilor organizatorice și tehnice adecvate pentru prevenirea distrugerii, modificării, copierii, răspândirii sau accesului neautorizat la date;

48.3. înregistrarea și raportarea incidentelor de securitate către Centrul Național pentru Protecția Datelor cu Caracter Personal, conform legislației în vigoare;

48.4. asigurarea respectării drepturilor persoanelor vizate.

49. Toate activitățile efectuate în SI RBCM sunt înregistrate și auditate automat prin serviciul guvernamental MLog, pentru garantarea trasabilității și integrității datelor. Înregistrările de audit sunt păstrate conform politicilor interne

ale SECBCM și STISC, în concordanță cu cerințele HG 562/2025 și standardele ISO/IEC 27001.

49.1. Toate operațiunile de introducere, modificare sau radiere a datelor în SI RBCM sunt asociate în mod obligatoriu cu identitatea registratorului și sunt confirmate prin semnătura electronică calificată aplicată prin MSign, conform art. 26 alin. (6) din Legea nr. 71/2007.

50. Accesul la SI RBCM se realizează exclusiv prin serviciul MPass, iar rolurile și permisiunile utilizatorilor sunt gestionate de către SECBCM în baza matricei de drepturi configurate după roluri și atribuții. Autentificarea multiplă, semnarea electronică și jurnalizarea completă asigură nivelul necesar de protecție și control asupra acțiunilor efectuate în sistem.

51. Sistemul dispune de proceduri interne de backup, restaurare și continuitate operațională, administrate de STISC, pentru a garanta funcționarea neîntreruptă a serviciilor și recuperarea rapidă a datelor în caz de incident.

Capitolul X

ÎNCHEIERE

52. Prezentul Concept stabilește cadrul organizațional, funcțional și tehnologic în baza căruia va fi conceput, dezvoltat și implementat SI RBCM.

Acesta asigură suportul informatic necesar pentru SECBCM, Serviciul Vamal al Republicii Moldova și alte autorități competente, în vederea gestionării proceselor de evidență, expertizare, autorizare și circulație a bunurilor culturale mobile, în conformitate cu Legea nr. 280/2011 privind protejarea patrimoniului cultural național mobil și Hotărârea Guvernului nr. 470/2023.

REGULAMENTUL
resursei informaționale formate de
Sistemul informațional „Registrul circulației bunurilor culturale mobile”

Capitolul I
DISPOZIȚII GENERALE

1. Regulamentul resursei informaționale formate de Sistemul Informațional „Registrul circulației bunurilor culturale mobile” (în continuare – *Regulament*) are drept scop implementarea Conceptului Sistemului Informațional „Registrul circulației bunurilor culturale mobile”, a funcțiilor, a subiecților, a atribuțiilor, a interoperabilității și a modului de menținere a Sistemului Informațional „Registrul circulației bunurilor culturale mobile” (în continuare – *SI RBCM*). În sensul Legii nr. 71/2007 cu privire la registre, SI RBCM reprezintă registru de stat departamental.

2. SI RBCM este o resursă informațională de stat, care cuprinde date sistematizate referitoare la domeniul evidenței și circulației interne și externe a bunurilor culturale mobile, inclusiv date despre subiecții supuși monitorizării și autoritățile de monitorizare și supraveghere a domeniului, activitățile desfășurate și măsurile luate de către acestea, cererile, notificările, certificatele și adeverințele și deciziile de interdicere a punerii bunurilor culturale în liberă circulație. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută la pct.10 din anexa nr. 1 la prezenta hotărâre.

Capitolul II
SUBIECȚII RAPORTURILOR JURIDICE ÎN
DOMENIUL CREĂRII, ADMINISTRĂRII, MENTENANȚEI,
DEZVOLTĂRII ȘI UTILIZĂRII SI RBCM ȘI ATRIBUȚIILE ACESTORA

3. Subiecții raporturilor juridice din domeniul creării, administrării, mentenanței, dezvoltării și utilizării conținutului SI RBCM sunt:

- 3.1. proprietarul;
- 3.2. posesorul;
- 3.3. deținătorul;
- 3.4. administratorul;
- 3.5. registratorii;
- 3.6. furnizorii de date;
- 3.7. utilizatorii.

4. Proprietarul SI RBCM este statul, care își realizează dreptul de proprietate.

5. Posesorul SI RBCM este Ministerul Culturii, care asigură condițiile juridice, organizaționale, metodologice, financiare și tehnice pentru crearea, administrarea și dezvoltarea sistemului.

6. Deținătorul SI RBCM este Serviciul Tehnologia Informației și Securitate Cibernetică (STISC), care asigură găzduirea sistemului în infrastructura guvernamentală comună (MCloud), mentenanța tehnică la nivel de infrastructură, precum și măsurile de securitate cibernetică, arhivarea și realizarea copiilor de rezervă, în conformitate cu prevederile Hotărârii Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud) și Hotărârea Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetică de către furnizorii de servicii în sectoarele critice.

7. Administratorul SI RBCM este Serviciul de Evidență și Circulație a Bunurilor Culturale Mobile (în continuare SECBCM), autoritate administrativă subordonată Ministerului Culturii. SECBCM exercită atribuțiile de administrare tehnică și operațională a sistemului, asigurând:

7.1 administrarea bazelor de date, a fluxurilor informaționale și a componentelor funcționale;

7.2. gestionarea drepturilor de acces și atribuirea nivelurilor de acces utilizatorilor, prin intermediul serviciului guvernamental Mpass;

7.3. gestionarea și actualizarea tipurilor de documente utilizate în sistem;

7.4. monitorizarea activităților și auditarea evenimentelor prin MLog;

7.5. aplicarea măsurilor de securitate cibernetică, confidențialitate și integritate a datelor, conform SM EN ISO/IEC 27001–27002 și Hotărârii Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetică de către furnizorii de servicii în sectoarele critice;

7.6. coordonarea proceselor de interoperabilitate funcțională, semnătură electronică (MSign), notificare (MNotify) și plăți electronice (MPay) în cadrul infrastructurii MConnect și MCloud;

7.7. instruirea și suportul pentru utilizatorii autorizați.

8. Registratorii de date în cadrul SI RBCM sunt autoritățile competente în domeniul gestionării și circulației bunurilor culturale mobile, după cum urmează:

8.1. Ministerul Culturii – posesor al sistemului și autoritate responsabilă de elaborarea și implementarea politicilor de stat în domeniul protejării și circulației bunurilor culturale mobile;

8.2. Serviciul de Evidență și Circulație a Bunurilor Culturale Mobile – administrator și coordonator funcțional al SI RBCM;

8.3. Serviciul Vamal al Republicii Moldova – partener instituțional, responsabil de verificarea și monitorizarea operațiunilor de export și import ale bunurilor culturale mobile;

9. Furnizorii de date sunt persoanele fizice și juridice de drept public sau de drept privat care livrează date aferente obiectelor informaționale ale SI RBCM.

10. Utilizatorii datelor din SI RBCM sunt persoanele juridice și fizice de drept public sau privat care utilizează informațiile generate de sistem potrivit competențelor legale, în scopul exercitării atribuțiilor funcționale, al procesului decizional și al informării publice. Drepturile și obligațiile acestora se stabilesc de legislația privind accesul la informație și de legislația cu privire la schimbul de date și interoperabilitate.

11. Utilizatorul este responsabil de modul de accesare și de utilizare a datelor,

precum și de întreprinderea măsurilor pentru evitarea accesului neautorizat al persoanelor terțe la datele cu caracter personal.

12. Utilizatorul poate raporta posesorului problemele ce țin de accesarea informațiilor conținute în SI RBCM.

13. Destinatarii datelor SI RBCM sunt în drept să primească datele autorizate prin lege, prin platforma MConnect, conform art. 15 din Legea nr. 71/2007.

Capitolul III

ȚINEREA SI ASIGURAREA FUNCȚIONĂRII SI RBCM

14. Fiecărui obiect înregistrat în SI RBCM i se atribuie un identificator unic și invariabil, păstrat pentru întreaga durată de existență a obiectului în registru, conform art. 20 alin. (2) din Legea nr. 71/2007.

15. Orice modificare asupra unui obiect din registru se efectuează exclusiv în baza deciziei registratorului și se înregistrează în istoricul obiectului, fără posibilitatea ștergerii datelor anterioare, conform art. 20 alin. (4) din Legea nr. 71/2007.

16. Radierea unui obiect din SI RBCM se realizează prin înscrierea unei note speciale în registru, fără eliminarea fizică a datelor, conform art. 20 alin. (5) din Legea nr. 71/2007.

17. Ținerea și asigurarea funcționării SI RBCM se realizează prin responsabilitățile cumulative ale posesorului, deținătorului și administratorului tehnic, fiecare în limitele competențelor stabilite prin Conceptul SI RBCM, după cum urmează:

17.1. interacțiunea utilizatorilor cu SI RBCM se realizează prin intermediul unei interfețe web cu acces securizat, utilizând certificatele SSL (certificat de securitate), cu autentificare obligatorie prin serviciul electronic guvernamental de autentificare și control al accesului (MPass).

17.2 introducerea datelor în SI RBCM se efectuează în conformitate cu ghidurile de utilizare a sistemului.

18. SI RBCM asigură istoricul introducerii/modificărilor datelor în acesta; toate înregistrările și modificările operate în SI RBCM se păstrează în ordine cronologică.

19. Datele/informațiile/documentele introduse în SI RBCM sunt stocate și păstrate în arhiva SI RBCM în conformitate cu termenii de păstrare prevăzuți de cadrul normativ în conformitate cu prevederile STISC.

20. Vizualizarea datelor/informațiilor și documentelor stocate și păstrate în arhiva SI RBCM poate fi efectuată de către utilizatorii autorizați ai SI RBCM, în limitele rolului și nivelului de acces predefinit, stabilite prin serviciul guvernamental de autentificare și control al accesului (MPass).

21. Obiectele informaționale și identificadorii acestora din SI RBCM, componentele sistemului, funcționalitățile de bază, platformele și serviciile guvernamentale cu care acesta este integrat pentru schimbul de date, interoperabilitate și utilizarea serviciilor electronice se stabilesc în conformitate cu

Capitolul IV DREPTURILE ȘI OBLIGAȚIILE SUBIECȚILOR RAPORTURILOR JURIDICE SI RBCM

Secțiunea 1

Drepturile și obligațiile posesorului SI RBCM

22. Posesorul SI RBCM are următoarele drepturi:

18.1. să elaboreze și să perfecționeze, în limita competențelor sale, cadrul normativ privind funcționarea SI RBCM;

18.2. să propună soluții de eficientizare a proceselor operaționale ale SI RBCM;

18.3. să supravegheze respectarea cerințelor de securitate a informației de către participanții la SI RBCM și să documenteze cazurile sau tentativele de încălcare a acestora;

18.4. să solicite inițierea procedurii de suspendare a drepturilor de acces la SI RBCM pentru utilizatorii care nu respectă regulile, standardele și normele general acceptate în domeniul securității informaționale.

23. Posesorul are următoarele obligații:

19.1. să informeze participanții SI RBCM despre modificările condițiilor tehnice de funcționare a acestuia;

19.2. să utilizeze informația obținută din baza de date a SI RBCM doar în scopurile stabilite de cadrul normativ;

19.3. să stabilească condițiile juridice, financiare și organizatorice pentru administrarea și mentenanța SI RBCM.

Secțiunea a 2-a

Drepturile și obligațiile deținătorului SI RBCM

24. Deținătorul SI RBCM are dreptul să propună soluții pentru îmbunătățirea și eficientizarea funcționării sistemului.

25. Deținătorul SI RBCM are următoarele obligații:

a. să garanteze continuitatea operării infrastructurii;

b. să implementeze măsuri tehnice pentru protecția și confidențialitatea datelor, prevenind accesul, modificarea, blocarea sau diseminarea neautorizată a informațiilor;

c. să asigure aplicarea măsurilor necesare pentru protecția datelor cu caracter personal, în conformitate cu legislația;

d. să asigure accesul securizat la informațiile din SI RBCM și respectarea regulilor de exploatare;

e. să utilizeze datele din SI RBCM exclusiv în scopurile prevăzute de legislație.

Secțiunea a 3-a

Drepturile și obligațiile registratorului SI RBCM

- 26. Registratorul are următoarele drepturi:**
- 26.1 să vizualizeze informațiile din SI RBCM în funcție de rolul atribuit;
 - 26.2 să acceseze spațiul informațional al SI RBCM în limitele permisiunilor stabilite;
 - 26.3 să consulte informațiile introduse de el în sistem;
 - 26.4 să solicite asistență metodologică și tehnică din partea posesorului;
 - 26.5 să ceară informații despre disponibilitatea și funcționarea serviciilor SI RBCM, în limitele rolului și competențelor sale;
 - 26.6 să propună măsuri pentru îmbunătățirea funcționării SI RBCM.
- 27. Registratorul are următoarele obligații:**
- 27.1. să garanteze corectitudinea, autenticitatea și veridicitatea datelor introduse;
 - 27.2. să asigure actualizarea periodică a datelor;
 - 27.3. să corecteze erorile ca urmare a înregistrării greșite a datelor, precum și orice altă eroare constatată aferentă calității datelor;
 - 27.4. să prevină accesul neautorizat al terților;
 - 27.5. să utilizeze funcționalitățile SI RBCM exclusiv conform destinației lor, în conformitate cu legislația aplicabilă;
 - 27.6. să utilizeze informațiile din SI RBCM doar în scopurile permise de lege.

Secțiunea a 4-a

Drepturile și obligațiile furnizorului de date SI RBCM

- 28. Furnizorul de date SI RBCM are dreptul:**
- 24.1. să propună soluții pentru optimizarea funcționării SI RBCM;
 - 24.2. să solicite și să primească suport metodologic din partea posesorului SI RBCM și suport tehnic din partea administratorului tehnic al SI RBCM;
 - 24.3. să prezinte posesorului SI RBCM propuneri privind îmbunătățirea și eficientizarea funcționării acestuia.
- 29. Furnizorul de date SI RBCM este obligat:**
- 29.1. să asigure corectitudinea, autenticitatea și veridicitatea datelor, inclusiv a datelor cu caracter personal furnizate, autenticitatea transmiterii datelor și actualizarea permanentă în baza corectărilor prezentate conform reglementărilor;
 - 29.2. să furnizeze informația doar în scopurile stabilite de legislație;
 - 29.3. să întreprindă măsurile organizatorice și tehnice interne necesare pentru asigurarea protecției și a confidențialității datelor transmise către SI BCM.

Capitolul V

REGIMUL JURIDIC DE UTILIZARE A DATELOR SI RBCM

31. Utilizatorii beneficiază de drepturi de acces la informațiile din SI RBCM conform atribuțiilor și funcțiilor deținute și regimului juridic al informațiilor accesate. Nivelul de acces la informație pentru fiecare participant corespunde funcției de serviciu și profilului de acces. Accesarea informațiilor din SI RBCM se realizează în conformitate cu Legea nr. 148/2023 privind accesul la informațiile de

interes public și în limitele stabilite de aceasta, precum și în conformitate cu alte acte normative.

32. Datele recepționate din SI RBCM nu pot fi transmise persoanelor terțe, dacă legislația sau tratatele internaționale la care Republica Moldova este parte nu prevede acest lucru.

33. Accesul la SI RBCM este segmentat pentru utilizatori interni, care accesează datele SI RBCM prin interfața web a sistemului, și pentru utilizatori externi, care accesează datele prin intermediul platformei de interoperabilitate.

34. Utilizatori interni ai SI RBCM sunt posesorul, deținătorul, registratorul și alți utilizatori ale căror drepturi de acces sunt definite în acte normative.

35. Se interzice dezvăluirea datelor cu caracter personal extrase din SI RBCM în scopuri ce contravin legii.

36. Exploatarea SI RBCM fără autorizare nominală este strict interzisă și urmează a fi considerată ca acces neautorizat la un sistem informațional public.

37. Dreptul de acces la SI RBCM nu este unul permanent, acesta poate fi suspendat sau revocat. Introducerea și/sau modificarea datelor în SI RBCM prin utilizarea numelui sau a profilului unui utilizator străin este strict interzisă, urmând a fi considerată ca acces neautorizat. Utilizatorii urmează să se asigure de faptul că profilul de utilizator și semnătura electronică sunt confidențiale.

38. Revocarea/suspendarea dreptului de acces la SI RBCM se efectuează de către administratorul SI RBCM, în una dintre următoarele situații:

38.1. încetarea/suspendarea raporturilor de serviciu/de muncă ale utilizatorului;

38.2. modificarea raporturilor de serviciu/de muncă, atunci când noile atribuții nu impun accesul la datele din SI RBCM;

38.3. constatarea încălcării securității informaționale;

38.4. alte cazuri, conform prevederilor legale.

39. Lucrările profilactice planificate asupra componentelor software ale SI RBCM se efectuează de către administratorul SI RBCM, după notificarea în scris sau prin e-mail a utilizatorilor interni, cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului estimat de finalizare, dacă acest lucru este posibil. Lucrările profilactice neplanificate se efectuează de administratorul SI RBCM în situațiile în care complexul de mijloace software nu funcționează sau funcționează necorespunzător, cu informarea imediată a posesorului și a utilizatorilor afectați.

40. Punerea la dispoziție a datelor din SI RBCM către autoritățile publice se realizează exclusiv prin platforma de interoperabilitate MConnect, conform art. 29 alin. (1) lit. a) din Legea nr. 71/2007.

41. Documentele reproduse pe suport de hârtie din SI RBCM conțin obligatoriu un identificator electronic unic (cod QR) care permite verificarea autenticității acestora, conform art. 29 alin. (3¹) din Legea nr. 71/2007.

Capitolul VI

INTEROPERABILITATEA CU ALTE SISTEME INFORMAȚIONALE

42. Pentru asigurarea actualizării operative și automate a conținutului informațional al SI RBCM cu informații veridice, se poate efectua interacțiunea și sincronizarea datelor cu alte sisteme informaționale, importându-se automat sau exportându-se date, în vederea verificării și/sau completării conținutului informațional al SI RBCM.

43. SI RBCM se interconectează cu platformele și serviciile guvernamentale comune, în conformitate cu Legea nr. 142/2018 privind schimbul de date și interoperabilitate și Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect) partajate, conform pct. 24 din Anexa nr. 1.

44. Schimbul de date dintre subiecții SI RBCM se realizează prin mesaje standardizate — înștiințare de recepționare, înștiințare de acceptare, înștiințare de refuz — transmise prin MConnect, semnate electronic prin MSign și jurnalizate prin MLog.

Capitolul VII ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI SI RBCM

45. Asigurarea protecției și securității informației se realizează prin totalitatea măsurilor normative, organizatorice și economice, precum și prin mijloacele software hardware, care sunt orientate spre asigurarea unui nivel necesar al integrității, al confidențialității și al accesibilității resurselor informaționale ale SI RBCM.

46. Datele din SI RBCM fac parte din categoria datelor care necesită a fi protejate. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul SI RBCM se efectuează de către subiecții cu drepturi de acces la sistem și cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

47. Măsurile de protecție și securitate a informației cu caracter personal din SI RBCM se efectuează neîntrerupt de către toți subiecții acestuia.

48. Obiectele supuse măsurilor de protecție și securitate a datelor din SI RBCM includ tot complexul de mijloace software care asigură realizarea proceselor informaționale, și anume:

b

48.1. aza de date, sistemele informaționale, sistemele operaționale, sistemele de gestiune a bazelor de date, sistemele de evidență și alte aplicații care asigură funcționarea SI RBCM;

si

48.2. stemele de comunicații electronice, rețelele, serverele, calculatoarele și alte mijloace tehnice de prelucrare a datelor.

49. Securitatea informațională a SI RBCM se efectuează prin aplicarea metodelor și efectuarea acțiunilor prevăzute în Planul de continuitate al acestuia și, după caz, a procedurilor operaționale.

50. Protecția datelor din SI RBCM se efectuează prin următoarele metode:

50.1. evenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor; Pr

50.2. lizarea obligatorie a produselor de program licențiate și aprobate; uti

50.3. nitorizarea procesului de exploatare al SI RBCM prin intermediul mecanismului de jurnalizare efectuat de către deținătorul acestuia. mo

51. Subiecții, la utilizarea și exploatarea SI RBCM, asigură implementarea normelor de securitate, acestea urmând să conțină acte ce confirmă:

51.1. identitatea persoanei responsabile de implementarea normelor de securitate și împuternicirile acesteia;

51.2. implementarea principalelor măsuri tehnico-organizatorice necesare pentru asigurarea funcționării SI RBCM;

51.3. implementarea procedurilor interne ce exclud cazurile de modificare neautorizată a mijloacelor software și/sau a informațiilor din SI RBCM;

51.4. informarea și instruirea utilizatorilor interni privind modalitățile și mecanismele de asigurare a securității informaționale;

51.5. procedurile de control intern pentru verificarea respectării normelor de securitate informațională de către subiecții SI RBCM.

52. Schimbul informațional se efectuează cu utilizarea mijloacelor software exclusiv prin canale securizate, asigurând integritatea și securitatea datelor transmise.

53. Utilizatorii interni desemnează o persoană subordonată nemijlocit conducătorului instituției, responsabilă de implementarea și monitorizarea respectării normelor de securitate informațională.

54. Normele de securitate informațională se aduc la cunoștința fiecărui utilizator intern și se semnează de acesta. Fiecare utilizator intern este obligat să cunoască normele securității informaționale și procedurile pe care trebuie să le respecte în strictă concordanță cu politica de securitate.

55. Utilizatorii interni asigură instruirea angajaților privind metodele și procedeele de contracarare a pericolelor informaționale.

56. Toate operațiunile de introducere, modificare și radiere a datelor sunt asociate obligatoriu identității registratorului și sunt confirmate prin semnătura electronică calificată aplicată prin MSign, conform art. 25 alin. (6) din Legea nr. 71/2007.

Capitolul VIII

ASIGURAREA CONTROLULUI INTERN ȘI EXTERN AL SI RBCM

57. Ținerea SI RBCM este supusă controlului intern. Controlul intern privind organizarea și funcționarea SI RBCM se efectuează de către posesor.

58. Utilizatorii, în atribuțiile cărora intră ținerea SI RBCM, introducerea datelor, furnizarea informațiilor și asigurarea funcționării SI RBCM, poartă răspundere personală, în conformitate cu legislația, pentru completitudinea, autenticitatea, veridicitatea, integritatea informațiilor, precum și pentru păstrarea și

utilizarea acestora. Utilizatorii care încalcă prezentul Regulament poartă răspundere civilă, contravențională, disciplinară sau penală.

59. Toți subiecții SI RBCM, precum și solicitanții informațiilor ce conțin date cu caracter personal, poartă răspundere, conform legislației, pentru prelucrarea, divulgarea, transmiterea acestor informații din sistem persoanelor terțe, contrar prevederilor legale.

60. Controlul legalității operațiunilor de prelucrare a datelor cu caracter personal desfășurate în cadrul SI RBCM se efectuează de către Centrul Național pentru Protecția Datelor cu Caracter Personal.

61. Pentru asigurarea funcționalității eficiente și neîntrerupte a SI RBCM, schimbul informațional de date SI RBCM este asigurat în regim nonstop. În cazul apariției circumstanțelor de forță majoră și a dificultăților tehnice în funcționarea complexului de mijloace software al SI RBCM din vina terțelor persoane, funcționarea sistemului poate fi sistată, cu informarea subiecților SI RBCM.

62. Păstrarea SI RBCM este asigurată de posesor până la adoptarea deciziei de scoatere din exploatare a acestuia. În cazul scoaterii din exploatare, datele și documentele conținute în acesta se transmit în arhivă conform legislației.

