**pentru aprobarea Regulamentului resursei informaționale formată de Subsistemului informațional ,,Platforma de Analiză și Generare Rapoarte”**

În temeiulart.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 aprobă Regulamentul resursei informaționale formate de Subsistemului informațional ,,Platforma de Analiză și Generare Rapoarte ” *(se anexează)*.
2. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Infrastructurii și Dezvoltării Regionale.
3. Prezenta hotărâre intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

**Prim-ministru DORIN RECEAN**

Contrasemnează:

Viceprim-ministru,

ministrul dezvoltării

economice și digitalizării Dumitru ALAIBA

Ministrul infrastructurii

și dezvoltării regionale Andrei SPÎNU

Aprobat

prin Hotărârea Guvernului

nr.\_\_\_\_\_\_/2023

**REGULAMENT**

**resursei informaționale formate de Subsistemului informațional ,,Platforma de Analiză și Generare Rapoarte ”**

**Capitolul I**

**DISPOZIŢII GENERALE**

1. Regulamentul resursei informaționale formate de Subsistemului informațional ,,Platforma de Analiză și Generare Rapoarte ” *(în continuare – Regulament)* este elaborat în vederea reglementării modului de organizare și implementare a subsistemului informațional din cadrul Sistemului de management integrat în domeniul transportului rutier destinat generării de rapoarte, statistici, indicatori de performanță necesare proceselor de monitorizare și luare a deciziilor, utilizat de către Agenția Națională de Transport Auto (în continuare – ANTA) și angajaților autorităților publice, *(în continuare - Destinatari)*.
2. Obiectivele resursei informaționale a Subsistemului informațional Platforma de Analiză și Generare Rapoarte *(în continuare – RI SI PAGR* ) sunt:
3. implementarea unui mecanism care permite generarea de rapoarte destinate activității ANTA;
4. automatizarea proceselor de schimb de informații cu alte sisteme informaționale statale;
5. sporirea eficienței activității ANTA.
6. În sensul prezentului Regulament, noțiunile de mai jos au următoarele semnificații:
7. **Participanți la RI SI PAGR** – posesorul și deținătorul sistemului, destinatarii, administratorul tehnic și administratorul de sistem;
8. **Posesor și deținător al resursei informaționale a Subsistemului informațional PAGR** – ANTA care este împuternicit să asigure funcționarea și dezvoltarea SI PAGR;
9. **Administrator tehnic al RI SI ,,PAGR”** *(în continuare – operator)* – este Instituția publică „Serviciului Tehnologia Informației și Securitate Cibernetică” care își exercită atribuțiile în conformitate cu cadrul normativ privind administrarea tehnică a sistemelor și resurselor informaționale de stat;
10. **Administrator de sistem al RI SI PAGR** – este una sau mai multe persoane desemnate de ANTA. Administrarea totală a conținutului SI ,,PAGR”este efectuată de specialiștii din cadrul ANTA;
11. **Furnizor de date -** persoana fizică sau juridică, de drept public sau privat, care funcționează în conformitate cu legislația Republicii Moldova ce furnizează datele necesare pentru generarea rapoartelor;
12. **Destinatarii datelor RI SI PAGR** *(în continuare – Destinatar)* **–** persoane fizice sau juridice, de drept public sau privat, care activează în conformitate cu legislația Republicii Moldova și care beneficiază de funcționalitățile oferite de către RI SI ,,PAGR” în scopul executării sarcinilor de serviciu;
13. **e-Bilet -** Subsistemul informațional e-Bilet - posesorul, deținătorul căruia este ANTA;
14. **e-GPS -** Subsistemul informațional e-GPS - posesorul, deținătorul căruia este ANTA.

**Capitolul II**

**CADRUL LEGAL**

1. Cadrul normativ în care se înscrie procesul de implementare și operare a RI SI PAGR este compus din legislația națională, tratatele și convențiile internaționale, după cum urmează:
2. Codul Transporturilor Rutiere nr.150/2014;
3. Codul administrativ al Republicii Moldova nr.116/2018;
4. Legea nr. 133/2011 privind protecția datelor cu caracter personal;
5. Legea nr. 148/2023 privind accesul la informațiile de interes public
6. Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;
7. Hotărârea Guvernului nr.854/2006 cu privire la Regulamentul transporturilor auto de călători și bagaje;
8. Hotărârea Guvernului nr. 1141/2017 pentru aprobarea Regulamentului privind modalitatea de aplicare a semnăturii electronice pe documentele electronice de către funcționarii persoanelor juridice de drept public în cadrul circulației electronice ale acestora;
9. Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;
10. Standardul Republicii Moldova SMV ISO CEI 15288:2009 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului;
11. Reglementarea tehnică „Procesele ciclului de viață al software-lui” RT 38370656-002:2006;
12. Alte legi și acte normative relevante domeniului.

**Capitolul III**

**FUNCȚIILE SUBSISTEMULUI INFORMAȚIONAL**

1. RI SI PAGR oferă mecanism care permite generarea rapoartelor de analiză necesare în activitatea ANTA.
2. RI SI PAGR oferă mecanism ce permite configurarea sau modificarea tipurilor de rapoarte noi sau existente.
3. Funcțiile principale ale RI SI PAGR sunt:
4. preluarea, transformarea și încărcarea datelor din diferite surse de date în repozitoriul PAGR;
5. efectuarea analizelor operaționale și generării totalității rapoartelor și documentelor destinate activității ANTA;
6. configurarea documentelor și rapoartelor generate;
7. realizarea, prin intermediul platformei de interoperabilitate (MConnect), a schimbului de date cu alte sisteme și resurse informaționale de stat în scopul recepționării datelor necesare generării rapoartelor;
8. generarea rapoartelor statistice și analitice pentru prezentarea către autoritățile administrației publice centrale și locale, persoanelor fizice și juridice, în conformitate cu prevederile legislației.

**Capitolul IV**

**ATRIBUȚIILE PARTICIPANȚILOR**

**Secțiunea** **1**. **Atribuțiile posesorului/deținătorului**

1. Posesorul RI SI PAGR are următoarele atribuții:
2. definește strategia de dezvoltare a RI SI PAGR;
3. definește și promovează cadrul normativ ce ține de funcționarea RI SI PAGR;
4. aprobă prioritățile și planurile de dezvoltare RI SI PAGR;
5. monitorizează utilizarea și dezvoltarea RI SI PAGR;
6. asigură administrarea, funcționarea, securitatea și protecția datelor din RI SI PAGR;
7. stabilește prioritățile de dezvoltare a RI SI PAGR, inclusiv asigură implementarea componentelor noi, precum și extinderea capacității acestuia;
8. elaborează, aprobă și revizuiește:
9. procedurile necesare utilizării și administrării RI SI PAGR;
10. procedurile de evaluare a eficienței utilizării și administrării RI SI PAGR;
11. procedurile de gestionare a riscurilor operaționale și securitate a informației;
12. procedurile de asigurare a securității RI SI PAGR;
13. procedurile de măsurare a volumului și calității serviciilor prestate de către RI SI PAGR.
14. definește parametrii și indicatorii de performanță ai RI SI PAGR;
15. desemnează administratorul de sistem al RI SI PAGR;
16. asigură monitorizarea și controlul utilizării RI SI PAGR;
17. va aproba lista tipurilor de rapoarte predefinite în RI SI PAGR;
18. asigură ținerea auditului operațiunilor de prelucrare a datelor cu caracter personal în RI SI PAGR, în funcție de criterii și indicatori specifici.

## Secțiunea 2-a. Atribuțiile administratorului tehnic

1. Operatorul RI SI PAGR are următoarele atribuții:
2. monitorizează utilizarea resurselor de către RI SI PAGR și asigură necesitățile de resurse pentru funcționarea eficientă a subsistemului respectiv;
3. administrează componentele tehnologice a RI SI PAGR la parametrii de calitate stabiliți;
4. implementează cele mai bune practici și standarde naționale și internaționale în vederea administrării eficiente a componentelor tehnologice a RI SI PAGR, inclusiv asigurării securității acestuia;
5. asigură continuitatea funcționării platformei tehnologice a RI SI PAGR în situații de dezastru;
6. înregistrează și soluționează, în limitele competenței, toate reclamațiile și sesizările primite de la posesor și destinatarii ai RI SI PAGR ;
7. colaborează cu posesorul în vederea optimizării parametrilor de calitate componentele tehnologice a RI SI PAGR, precum și pentru soluționarea eficientă a eventualelor incidente;
8. ia toate măsurile necesare pentru prevenirea și remedierea operativă a defecțiunilor apărute în infrastructura aferentă RI SI PAGR, precum și pentru înlăturarea consecințelor și pagubelor rezultate;
9. acordă, la solicitarea posesorului, asistență în ceea ce privește organizarea utilizării eficiente a RI SI PAGR de către beneficiari;
10. monitorizează respectarea indicatorilor de performanță ai utilizării și administrării RI SI PAGR și întreprinde măsuri de îmbunătățire a acestora.

**Secțiunea 3-a. Atribuţiile administratorului de sistem**

1. Administratorul de sistem al RI SI PAGR are următoarele atribuții:
2. are acces nelimitat la toate funcționalitățile RI SI PAGR în vederea gestionării depline a acestuia conform procedurilor de administrare a subsistemului respectiv;
3. administrează *(adaugă, modifică, șterge)* conturile utilizatorilor în RI SI PAGR;
4. administrează *(adaugă, modifică, șterge)* entitățile organizaționale în RI SI PAGR;
5. configurează lista de rapoarte în cadrul RI SI PAGR;
6. acordă suport la conectarea RI SI PAGR la sistemele furnizorilor de date.

**Secțiunea 4-a. Atribuțiile destinatarilor**

1. Destinatarii RI SI PAGR au următoarele atribuții:
2. asigură autenticitatea și veridicitatea datelor transmise pentru crearea conturilor în RI SI PAGR;
3. asigură confidențialitatea oricăror informații de autentificare asociate în cadrul RI SI PAGR;
4. utilizează funcționalitățile RI SI PAGR în exclusivitate conform destinației acestora și în strictă conformitate cu legislația;
5. anunță posesorul/administratorul de sistem a RI SI PAGR despre orice eveniment observat care poate compromite buna funcționare a subsistemului respectiv.

**Secțiunea 5-a. Atribuțiile furnizorilor de date**

1. Furnizorii de date au următoarele atribuții:
2. implementează măsuri organizatorice și tehnice necesare pentru furnizarea datelor din sistemele informaționale pe care le deține;
3. asigură disponibilitatea datelor din sistemele informaționale pe care le deține și furnizarea acestora în RI SI PAGR în conformitate cu legislația;
4. asigură veridicitatea, autenticitatea și integritatea datelor furnizate;
5. asigură actualizarea datelor furnizate în modul stabilit de legislație;
6. în cazul modificării formei sau modului de furnizare a datelor informează autoritatea competentă, care, la rândul său, informează consumatorul de date în modul stabilit;
7. prezintă în conformitate cu cerințele din actele normative aplicabile în domeniul autorității competente informația necesară pentru înlăturarea erorilor și vulnerabilităților, precum și pentru soluționarea incidentelor de securitate;
8. implementează măsurile necesare pentru asigurarea securității și protecției datelor, inclusiv a celor cu caracter personal în sistemele sale informaționale integrate cu PAGR.

**Capitolul V**

**DREPTURILE ȘI OBLIGAȚIILE SUBIECȚILOR**

1. Posesorul și deținătorul au următoarele drepturi:
2. dreptul de folosință;
3. dreptul să desemneze administratorul de sistem al RI SI PAGR;
4. dreptul să elaboreze și/sau să aprobe, conform competenței, cadrul normativ cu privire la RI SI PAGR;
5. dreptul să supravegheze respectarea cerințelor de securitate a informației de către furnizorii de date, să fixeze cazurile și tentativele de încălcare a acestora;
6. dreptul să inițieze procedura de suspendare a drepturilor de acces la RI SI PAGR pentru furnizorii de date și destinatari care nu respectă regulile, standardele și normele general acceptate în domeniul securității informaționale;
7. dreptul să verifice autenticitatea și veridicitatea datelor transmise de furnizori de date;
8. dreptul să solicite de la furnizori de date actualizarea sau corectarea datelor în RI SI PAGR în caz de depistare a omisiunilor și erorilor;
9. dreptul să vizualizeze informațiile din RI SI PAGR;
10. dreptul să acceseze spațiul informațional al RI SI PAGR;
11. dreptul să acceseze informațiile care se conțin în RI SI PAGR și care au fost prezentate de către acesta;
12. dreptul să propună soluții pentru perfecționarea și eficientizarea procesului de funcționare a RI SI PAGR, precum și să le pună în aplicare după aprobarea acestora.
13. Posesorul și deținătorul au următoarele obligații:
14. obligația să asigure funcționarea și dezvoltare, monitorizarea și controlul Subsistemului informațional;
15. obligația să asigure condițiile juridice, organizatorice și financiare pentru crearea și ținerea Subsistemului informațional;
16. obligația să asigure autenticitatea, plenitudinea și integrarea datelor din sistemul informațional, securitatea și protecția datelor din Subsistemul informațional;
17. să asigure atribuirea rolurilor și drepturilor de acces la interfețele RI SI PAGR și datele acestuia.
18. Destinatarii RI SI PAGR au următoarele drepturi:
19. dreptul la acces;
20. dreptul la activare;
21. dreptul la suspendare.
22. Destinatarii RI SI PAGR au următoarele obligații:

1) obligația de a utiliza RI SI PAGR numai în scopuri ce rezultă din necesitățile sale de activitate;

2) obligația să asigure autenticitatea și veridicitatea datelor transmise.

1. Administratorul tehnic are următoarele drepturi:
2. dreptul să monitorizeze utilizarea resurselor de către Subsistemul informațional;
3. dreptul să administreze componentele tehnologice.
4. Administratorul tehnic are următoarele obligații:
5. obligația de a funcționa în conformitate cu legislația Republicii Moldova;
6. obligația de a asigura un nivel de securitate și confidențialitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor.
7. Administratorul de sistem are următoarele drepturi:
8. dreptul la acces nelimitat la toate funcționalitățile Subsistemului informațional;
9. dreptul să administreze (adaugă, modifică, șterge) conturile utilizatorilor, entităților organizaționale.
10. Administratorul de sistem al RI SI PAGR are obligația de a asigura un nivel de securitate și confidențialitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor.
11. Furnizorii de date au următoarele drepturi:
12. dreptul să implementeze măsuri organizatorice și tehnice necesare pentru furnizarea datelor din sistemele informaționale pe care le deține;
13. dreptul să primească de la posesorul Subsistemului informațional toate datele despre obiect care se conțin în sistem în limitele și conform rolului atribuit.
14. Furnizorii de date au următoarele obligații:

1) obligația de a asigura disponibilitatea datelor din sistemele informaționale pe care le dețin;

2) obligația de a furniza datele;

1. obligația de a asigura veridicitatea, autenticitatea și integritatea datelor furnizate și actualizarea acestora în modul stabilit de lege sau acord.

**Capitolul VI**

**SOLICITAREA, UTILIZAREA ȘI SUSPENDAREA ACCESULUI LA**

**RI SI PAGR**

**Secțiunea 1. Solicitarea accesului la RI SI PAGR**

1. Solicitarea accesului de către destinatarii datelor se efectuează în baza cererii adresate posesorului.
2. Cererea este examinată de către posesorul RI SI PAGR în termen de 15 zile lucrătoare de la data recepționării cererii.
3. Ca rezultat al acceptării cererii, posesorul va asigura crearea conturilor de acces, precum și configurarea accesului la funcționalitățile necesare.
4. Autentificarea utilizatorilor în cadrul RI SI PAGR se realizează prin intermediul serviciului guvernamental de autentificare și control al accesului (MPass).
5. În cazul situațiilor excepționale *(indisponibilitatea serviciilor MPass)*, deținătorul RI SI PAGR poate crea și credențiale de autorizare și autentificare în sistem pentru registratori cu identitatea verificată prin serviciul electronic guvernamental de autentificare și control al accesului, dar care se utilizează doar pe perioada situației de urgență.
6. Posesorul pune la dispoziția beneficiarului adresa de acces la RI SI PAGR, precum și credențialele de autorizare și autentificare.

 **Secțiunea 2-a. Utilizarea RI SI PAGR**

1. Utilizarea funcționalităților RI SI PAGR se efectuează numai în scopuri ce rezultă din necesitățile de activitate ale beneficiarului.
2. Funcționalitățile RI SI PAGR nu se utilizează:
3. în scopuri ce contravin legislației;
4. în scopuri ce pot periclita imaginea participanților în cadrul RI SI PAGR;
5. pentru crearea, stocarea sau transmiterea informației ofensatoare, defăimătoare sau discriminatorii.

**Secțiunea 3-a. Suspendarea accesului la RI SI PAGR**

1. Accesul la RI SI PAGR poate fi suspendat temporar sau definitiv la inițiativa destinatarului, printr-o cerere adresată posesorului.
2. Accesul la RI SI PAGR poate fi suspendat de către posesor fără consimțământul destinatarului, cu notificarea ulterioară a acestuia în situații de forță majoră. În acest caz accesul se suspendă doar pentru a remedia situația creată și a repune în funcțiune RI SI PAGR, asigurându-se și reacordarea accesului la subsistem a destinatarului.
3. Accesul la RI SI PAGR poate fi suspendat de către posesor fără consimțământul beneficiarului, cu notificarea ulterioară a acestuia în baza deciziei instanței de judecata, în baza unui act administrativ emis de posesor și alte cazuri prevăzute de legislație.

**Capitolul VII**

**CONECTARE CU SISTEMELE INFORMAȚIONALE TERȚE**

1. RI SI PAGR se conectează la sisteme informaționale ale furnizorilor de date în vederea încărcării datelor necesare pentru generarea rapoartelor specifice.
2. Conectarea dintre sistemele informaționale ale furnizorului de date și RI SI PAGR se realizează fie direct, prin API-rile expuse de către sistemului informațional ce furnizează date către resursa infromațională a Subsistemul informațional PAGR, fie prin intermediul platformei de interoperabilitate *(MConnect)* în conformitate cu cadrul normativ care reglementează domeniul interoperabilității și schimbului de date.
3. Conectarea prin metoda directă se efectuează în cazul utilizării datelor din sistemele informaționale gestionate de către ANTA.
4. Conectarea prin platforma de interoperabilitate *(MConnect)* se efectuează în cazul utilizării datelor din sistemele informaționale gestionate de către alte autorități publice.
5. Regulile și procedurile de conectare sunt definite de către autoritatea publică care gestionează sistemul informațional la care se conectează RI SI PAGR.

**Capitolul VIII**

**SECURITATEA INFORMAȚIEI ȘI PRELUCRAREA DATELOR CU CARACTER PERSONAL**

1. Nivelul central al RI SI PAGR este găzduit pe platforma tehnologică guvernamentală comună *(MCloud)* și se conformează cerințelor de securitate a platformei respective.
2. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul RI SI PAGR se efectuează de către subiecții cu drepturi de acces la sistem, cu respectarea strictă a cerințelor față de asigurarea securității informației și a prevederilor legislației din domeniul protecției datelor cu caracter personal.
3. Obiecte ale asigurării protecției și securității informației din cadrul RI SI PAGR se consideră tot complexul de mijloace software și hardware care asigură realizarea proceselor informaționale:
4. baza de date, sistemele informaționale, sistemele operaționale, sistemele de gestiune a bazelor de date și alte aplicații care asigură funcționarea RI SI PAGR;
5. sistemele de telecomunicații, rețelele, serverele, calculatoarele și alte mijloace tehnice de prelucrare a informației.
6. Protecția informației în cadrul RI SI PAGR se asigură prin următoarele metode:
7. asigurarea măsurilor de protecție a datelor, prin folosirea metodelor criptografice de transmitere a informației prin rețelele de transport de date guvernamentale;
8. excluderea accesului neautorizat la datele din cadrul RI SI PAGR, prin utilizarea funcționalităților de autentificare ale serviciului guvernamental de autentificare și control al accesului *(MPass)*;
9. prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor;
10. efectuarea periodică planificată a copiilor de rezervă ale datelor și fișierelor mijloacelor de program;
11. utilizarea obligatorie a produselor de program licențiate aprobate;
12. monitorizarea procesului de exploatare a RI SI PAGR prin intermediul mecanismului de jurnalizare;
13. prevenirea acțiunilor speciale tehnice și de program care duc la distrugerea, denaturarea datelor sau care cauzează defecțiuni în funcționarea complexului tehnic și de program;
14. efectuarea tuturor măsurilor aferente asigurării restabilirii și continuității funcționării RI SI PAGR în cazul incidentelor.
15. Schimbul informațional se efectuează cu utilizarea mijloacelor software și hardware, doar prin canale securizate, asigurând integritatea și securitatea datelor.
16. Subiecții RI SI PAGR elaborează și implementează politica de securitate informațională pentru asigurarea respectării regulilor, standardelor și normelor general acceptate în domeniul securității informaționale, incluzând:
17. identitatea persoanei responsabile de politica de securitate;
18. principalele măsuri tehnico-organizatorice necesare asigurării funcționării

 resursei informaționale a Subsistemului informațional PAGR;

1. procedurile interne ce exclud cazurile de modificare nesancționată a mijloacelor software și/sau a informației în cadrul RI SI PAGR;
2. responsabilitățile personalului subiectului RI SI PAGR privind asigurarea securității informaționale;
3. procedurile de control intern al subiectului RI SI PAGR privind respectarea condițiilor de securitate informațională.
4. Fiecare subiect al RI SI PAGR asigură informarea și instruirea utilizatorilor privind metodele și procedeele de contracarare a pericolelor informaționale.
5. Prelucrarea datelor cu caracter personal se efectuează în conformitate cu cadrul normativ privind protecția datelor cu caracter personal.
6. În cadrul RI SI PAGR vor fi prelucrate datele cu caracter personal strict necesare, neexcesive scopului prestabilit de acesta, asigurând-se un nivel de securitate și confidențialitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor.
7. Termenul de păstrare a datelor cu caracter personal în cadrul RI SI PAGR constituie 5 ani de la data finalizării tranzacției. După expirarea termenului, datele cu caracter personal vor fi depersonalizate și stocate exclusiv în scopuri statistice, de cercetare istorică.