

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII al REPUBLICII MOLDOVA

INSTITUȚIA PUBLICĂ COLEGIUL „ALEXEI MATEEVICI” DIN CHIȘINĂU



Aprobat:
**Directorul Colegiului
„Alexei Mateevici” din Chișinău
Victoria BERCU**

REGULAMENT PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

*Discutat și aprobat:
la Consiliul de administrație
din 03.02.2026
proces verbal nr. 6*

Chișinău, 2026

CONȚINUT:

I. PREAMBUL	3
II. DEFINIȚII	4
III. SCOPUL ȘI DOMENIUL DE APLICABILITATE	7
IV. DISPOZIȚII PRIVIND IERARHIA ȘI RESPONSABILITATEA PERSOANEI RESPONSABILE DE POLITICA DE SECURITATE	8
V. MIJLOACELE SUPUSE PRINCIPIILOR DE PROTECȚIE A DATELOR CU CARACTER PERSONAL	9
VI. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL:	9
VII. METODELE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMELE INFORMAȚIONALE	9
VIII. PROCEDURILE ORGANIZATORICE ȘI TEHNICE CARE URMEAZĂ A FI RESPECTATE ÎN CADRUL COLEGIULUI LA PRELUCRAREA DATELOR CU CARACTER PERSONAL	10
8.1. <i>Măsurile generale de administrare a securității informaționale</i>	10
8.2. <i>Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal</i>	11
8.3. <i>Identificarea și autentificarea utilizatorilor</i>	11
8.4. <i>Identificarea și autentificarea echipamentului</i>	12
8.5. <i>Administrarea identificatorilor utilizatorilor</i>	12
8.6. <i>Utilizarea parolelor în procesul asigurării securității informaționale</i>	12
8.7. <i>Controlul administrării accesului</i>	12
8.8. <i>Accesul de la distanță</i>	12
8.9. <i>Limitarea folosirii tehnologiilor fără fir</i>	13
8.10. <i>Securitatea electroenergetică</i>	13
8.11. <i>Controlul instalării și scoaterii componentelor T.I.</i>	13
8.12. <i>Dezvăluirea datelor cu caracter personal</i>	13
8.13. <i>Drepturile subiecților de date cu caracter personal</i>	15
8.14. <i>Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate</i>	16
8.15. <i>Auditul sistemelor informaționale gestionate</i>	16
8.16. <i>Asigurarea protecției contra programelor dăunătoare (virusilor)</i>	17
8.17. <i>Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de date cu caracter personal</i>	17
8.18. <i>Gestionarea incidentelor de securitate</i>	17
8.19. <i>Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum și a informațiilor cu accesibilitate limitată</i>	18
IX. DISPOZIȚII FINALE	18

I. PREAMBUL

La prelucrarea datelor cu caracter personal în cadrul Colegiului "Alexei Mateevici" din Chișinău, cu sediul înregistrat în mun. Chișinău str. Alexandr Pușkin 54 (în continuare „**Colegiul**”) sunt aplicate principiile prevăzute de următoarele acte normative naționale și internaționale:

- 1) Declarația Universală a drepturilor omului din 10 decembrie 1948;
- 2) Convenția cu privire la drepturile copilului din 29 noiembrie 1989;
- 3) Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal nr. 208 din 28 ianuarie 1981;
- 4) Constituția Republicii Moldova din 29 iulie 1994;
- 5) Codul Educației al Republicii Moldova nr. 152 din 17.07.2014;
- 6) Codul Muncii al Republicii Moldova nr. 154 din 28.03.2003;
- 7) Codul de etică al cadrului didactic aprobat prin Ordinul Ministerului Educației al Republicii Moldova nr. 861 din 07.09.2015;
- 8) Codul Contravențional al Republicii Moldova nr. 218 din 24.10.2008;
- 9) Codul Penal al Republicii Moldova nr. 985 din 18.04.2002;
- 10) Legea privind protecția datelor cu caracter personal nr. 133 din 08.07.2011 ;
- 11) Legea privind accesul la informațiile de interes public nr. 148 din 09.06.2023;
- 12) Legea privind transparența în procesul decizional nr. 239-XVI din 13.11.2008;
- 13) Regulamentul privind modul de ținere a Registrului de stat format de Sistemul informațional de management în educație, aprobat prin Hotărârea Guvernului nr. 320 din 30.04.2024;
- 14) Ordinul Centrului Național pentru Protecția Datelor cu Caracter Personal cu privire la aprobarea Instrucțiunilor privind prelucrarea datelor cu caracter personal în sectorul educațional nr. 3 din 21 ianuarie 2015;
- 15) Decizia Centrului Național pentru Protecția Datelor cu Caracter Personal nr. 581 din 10.09.2015 cu privire la aprobarea formularului tipizat de informare privind efectuarea supravegherii prin mijloace video;
- 16) Statutul Colegiului „Alexei Mateevici” din Chișinău aprobat de către Consiliul profesoral din 13.03.2019 (în continuare „**Statutul**”), înregistrat prin decizia I.P. „Agenția Servicii Publice” nr. 127 din 16.05.2019;
- 17) Regulamentul intern de organizare și funcționare a colegiului „Alexei Mateevici” din Chișinău, aprobat de către Consiliul de administrație din 22.01.2025 (în continuare „**Regulamentul intern**”).

Prezentul Regulament privind prelucrarea datelor cu caracter personal (în continuare „**Regulament**”) este aprobat de către Consiliul profesoral al Colegiului „Alexei Mateevici” din Chișinău, după examinarea acestuia în Consiliul de administrație, și se pune în aplicare prin ordinul Directorului Colegiului, care coordonează implementarea și monitorizează respectarea Regulamentului, în baza Statutului și Regulamentului intern.

II. DEFINIȚII

În prezentul Regulament, sunt definite și utilizate următoarele noțiuni:

1.	„autentificare”	verificarea identicatorului atribuit subiectului de acces, confirmarea autenticității;
2.	„categorii speciale de date cu caracter personal”	datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale;
3.	„consimțământul”	subiectului datelor cu caracter personal / persoanei vizate – orice manifestare de voință liberă, expresă și necondiționată, în formă scrisă sau electronică, conform cerințelor documentului electronic, prin care subiectul datelor cu caracter personal acceptă să fie prelucrate datele care îl privesc;
4.	„control de securitate”	acțiuni întreprinse de către Colegiu, în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute;
5.	„date cu caracter personal”	orice informație referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale;
6.	„depersonalizarea datelor”	modificarea datelor cu caracter personal astfel încât detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condițiile unei investigații care necesită cheltuieli disproporționate de timp, mijloace și forță de muncă;
7.	„fișiere temporare”	ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat până la inițierea îndeplinirii sarcinilor pentru care au fost desemnate;
8.	„identificare”	atribuirea unui identicator subiecților și obiectelor de acces și/sau compararea identicatorului prezentat cu lista identificatoarelor atribuite;
9.	„integritate”	certitudinea, necontradictorialitatea și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;

Regulament privind prelucrarea datelor cu caracter personal

10.	„mijloace de protecție criptografică a informației care conține date cu caracter personal”	de mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acestora prin canalele de comunicații;
11.	„nivel de protecție”	nivel de securitate proporțional riscului pe care îl comportă prelucrarea față de datele cu caracter personal respective, precum și față de drepturile și libertățile persoanelor, elaborat și actualizat corespunzător nivelului dezvoltării tehnologice și costurilor implementării acestor măsuri;
12.	„operator”	persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare;
13.	„perimetru de securitate”	de zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic și/sau tehnic al accesului;
14.	„persoană împuternicită către operator”	de persoană împuternicită de către operator – persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator;
15.	„persoana responsabilă de politica de securitate a datelor cu caracter personal”	de persoana responsabilă de funcționarea corespunzătoare a sistemului complex de protecție a informației care conține date cu caracter personal, precum și de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a deținătorului de date cu caracter personal;
16.	„politica de securitate a datelor cu caracter personal”	de document, elaborat de către operatorul de date, care oferă o descriere precisă a măsurilor de securitate și trăsăturilor de protecție selectate pentru securitatea datelor, ținându-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și riscurile reale la care sunt expuse acestea;
17.	„prelucrarea datelor cu caracter personal”	orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvoltarea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

Regulament privind prelucrarea datelor cu caracter personal

18.	„protecția informației contra acțiunilor neintenționate”	ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informației care conține date cu caracter personal;
19.	„purător de date cu caracter personal”	suport magnetic, optic, laser, de hârtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia;
20.	„restaurarea datelor”	procedurile cu privire la reconstituirea/prestabilirea datelor cu caracter personal în starea în care se aflau pînă la momentul pierderii sau distrugerii acestora;
21.	„sesiune de lucru”	perioada care durează din momentul pornirii calculatorului și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și pînă la momentul opririi acestora;
22.	„sistem de evidență a datelor cu caracter personal”	orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice;
23.	„sistem informațional de date cu caracter personal”	totalitatea resurselor și tehnologiilor informaționale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informație care conține date cu caracter personal;
24.	„stocare”	păstrarea pe orice fel de suport a datelor cu caracter personal;
25.	„tehnologie informațională”	totalitatea metodelor, procedeelelor și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;
26.	„utilizator”	persoana care acționează sub autoritatea deținătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaționale de date cu caracter personal;

III. SCOPUL ȘI DOMENIUL DE APLICABILITATE

Obiectivele principale ale Regulamentului sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de Colegiu, atât în cadrul prelucrării manuale, cât și în cadrul sistemelor și proceselor de tehnologie informațională. Securitatea reprezintă o componentă esențială a derulării optime a proceselor bazate pe IT în cadrul Colegiului.

Baza unei securități IT adecvate o constituie respectarea prezentului Regulament. Aceasta cuprinde cerințe și reguli pentru protecția tuturor informațiilor, inclusiv a datelor cu caracter personal, a sistemelor și a proceselor IT împotriva influențelor naturale, erorilor umane și tehnice, precum și împotriva acțiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislației. Având în vedere că siguranța IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezentul Regulament vizează, de asemenea, aspecte de ordin organizatorico-juridic și de altă natură.

Prezentul Regulament are drept scop stabilirea principiilor de bază ale prelucrării datelor cu caracter personal, metodologia de lucru, precum și reguli pentru angajații Colegiului menite să asigure disponibilitatea, integritatea și confidențialitatea datelor personale în operațiunile de prelucrare a datelor personale efectuate de Colegiu, în conformitate cu legislația aplicabilă.

Colegiul procesează date cu caracter personal care aparțin angajaților și elevilor în următoarele scopuri:

- ✓ Furnizarea de servicii educaționale, începând cu procesul de admitere, înscrierea elevilor, administrarea clasei și orarul, activități didactice, administrarea examenelor interne și publice, concursurilor naționale și internaționale, eliberarea de registre matricole și rapoarte de evaluare;
- ✓ Furnizarea de servicii educaționale complementare: dezvoltare personală, consiliere personală, acces la biblioteca școlii, activități extrașcolare, cluburi, excursii școlare, gestionare a publicațiilor școlare, crearea unui mediu virtual de învățare și acordarea accesului la rețeaua de internet ale școlii;
- ✓ Asigurarea securității și a bunei desfășurări a examenelor naționale prin utilizarea mijloacelor de supraveghere video;
- ✓ Asigurarea asistenței medicale și a consilierii psihologice în caz de nevoie;
- ✓ Administrarea Colegiului: gestionarea dosarelor și documentelor educaționale ale elevilor, gestionarea facturilor și plăților, audituri și controale interne, elaborarea de rapoarte, implementarea politicilor școlare, asigurarea colaborării cu alte școli, arhivarea, evaluarea calității serviciilor noastre;
- ✓ Comunicarea în Colegiu: transmiterea mesajelor în legătură cu elevii și activitățile școlii prin orice mijloace de comunicare;

IV. DISPOZIȚII PRIVIND IERARHIA ȘI RESPONSABILITATEA PERSOANEI RESPONSABILE DE POLITICA DE SECURITATE

Prin prezentul Regulament, Colegiul, în calitate de operator de date cu caracter personal, reieșind din specificul activității, transpune procedurile și măsurile necesare în vederea asigurării nivelului adecvat de protecție la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidență gestionate, inclusiv în cadrul sistemului informațional utilizat pentru evidența elevilor (în continuare „SIME”), precum și în cadrul dosarelor fizice ale elevilor.

Regulamentul în mod obligatoriu va fi adus la cunoștință, sub semnătură, tuturor angajaților responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecție a datelor cu caracter personal. În acest sens, în temeiul ordinelor interne, accesul la prelucrarea datelor elevilor și administrarea bazelor de date SIME este realizat de către Directorul adjunct pentru instruire și educație și de către șefii secțiilor didactice, care au calitatea de administratori ai bazelor de date SIME, iar diriginții grupelor sunt desemnați, prin ordin, responsabili de gestionarea datelor elevilor din grupele lor în SIME și de păstrarea/gestionarea dosarelor elevilor aferente grupelor respective.

Responsabil de implementarea și monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal va fi desemnată persoana care, conform fișei postului și/sau ordinului intern, va dispune de resurse suficiente (timp, resurse umane, echipament și buget) și va avea acces liber la informația necesară pentru îndeplinirea funcțiilor sale în măsura în care aceasta nu operează în afara cadrului prezentului Regulament.

Pentru coordonarea aplicării prezentului Regulament la nivelul evidențelor de personal și documentelor aferente resurselor umane, precum și pentru comunicarea operativă pe subiectele ce țin de datele cu caracter personal în relația cu salariații, este desemnată persoana de contact din cadrul instituției: specialist resurse umane.

Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilități cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare și prelucrare), precum și operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.

Persoana responsabilă de politica de securitate a datelor cu caracter personal va defini clar responsabilitățile și procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizațională și de funcționare generală, va asigura măsuri tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal, va elabora procedurile de clasificare a informației care conține date cu caracter personal astfel încât să fie posibil de întocmit un nomenclator și toate datele cu caracter personal care sunt prelucrate să fie localizate, indiferent de tipul purtătorului de date, va instrui persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii

Regulament privind prelucrarea datelor cu caracter personal

de către acestea a atribuțiilor funcționale și asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora.

V. MIJLOACELE SUPUSE PRINCIPIILOR DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

Protecția datelor cu caracter personal în cadrul Colegiului (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

Sunt supuse protecției prin mijloace/procedee specifice, toate resursele informaționale ale operatorului de date cu caracter personal gestionate, care conțin date cu caracter personal, păstrate pe:

- suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
- sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

VI. MĂSURILE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL:

Măsurile de protecție a datelor cu caracter personal sunt asigurate în scopul:

- preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
- neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;
- eficientizarea resurselor informaționale atât pe suport de hârtie cât și cel în format electronic.

VII. METODELE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMELE INFORMAȚIONALE

Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele măsuri:

- preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
- excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

Regulament privind prelucrarea datelor cu caracter personal

- preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, precum și utilizarea canalelor VPN;
- preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță;
- preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaționale, care se efectuează permanent;
- stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență instituite atât pentru utilizatorii interni cât și pentru cei externi.

VIII. PROCEDURILE ORGANIZATORICE ȘI TEHNICE CARE URMEAZĂ A FI RESPECTATE ÎN CADRUL COLEGIULUI LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

8.1. Măsurile generale de administrare a securității informaționale

- a) În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie;
- b) Computerele, terminalele de acces și imprimantele sunt deconectate la terminarea sesiunilor de lucru;
- c) Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere;
- d) Este asigurată securitatea și accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate;
- e) Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii;
- f) Toate programele utilizate în cadrul sistemului informatic respectă condițiile de licențiere.
- g) Este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

8.2. Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal

- a) accesul în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare);
- b) se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces;
- c) perimetrul de securitate a Colegiului reprezintă perimetrul oficiilor în care se prelucrează/stochează date cu caracter personal;
- d) perimetrul clădirii sau încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereții exteriori ai încăperilor sunt rezistenți, intrările sunt echipate cu lacăte și semnalizare;
- e) amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri;
- f) ușile și ferestrele se încuie în cazul în care în încăperea lipsesc membrii;
- g) computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine;
- h) accesul în perimetrul de securitate a clădirii Colegiului, unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ținând cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 și art. 30 ale Legii privind protecția datelor cu caracter personal;
- i) folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezentei unei permisiuni speciale a conducerii.

8.3. Identificarea și autentificarea utilizatorilor

- a) Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori;
- b) Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificador personal (ID-ul utilizatorului), care nu conține semnamentele nivelului de accesibilitate al utilizatorului;
- c) Pentru confirmarea ID-ului utilizatorului sunt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice și individuale ale persoanei;
- d) În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă

îndelungată, codurile de identificare și autentificare se revocă sau se suspendă de administratorul I.T;

8.4. Identificarea și autentificarea echipamentului

Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal, cu menținerea acestor informații pentru o perioadă îndelungată.

8.5. Administrarea identificatorilor utilizatorilor

Administrarea identificatorilor utilizatorilor include:

- identificarea univocă a fiecărui utilizator,
- verificarea autenticității fiecărui utilizator.

8.6. Utilizarea parolelor în procesul asigurării securității informaționale

Sunt respectate regulile de asigurare a securității informaționale în cazul alegerii și folosirii parolelor care includ:

- păstrarea confidențialității parolelor;
- interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia;
- modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului sau parolei;
- alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sunt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu sunt compuse integral din grupuri de cifre sau litere;
- modificarea parolelor peste intervale de 3 luni,
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

8.7. Controlul administrării accesului

Este efectuat controlul sistematic al acțiunilor utilizatorilor în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

8.8. Accesul de la distanță

- a) Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum și sunt documentate, supuse monitorizării și controlului;

Regulament privind prelucrarea datelor cu caracter personal

- b) Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal este autorizată de persoanele responsabile ale Colegiului și permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

8.9. Limitarea folosirii tehnologiilor fără fir

- a) accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului;
- b) accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației;
- c) folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale Colegiului.

8.10. Securitatea electroenergetică

- a) Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesanționate, prin montarea lor în nișe speciale;
- b) În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI;
- c) Sunt implementate sisteme automatizate de depistare și semnalizare a incendiilor în birourile unde sunt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

8.11. Controlul instalării și scoaterii componentelor T.I.

- a) Este exercitat controlul și evidentă instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal;
- b) Informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitându-se folosirea funcțiilor standard de nimicire.

8.12. Dezvăluirea datelor cu caracter personal

- a) Dezvăluirea formatului electronic al datelor cu caracter personal conținute în sistemele de evidență, prin rețele comunicaționale ori pe alt suport digital de stocare și păstrare, urmează a fi asigurată criptarea acestei informații sau examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidență a datelor cu caracter personal este permis doar utilizatorilor autorizați. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieșind din posibilitățile tehnice asigurate de destinatar și operator, precum și în corespundere cu măsurile organizatorice și tehnice implementate de părți. În

Regulament privind prelucrarea datelor cu caracter personal

cazul în care rețelele comunicaționale prezintă riscuri pentru confidențialitatea și securitatea datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere (expediere poștală cu aviz recomandat, înmânarea personală, etc.).

- b) Sunt interzise operațiunile de dezvăluire a datelor cu caracter personal între Colegiu și alte entități care sunt amplasate geografic în stânga Nistrului care refuză să se supună juridic legislației Republicii Moldova, reieșind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părți teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecția datelor cu caracter personal.
- c) Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hârtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luându-se în considerare necesitatea asigurării unui nivel adecvat de protecție a datelor cu caracter personal.
- d) Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecția datelor cu caracter personal, în special în cazurile când tratatul internațional în baza căruia se efectuează transmiterea nu conține garanții privind protecția drepturilor subiectului de date cu caracter personal. f) Volumul și categoriile datelor cu caracter personal colectate în scopul ținerii evidenței statistice, este limitat la strictul necesar pentru realizarea scopurilor declarate.
- e) Acces la sistemele informaționale gestionate în cadrul Colegiului, din partea Procuraturii Generale (după caz procuraturile teritoriale/specializate), Ministerului Afacerilor Interne, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 și art. 212 Cod de procedură penală.

Se explică că în conformitate cu prevederile art. 157 Cod de procedură penală, documentele în orice formă (scrisă, audio, video, electronică etc.) care provin de la persoane oficiale fizice sau juridice dacă în ele sunt expuse ori adevărate circumstanțe care au importanță pentru cauză, (inclusiv informația stocată în auditul sistemelor informaționale și de evidență), pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art. 214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate și răspândite fără necesitate informație oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată (inclusiv operatorii de date cu caracter personal) au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informații o explicație în scris care ar confirma necesitatea furnizării datelor menționate.

Urmează a ține cont de faptul că în conformitate cu prevederile art.8 al Legii privind accesul la informațiile de interes public nr. 148 din 09.06.2023, datele cu caracter personal fac parte din

categoria informației oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoștință cu fișa personală a clientului, aceștia urmează a fi informați în scris despre obligațiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 și 30 ale Legii privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 74¹ Cod contravențional.

8.13. Drepturile subiecților de date cu caracter personal

- a) În cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecția datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informații, exceptând cazul în care el deține deja informațiile respective:
- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidență al operatorilor de date cu caracter personal);
 - privind scopul concret al prelucrării datelor cu caracter personal colectate;
 - privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
 - existența drepturilor la informare și de acces la datele colectate; de intervenție asupra datelor (*în special de a rectifica, actualiza, bloca sau șterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora*) și de opoziție, precum și condițiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația.
- b) Subiecților de date cu caracter personal le este asigurat dreptul de acces și posibilitatea de a lua cunoștință cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluserii sau includerii incorecte a unor date, precum și împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alți subiecți, conținute în fișele personale (alte materiale), cu excepția cazurilor în care solicitantii își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal.
- c) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entitățile ce asigură mentenanța sistemului și sau prestează servicii externalizate ale operatorului) tuturor persoanelor supuse prelucrării.
- d) În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenție, datele inexacte vor fi actualizate prin rectificare sau ștergere, ca bază servind doar surse

Regulament privind prelucrarea datelor cu caracter personal

legale (acte de identitate, de stare civilă, resurse informaționale principale de stat etc.), modificarea urmând a fi efectuată în toate sistemele informaționale și de evidență gestionate.

8.14. Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate

- a) Accesul în spațiile/perimetrul unde sunt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate instituționale /regulamentelor departamentale aprobate;
- b) Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sunt conectate la internet, nu sunt echipate cu mijloace de protecție speciale tehnice și de program și nu au instalate programe licențiate, programe antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului - este interzisă;
- c) Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sunt încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul Colegiului;
- d) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hârtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

8.15. Auditul sistemelor informaționale gestionate

- a) Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:
 - data și timpul tentativei intrării/ieșirii;
 - ID-ul utilizatorului;
 - rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.
- b) Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
 - data și timpul tentativei de obținere a accesului (executate a operațiunii);
 - denumirea (identificatorul) aplicației sau procesului, o ID-ul utilizatorului;
 - specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);

Regulament privind prelucrarea datelor cu caracter personal

- tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
 - rezultatul tentativei de obținere a accesului (executare a operațiunii) — pozitivă sau negativă.
- c) Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:
- data și timpul modificării competențelor;
 - ID-ul administratorului care a efectuat modificările;
 - ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.
- d) Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri:
- data și timpul eliberării;
 - denumirea informației și căile de acces la aceasta;
 - specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
 - ID-ul utilizatorului, care a solicitat informația.

8.16. Asigurarea protecției contra programelor dăunătoare (virusilor)

Este asigurată protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, prin existența programelor licențiate anti-virus.

8.17. Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de date cu caracter personal

Se asigură testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal (automat la pornirea sistemului și lunar la solicitarea utilizatorului autorizat în acest scop).

8.18. Gestionarea incidentelor de securitate

- a) Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.
- b) Personalul Colegiului, informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.
- c) Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității.

Regulament privind prelucrarea datelor cu caracter personal

- d) Până la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Autoritatea națională pentru protecția datelor cu caracter personal despre incidentele de securitate constatate.

8.19. Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum și a informațiilor cu accesibilitate limitată

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, pentru nerespectarea dispozițiilor Regulamentului - poartă răspundere civilă (delictuală, în conformitate cu prevederile Codului Civil), contravențională (conform art. 74¹ Cod contravențional) și penală (conform art. 177, 178, 180 Cod Penal).

IX. DISPOZIȚII FINALE

Prezentul Regulament intră în vigoare din data aprobării de către Consiliul de administrație a Colegiului.