Aprobat
prin Ordinul Ministerului Educației
nr. 1056 din 10 octombrie 2014

Completat prin Ordinul nr. 1120 din 31 octombrie 2014
Completat prin Ordinul nr. 1140 din 12 noiembrie 2014

Regulamentul
de asigurare a securității datelor cu caracter personal
prelucrate de către Ministerul Educației în procesul de utilizare a
Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor

I. Dispozițiile generale

1. În vederea realizării prevederilor Legii 133 din 8 iulie 2011 privind protecția datelor cu caracter personal şi în conformitate cu Hotărârea Guvernului nr. 1123 din 14 decembrie 2010 „Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal", Ministerul Educației, reieşind din specificul activității, a elaborat şi organizează implementarea prevederilor documentului respectiv, care stabileşte politica de securitate a datelor cu caracter personal prelucrate de către Ministerul Educației în procesul de utilizare a Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor.

2. Pentru ca politica de securitate a datelor cu caracter personal să fie cunoscută tuturor, aceasta va fi adusă la cunoştință utilizatorilor şi altor angajați ai operatorului, în limitele competențelor funcționale şi nivelului de acces acordat.

3. În sensul prezentului regulament, Ministerul Educației are calitatea de *Operator*, iar instituțiile (Centrul Tehnologii Informaționale şi Comunicaționale în Educație, direcțiile de învățământ ale raioanelor, municipiilor şi UTA Găgăuzia, şcolile primare, gimnaziile, liceele) au calitatea de *Persoană împuternicită de operator*.

4. Responsabili de securitatea datelor sunt administratorii Sistemului de Cartografiere a şcolilor primare, gimnaziilor şi liceelor, care, în funcție de categoriile de date la care au acces, se clasifică pe următoarele nivele:

a) administratori naționali;
b) administratori raionali, municipali, ai UTA Găgăuzia;
c) administratori şcolari.

5. Administratorii naționali se desemnează prin ordinul Ministerului Educației şi sunt responsabili la nivel de Minister de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, persoanele desemnate neavând atribuții/ sarcini/ responsabilități incompatibile cu sarcinile funcției de implementare a politicii.

6. Administratori raionali, municipali, ai UTA Găgăuzia se desemnează prin ordinile direcțiilor de învățământ din unitatea teritorială respectivă,şi sunt responsabili de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de

securitate a datelor cu caracter personal în direcțiile în cauză, persoanele desemnate neavând atribuții/ sarcini/ responsabilități incompatibile cu sarcinile funcției de implementare a politicii.

7. Administratorii şcolari se desemnează prin ordinile instituțiilor de învățământ şi sunt responsabili de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal în instituțiile în cauză, persoanele desemnate neavând atribuții/sarcini/responsabilități incompatibile cu sarcinile funcției de implementare a politicii.

8. Administratorii vor dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi vor avea acces liber la informația necesară pentru îndeplinirea funcțiilor lor în măsura în care acesta nu operează în afara cadrului acestei politici. Acesta asigură definirea clară a diferitelor responsabilități cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.

9. Administratorii vor avea dreptul să înregistreze în Sistemul de cartografiere în calitate de utilizatori doar persoanele care au fost explicit desemnate prin ordine ale conducătorilor, după caz, ai Ministerului Educației, Centrului de Tehnologii Informaționale şi Comunicaționale în Educație, direcțiilor raionale/ municipale/ UTA Găgăuzia de învățământ, ai instituțiilor de învățământ.

II. Scopul

10. Prezentul Regulament stabileşte măsurile de asigurare a securității datelor cu caracter personal prelucrate de către operator în procesul de utilizare a Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor.

11. Scopul documentului este descrierea politicii de securitate privind introducerea, stocarea, actualizarea şi prelucrarea datelor referitoare la învățământul general şi măsurile de protecție luate de operator pentru a proteja datele cu caracter personal.

12. Scopul introducerii, stocării, actualizării şi prelucrării datelor referitoare la învățământul general constă în efectuarea unui management educațional bazat pe date relevante şi veridice, identificarea copiilor ce au abandonat învățământul obligatoriu, depistarea cazurilor de îngrădire a drepturilor copiilor la studii, asigurarea accesului universal la educație, excluderea fraudelor.

III. Cerințele de securitate față de modul de amplasare a componentelor Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor

13. Sistemul de cartografiere a şcolilor primare, gimnaziilor şi liceelor include următoarele componente:

a) serverul Sistemului de cartografiere;
b) stațiile de lucru ale utilizatorilor;
c) rețeaua securizată de comunicații.

14. Serverul Sistemului de cartografiere va fi amplasat într-o încăpere special amenajată a Centrului de Tehnologii Informaționale şi Comunicaționale în Educație. Încăperea în care va fi amplasat serverul trebuie să corespundă următoarelor cerințe:

1) perimetrul încăperii este integru din punct de vedere fizic;

2) dacă încăperea se află la parter şi/sau la ultimul etaj al clădirii, precum şi în cazul existenței balcoanelor, scărilor anti-incendiare etc., ferestrele încăperii trebuie să aibă gratii;

3) pereții exteriori ai încăperii sunt rezistenți;

4) intrarea în încăpere este securizată cu ajutorul lacătelor, mijloacelor de control al accesului, semnalizare.

15. Încăperea în care va fi amplasat serverul Sistemului de cartografiere va fi dotată cu echipamentele necesare pentru a asigura protecția contra accesului nesancționat, furturilor, incendiilor, inundațiilor şi altor riscuri posibile. În cazurile în care în încăperea în care se află Serverul lipsesc utilizatorii, uşile şi ferestrele încăperii în cauză vor fi permanent încuiate.

16. Agendele şi/sau cărțile de telefoane în care se conțin indicii despre locul amplasării serverul Sistemului de cartografiere nu sunt accesibile persoanelor străine.

17. Purtătorii de informații şi mijloacele de stocare şi prelucrare a datelor Sistemului de cartografiere scoase din încăperile aflate în perimetrul de securitate nu sunt lăsate fără supraveghere în locuri publice.

18. Stațiile de lucru vor fi amplasate în săli special amenajate, în incinta Ministerului Educației, Centrului de Tehnologii Informaționale şi Comunicaționale în Educație, direcțiilor de învățământ ale raioanelor, municipiilor, UTA Găgăuzia, instituțiilor de învățământ.

19. Conducătorii subdiviziunilor din componența Ministerului Educației, conducătorii Centrului de Tehnologii Informaționale şi Comunicaționale în Educație, şefii direcțiilor de învățământ ale raioanelor, municipiilor, UTA Găgăuzia, directorii instituțiilor de învățământ vor asigura ca încăperile în care sun instalate stațiile de lucru ale Sistemului de cartografiere să corespundă următoarelor cerințe:

a) spațiul rezervat pentru locurile de muncă ale utilizatorilor Sistemului de cartografiere corespund normelor tehnice şi sanitare privind exploatarea calculatoarelor personale;

b) sunt implementate măsurile de siguranță şi protecție împotriva incendiilor (inclusiv interzicerea utilizării neautorizate a aparatelor suplimentare de încălzire, fumatul, blocarea căilor de evacuare şi acces pentru pompieri etc.);

c) este imposibilă conectarea stațiilor de lucru la alte rețele de comunicații în afară de cea a Sistemului de cartografiere;

d) în încăperile în cauză nu sunt mijloace tehnice ce ar putea fi utilizate pentru transmiterea neautorizată a datelor;

e) încăperile dispun de mijloace tehnice (lacăte, semnalizare) ce asigură îngrădirea accesului persoanelor neautorizate la stațiile de lucru ale Sistemului de cartografiere.

20. Securizarea rețelei de comunicații va fi efectuată cu ajutorul mijloacelor de program bazate pe utilizarea protocolului HTTPS.

IV. Protejarea securității informațiilor

21. Pentru a asigura securitatea informațională a Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor, vor fi implementate următoarele măsuri tehnice şi organizatorice:

a) limitarea timpului de schimburi de date cu caracter personal, care vor putea fi accesate doar în perioade limitate de timp, stabilite explicit prin ordinul Ministerului Educației, de obicei, la începutul şi sfârşitul fiecărui an de studiu;

b) stocarea datelor se va efectua doar pe Serverul Sistemului de cartografiere, fără ca date în cauză să fie stocate şi pe stațiile de lucru ale utilizatorilor;

c) mediul de stocare (Serverul) se va afla într-un spațiu securizat, protejat prin măsuri de securitate fizică;

d) fiecare utilizator al Sistemului de cartografiere a instituțiilor de învățământ general va semna, conform modelului specificat în *Anexa nr. 1*, declarația-angajament privind confidenţialitatea datelor cu caracter personal, prin care se va obliga să respecte prevederile legale în domeniu. Declarația semnată se va păstra în dosarul personal al angajatului;

e) împuternicirile de a acorda sau de a retrage dreptul de acces la Sistemul de cartografiere şi de a modifica rolurile utilizatorilor înregistrați deja conform procedurilor generale de acces la sistemele informatice automatizate, le vor avea doar administratorii Sistemului de cartografiere;

f) accesul fiecărui administrator şi utilizator al Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor este limitat doar la nivelul clasei/ instituției de învățământ/ unității teritorial-administrative de care este responsabil;

g) analiştii Sistemului de cartografiere nu au acces la datele cu caracter personal, putând extrage doar rapoarte statistice;

h) administratorii Sistemului de cartografiere vor ține în permanență o listă actualizată a tuturor persoanelor care au dreptul de acces, cu specificarea rolului fiecărui utilizator, modelul căreia este specificat în *Anexa nr. 2*;

i) toate accesările Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor vor fi înregistrate în mod automat în jurnalul de sistem (log) şi vor fi păstrate pe întreaga durată de viață a sistemului;

j) imediat după terminarea sesiunii de lucru, fiecare utilizator va fi obligat sa se asigure că toate fişierele create de el, şi care ar putea să conțină date personale, sunt înlăturate de pe stațiile de lucru şi purtătorii de informație de orice tip.

V. Durata de stocare

22. Durata de stocare a datelor cu caracter personal în Sistemul de cartografiere a şcolilor primare, gimnaziilor şi liceelor se stabileşte după cum urmează:

a) în cazul elevilor – pe întreaga durată a înrolării în învățământul general plus un an după absolvire;

b) în cazul cadrelor didactice, de conducere şi auxiliare – pe întreaga durată de angajare într-o instituție de învățământ general plus un an după expirarea contractului de muncă.

23. Administratorii Sistemului de cartografiere sunt obligați să şteargă datele cu caracter personal, durata de stocare a cărora depăşeşte termenul stabilit. Dacă în procesul de exploatare a sistemului, din motive legal întemeiate, apare necesitatea prelungirii termenului de stocare a datelor cu caracter personal, acestea vor fi

înregistrate de administratorii sistemului în Registrul înregistrărilor care depăşesc durata de stocare. Modelul de Registru este specificat în *Anexa nr. 3*.

VI. Drepturile elevilor, reprezentanților legali ai acestora şi angajaților instituțiilor de învățământ

24. Operatorul garantează respectarea, conform legii, a tuturor drepturilor ce revin elevilor, reprezentanților legali ai acestora şi angajaților instituțiilor de învățământ. Toate persoanele implicate în administrarea şi utilizarea Sistemului de cartografiere, vor respecta procedurile de acces la datele cu caracter personal.

25. Având în vedere dispozițiile alineatului (5) al art. 5 din Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal, care prescrie mai multe situații în care prelucrarea datelor cu caracter personal poate fi realizată şi în lipsa consimțământului subiectului datelor cu caracter personal, raportând excepțiile respective la cazul prelucrării informațiilor în Sistemul de cartografiere a şcolilor primare, gimnaziilor şi liceelor, realizarea operațiunilor de introducere, actualizare, stocare şi ştergere a datelor cu caracter personal se face fără consimțământul elevilor, reprezentanților legali ai acestora şi angajaților instituțiilor de învățământ.

26. Operatorul asigură ca elevii adulți sau, în cazul elevilor minori, reprezentanții legali ai acestora, şi angajații instituțiilor de învățământ să fie informați în scris conform *Anexei nr. 4* despre procedurile de introducere, modificare, prelucrare şi stocare a datelor cu caracter personal, despre scopul acestor proceduri şi beneficiile avute de ei de pe urma acestora.

27. Elevii, reprezentanții legali ai acestora, angajații instituțiilor de învățământ pot face cunoştință cu conținutul datelor cu caracter personal care le aparțin şi pot cere corectarea eventualelor greşeli. Corectarea datelor se va efectua în baza actelor doveditoare, sau, în cazul datelor cu caracter de autoidentificare, în baza declarațiilor pe propria răspundere.

VII. Securitatea mediului fizic şi a tehnologiilor informației folosite în procesul prelucrării datelor cu caracter personal

Secțiunea 1
Autorizarea accesului fizic

28. Accesul în încăperile în care sunt amplasate stațiile de lucru ale Sistemului de cartografiere, în perioada introducerii şi/ sau accesării datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară şi doar în timpul orelor de program.

29. Conducerea Ministrul Educației, Centrului Tehnologii Informaționale şi Comunicaționale în Educație, direcțiilor raionale, municipale, a UTA Găgăuzia, a instituțiilor de învățământ aprobă listele de acces, care se revizuiesc după necesitate.

Secțiunea 2
Administrarea şi monitorizarea accesului fizic

30. Administratorii Sistemului de cartografiere administrează şi monitorizează accesul fizic al persoanelor în încăperile şi la stațiile de lucru în perioada introducerii şi/ sau accesării datelor cu caracter personal. În caz de încălcare a regimului de acces, administratorii deconectează stațiile de lucru de la serverul Sistemului de cartografiere şi raportează conducerii instituției în cauză despre încălcările depistate.

Secțiunea 3
Controlul instalării şi scoaterii componentelor TI

31. Se exercită controlul şi evidența instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal.

32. La expirarea termenului de păstrare informațiile, care conțin date cu caracter personal şi care se conțin pe purtătorii de informații, se distrug.

Secțiunea 4
Măsurile generale de administrare a securității informaționale

33. În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie, magnetic, optic sau electronic, care conțin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.

34. Calculatoarele, terminalele de acces şi imprimantele sunt deconectate imediat după terminarea sesiunilor de lucru.

35. Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere.

36. Accesul fizic la mijloacele de afişaj a informației care conține date cu caracter personal necesită administrare pentru blocarea vizualizării acesteia de către persoane neautorizate.

37. 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 operatorului.

38. Scoaterea şi introducerea mijloacelor de prelucrare a datelor cu caracter personal din/în perimetrul de securitate se înregistrează.

VIII. Identificarea şi autentificarea utilizatorului Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor

Secțiunea 1
Identificarea şi autentificarea utilizatorului

39. Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.

40. Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii şi administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmentele nivelului de accesibilitate al utilizatorului.

41. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole.

42. În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate şi 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 şi autentificare sunt revocate sau sunt suspendate de către deținătorul de date cu caracter personal.

Secțiunea 2
Administrarea mijloacelor de autentificare

43. Operatorul determină procedurile administrative, care reglementează procesul distribuirii şi ridicării mijloacelor de autentificare a utilizatorilor, inclusiv acțiunile în cazul pierderii/compromiterii sau defecțiunii acestora.

44. După instalarea Sistemului de cartografiere, se schimbă toate informațiile de autentificare a utilizatorilor utilizate anterior.

Secțiunea 3
Asigurarea conexiunii bilaterale în cazul introducerii informației de autentificare a utilizatorilor

45. Se asigură conexiunea bilaterală a operatorului cu utilizatorul în momentul trecerii de către acesta a procedurilor de autentificare, care nu compromite mecanismul de autentificare.

Secțiunea 4
Utilizarea parolelor în procesul asigurării securității informaționale

46. Se respectă regulile de asigurare a securității informaționale în cazul alegerii şi folosirii parolelor, care includ:

a) păstrarea confidențialității parolelor;

b) interzicerea înscrierii parolelor pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestuia;

c) modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului sau parolei;

d) 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 şi nu sunt compuse integral din grupuri de cifre sau litere;

e) modificarea parolelor peste intervale de maximum 3 luni;

f) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

Secțiunea 5
Administrarea parolelor utilizatorilor

47. Se folosesc identificatoare individuale (nume de utilizator) pentru fiecare utilizator şi parole individuale ale acestora pentru asigurarea posibilității de stabilire a responsabilității.

48. Se asigură blocarea accesului după trei tentative greşite de autentificare.

49. Este asigurată păstrarea istoriilor anterioare ale parolelor în formă de *hash* a utilizatorilor (pentru o perioadă de un an) şi prevenirea folosirii repetate a acestora.

50. La momentul introducerii, parolele nu se reflectă în clar pe monitor.

51. Parolele se păstrează în formă cifrată, utilizându-se algoritmul criptografic unilateral (funcții de tipul *hash*).

IX. Administrarea accesului utilizatorilor

52. Operatorul impune limite în privința persoanelor care au dreptul să vizualizeze, să copieze, să descarce, să şteargă sau să modifice orice date cu caracter personal.

53. Toți membrii personalului cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor.

54. Administratorul asigură că întregul personal cu drepturi de acces, implicat în operarea Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor, este instruit şi informat cu privire la toate aspectele funcționale, operaționale şi administrative ale acestei activități.

55. Orice activitate de dezvăluire a datelor personale către terți va fi documentată şi supusă unei analize riguroase privind, pe de-o parte, necesitatea comunicării, şi, pe de altă parte, compatibilitatea dintre scopul în care se face comunicarea şi scopul în care aceste date au fost colectate inițial pentru prelucrare. În aceste cazuri, va fi consultată şi persoana responsabilă de realizarea politicii de securitate.

56. Orice încălcare a securității datelor cu caracter personal este înregistrată în registrul de monitorizare a Sistemului de cartografiere, iar persoana responsabilă de realizarea politicii de securitate este informată în legătură cu acest lucru cât mai repede posibil.

57. Drepturile de acces ale utilizatorilor la sistemele informaționale de date cu caracter personal sunt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare şase luni) şi după oricare schimbare de rol al utilizatorului.

58. Este efectuată administrarea conturilor de acces ale utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora.

59. Sunt folosite mijloace automatizate de suport în scopul administrării conturilor de acces.

60. Valabilitatea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea unei perioade stabilite în timp (pentru fiecare tip de cont de acces în parte).

61. Sunt dezactivate automat, după o perioadă de maximum trei luni, conturile de acces ale utilizatorilor neactivi, care prelucrează date cu caracter personal.

62. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acțiunii conturilor de acces.

63. Se autorizează de către operator realizarea fluxurilor informaționale în procesul transmiterii acestora în interiorul şi în afara Sistemului de cartografiere.

64. Repartizarea obligațiilor subiecților care asigură funcționarea Sistemului de cartografiere este efectuată prin intermediul învestirii cu drepturi/competențe corespunzătoare de acces.

65. Utilizatorii Sistemului de cartografiere se învestesc doar cu acele drepturi/competențe, care sunt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

66. Înainte de acordarea accesului în Sistemul de cartografiere, utilizatorii sunt informați despre faptul că folosirea Sistemului este controlată şi că folosirea neautorizată a acestora este sancționată în conformitate cu legislația.

67. Se efectuează controlul acțiunilor utilizatorului în vederea evaluării corectitudinii şi conformării operațiunilor şi acțiunilor efectuate prin intermediul stațiilor de lucru ale Sistemului de cartografiere.

X. Auditul securității în Sistemul de cartografiere a şcolilor primare, gimnaziilor şi liceelor

68. Se organizează generarea înregistrărilor de audit a securității în Sistemul de cartografiere pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

69. Se efectuează înregistrarea tentativelor de intrare/ieşire a utilizatorului în sistem, conform următorilor parametri:

a) data şi timpul tentativei intrării/ieşirii;
b) ID-ul utilizatorului;
c) rezultatul tentativei de intrare/ieşire – reuşit sau eşuat.

70. Se efectuează înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:

a) data şi timpul tentativei de pornire;

b) denumirea/identificatorul programului aplicativ sau procesului;

c) ID-ul utilizatorului;

d) rezultatul tentativei de pornire – reuşită sau eşuată.

71. Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

a) data şi timpul tentativei de obținere a accesului (executare a operațiunii);

b) denumirea (identificatorul) aplicației sau procesului;

c) ID-ul utilizatorului;

d) specificațiile resursei protejate (identificator, nume logic, nume fişier, număr etc.);

e) tipul operațiunii solicitate (citire, înregistrare, ştergere etc.);

f) rezultatul tentativei de obținere a accesului (executare a operațiunii) – ruşită sau eşuată.

72. Se efectuează înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:

a) data şi timpul modificării competențelor;

b) ID-ul administratorului care a efectuat modificările;

c) ID-ul utilizatorului şi competențele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

73. Se efectuează înregistrarea ieşirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților şi statutul obiectelor de acces, conform următorilor parametri:

a) data şi timpul eliberării;

b) denumirea informației şi căile de acces la aceasta;

c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);

d) ID-ul utilizatorului, care a solicitat informația;

e) volumul documentului eliberat (numărul paginilor, a filelor, copiilor) şi rezultatul eliberării – pozitiv sau negativ.

74. În caz de deranjament al auditului securității în Sistemul de cartografiere sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informată persoana responsabilă de politica de securitate a datelor cu caracter personal şi întreprinse acțiuni în vederea restabilirii capacității de lucru a sistemului de audit.

75. Se efectuează monitorizarea permanentă şi analiza înregistrărilor de audit a securității în Sistemul de cartografiere, în scopul depistării activităților neobişnuite sau suspecte de utilizare a acestor sisteme informaționale, cu întocmirea raportului referitor

la cazurile depistării acestor activități, stocate în mijloacele electronice de calcul şi întreprinderea acțiunilor prestabilite în politica de securitate pentru astfel de cazuri.

76. Rezultatele auditului securității în Sistemul de cartografiere, care reprezintă operațiuni de prelucrare a datelor cu caracter personal şi mijloacele de efectuare a auditului, se vor proteja contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidențialității şi integrității acestora.

77. Durata stocării rezultatelor auditului securității este de 2 ani, pentru a fi posibilă folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare.

78. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

XI. Asigurarea integrității informației care conține date cu caracter personal şi a tehnologiilor informației

79. Se asigură identificarea, protocolarea şi înlăturarea deficiențelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor şi pachetelor de reînnoire a acestor soft-uri.

80. Se asigură protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate şi la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare şi signaturilor de virus.

81. Se utilizează tehnologii şi mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistem şi constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaționale.

82. Se asigură protecția şi posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal şi informației care conține date cu caracter personal.

83. Se asigură testarea funcționării corecte a funcțiilor de securitate a sistemului (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).

XII. Copiile de rezervă şi restabilirea informației care conține date cu caracter personal

84. În dependență de volumul prelucrărilor efectuate, individual, se stabileşte de către operator intervalul de timp în care se execută copiile de siguranță a informațiilor care conțin date cu caracter personal şi soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal.

85. Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații şi integrității informației care conține date cu caracter personal.

86. Procedurile de restabilire a copiilor de siguranță se actualizează şi se testează cu regularitate, în scopul asigurării eficacității acestora.

XIII. Controalele de securitate a Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor

87. Operatorul verifică cu regularitate, îndeplinirea măsurilor tehnice şi/sau organizaționale luate pentru detectarea unor disfuncționalități în ceea ce priveşte folosirea în procesul prelucrării datelor cu caracter personal a sistemelor de telecomunicații şi/ sau efectuarea îmbunătățirilor, în caz de necesitate.

88. Controalele de securitate sunt actualizate de fiecare dată când operatorul este reorganizat sau îşi schimbă infrastructura.

XIV. Gestionarea incidentelor de securitate a Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor

89. Personalul care asigură exploatarea Sistemului de cartografiere va trece instruirea referitoare la responsabilitățile şi obligațiile în cazul executării acțiunilor de gestionare şi reacționare la incidentele de securitate.

90. Este asigurat mecanismul de informare neîntârziată a conducerii operatorului despre incidentele care încalcă securitatea sistemului.

91. Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securității.

92. Incidentele de securitate a Sistemului de cartografiere se urmăresc şi se documentează în regim permanent.

93. Anual, către 31 ianuarie, Ministerul Educației va prezenta Centrului Naţional pentru Protecția Datelor cu Caracter Personal raportul generalizat despre incidentele de securitate ale Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor.

Anexa nr. 1
la Regulamentul de asigurare a securității
datelor cu caracter personal prelucrate de către
Ministerul Educației în procesul de utilizare a
Sistemului de cartografiere a şcolilor primare,
gimnaziilor şi liceelor

Declaraţie – angajament
a utilizatorului Sistemului de cartografiere a şcolilor
primare, gimnaziilor şi liceelor privind confidenţialitatea
datelor cu caracter personal

Subsemnatul _____,
(numele, prenumele)

IDNP |__|__|__|__|__|__|__|__|__|__|__|__|,

angajat al _____

_____
(denumirea instituţiei, adresa, telefon)

Funcţia _____

_____
(denumirea funcției/postului ocupat)

Locul desfăşurării activităţii _____

_____
(denumirea raionului/municipiului/UTA, localității şi adresa sediului instituției)

În conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal şi a Hotărârii Guvernului nr. 1123 din 14 decembrie 2010 „Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal”, mă oblig să respect drepturile şi libertățile fundamentale ale persoanelor cu privire la prelucrarea, confidențialitatea şi securitatea datelor cu caracter personal.

Conştientizez că în cazul divulgării datelor cu caracter personal voi purta răspundere în conformitate cu legislația în vigoare.

Data _____ Semnătura _____

Anexa nr. 2
la Regulamentul de asigurare a securității datelor cu caracter personal prelucrate de către Ministerul Educației în procesul de utilizare a Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor

Lista
utilizatorilor Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor

din _____
denumirea instituţiei, adresa, telefonul

Nr. crt.	Numele, Prenumele	Postul / Funcția	Numele de utilizator	Rolul de utilizator	Data înregistrării	Semnătura utilizatorului	Data radierii	Semnătura utilizatorului
1.								
2.								
3.								

Administrator al Sistemului de cartografiere _____
numele, prenumele, semnătura

Anexa nr. 3
la Regulamentul de asigurare a securității datelor cu caracter personal prelucrate de către Ministerul Educației în procesul de utilizare a Sistemului de cartografiere a şcolilor primare, gimnaziilor şi liceelor

Registrul
înregistrărilor care depăşesc durata de stocare
în Sistemul de cartografiere a şcolilor primare, gimnaziilor şi liceelor

din _____

denumirea instituţiei, adresa, telefonul

Nr. crt.	Data	Numele, Prenumele	Tipul obiectului informatic	Cauza prelungirii	Data până la care este prelungit termenul de stocare	Note
1.						
2.						
3.						

Administrator al Sistemului de cartografiere _____

Anexa nr. 4
la Regulamentul de asigurare a securității
datelor cu caracter personal prelucrate de către
Ministerul Educației în procesul de utilizare a
Sistemului de cartografiere a şcolilor primare,
gimnaziilor şi liceelor

Modelul notei de informare
cu privire la prelucrarea datelor cu caracter personal

Administrația şcolară vă informează că în vederea efectuării unui management educațional bazat pe date relevante şi veridice, identificării copiilor ce au abandonat învățământul obligatoriu, depistării cazurilor de îngrădire a drepturilor copiilor la studii, asigurării accesului universal la educație, excluderea fraudelor, va colecta şi va pune la dispoziția Ministerului Educației categoriile de date cu caracter personal indicate în Concepția sistemului informațional educațional, aprobată prin Hotărârea Guvernului nr. 270 din 13.04.2007.

Accesul la datele cu caracter personal va avea loc doar în strictă conformitate cu prevederile Legii nr. 133 din 07.08.2011 privind protecția datelor cu caracter personal, a Regulamentului privind sistemul de cartografiere a şcolilor primare, gimnaziilor şi liceelor, aprobat prin Hotărârea Guvernului 899 din 27 octombrie 2014 şi a Regulamentului de asigurare a securității datelor cu caracter personal prelucrate de către Ministerul Educației în procesul de utilizare a Sistemului de Cartografiere a şcolilor primare, gimnaziilor şi liceelor, aprobat de către Ministerul Educației.

Durata de stocare a datelor cu caracter personal în Sistemul de cartografiere a instituțiilor de învățământ general va constitui:

a) în cazul elevilor – întreaga durată a înrolării în învățământul general plus un an după absolvire;

b) în cazul cadrelor didactice, de conducere şi auxiliare – întreaga durată de angajare într-o instituție de învățământ general plus un an după expirarea contractului de muncă.

În cazul în care datele cu caracter personal sunt colectate direct de la subiectul datelor, operatorul sau persoana împuternicită de către operator este obligată să-i furnizeze următoarele informații, exceptând cazul în care acesta deține deja informațiile respective

1) identitatea operatorului sau, după caz, a persoanei împuternicite de către operator;

2) scopul prelucrării datelor colectate;

3) informații suplimentare, precum:

a) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;

b) existența drepturilor de acces la date, de intervenție asupra datelor şi de opoziție, precum şi condițiile în care acestea pot fi exercitate;

c) dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, precum şi consecințele posibile ale refuzului de a răspunde.

Orice subiect al datelor cu caracter personal are dreptul să obțină de la operator, la cerere, fără întârziere şi în mod gratuit:

a) confirmarea faptului că datele care îl privesc sunt sau nu sunt prelucrate de acesta, de asemenea informații referitoare la scopurile prelucrării, categoriile de date avute în vedere şi destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele;

b) comunicarea, într-o formă inteligibilă şi într-un mod care nu necesită un echipament suplimentar, a datelor cu caracter personal care fac obiectul prelucrării, precum şi a oricărei informații disponibile privind originea acestor date;

c) informații privind principiile de funcționare a mecanismului prin care se efectuează prelucrarea automatizată a datelor care vizează subiectul datelor cu caracter personal;

d) informații cu privire la consecințele juridice generate de prelucrarea datelor cu caracter personal pentru subiectul acestor date;

e) informații privind modul de exercitare a dreptului de intervenție asupra datelor cu caracter personal.

Operator înregistrat în Registrul de evidență al operatorilor de date cu caracter personal cu nr. 0000034.