MINISTERUL EDUCAȚIEI CULTURII ȘI CERCETĂRII

AL REPUBLICII MOLDOVA

CONSILIULUI MUNICIPAL CHIȘINĂU

DIRECȚIA GENERALĂ EDUCAȚIE, TINERET ȘI SPORT

APROBAT
la ședința Consiliului de Administrație nr. 2
din 29.10.2020
IP Școala Primară- Grădiniță nr. 199
Director interimar /Viorica Pelivan/

POLITICA DE SECURITATE

A PRELUCRĂRII DATELOR CU CARACTER PERSONAL ÎN CADRUL IP ȘCOALA PRIMARĂ-GRĂDINIȚĂ NR. 199

Chișinău, 2020

1

I. CONSIDERAȚII GENERALE

1. Instituția Publică Școala Primară-Grădiniță nr. 199 la prelucrarea datelor cu caracter personal în cadrul entității a aplicat principiile prevazute de actele internaționale - Constituția Republicii Moldova, Declarația universală a drepturilor omului, Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Legea nr. 133/2011 privind protecția datelor cu caracter personal, Legea nr. 982/2000 privind accesul la informație, HG nr. 1123/2010 „Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal", HG nr. 296/2012 privind aprobarea Regulamentului Registrului de evidență al operatorilor de date cu caracter personal.
2. Instituția Publică Școala Primară-Grădiniță nr. 199 (în continuare – IPȘPG nr. 199) are sediul înregistrat pe strada A. Doga 32/1, mun. Chisinau, Republica Moldova cu IDNO: 1015620000106.
3. Politica de securitate a prelucrării datelor cu caracter personal, în contunuare Politica, este aprobată de catre IPȘPG nr. 199 care acționează în baza Statutului instituției, Regulamentului intern și alte acte normative și legislative în vigoare. Prezenta Politica este aprobată, inclusiv, în vederea conformarii IPȘPG nr. 199 cu prevederile Hotărârii Guvernului Republicii Moldova nr.1123 din data de 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" și Legii Republicii Moldova nr.133 din 08.07.2011 "Privind protecția datelor cu caracter personal".

II. NOȚIUNI GENERALE

4. În prezenta Politică de Securitate, sunt definite/utilizate următoarele noțiuni:
   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;
   categorii speciale de date cu caracter personal - datele care dezvăluie originea rasială sau etnica a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viață sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancțiunile contravenționale;

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 prevazute în mod expres de legislația în vigoare;
persoană împuternicită de către operator - persoană fizică sau persoană 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;
autentificare - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticității;
control de securitate - acțiuni intreprinse de catre instituție în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau a registrelor ținute;
identificare - atribuirea unui identificator subiecților și obiectelor de acces și/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;
i***ntegritate*** - certitudinea, necontradictorialitatea și actualitatea informației care conține date cu caracter personal, protecția ei de distrugere și modificare neautorizată;
mijloace de protecție criptografică a informației care conține date cu caracter personal - 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 acesteia prin canalele de comunicații;
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; ***politica de securitate a datelor cu caracter personal*** - document, elaborat de către operatorul de date - instituția, 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;
perimetru de securitate - zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic și/sau tehnic al accesului;
persoana responsabilă de politica de securitate a datelor cu caracter personal - 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 deținatorului de date cu caracter personal; ***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;
purtător 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 pastrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia;
restaurarea datelor - procedurile cu privire la reconstituirea/prestabilirea datelor cu caracter personal în starea în care se aflau pâna la momentul pierderii sau distrugerii acestora;
tehnologie informațională ((TI) eng. Informational Technology) - totalitatea metodelor, procedeelor și mijloacelor de prelucrare și transmitere a informației care conține date cu caracter personal și regulile de aplicare a acesteia;
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;
sesiune de lucru — perioada care durează din momentul pornirii calculatorului și aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale și până la momentul opririi acestora;
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;
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, dezvaluirea prin transmitere, diseminare sau în orice alt mod, alaturarea ori combinarea, blocarea, ștergerea sau distrugerea;
stocare - pastrarea pe orice fel de suport a datelor cu caracter personal;
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 dupa criterii funcționale sau geografice;
consimțământul subiectului datelor cu caracter personal - 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; ***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 forța de muncă.

III. SCOPUL POLITICII DE SECURITATE

5. Scopul asigurării securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal constă în stabilirea regulilor minime de implementare de către instituție a măsurilor tehnice și organizatorice necesare pentru asigurarea securității, confidențialității și integrității datelor cu caracter personal prelucrate în cadrul sistemelor informaționale de date cu caracter personal și/sau a registrelor ținute manual.
6. Securitatea reprezintă o componentă esențială a derulării optime a proceselor bazate pe TI în cadrul instituției. Baza unei securități a TI adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerințe și reguli pentru protecția tuturor informațiilor, inclusiv datele cu caracter personal, sistemelor și proceselor TI 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 TI nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic și de altă natură.
7. Instituția va proteja datele cu caracter personal atât a participanților la proces/vizitatori, cât și a angajaților săi.
8. Reglementările prezentei Politici reprezintă un standard minim pentru IPȘPG nr. 199, inclusiv pentru toți angajații instituției. Pornind de la această reglementare, toți angajații IPȘPG nr. 199 urmează să respecte strict prevederile Politicii și regulilor interne ale instituției privind protecția datelor cu caracter personal și sistemelor TI.

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

9. Operatorul de date cu caracter personal reieșind din specificul activității, prin prezenta Politică de securitate, transpune procedurile și măsurile necesare în vederea asigurării nivelului adecvat de protecție la prelucrarea datelor cu caracter personal în cadrul sistemelor de evidență gestionate.
10. Politica de securitate a datelor cu caracter personal se va revizui periodic ca rezultat al modificărilor sau reevaluării competențelor entității, fiind pusă în sarcina directorului, de a desemna persoana/ele care vor participa nemijlocit la ajustarea prevederilor prezentului act.

11. Politica de securitate, în mod obligatoriu va fi adusă la cunoștință, sub semnatură, tuturor angajaților responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv și la operarea modificărilor odată cu necesitatea asigurarii nivelului adecvat de protecție a datelor cu caracter personal.
12. 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 va avea acces liber la informația necesară pentru îndeplinirea funcțiilor sale în masura în care aceasta nu operează în afara cadrului acestei politici.
13. Persoana responsabilă desemnată, indiferent de funcțiile exercitate, în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit conducatorului – directorului IPȘPG nr. 199 sau persoanei care îndeplinește interimatul funcției.
14. 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.
15. 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, va asigură 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 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

16. Protecția datelor cu caracter personal în cadrul IPȘPG nr. 199 (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntimpinare a prelucrării ilicite a datelor cu caracter personal.
17. Toate resursele informaționale ale operatorului de date cu caracter personal gestionate, care conțin date cu caracter personal, sunt supuse protecției prin

mijloace/procedee specifice, pastrate pe suporturi ale informației electronice și baze de date (sisteme informaționale, rețele, sisteme operaționale, sisteme de gestionare a bazelor de date și alte aplicații, sisteme de telecomunicații, inclusiv mijloace de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației).

VI. MĂSURI DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

18. Masurile de protecție a datelor cu caracter personal sunt asigurate în scopul:
    a) preîntîmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
    b) preîntimpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
    c) neadmiterii dezvăluirii terților a informației cu accesibilitate limitată;
    d) eficientizării resurselor informaționale atât pe suport de hârtie cât și cel în format electronic.

VII. PROTECȚIA DATELOR CU CARACTER PERSONAL PRELUCRATE ÎN SISTEMUL INFORMAȚIONAL

19. Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele metode:
    a) preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
    b) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
    c) preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
    d) 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;
    e) preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legatură, este asigurată prin folosirea metodelor de cifrare a acestei informații;
    f) 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;

g) stabilirea exactă a ordinii de acces la informația care conâine date cu caracter personal, prelucrate în cadrul sistemelor informațional 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 IPȘPG NR. 199 LA PRELUCRAREA DATELOR CU CARACTER

1. Măsurile generale de administrare a securității informaționale

20. 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.
21. Computerele și imprimantele sunt deconectate la terminarea sesiunilor de lucru.
22. Se asigură securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere.
23. Se asigură securitatea și accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul impiedicării vizualizării acesteia de catre persoane neautorizate.
24. 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 directorului.
25. Toate programele utilizate în cadrul sistemului informatic respectă condițiile de licențiere.
26. Este interzisă instalarea programelor, fără aprobarea administratorului sistemului informatic.

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

27. 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 insemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).
28. Directorul instituției asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv reacționează la încălcarea regimului de acces.

29. Perimetrul de securitate a IPȘPG nr. 199 reprezintă perimetru birourilor/cabinetelor în care se prelucrează/stochează datele cu caracter personal (birourile directorului, secretarului, contabilității, cabinetul medical).
30. 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.
31. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri. Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc membrii.
32. Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.
33. Accesul în perimetrul de securitate a cladirii IPȘPG nr. 199 unde se prelucrează/stochează datele 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, prevazut de art. 29 și art. 30 ale Legii 133/2011, privind protecția datelor cu caracter personal, precum și pct. 26 din HG nr. 123/2010, privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.
34. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenței unei permisiuni speciale a conducerii.

3. Identificarea și autentificarea utilizatorilor

35. În instituție este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori.
36. Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conține semnalmentele nivelului de accesibilitate al utilizatorului.
37. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole, bazate pe caracteristici unice și individuale ale persoanei.
38. 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 perioada indelungată, codurile de identificare și autentificare se revocă sau se suspendă de administratorul TI.

4. Identificarea și autentificarea echipamentului

39. Posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal, este asigurată cu menținerea acestor informații pentru o perioada îndelungată.

5. Administrarea identificatorilor utilizatorilor

40. Administrarea identificatorilor utilizatorilor include:
    - identificarea univoca a fiecarui utilizator,
    - verificarea autenticitajii fiecarui utilizator.

6. Utilizarea parolelor în procesul asigurării securității informaționale

41. Regulile de asigurare a securității informaționale sunt respectate 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 marime 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 cu intervalul de 3 luni,
    - dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

7. Controlul administrării accesului

42. Controlul sistematic al acțiunilor utilizatorilor în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor se efectuează prin intermediul sistemelor informaționale de date cu caracter personal.

8. Accesul de la distanță

43. Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sunt securizate, precum și sunt documentate, supuse monitorizării și controlului.

44. Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal este autorizată de persoanele responsabile ale IPȘPG nr. 199 și permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

9. Limitarea folosirii tehnologiilor fără fir

45. Accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului.
46. Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației.
47. Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale IPȘPG nr. 199.

10. Securitatea electroenergetică

48. Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesancționate, prin montarea lor în nișe speciale.
49. 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 deconectarii oricărui component TI.
50. Sistemele automatizate de depistare și semnalizare a incendiilor sunt implementate în birourile unde sînt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

11. Controlul instalării și scoaterii componentelor TI

51. Controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, este exercitat în cadrul sistemelor informaționale de date cu caracter personal utilizate.
52. 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, evitindu-se folosirea funcțiilor standarde de nimicire.

12. Dezvaluirea datelor cu caracter personal

53. 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 prin criptarea acestei informații sau

examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat. 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 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 personala, etc.).

54. Se interzice dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale ce nu corespund cerințelor, (spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.).
55. Se interzic operațiunile de dezvăluire a datelor cu caracter personal între IPȘPG nr. 199 și alte entități care sunt amplasate geografic în stânga Nistrului care refuză să se supună juridic legislației Republicii Moldova, reiesind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei parți teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal conform prevederilor Legii privind protecția datelor cu caracter personal.
56. 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 printr-un acord bilateral între MECC sau DGETS și entitățile din stînga Nistrului, luându-se în considerare necesitatea asigurării unui nivel adecvat de protecție a datelor cu caracter personal.
57. 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.
58. Volumul și categoriile datelor cu caracter personal colectate în scopul ținerii evidenței IPȘPG nr. 199, este limitat la strictul necesar pentru realizarea scopurilor declarate.
59. Accesul la sistemele informaționale gestionate în cadrul IPȘPG nr. 199, din partea Procuraturii Generale (după caz procuraturile teritoriale/specializate), Ministerului Afacerilor Interne, Centrului National Anticoruptie etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 și art. 212, Cod de procedură penală. În conformitate cu prevederile art.157, Cod de procedură penala, documentele în orice formă (scrisă, audio, video, electronică etc.) care provin de la persoane oficiale fizice sau juridice dacă în ele sunt expuse ori adeverite 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 urmarire 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 informațiile oficiale cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informația 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 informația oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informația 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 informație, 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 angajatului din instituție, acesta urmează a fi informat în scris despre obligațiile ce îi revin în conformitate cu prevederile art. 15, Cod de procedura penala, art. 29 și 30 ale Legii privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevazută de art. 741, Cod contravențional.

13.Drepturile subiecților de date cu caracter personal

60. 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 urmatoarele informații, exceptând cazul în care el deține deja informațiile respective:
    - privind identitatea operatorului său, dupa 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 caror 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 intrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația.

61. 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 neincluderii 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 solicitanții își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal.
62. Dreptul de informare este asigurat de către operatorul datelor cu caracter personal tuturor persoanelor supuse prelucrării.
63. 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 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.

14. Stocarea, pastrarea și distrugerea datelor cu caracter personal prelucrate

64. Accesul în spațiile 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.
65. Este interzisă stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sunt conectate la internet și 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.
66. Este interzisă introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu. 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 IPȘPG nr. 199.
67. 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 pastrează 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. Se interzice scoaterea, fără autorizare, a purtatorilor de date cu caracter personal din perimetrul de securitate al operatorului.

15. Auditul sistemelor informational gestionate

68. Înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, se efectuează conform următorilor parametri:
    - data și timpul tentativei intrării/ieșirii;
    - ID-ul utilizatorului;
    - rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.
69. Înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) se efectuează pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform urmatorilor parametri:
    - data și timpul tentativei de obținere a accesului (executate a operațiunii),
    - denumirea (identificatorul) aplicației sau procesului,
    - ID-ul utilizatorului,
    - specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.),
    - tipul operațiunii solicitate (citire, înregistrare, ștergere etc.),
    - rezultatul tentativei de obținere a accesului (executare a operațiunii) — pozitivă sau negativă.
70. Înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, se efectuează 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.
71. 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, se efectuează 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.

16. Asigurarea protecției contra programelor dăunatoare (virușilor)

72. Protecția contra infiltrării programelor dăunatoare în soft-urile destinate prelucrării datelor cu caracter personal este asigurată prin existența programelor licențiate anti-virus.

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

73. Testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal se asigură automat la pornirea sistemului și lunar la solicitarea utilizatorului autorizat în acest scop.

18. Gestionarea incidentelor de securitate

74. 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.
75. Personalul IPȘPG nr. 199 informează neântârziat conducerea despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.
76. Prelucrarea incidentelor include depistarea, analiza, preântâmpinarea dezvoltării, înlaturarea lor și restabilirea securității.

19. Marcarea documentelor

77. Toată informația care se intenționează a fi dezvaluită, și care conține date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidență al operatorilor de date cu caracter personal. Atenție! Documentul conține date cu caracter personal, prelucrate în cadrul sistemului de evidență nr. 000000X-00X, înregistrat în Registrul de evidență al operatorilor de date cu caracter personal www.registru.datepersonale.md.
78. Prelucrarea ulterioară a datelor cu caracter personal poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.

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

79. Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe dupa caz, pentru nerespectarea dispozițiilor Politicii de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 741 Cod contravențional) și penală (art. art. 177, 178, 180 Cod penal).