MINISTERUL
MEDIULUI
AL REPUBLICII MOLDOVA

MINISTRY
OF ENVIRONMENT
OF THE REPUBLIC OF MOLDOVA

ORDIN

mun. Chișinău

„09" decembrie 2021 Nr. 27

Cu privire la aprobarea și punerea în aplicare a Politicii de securitate privind datele cu caracter personal în cadrul Ministerului Mediului

În scopul asigurării respectării Legii nr.133/2011 privind protecția datelor cu caracter personal, Legii nr.982/2000 privind accesul la informații, Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123/2010 și Regulamentul Registrului de evidență al operatorilor de date cu caracter personal, aprobat prin Hotărîrea Guvernului nr.296/2012, precum și în temeiul pct. 7, subpct. 10), pct. 8 subpct. 6) și 14), pct. 9 subpct. 4), 5) și 11) al Regulamentului privind organizarea și funcționarea Ministerului Mediului, aprobat prin Hotărîrea Guvernului nr.145/2021,

ORDON:

1. Se aprobă Politica de securitate privind datele cu caracter personal a Ministerului Mediului, conform anexei.
2. Serviciul tehnologii informaționale și comunicații se desemnează responsabil de implementarea și executarea Politicii privind datele cu caracter personal.
3. Serviciul informare și comunicare cu mass-media va asigura plasarea Politicii de securitate privind datele cu caracter personal pe pagina web a Ministerului.
4. Prezentul Ordin se aduce la cunoștință tuturor angajaților Ministerului Mediului și a autorităților administrative din subordinea Ministerului, iar, controlul asupra executării acestuia mi-l asum.

Ministru **Iuliana CANTARAGIU**

APROBAT

Anexă la Ordinul Ministerului Mediului

Nr. 27 din 09. 12. 2021

POLITICA DE SECURITATE

privind protecția datelor cu caracter personal în cadrul Ministerului Mediului

Chișinău 2021

Cuprins

I. Introducere

1.1. Ministerul Mediului (în continuare – *Minister*) este organul central de specialitate al administrației publice care asigură realizarea politicii guvernamentale în domeniile de activitate care îi sunt încredințate, care funcționează în baza Hotărîrii Guvernului nr.145/2021 cu privire la organizarea și funcționarea Ministerului Mediului.

1.2. Ministerul are sediul înregistrat în mun. Chișinău, bd. Ștefan cel Mare și Sfânt, 162, MD-2004.

1.3. La prelucrarea datelor cu caracter personal în cadrul entității sunt aplicate principiile prevăzute de actele normative:

1) Constituția Republicii Moldova;

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

3) Legea privind accesul la informație nr.982/2000;

4) Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123/2010 (în continuare - Cerințe);

5) Regulamentul Registrului de evidenta al operatorilor de date cu caracter personal, aprobat prin Hotărîrea Guvernului nr.296/2012;

6) alte acte normative de profil.

II. Noțiuni generale

2.1. În prezenta Politică de Securitate, sunt definite/utilizate următoarele noțiuni:

1) *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;

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) *operator* - persoană fizică sau persoană 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;

4) *persoana 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;

5) *autentificare* - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticității;

6) *control de securitate* - acțiuni întreprinse de către operator în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și/sau registrelor ținute;

7) *identificare* - atribuirea unui identificator subiecților și obiectelor de acces și/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

8) *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;

9) *politica de securitate a datelor cu caracter personal* - document, elaborat de către operatorul de date - Minister, 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;

10) *perimetru de securitate* - zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic și/sau tehnic al accesului, la caz, perimetrul de securitate a Ministerului reprezintă perimetru oficiilor în care se prelucrează/stochează date cu caracter personal;

11) *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 deținătorului de date cu caracter personal;

12) *protecția informației contra acțiunilor neintenționate* - ansamblu de masuri 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;

13) *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 păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia;

14) *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;

15) *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;

16) *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;

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, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

18) *stocare* - păstrarea pe orice fel de suport a datelor cu caracter personal;

19) *sistem de evidență a datelor cu caracter personal* - orice serie structurata de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice;

20) *consimțământul subiectului datelor cu caracter personal* - orice manifestare de voință libera, expresă și necondiționată, în formă scrisă sau electronică, conform cerințelor documentului electronic, prin care subiectul datelor cu caracter personal accepta să fie prelucrate datele care îl privesc;

III. Obiectivele Politicii de Securitate

3.1. Obiectivele principale ale Politicii de Securitate sunt disponibilitatea, integritatea și confidențialitatea tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de Minister, atât în cadrul prelucrării manuale, cât și sistemelor și proceselor de tehnologie informațională. Securitatea reprezintă o componentă esențiala a derulării optime a proceselor bazate pe TI în cadrul Ministerului. Baza unei securități TI adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerințe și reguli pentru protecția tuturor informațiilor, inclusiv datelor 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 nemateriale, sau care pot duce la încălcări ale legislației. Având în vedere că siguranța TI nu poate fi garantata exclusiv cu ajutorul unor sisteme tehnice, prezenta Politica vizează, de asemenea, aspecte de ordin organizatoric-juridic și de altă natură.

3.2. Ministerul va proteja datele cu caracter personal ale angajaților săi, a candidaților la funcțiile vacante, a vizitatorilor precum și ale altor persoane ale căror date cu caracter personal vor fi prelucrate de către Minister.

3.3. Reglementările prezentei Politici de Securitate reprezintă un standard minim pentru Minister, inclusiv pentru toți angajații acestuia. Pornind de la această reglementare, toți salariații urmează să respecte strict prevederile Politicii de Securitate și regulile interne ale Ministerului privind protecția datelor cu caracter personal.

IV. Dispoziții privind ierarhia și responsabilitatea persoanei responsabile de Politica de Securitate

4.1. Politica de Securitate, în mod obligatoriu va fi adusa la cunoștință, sub semnătură, tuturor angajaților responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la

prelucrarea datelor cu caracter personal, inclusiv şi la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.

4.2. Persoana responsabilă de implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal este numita prin ordinul Ministrului şi va avea acces liber la informaţia necesara pentru îndeplinirea funcţiilor sale în măsură în care aceasta nu operează în afara cadrului acestei politici şi se subordonează nemijlocit ministrului Mediului sau persoanei care îndeplineşte interimatul funcţiei.

V. Descrierea procedurilor (organizatorice şi tehnice) de prelucrare şi de securitate

5.1. Mijloace supuse principiilor de protecţie a datelor cu caracter personal:

Sunt supuse protecţiei prin mijloace/procedee specifice, toate resursele informaţionale ale operatorului de date cu caracter personal gestionate, care conţin date cu caracter personal, păstrate pe:

1) suporturi magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale şi baze de date;

2) sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date şi alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informaţiei.

Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin:

1) preîntâmpinarea conexiunilor neautorizate la reţelele comunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;

2) excluderea accesului neautorizat la datele cu caracter personal prelucrate;

3) preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;

4) preîntâmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;

5) preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătura, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum şi utilizarea canalelor virtuale protejate (VPN);

6) preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor anti-virus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodica a copiilor de siguranţă;

7) preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaţionale, care se efectuează permanent;

8) stabilirea exacta a ordinii de acces la informaţia care conţine date cu caracter personal, prelucrate în cadrul sistemelor informaţionale şi de evidenta instituite atât pentru utilizatorii interni cât şi pentru cei externi.

5.2. Măsurile generale de administrare a securităţii informaţionale:

1) În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.

2) Computerele, terminalele de acces şi imprimantele sunt deconectate la terminarea sesiunilor de lucru.

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

4) Este asigurată securitatea şi accesul fizic la mijloacele de reprezentare a informaţiei care conţine date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.

5) Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine 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.

6) Toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere.

7) Este interzisă instalarea programelor de tip shareware sau freeware, fără aprobarea administratorului sistemului informatic.

5.3. Autorizarea accesului fizic:

1) Accesul în sediile/oficiile/birourile ori spaţiile unde sunt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar angajaţilor Ministerului sau vizitatorilor care sunt legitimaţi în prealabil, şi doar în timpul orelor de program, conform listei şi însemnelor corespunzătoare, pentru preîntâmpinarea accesului persoanelor neautorizate, fiind însoţiţi pe toata durata vizitei.

2) Accesul neautorizat în perimetrul de securitate a sediului Ministerului, unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video este interzis, ţinând cont de necesitatea asigurării regimului de confidenţialitate şi securitate a prelucrării datelor cu caracter personal, prevăzut de Legea privind protecţia datelor cu caracter personal şi Cerinţele fata de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale.

5.4. Administrarea şi monitorizarea accesului fizic:

1) Ministerul asigură administrarea şi monitorizarea accesului fizic în toate punctele de acces la sistemele informaţionale de date cu caracter personal, inclusiv se reacţionează la încălcarea regimului de acces. Înainte de acordarea accesului fizic la sistemele informaţionale şi/sau la registrele de date cu caracter personal, se verifica drepturile de acces ale fiecărui solicitant.

2) Perimetrul încăperilor în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sunt rezistenţi, intrările sunt echipate cu lacăte şi/sau semnalizare. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri. Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc angajaţii. Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.

3) Sunt utilizate mijloace automatizate care asigură identificarea cazurilor de acces neautorizat şi iniţierea acţiunilor de blocare a accesului, precum şi de stocare a informaţiilor privind tentativele de acces neautorizat.

4) Accesul vizitatorilor (persoanelor terţe) se va asigura în conformitate cu regulile prevăzute de legislaţia în vigoare cu privire la protecţia datelor cu caracter personal.

5) Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisa doar în cazul prezenţei unei permisiuni speciale a conducerii sau în conformitate cu procedura stabilită în Regulamentul privind supravegherea prin mijloace video.

5.5. Asigurarea protecţiei datelor cu caracter personal:

1) Salariaţii care în activitatea lor profesională intră în contact cu date considerate cu caracter personal sunt obligaţi să păstreze confidenţialitatea datelor şi să respecte întocmai prevederile cadrului normativ cu privire la protecţia datelor cu caracter personal.

2) Obligaţia privind păstrarea confidenţialităţii datelor cu caracter personal rămâne valabilă atât în cazul angajării sau transferării la un loc de muncă în cadrul Ministerului, precum şi după încetarea raportului de muncă.

3) Dispoziţiile prezentului articol se aplica, în acelaşi mod, pentru toate informaţiile deţinute de Minister referitoare la terţi, despre care salariatul ia cunoştinţă în cadrul activităţii sale.

5.6. Prelucrarea datelor cu caracter personal:

1) Este interzisă prelucrarea datelor cu caracter personal fără consimţământul subiectului datelor cu caracter personal, cu excepţia cazurilor prevăzute de legislaţia în vigoare.

2) Politica de securitate, în mod obligatoriu va fi adusă la cunoştinţă, sub semnătură, tuturor angajaţilor responsabili de prelucrarea datelor cu caracter personal, înaintea acordării accesului la prelucrarea datelor cu caracter personal, inclusiv şi la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecţie a datelor cu caracter personal.

3) La încheierea operaţiunilor de prelucrare a datelor cu caracter personal, dacă subiectul acestor date nu şi-a dat consimţământul pentru o altă destinaţie, pentru stocare sau pentru o prelucrare ulterioara, acestea vor fi distruse, transferate sau transformate şi stocate conform legislaţiei in vigoare.

5.7. Identificarea şi autentificarea utilizatorilor:

1) În cazul accesului la o bază de date deţinută pe un suport fizic, identificarea persoanei va fi efectuată de către persoana care deţine baza, cu înregistrarea obligatorie a numelui, prenumelui, funcţia,

data şi scopul solicitării de acces.

2) Utilizatorii, pentru a căpăta acces la o bază de date cu caracter personal prelucrată în sistemele TI şi deținută de Minister, trebuie să se identifice. Identificarea se va face prin introducerea unui cont de utilizator (sau „user-name") şi a parolei asociate respectivului cont de utilizator (parola de peste 8 caractere ce va fi formată din mai multe tipuri de caractere, respectiv cifre, litere şi caractere speciale).Identificarea utilizatorilor se poate face prin introducerea codului de identificare de la tastatură (un sir de caractere).

3) Fiecărui utilizator ce i se va permite accesul la bazele de date cu caracter personal ale Ministerului va avea propriul său user-name şi parolă, care vor fi unice la nivelul Ministerului. Administrarea identificatorilor utilizatorilor include (i) identificarea univoca a fiecărui utilizator, şi (ii) verificarea autenticității fiecărui utilizator.

4) User-name-urile nefolosite o perioadă mai îndelungata vor fi dezactivate şi distruse după un control prealabil intern al Operatorului. Această perioada după care conturile de utilizator vor fi dezactivate şi distruse este de maxim 90 de zile de la data ultimului acces (login) a respectivului utilizator. 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 perioada îndelungată, codurile de identificare şi autentificare se revocă sau se suspendă de administratorul TI.

5) Toţi utilizatorii se vor autentifica la conectare la bazele de date cu caracter personal ale Ministerului având în vedere faptul că sistemul informatic va refuza automat accesul utilizatorului la introducerea greşită a parolei.

6) Orice utilizator care primeşte un cont de utilizator şi o parolă asociată este obligat să respecte următoarele reguli:

- păstrarea confidențialității stricte a acestora, în caz contrar urmând să răspundă în fața Ministerului disciplinar, civil, penal etc., după caz, în conformitate cu legislația;
- 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 caractere, care nu sunt legate de informația cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sunt compuse integral din grupuri de cifre sau litere;
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

7) Ministerul administrează şi gestionează conturile de utilizator (şi implicit parolele asociate) ținând cont de prezenta Politică.

8) Ministerul va autoriza doar anumiți utilizatori pentru a revoca sau a suspenda un cont de utilizator şi parola asociată respectivului cont, dacă raporturile de serviciu cu utilizatorul au fost suspendate sau încetate, acesta a fost transferat în alt departament şi noile sarcini nu îi solicită accesul la date cu caracter personal, a abuzat de codurile primite sau dacă a absentat o perioada îndelungata (mai mult de 3 luni).

9) Accesul utilizatorilor la bazele de date cu caracter personal efectuate manual se va face pe baza unei liste aprobate de persoana responsabilă din cadrul Ministerului.

10) Drepturile de acces ale utilizatorilor la bazele de date cu caracter personal sunt revizuite/controlate cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate şi/sau după oricare schimbare de statut al utilizatorului. Controlul sistematic al acțiunilor utilizatorilor este, de asemenea, efectuat în vederea evaluării corectitudinii şi conformării operațiunilor şi acțiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

11) Accesul la funcțiile de securitate ale sistemelor informaţionale de date cu caracter personal şi la datele acestora este acordat în mod special doar persoanelor responsabile ale Operatorului, desemnate conform prevederilor prezentei Politici.

12) Sesiunea de lucru în sistemul informațional, destinat prelucrării datelor cu caracter personal, se blochează (la solicitarea utilizatorului sau în mod automat, după expirarea perioadei prestabilite de inactivitate a utilizatorului), fapt care face imposibil accesul de mai departe până în momentul când utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare şi autentificare.

5.8. Identificarea si autentificarea echipamentului:

Este asigurată posibilitatea identificării şi autentificării echipamentului folosit în operaţiunile de prelucrare a datelor cu caracter personal, cu menţinerea acestor informaţii pentru o perioada îndelungată.

5.9. Controlul administrării accesului:

Este efectuat controlul sistematic al acţiunilor utilizatorilor în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

5.10. Tipurile de acces:

5.10.1. Accesul de la distanţă:

1) Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizând-se VPN, criptarea, cifrarea etc.), precum şi sunt documentate, supuse monitorizării şi controlului.

2) Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal este autorizată de persoanele responsabile ale Ministerului şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

3) Accesul fără fir la sistemele informaţionale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării şi controlului. Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei. Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile a Ministerului.

5.10.2. Administrarea accesului portativ şi mobil

1) Pentru toate categoriile sistemelor informaţionale de date cu caracter personal sunt stabilite limitări şi sunt elaborate reguli de folosire a echipamentului portativ şi mobil care permit accesul la sistemele informaţionale de date cu caracter personal.

2) Accesul la sistemele informaţionale de date cu caracter personal cu folosirea echipamentului portativ şi mobil se documentează, este monitorizat şi controlat.

3) Folosirea echipamentului portativ şi mobil este autorizată de persoanele responsabile ale deţinătorului de date cu caracter personal.

5.11. Securitatea electroenergetică:

1) Echipamentul electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor şi conectărilor nesancţionate, prin montarea lor în nişe speciale.

2) În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, este asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

3) Sunt implementate sisteme automatizate de depistare şi semnalizare a incendiilor în birourile unde sunt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

4) Sunt prevăzute surse alternative de alimentare cu energie electrica de scurtă durată, care sunt folosite pentru terminarea corectă a sesiunii de lucru a sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică.

5.12. Controlul instalării şi scoaterii componentelor TI:

1) Este exercitat controlul şi evidenţa instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program utilizate în cadrul sistemelor informaţionale de date cu caracter personal.

2) Informaţiile, care conţin date cu caracter personal şi care se conţin pe purtătorii de informaţii, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitând-se folosirea funcţiilor standarde de nimicire.

5.13. Colectarea datelor cu caracter personal:

1) Ministerul colectează datele cu caracter personal de la subiecţii datelor cu caracter personal, cu informarea acestora despre categoriile de date şi scopul prelucrării datelor cu caracter personal. În acest sens, fiecare subiect al datelor cu caracter personal îşi exprimă consimţământul conform legislaţiei în vigoare.

2) Utilizatorii autorizaţi pentru operaţiile de colectare şi introducere de date cu caracter personal într-un sistem informaţional sunt desemnaţi de Ministrul Mediului.

3) Orice modificare a datelor cu caracter personal se poate face numai de către utilizatori

autorizați desemnați de Operator. Sistemul informațional va înregistra cine a făcut modificarea, data și ora modificării.

4) Nomenclatorul datelor cu caracter personal este indicat de către Minister în fiecare regulament care vizează sistemele notificate Centrului National pentru Protecția Datelor cu Caracter Personal. În cazul prelucrării unor date cu caracter personal suplimentare, Ministerul va efectua modificările de rigoare în regulamentele sistemelor notificate, cu informarea Centrului National pentru Protecția Datelor cu Caracter Personal.

5) Datele personale ale subiecților datelor cu caracter personal pot fi supuse următoarelor metode de prelucrare: colectare, înregistrare, organizare, stocare, păstrare, restabilire, adaptare ori modificare, extragere, consultare, utilizare, dezvăluire prin transmitere, diseminare sau în orice alt mod, alăturare ori combinare, blocare, ștergere sau distrugere, transmitere către autoritățile publice competente în conformitate cu legislația în vigoare și transmitere transfrontalieră.

6) În conformitate cu prevederile legislației în vigoare, subiectul datelor cu caracter personal este informat asupra drepturilor pe care le are în legătură cu prelucrarea datelor sale personale, în special despre:

- dreptul de acces la datele cu caracter personal;
- dreptul de intervenție asupra datelor cu caracter personal;
- dreptul de opoziție al subiectului datelor cu caracter personal;
- dreptul de a nu fi supus unei decizii individuale;
- alte drepturi.

7) În cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, este necesară informarea persoanei (exceptând cazul în care el deține deja informațiile respective) cu privire la:

- identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (denumirea, adresa juridica, IDNO-ul, numărul de înregistrare în Registrul de evidenta al operatorilor de date cu caracter personal);
- scopul concret al prelucrării datelor cu caracter personal colectate;
- destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- existenta 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 datorita 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.

8) 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.

9) Dreptul de informare este asigurat de către Minister în calitate de operatorul datelor cu caracter personal (sau entitățile ce asigură mentenanța sistemului Ministerului) tuturor persoanelor supuse prelucrării.

10) 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 civila, resurse informaționale principale de stat etc.), modificarea urmând a fi efectuata în toate sistemele informaționale și de evidență gestionate.

11) Ministerul va desemna utilizatorii autorizați pentru operațiile de colectare și introducere de date cu caracter personal într-un sistem informațional, urmând ca orice modificare a datelor cu caracter personal să fie efectuată numai de către respectivii utilizatori autorizați desemnați de Minister.

12) Sistemul informațional din cadrul Ministerului înregistrează, în permanență, cine a făcut modificarea, data și ora modificării și asigură menținerea în mod separat a datelor șterse sau modificate, fără ca acestea din urma să interfereze în vreun fel cu informațiile actualizate.

13) Datele personale pot fi dezvăluite, în condiţiile legii, către subiecţii datelor cu caracter personal, autorităţi publice centrale/locale, servicii sociale sau de sănătate, reprezentanţii legali ai subiecţilor datelor cu caracter personal, alte entităţi care oferă garanţii suficiente de protecţie a datelor personale.

14) Prelucrarea datelor cu caracter personal de către Minister va fi efectuată pe o perioadă care nu va depăşi durata necesară atingerii scopurilor pentru care acestea sunt prelucrate. După expirarea acestei perioade, datele cu caracter personal vor fi păstrate în formă arhivată în conformitate cu Indicatorul documentelor-tip şi al termenelor lor de păstrare pentru organele administraţiei publice, pentru instituţiile, organizaţiile şi întreprinderile Republicii Moldova, aprobat prin Ordinul nr.57 din 27.07.2016 al Serviciului de Stat de Arhiva.

5.14. Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate:

1) Stocarea şi păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidenţă, în computere care sunt conectate la internet, nu sunt echipate cu mijloace de protecţie speciale tehnice şi de program şi nu au instalate programe licenţiate, programe antivirus, sisteme de control al securităţii soft-ului, de asigurare a efectuării periodice a copiilor de siguranţa şi de efectuare a auditului - este interzisă.

2) Introducerea în perimetrul de securitate instituţional şi utilizarea calculatoarelor personale ori a purtătorilor de informaţii în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sunt protejate/restricţionate prin crearea profilurilor de utilizatori, iar drepturile de administrator sunt încredinţate doar persoanei responsabile desemnate din cadrul Ministerului.

3) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hârtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul şi 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 Ministerului este interzisă.

5.15. Dezvăluirea datelor cu caracter personal:

1) Dezvăluirea informaţiilor ce conţin date cu caracter personal în format electronic conţinute în sistemele de evidenţă, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată prin criptarea acestei informaţii sau examinarea posibilităţii utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidenţă a datelor cu caracter personal este permis doar utilizatorilor autorizaţi. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronica va fi examinat separat, reieşind din posibilităţile tehnice asigurate de destinatar şi Minister în calitate de operator de date cu caracter personal, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi. În cazul în care reţelele comunicaţionale prezinta riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere (expediere poştală cu aviz recomandat, înmânarea personală, etc.).

2) Dezvăluirea prin transmitere a datelor cu caracter personal prin reţele comunicaţionale ce nu corespund Cerinţelor, (spre exemplu: expedierea informaţiei prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com) etc, sunt interzise, cu excepţia cazurilor în care are loc transmiterea datelor cu caracter personal în adresa subiectului de date.

3) Sunt interzise operaţiunile de dezvăluire a datelor cu caracter personal între Minister şi alte entităţi care sunt amplasate geografic în stânga Nistrului care refuză să se supună juridic legislaţiei Republicii Moldova, reieşind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părţi teritoriale, inclusiv în partea ce tine de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecţia datelor cu caracter personal.

4) Transmiterea transfrontaliera a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile Legii privind protecţia datelor cu caracter personal, în special în cazurile când tratatul internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.

5) Volumul şi categoriile datelor cu caracter personal colectate în scopul tinerii evidentei Ministerului, este limitat la strictul necesar pentru realizarea scopurilor declarate.

6) Accesul la sistemele informaţionale gestionate în cadrul Ministerului, din partea agenţilor constatatori pe marginea cauzelor contravenţionale, organelor de urmărire penală sau instanţelor de judecată, va fi permisă doar în cazul în care solicitarea va corespunde prevederilor şi procedurilor prevăzute de legislaţie.

5.16. Computerele şi terminalele de acces:

1) Computerele şi terminalele de acces la informaţiile stocate au bazele în camere restricţionate şi securizate, la care au acces doar angajaţii numiţi prin ordinul ministrului Mediului. Acestea sunt protejate prin parole, iar bazele de date electronice sunt păstrate pe servere independente, sigure, localizate în zone controlate şi protejate.

2) Accesul la computere/terminale se face pe baza combinaţiei user/parolă.

3) În cazul monitoarelor pe al căror ecran apar date cu caracter personal asupra cărora nu se acţionează o perioada de maxim 15 (cincisprezece) minute, sesiunea de lucru se închide automat.

5.17. Auditul sistemelor informaţionale gestionate:

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

- data şi timpul tentativei intrării/ieşirii;
- ID-ul utilizatorului;
- rezultatul tentativei de intrare/ieşire - pozitivă sau negativă.

2) Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

- data şi timpul tentativei de obţinere a accesului (executate a operaţiunii),
- denumirea (identificatorul) aplicaţiei sau procesului, ori ID-ul utilizatorului,
- specificaţiile resursei protejate (identificator, nume logic, nume fişier, număr etc.),
- tipul operaţiunii solicitate (citire, înregistrare, ştergere etc.),
- rezultatul tentativei de obţinere a accesului (executare a operaţiunii) — pozitivă sau negativă.

3) Este efectuată înregistrarea modificărilor drepturilor de acces (competentelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:

- data şi timpul modificării competenţelor,
- ID-ul administratorului care a efectuat modificările,
- ID-ul utilizatorului şi competenţele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.

5.17.1. Se efectuează înregistrarea ieşirii din sistem a informaţiei care confinez date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecţilor şi statutul obiectelor de acces, conform următorilor parametri:

- data şi timpul eliberării,
- denumirea informaţiei şi căile de acces la aceasta,
- specificarea echipamentului (dispozitivului) care a eliberat informaţia (numele logic),
- ID-ul utilizatorului, care a solicitat informaţia.

5.18. Asigurarea protecţiei contra programelor dăunătoare (virusilor):

Este asigurata protecţia contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, prin existenta programelor licenţiate anti-virus.

5.19. Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal:

Se asigură testarea funcţionării corecte a sistemelor informaţionale de date cu caracter personal (automat la pornirea sistemului şi lunar la solicitarea utilizatorului autorizat în acest scop).

5.20. Gestionarea incidentelor de securitate:

1) Personalul Ministerului informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

2) În cazul producerii incidentelor de securitate în cadrul Ministerului, persoana responsabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia şi va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului National pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova.

3) În cadrul controalelor efectuate de Centrul National pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova, angajaţilor acestuia li se vor oferi suportul necesar şi li se va asigura accesul la informaţiile necesare relevante obiectului controlului, conform prevederilor legale în vigoare.

4) Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc şi se documentează în regim permanent prin mijloace automatizate. Prelucrarea incidentelor

include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.

5) Personalul care asigura exploatarea sistemelor informaţionale de date cu caracter personal trece instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.

6) Personalul întreprinderii informează neîntârziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.

7) Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea, înlăturarea şi restabilirea securităţii.

8) Până la 31 ianuarie a fiecărui an, Ministerul informează în scris Centrul National pentru Protecţia Datelor cu Caracter Personal despre incidentele de securitate constatate.

5.21. Marcarea documentelor:

1) Toata informaţia care se intenţionează a fi dezvăluita, şi care conţine date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidenţă al operatorilor de date cu caracter personal, conform următorului model:

2) Atenţie! Documentul conţine date cu caracter personal, prelucrate în cadrul sistemului de evidenţă nr.000000X-00X, înregistrat în Registrul de evidenta al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioara a acestor date poate fi efectuată numai în condiţiile prevăzute de Legea privind protecţia datelor cu caracter personal.

5.22. Responsabilitatea pentru asigurarea securităţii datelor cu caracter personal precum şi a informaţiilor cu accesibilitate limitata:

1) Pentru nerespectarea prevederilor dispoziţiilor Politicii de securitate, persoanele vinovate sunt pasibile de răspundere civila, contravenţionala sau penală, după caz.

2) Drepturile subiecţilor de date cu caracter personal:

În cazul în care datele cu caracter personal sunt colectate direct de la subiectul acestor date, în conformitate cu prevederile Legii privind protecţia datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informaţii, exceptând cazul în care el deţine deja informaţiile respective:

- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator *(denumirea, adresa juridica, IDNO-ul, numărul de înregistrare in Registrul de evidenţă 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;
- existenta drepturilor la informare şi de acces la datele colectate; de intervenţie asupra datelor *(în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora)* şi de opoziţie, precum şi condiţiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sunt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia.

3) Subiecţilor de date cu caracter personal le este asigurat dreptul de acces şi posibilitatea de a lua cunoştinţă cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi 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 vizate nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alţi subiecţi, conţinute în fişele personale (alte materiale), cu excepţia cazurilor în care solicitanţii îşi realizează un interes legitim care nu prejudiciază interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal.

4) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (sau entităţile ce asigura menţinerea sistemului) tuturor persoanelor supuse prelucrării.

5) În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenţie, datele inexacte vor fi actualizate prin rectificare sau ştergere, ca bază servind doar surse legale (acte de identitate, de stare civila, resurse informaţionale principale de stat etc), modificarea urmând a fi efectuată în toate sistemele informaţionale şi de evidenţă gestionate.