**APROBAT**

**Prin Ordin nr. \_\_\_\_ din**

**\_\_\_\_\_\_\_\_\_\_\_\_ 2018**

**Semnătura și Ștampila**

**POLITICA DE SECURITATE**

**PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL LA PRELUCRAREA ACESTORA ÎN CADRUL SISTEMELOR INFORMAȚIONALE GESTIONATE DE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. **Preambul**

La prelucrarea datelor cu caracter personal în cadrul entității sunt aplicate principiile prevăzute de actele **internaționale** - [**Declaraţia universală a drepturilor omului**](http://datepersonale.md/md/international004/), [**Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale**](http://datepersonale.md/md/international005/)**,** [Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal](http://datepersonale.md/md/international003/) și a celor **naționale** – Constituția Republicii Moldova, Legea privind protecția datelor cu caracter personal, Legea privind accesul la informație, Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010, Regulamentului Registrului de evidenţă al operatorilor de date cu caracter personal, aprobat prin Hotărîrea Guvernului nr. 296 din 15 mai 2012 și alte acte legislative/normative de profil.

1. Introducere

\_\_\_\_\_\_\_ are sediul înregistrat în \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, mun. \_\_\_\_\_\_ Republica Moldova.

Politica este aprobată de către \_\_\_\_\_\_\_, care acționează în baza legislației: Codul de procedură civilă, \_\_\_\_\_\_\_\_\_\_\_\_.

Prezenta Politică este aprobată, inclusiv, în vederea conformării \_\_\_\_\_\_\_\_ 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".

1. **NOŢIUNI GENERALE**

În prezenta Politică de Securitate, sînt definite/utilizate următoarele noţiuni:

***date cu caracter personal***– orice informaţie 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 identităţii sale fizice, fiziologice, psihice, economice, culturale sau sociale;  
***categorii speciale de date cu caracter personal***– datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenenţa socială, datele privind starea de sănătate sau viaţa sexuală, precum şi cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancţiunile contravenţionale;

***operator***– persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituţie ori organizaţie care, în mod individual sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislaţia în vigoare;  
***persoană împuternicită de către operator*** – persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele şi pe seama operatorului, pe baza instrucţiunilor primite de la operator;

***autentificare*** *-* verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;

***control de securitate*** *-* acţiuni întreprinse de către \_\_\_\_\_\_\_\_\_\_\_ în vederea asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi/sau registrelor ţinute;

***fişiere temporare*** *-* ansamblu de date sau informaţii pe suport digital creat pentru o perioadă de timp limitat pînă la iniţierea îndeplinirii sarcinilor pentru care au fost desemnate;

***identificare*** *-* atribuirea unui identificator subiecţilor şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

***integritate*** *-* certitudinea, necontradictorialitatea şi actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere şi modificare neautorizată;

***mijloace de protecţie criptografică a informaţiei care conţine date cu caracter personal*** — mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează algoritmi de conversie criptografică a informaţiei care conţine date cu caracter personal, destinate să asigure integritatea şi confidenţialitatea informaţiei în procesul de prelucrare, depozitare şi transmitere a acesteia prin canalele de comunicaţii;

***nivel de protecţie*** *-* nivel de securitate proporţional riscului pe care îl comportă prelucrarea faţă de datele cu caracter personal respective, precum şi faţă de drepturile şi libertăţile persoanelor, elaborat şi actualizat corespunzător nivelului dezvoltării tehnologice şi costurilor implementării acestor măsuri;

***politica de securitate a datelor cu caracter personal -*** document, elaborat de către operatorul de date – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecţie selectate pentru securitatea datelor, ţinîndu-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sînt expuse acestea;

***perimetru de securitate —*** zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control fizic şi/sau tehnic al accesului;

***persoana responsabilă de politica de securitate a datelor cu caracter personal —*** persoana responsabilă de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei care conţine date cu caracter personal, precum şi de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a deţinătorului de date cu caracter personal;

***protecţia informaţiei contra acţiunilor neintenţionate —*** ansamblu de măsuri orientate spre prevenirea acţiunilor neintenţionate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informaţiei, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informaţie, precum şi la pierderea, distrugerea acesteia sau la defectarea suportului material al informaţiei care conţine date cu caracter personal;

***purtător de date cu caracter personal*** - suport magnetic, optic, laser, de hîrtie 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;

***restaurarea datelor*** - procedurile cu privire la reconstituirea/prestabilirea datelor cu caracter personal în starea în care se aflau pînă la momentul pierderii sau distrugerii acestora;

***tehnologie informaţională*** *-* totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei care conţine date cu caracter personal şi regulile de aplicare a acesteia;

***utilizator*** – persoana care acţionează sub autoritatea deţinătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal;

***sesiune de lucru*** — perioada care durează din momentul pornirii calculatorului şi aplicaţiei de utilizare a resursei informaţionale sau din momentul pornirii resursei informaţionale şi pînă la momentul opririi acestora;

***sistem informaţional de date cu caracter personal -*** totalitatea resurselor şi tehnologiilor informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie care conţine date cu caracter personal;

***prelucrarea datelor cu caracter personal*** – orice operaţiune sau serie de operaţiuni 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, ştergerea sau distrugerea;

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

***sistem de evidenţă a datelor cu caracter personal*** – orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcţionale sau geografice;

***consimţămîntul subiectului datelor cu caracter personal***– orice manifestare de voinţă liberă, expresă şi necondiţionată, în formă scrisă sau electronică, conform cerinţelor 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 încît detaliile privind circumstanţele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condiţiile unei investigaţii care necesită cheltuieli disproporţionate de timp, mijloace şi forţă de muncă.

1. **Obiectivile Politicii de Securitate**

Obiectivele principale ale Politicii sunt disponibilitatea, integritatea şi confidenţialitatea tuturor informaţiilor, inclusiv datelor cu caracter personal prelucrate de \_\_\_\_\_\_\_\_\_\_\_\_\_\_, atît în cadrul prelucrării manuale, cît și sistemelor şi proceselor de tehnologie informațională. Securitatea reprezintă o componentă esenţială a derulării optime a proceselor bazate pe IT în cadrul \_\_\_\_\_\_\_\_\_\_. Baza unei securităţi IT adecvate o constituie respectarea prezentei Politici. Aceasta cuprinde cerinţe şi reguli pentru protecţia tuturor informaţiilor, inclusiv datele cu caracter personal, sistemelor şi proceselor IT împotriva influenţelor naturale, erorilor umane şi tehnice, precum şi împotriva acţiunilor deliberate care pot provoca pagube materiale, respectiv imateriale, sau care pot duce la încălcări ale legislației. Avînd în vedere că siguranţa IT nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic şi de altă natură.

\_\_\_\_\_\_\_\_\_\_\_va proteja datele cu caracter personal atît a participanților la proces/vizitatori, cît și a angajaților săi.

Reglementările prezentei Politici reprezintă un standard minim pentru \_\_\_\_\_\_\_\_\_\_, inclusiv toți angajații \_\_\_\_\_\_\_\_\_\_\_\_\_\_. Pornind de la această reglementare, toți angajații \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ urmează să respecte strict prevederile Politicii și regulilor interne ale \_\_\_\_\_\_\_\_\_\_\_\_\_\_ privind protecția datelor cu caracter personal și sistemelor IT.

1. **Dispoziții privind ierarhia și responsabilitatea persoanei responsabile de Politica de securitate**

Operatorul de date cu caracter personal reieşind din specificul activităţii, 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.

Politica de securitate a datelor cu caracter personal se va revizui cel puţin o dată în an ca rezultat al modificărilor sau reevaluării competențelor entității, fiind pusă în sarcina conducătorilor, de a desemna persoana/ele care vor purcede nemijlocit la ajustarea prevederilor prezentului act.

Politica de securitate, în mod obligatoriu va fi adusă la cunoștință, sub semnătură, 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 asigurării nivelului adecvat de protecție a datelor cu caracter personal.

Responsabil de implementarea şi 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 şi buget) şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

Persoana responsabilă desemnată, indiferent de funcțiile exercitate, în cadrul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit conducătorului \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ sau persoanei care îndeplinește interimatul funcției.

Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilităţi 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.

Persoana responsabilă de politica de securitate a datelor cu caracter personal va defini clar responsabilităţile şi procesele de management al securităţii datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizaţională şi de funcţionare generală, va asigura măsuri tehnice şi organizaţionale necesare organizării procesului de management al securităţii datelor cu caracter personal, va elabora procedurile de clasificare a informaţiei care conţine date cu caracter personal astfel încît să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sînt 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 atribuţiilor funcţionale şi asumării responsabilităţilor de securitate a datelor cu caracter personal, inclusiv asupra confidenţialităţii acestora.

1. **Mijloacele supuse principiilor de protecție a datelor cu caracter personal**

Protecţia datelor cu caracter personal în cadrul \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (în calitate de operator de date cu caracter personal) este asigurată printr-un complex de măsuri tehnice şi organizatorice de preîntîmpinare a prelucrării ilicite a datelor cu caracter personal.

Sînt 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:

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

- 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.

1. **Măsurile de protecţia datelor cu caracter personal sînt asigurate în scopul:**

* preîntîmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
* preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele telecomunicaţionale şi resursele informaţionale;
* neadmiterea dezvăluirii terților a informației cu accesibilitate limitată;
* eficientizarea resurselor informaționale atît pe suport de hîrtie cît și cel în format electronic.

1. **Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:**

* preîntâmpinarea conexiunilor neautorizate la reţelele telecomunicaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele,
* excluderea accesului neautorizat la datele cu caracter personal prelucrate;
* preîntîmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program,
* preîntîmpinarea 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,
* preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, precum și utilizarea canalelor VPN,
* preîntîmpinarea 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 antivirus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă,
* preîntîmpinarea scurgerii de informaţii care conţin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaționale, care se efectuează permanent.
* stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență instituite atît pentru utilizatorii interni cît și pentru cei externi.

1. **Procedurile organizatorice și tehnice care urmează a fi respectate în cadrul** \_\_\_\_\_\_\_\_\_\_\_\_\_ **la prelucrarea datelor cu caracter personal**
2. **Măsurile generale de administrare a securităţii informaţionale**
3. În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hîrtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeuri sau dulapuri metalice care se încuie.
4. Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru.
5. Este asigurată securitatea punctelor de primire/expediere a corespondenţei, precum şi securitatea contra accesului neautorizat la aparatele fax şi de copiere.
6. 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.
7. Mijloacele de prelucrare a datelor cu caracter personal, informaţia care conţine date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.
8. Toate programele utilizate în cadrul sistemului informatic respectă condiţiile de licenţiere.
9. Este interzisă instalarea programelor de tip Shareware sau freeware, fară aprobarea administratorului sistemului informatic.
10. **Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal**
11. Accesul în sediile/oficiile/birourile ori spaţiile unde sînt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară, conform listei sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).
12. Se 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.
13. Perimetrul de securitate a \_\_\_\_\_\_\_\_\_\_\_ reprezintă perimetru oficiilor în care se prelucrează/stochează date cu caracter personal.
14. Perimetrul clădirii sau încăperilor în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereţii exteriori ai încăperilor sînt rezistenţi, intrările sunt echipate cu lacăte şi semnalizare.
15. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.
16. Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc membrii.
17. Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.
18. Accesul în perimetrul de securitate a clădirii \_\_\_\_\_\_\_\_\_\_\_ unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ţinînd cont de necesitatea asigurării regimului de confidenţialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de art. 29 și art. 30 ale Legii privind protecţia datelor cu caracter personal, precum şi pct. 26 din Cerinţe.
19. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenţei unei permisiuni speciale a conducerii.
20. **Identificarea şi autentificarea utilizatorilor**
21. Este efectuată identificarea şi autentificarea utilizatorilor sistemelor informaţionale de date cu caracter personal şi a proceselor executate în numele acestor utilizatori.
22. Toţi utilizatorii (inclusiv personalul care asigură susţinerea tehnică, administratorii de reţea, programatorii şi administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu conţine semnalmentele nivelului de accesibilitate al utilizatorului.
23. Pentru confirmarea ID-ului utilizatorului sînt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice şi individuale ale persoanei.
24. 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 se revocă sau se suspendă de administratorul I.T.
25. **Identificarea şi autentificarea echipamentului**

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

1. **Administrarea identificatorilor utilizatorilor**

Administrarea identificatorilor utilizatorilor include:

* identificarea univocă a fiecărui utilizator,
* verificarea autenticităţii fiecărui utilizator.

1. **Utilizarea parolelor în procesul asigurării securităţii informaţionale**

Sunt respectate regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:

* păstrarea confidenţialităţii parolelor,
* interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia,
* modificarea parolelor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri a sistemului sau parolei,
* alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sînt compuse integral din grupuri de cifre sau litere,
* modificarea parolelor peste intervale de 3 luni,
* dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

1. **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.

1. **Accesul de la distanţă**
2. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi sînt documentate, supuse monitorizării şi controlului.
3. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal este autorizată de persoanele responsabile ale \_\_\_\_\_\_\_\_\_\_\_\_\_ şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.
4. **Limitarea folosirii tehnologiilor fără fir**
5. Accesul fără fir la sistemele informaţionale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării şi controlului.
6. Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecţie a informaţiei.
7. Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
8. **Securitatea electroenergetică**
9. 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.
10. 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.
11. Sunt implementate sisteme automatizate de depistare şi semnalizare a incendiilor în birourile unde sînt amplasate sistemele informaţionale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.
12. **Controlul instalării şi scoaterii componentelor T.I.**
13. 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.
14. 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, evitîndu-se folosirea funcţiilor standarde de nimicire.
15. **Dezvăluirea datelor cu caracter personal**

a) Dezvăluirea formatului electronic al datelor cu caracter personal conţinute în sistemele de evidență, prin reţele comunicaţionale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată criptarea acestei informații 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 autorizați. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieşind din posibilităţile tehnice asigurate de destinatar şi operator, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părţi. În cazul în care rețelele comunicaționale prezintă riscuri pentru confidenţialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiţionale de transmitere *(expediere poştală cu aviz recomandat, înmînarea personală, etc.*).

b) Dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale ce nu corespund Cerinţelor, *(spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.)* sînt interzise.

c) Sînt interzise operaţiunile de dezvăluire a datelor cu caracter personal între \_\_\_\_\_\_\_\_\_ și alte entități care sunt amplasate geografic în stînga Nistrului care refuză să se supună juridic legislaţiei Republicii Moldova, reieșind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părţi teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecţia datelor cu caracter personal.

d) Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie și/sau suport digital, peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ instituțional/acord bilateral luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecţie a datelor cu caracter personal.

e) Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecţia datelor cu caracter personal, în special în cazurile cînd tratatul internaţional în baza căruia se efectuează transmiterea nu conţine garanţii privind protecţia drepturilor subiectului de date cu caracter personal.

f) Volumul şi categoriile datelor cu caracter personal colectate în scopul ținerii evidenței \_\_\_\_\_\_\_\_\_\_\_\_\_\_, este limitat la strictul necesar pentru realizarea scopurilor declarate.

g) Acces la sistemele informaționale gestionate în cadrul \_\_\_\_\_\_\_\_\_\_\_, din partea Procuraturii General *(după caz procuraturile teritoriale/specializate)*, Ministerului Afacerilor Interne, Centrului Național Anticorupție etc.*,* va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 şi art. 212 Cod de procedură penală.

Se explică că în conformitate cu prevederile art.157 Cod de procedură penală, documentele în orice formă *(scrisă, audio, video, electronică etc.)* care provin de la persoane oficiale fizice sau juridice dacă în ele sînt expuse ori adeverite circumstanţe care au importanţă pentru cauză, *(inclusiv informația stocată în auditul sistemelor informaționale și de evidență),* pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art.214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate şi răspîndite fără necesitate informaţie oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanţa le solicită să comunice sau să prezinte informaţie 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 instanţa le solicită să comunice sau să prezinte informaţie oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informaţii o explicaţie în scris care ar confirma necesitatea furnizării datelor menţionate.

Urmează a ţine cont de faptul că în conformitate cu prevederile art.8 al Legii privind accesul la informație, datele cu caracter personal fac parte din categoria informaţiei oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislaţiei privind protecţia datelor cu caracter personal.

În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoştinţă cu fișa personală a clientului, aceştia urmează a fi informaţi în scris despre obligaţiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 şi 30 ale Legii privind protecţia datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 741 Cod contravenţional.

1. **Drepturile subiecţilor de date cu caracter personal**
2. În cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecția datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informaţii, exceptînd cazul în care el deţine deja informaţiile respective:

* privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator *(denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidență al operatorilor de date cu caracter personal);*
* privind scopul concret al prelucrării datelor cu caracter personal colectate;
* privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
* existenţa drepturilor la informare și 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 și condiţiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecinţele posibile ale refuzului de a răspunde la întrebările prin care se colectează informaţia.

b) Subiecţilor de date cu caracter personal le este asigurat dreptul de acces și 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 care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alţi subiecţi, conţinute în fișele personale *(alte materiale),* cu excepţia cazurilor în care solicitanţii își realizează un interes legitim care nu prejudiciază interesele sau drepturile şi libertăţile fundamentale ale subiectului datelor cu caracter personal.

c) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal *(sau entitățile ce asigură mentenața sistemului și sau prestează servicii externalizate ale operatorului)* tuturor persoanelor supuse prelucrării.

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

1. **Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate**

a) Accesul în spaţiile/perimetrul unde sînt amplasate sistemele informaţionale și de evidență a datelor cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară conform politicii de securitate instituţionale /regulamentelor departamentale aprobate.

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

c) 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 sînt încredinţate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul \_\_\_\_\_\_\_\_\_\_\_\_.

d) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie 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 operatorului este interzisă.

1. **Auditul sistemelor informaționale gestionate**
2. 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.

1. Seefectuează 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, o 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.

1. Este efectuată înregistrarea modificărilor drepturilor de acces (competenţelor) 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.

1. Se efectuează înregistrarea ieşirii din sistem a informaţiei care conţine 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.

1. **Asigurarea protecţiei contra programelor dăunătoare (viruşilor)**

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

1. **Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal**

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

1. **Gestionarea incidentelor de securitate**
2. Personalul care asigură exploatarea sistemelor informaţionale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilităţile şi obligaţiile în cazul executării acţiunilor de gestionare şi reacţionare la incidentele de securitate.
3. Personalul \_\_\_\_\_\_\_\_\_\_\_\_ informează neîntîrziat conducerea despre incidentele care încalcă securitatea sistemelor informaţionale de date cu caracter personal.
4. Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securităţii.
5. Pînă la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Centrul Național pentru Protecția Datelor cu Caracter Personal despre incidentele de securitate constatate.
6. ”În cazul producerii incidentelor de securitate în cadrul XXXXX, persoana resposabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova.
7. În cadrul controalelor efectuate de Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova i se va oferi suportul necesar și asigurat accesul la informațiile necesare relevante obiectului controlului.”

1. **Marcarea documentelor**

Toată informația care se intenționează a fi dezvăluită, 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.

Model Atenţie! Documentul conţine date cu caracter personal, prelucrate în cadrul sistemului de evidenţă nr. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, înregistrat în Registrul de evidenţă al operatorilor de date cu caracter personal [www.registru.datepersonale.md](http://www.registru.datepersonale.md/). Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal

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

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, semnatari a anexei nr. 1, 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).