



CONSILIUL MUNICIPAL CHIȘINĂU
PRIMAR GENERAL AL MUNICIPIULUI CHIȘINĂU
DIRECȚIA GENERALĂ ASISTENȚĂ MEDICALĂ ȘI SOCIALĂ

ORDIN

nr. 402-b

din 25 octombrie 2024

Cu privire la aprobarea Politicii de securitate privind protecția datelor cu caracter personal din cadrul Direcției generale asistență medicală și socială

În conformitate cu prevederile Legii nr.133/2011 privind protecția datelor cu caracter personal, Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123/2010, în temeiul pct. 12.4, 13.2 și 13.6 al Regulamentului de organizare și funcționare a Direcției generale asistență medicală și socială, aprobat prin Decizia Consiliului municipal Chișinău nr. 10/11 din 29.10.2021, dispoziției Primarului General nr. 1094-dc din 02.08.2024, **ORDON:**

1. Se aprobă Politica de securitate privind protecția datelor cu caracter personal din cadrul Direcției generale asistență medicală și socială, conform anexei.
2. Se pune în responsabilitatea titularilor funcțiilor de șefi ai subdiviziunilor structurale, conducători ai instituțiilor subordonate Direcției generale asistență medicală și socială, de a informa angajații din subordine despre prevederile prezentului ordin.
3. Persoanele împuternicite de către Direcția generală asistență medicală și socială care dețin și prelucrează datele cu caracter personal în cadrul sistemelor informaționale gestionate, precum și utilizatorii cu drept de acces la sistemele informaționale de date cu caracter personal, vor asigura implementarea prevederilor prezentei Politici de securitate.
4. Se abrogă ordinul nr. 91-b din 16.04.2021 "Cu privire la aprobarea Politicii de Securitate privind protecția datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor de evidență din cadrul Direcției generale asistență socială și sănătate".
5. Controlul îndeplinirii prevederilor prezentului ordin mi-l asum.

Șef adjunct Direcție

Vladimir BOLOCAN

POLITICA **de securitate a datelor cu caracter personal** **în cadrul Direcției generale asistență medicală și socială**

I. Introducere

La prelucrarea datelor cu caracter personal în cadrul Direcției generale asistență medicală și socială (în continuare – DGAMS) sunt aplicate principiile prevăzute de actele **internaționale** - Declarația universală a drepturilor omului, Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, Convenția nr. 108 a Consiliului Europei, Protocolul de amendare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27.04.2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), precum și a celor **naționale** – Constituția Republicii Moldova; Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal; Legea nr. 148 din 09.06.2023 privind accesul la informațiile de interes public, Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010, Decizia Consiliului municipal Chișinău nr. 10/11 din 29.10.2021, precum și alte acte legislative/normative atribuite.

Politica de securitate a datelor cu caracter personal (în continuare - Politică) este aprobată de către șef adjunct DGAMS dl Vladimir BOLOCAN, care acționează în baza dispoziției Primarului General nr. 1094-dc din 02.08.2024, în scopul conformării entității publice cu prevederile actelor normative menționate supra.

II. Noțiuni principale

În prezenta Politică, expresiile utilizate au următoarele semnificații:
politica de securitate a datelor cu caracter personal — document, elaborat de către deținătorul de date cu caracter personal, care oferă o descriere expresă a măsurilor de confidențialitate și securitatea prelucrării datelor cu caracter

personal, ținându-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și riscurile reale la care sunt expuse acestea;

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 etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate, viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale;

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;

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

operator – persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare;

persoană împuternicită de către operator – persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator;

terț - persoană fizică sau persoană juridică de drept public ori de drept privat, alta decât subiectul datelor cu caracter personal, decât operatorul ori persoana împuternicită de către operator și decât persoana care sub autoritatea directă a operatorului sau a persoanei împuternicite este autorizată să prelucreze date cu caracter personal;

destinatar — orice persoană fizică sau persoană juridică de drept public ori de drept privat, inclusiv autoritatea publică și subdiviziunile ei teritoriale, căreia îi sunt dezvăluite date cu caracter personal, indiferent dacă este sau nu terț. Nu sunt considerate destinatari organele din domeniul apărării naționale, securității

statului și ordinii publice, organele de urmărire penală și instanțele judecătorești cărora li se comunică date cu caracter personal în cadrul exercitării competențelor stabilite de lege;

consimțământul subiectului datelor cu caracter personal – manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a subiectului de date prin care acesta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care îl privesc să fie prelucrate;

depersonalizarea datelor – modificarea datelor cu caracter personal astfel încât detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile ori să permită atribuirea doar în condițiile unei investigații care necesită cheltuieli disproporționate de timp, mijloace și forță de muncă;

creare de profiluri – formă de prelucrare automată a datelor cu caracter personal, care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte referitoare la o persoană fizică, în special pentru a analiza sau a stabili aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele, interesele, fiabilitatea, comportamentul, locul în care se află persoana respectivă și deplasările acesteia;

autentificare - verificarea identicatorului atribuit subiectului de acces, confirmarea autenticității;

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

fișiere temporare - ansamblu de date sau informații pe suport digital creat pentru o perioadă de timp limitat până la inițierea îndeplinirii sarcinilor pentru care au fost desemnate;

identificare - atribuirea unui identicator subiecților și obiectelor de acces și/sau compararea identicatorului prezentat cu lista identificatoarelor atribuite;

integritate - 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 (N-1 sau N-2);

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 deținătorului 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 hîrtie 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;

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 informațională (TI) - totalitatea metodelor, procedeele 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 pînă 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;

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

administrator — subdiviziunea responsabilă de gestionarea și operarea resurselor informaționale ale sistemelor de evidență a datelor cu caracter personal.

III. Dispoziții generale

Politica reglementează prelucrarea datelor cu caracter personal de către subdiviziunile structurale ale DGAMS, stabilește rapoartele juridice care apar în procesul de prelucrare a datelor cu caracter personal, inclusiv celor care constituie categorii speciale de date cu caracter personal, care fac parte dintr-un sistem de evidență sau care urmează a fi incluse într-un asemenea sistem, efectuată în totalitate sau în parte prin mijloace automatizate, precum și prin alte mijloace decât cele automatizate.

Reglementările reprezintă un set minim pentru entitate și angajații săi, care urmează să respecte strict prevederile Politicii și regulile interne ale DGAMS privind protecția datelor cu caracter personal și sistemelor informaționale.

Securitatea reprezintă o componentă esențială a derulării optime a proceselor, inclusiv cele bazate pe TI. Aceasta cuprinde cerințe, măsuri și proceduri tehnice aplicate pentru asigurarea protecției tuturor informațiilor deținute, 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.

Reieșind din specificul activității, în calitate de operator, DGAMS stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare, precum și măsurile/metodele necesare în vederea asigurării nivelului adecvat de securitate la prelucrarea datelor cu caracter personal în cadrul sistemelor informaționale gestionate.

Calitatea de persoane împuternicite de către operator au subdiviziunile structurale și instituțiile subordonate DGAMS, care prelucrează date cu caracter personal în numele și pe seama operatorului, pe baza instrucțiunilor primite de la operator.

IV. Măsurile de protecție a datelor cu caracter personal

Măsurile de protecție a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a sistemului informațional de date cu caracter personal și vor fi efectuate neîntrerupt de către deținătorii de date cu caracter personal din cadrul DGAMS și instituțiilor subordonate acesteia.

Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal în cadrul DGAMS este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

Măsurile de protecție a datelor cu caracter personal se desfășurează ținându-se cont de necesitatea asigurării confidențialității acestor măsuri.

Protecției sînt supuse toate resursele informaționale ale deținătorilor de date cu caracter personal gestionate, care conțin date cu caracter personal, inclusiv:

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

Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal este asigurată în scopul:

- preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
- preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
- asigurării caracterului complet, integru, veridic al datelor cu caracter personal în rețelele telecomunicaționale și resurselor informaționale;
- păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal.

V. Metodele de protecție datelor cu caracter personal

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

- preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
- excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;
- preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor membri ai operatorului/persoanelor împuternicite de către operator, care

condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

- preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, prin folosirea metodelor de cifrare a acestei informații, precum și utilizarea după posibilitate a canalelor VPN, (Mcloud sau Mpass);
- preîntâmpinarea accesului neautorizat la informațiile care conțin date cu caracter personal, și circulă sau se păstrează în mijloace tehnice, prin folosirea mijloacelor de speciale tehnice și de program, cifrării acestor informații, inclusiv prin măsurile organizaționale și de regim;
- 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, STISC;
- stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență de către utilizatori.

VI. Procedurile organizaționale și tehnice necesare procesului de management al securității datelor cu caracter personal

Secțiunea 1. Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal

Accesul în sediile/oficiile/birourile ori spațiile unde sînt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară și doar în timpul orelor de program, conform listei corespunzătoare.

Conducătorul DGAMS elaborează și aprobă listele de acces, care se revizuiesc *nu mai rar decît o dată în lună*.

Administrarea și monitorizarea accesului fizic se efectuează în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces.

Înainte de acordarea accesului fizic la sistemele informaționale de date cu caracter personal se verifică competențele de acces.

În procesul monitorizării, se utilizează mijloace automatizate (*camere video, semnalizare etc.*) care asigură identificarea cazurilor de acces neautorizat și întreprinderea acțiunilor de îngrădire a accesului.

Perimetrul de securitate se determină în funcție de amplasare și căile de acces în spațiile în care se prelucrează/stochează date cu caracter personal.

Perimetrul clădirii sau încăperilor în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal trebuie să fie integru din punct de vedere fizic. Pereții exteriori ai încăperilor sînt rezistenți, intrările sunt echipate cu lacăte și semnalizare.

În cazul amplasării încăperilor la parter și/sau la ultimul etaj al clădirii, precum și în cazul existenței balcoanelor, scărilor antiincendiare, la ferestrele încăperilor respective se instalează gratii.

Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.

Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc angajații.

Amplasarea mijloacelor de prelucrare a datelor cu caracter personal trebuie să corespundă necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

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 DGAMS, iar accesul în perimetrul de securitate a clădirii/încăperii unde se prelucrează/stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis.

Purtătorii de informații și mijloace de prelucrare a datelor cu caracter personal scoase din încăperile aflate în perimetrul de securitate nu trebuie lăsate fără supraveghere.

Controlul accesului fizic al vizitatorilor în încăperile unde sunt amplasate sistemele informaționale de date cu caracter personal trebuie să fie asigurat de către deținătorii și utilizatorii acestor date.

Securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal și a cablurilor electrice contra deteriorărilor și conectărilor nesancționate, prin instalarea acestora în locuri speciale, conform cerințelor tehnice.

În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, trebuie asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

Totodată, trebuie prevăzute surse autonome de alimentare cu energie electrică 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.

Cablurile de rețea, prin care se efectuează operațiuni de prelucrare a datelor cu caracter personal, trebuie protejate contra conectărilor nesanctionate sau deteriorărilor.

Cablurile de tensiune trebuie separate de cele comunicaționale, pentru a exclude bruiatul.

În scopul verificării cazurilor de conectare neautorizată la cablurile de rețea, se efectuează controale periodice (*nu mai rar decât odată în lună*).

Se prevăd și se instalează mijloacele de asigurare a securității antiincendiară a sediilor/oficiilor/birourilor unde sunt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

Este exercitat controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal.

Informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitându-se folosirea funcțiilor standard de nimicire.

Măsurile generale de administrare a securității informaționale:

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 care se încuie.

Computerele, terminalele de acces și imprimantele sânt deconectate la terminarea sesiunilor de lucru.

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

Este administrat accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acestora de către persoane neautorizate.

Mijloacele de prelucrare a datelor cu caracter personal, informația care conține 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 DGAMS.

Toate programele utilizate în cadrul sistemului informațional respectă condițiile de licențiere.

Este interzisă instalarea programelor de tip shareware sau freeware, precum și oricare alte programe, fără aprobarea administratorului sistemului informatic.

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

Secțiunea 2. Identificarea și autentificarea utilizatorilor

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

În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și noile sarcini nu necesită accesul la date cu caracter personal, ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare și autentificare se revocă sau se suspendă de către administratorul TI.

Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal.

Administrarea identificatorilor utilizatorilor include:

- a) identificarea univocă a fiecărui utilizator;
- b) verificarea autenticității fiecărui utilizator.

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

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

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

Se folosesc identificatoare individuale pentru fiecare utilizator și parole individuale ale acestora pentru asigurarea posibilității de stabilire a responsabilității.

Este asigurată posibilitatea utilizatorilor de a alege și schimba parolele individuale, inclusiv de activare a procedurii de evidență a introducerilor greșite ale acestora.

Se asigură blocarea accesului după trei tentative greșite de autentificare.

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

Parolele se păstrează în formă cifrată, utilizându-se algoritmul criptografic unilateral (funcția hash).

Secțiunea 3. Administrarea accesului utilizatorilor

Este efectuată administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea și ștergerea acestora, pentru ce sunt folosite mijloace automatizate de suport.

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

Accesul la sistemele informaționale de date cu caracter personal este autorizat în conformitate cu politica de administrare a accesului stabilită de DGAMS în calitate de deținătorul de date cu caracter personal.

Drepturile de acces ale utilizatorilor la sistemele informaționale de date cu caracter personal sînt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare 6 luni) și după oricare schimbare de statut al utilizatorului.

În calitate de deținătorul de date cu caracter personal, DGAMS autorizează realizarea fluxurilor informaționale în procesul transmiterii acestora în interiorul și în afara sistemelor informaționale de date cu caracter personal.

Utilizatorii sistemelor informaționale de date cu caracter personal se investesc doar cu acele drepturi/competențe, care sînt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

Înainte de acordarea accesului în sistem, utilizatorii sînt informați despre faptul că folosirea sistemelor informaționale de date cu caracter personal este controlată și că folosirea neautorizată a acestora se urmărește în conformitate cu legislația în vigoare.

Sesiunea de lucru în sistemul informațional, destinat prelucrării datelor cu caracter personal, se blochează (la solicitarea utilizatorului sau automat, după maximum 15 minute de perioada inactivă a utilizatorului), fapt care face imposibil accesul de mai departe pînă în momentul cînd utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare și autentificare.

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

Informația care urmează a fi dezvăluită și care conține date cu caracter personal, se marchează, indicîndu-se prescripții pentru prelucrarea ulterioară și răpîndirea acesteia indicîndu-se numărul de identificare unic al deținătorului de date cu caracter personal (DGAMS).

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

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

Accesul fără fir la sistemele informaționale de date cu caracter personal este limitat și reglementat, totodată documentat, supus monitorizării și controlului permanent.

Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației.

Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile ale DGAMS.

Accesul la sistemele informaționale de date cu caracter personal cu folosirea echipamentului portativ și mobil se documentează, este monitorizat și controlat.

Folosirea echipamentului portativ și mobil este autorizată de persoanele responsabile ale DGAMS.

Secțiunea 4. Protecția sistemelor informaționale și comunicațiilor în care sunt prelucrate date cu caracter personal

Este asigurată separarea posibilităților funcționale ale utilizatorului de posibilitățile funcționale de gestionare a sistemelor informaționale de date cu caracter personal.

Este asigurată izolarea funcțiilor de securitate de funcțiile care nu se atribuie la securitatea sistemelor informaționale de date cu caracter personal.

Sunt preîntîmpinate tentativele dezvăluirii neautorizate sau neintenționate a informației restante care conține date cu caracter personal, prin intermediul resurselor informaționale general accesibile.

Se efectuează monitorizarea permanentă și controlul comunicațiilor la perimetrul exterior al sistemelor informaționale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme.

Este asigurată imposibilitatea accesului din exterior a utilizatorilor la rețeaua internă în care se prelucrează date cu caracter personal.

Se asigură integritatea și confidențialitatea datelor cu caracter personal transmise, utilizîndu-se mijloacele de protecție criptografică a informației și semnătura digitală.

Secțiunea 5. Auditul securității în sistemele informaționale de date cu caracter personal

DGAMS organizează generarea înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal pentru evenimentele supuse auditului.

De către Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:

- data și timpul tentativei intrării/ieșirii;
- ID-ul utilizatorului;
- rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.

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

- data și timpul tentativei de obținere a accesului (executare 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.

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

- data și timpul modificării competențelor;
- ID-ul administratorului care a efectuat modificările;
- ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

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

- data și timpul eliberării;
- denumirea informației și căile de acces la aceasta;
- specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
- ID-ul utilizatorului, care a solicitat informația;
- volumul documentului eliberat (numărul paginilor, a filelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.

Se efectuează monitorizarea permanentă și analiza înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal, în scopul depistării activităților neobișnuite sau suspecte de utilizare a acestor sisteme informaționale, cu întocmirea raportului referitor la cazurile depistării acestor activități, stocate în mijloacele electronice de calcul și întreprinderea acțiunilor presatbilite în prezenta Politică pentru astfel de cazuri.

Rezultatele auditului securității în sistemele informaționale de date cu caracter personal, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate.

Secțiunea 6. Asigurarea integrității informației care conține date cu caracter personal și a tehnologiilor informaționale

Este asigurată identificarea, documentarea și înlăturarea deficiențelor de soft-uri destinate prelucrării datelor cu caracter personal.

Protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal este asigurată prin administrarea centralizată a mecanismelor de protecție, instalarea și reînnoirea la timp a programelor licențiate anti-virus.

Se utilizează tehnologii și mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaționale de date cu caracter personal și constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaționale.

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

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

Secțiunea 7. Copiile de rezervă și restabilirea informației care conține date cu caracter personal și TI

Se stabilește de către DGAMS intervalul de timp în care se execută copiile de siguranță a informațiilor care conțin date cu caracter personal și soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, dar în orice caz acest termen este mai mic de un an, care se păstrează în locuri protejate, în afara zonei de amplasare a acestei informații și soft-urile de bază.

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

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

Secțiunea 8. Controalele de securitate a sistemelor informaționale de date cu caracter personal

DGAMS verifică cu regularitate, *cel puțin odată pe an*, îndeplinirea măsurilor tehnice și/sau organizaționale luate pentru detectarea unor disfuncționalități în ceea ce privește folosirea în procesul prelucrării datelor cu caracter personal a sistemelor de telecomunicații și/sau efectuarea îmbunătățirilor, în caz de necesitate.

Controalele de securitate sînt actualizate de fiecare dată cînd deținătorul de date cu caracter personal este reorganizat sau își schimbă infrastructura.

În scopul verificării nivelului de protecție a sistemelor informaționale de date cu caracter personal, Centrul Național pentru Protecția Datelor cu Caracter Personal (în continuare – Centrul) întreprinde periodic controale de securitate, inclusiv cu efectuarea unor măsuri tehnice speciale pentru simularea unui model de accesare a sistemelor informaționale de date cu caracter personal.

În cadrul controalelor efectuate de Centrul, i se va oferi suportul necesar și asigurat accesul la informațiile necesare relevante obiectului controlului.

Rezultatele controalelor efectuate de Centrul sunt puse imediat la dispoziția DGAMS, cu prescrierea, în caz de necesitate, a acțiunilor necesare de a fi întreprinse în vederea asigurării securității prelucrării datelor cu caracter personal.

Secțiunea 9. Gestionarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal

Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal, trece anual, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

Este asigurat mecanismul de informare neîntîrziată a conducerii DGAMS despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.

Incidentele de securitate a sistemelor informaționale de date cu caracter personal se monitorizează și se documentează în regim permanent.

În cazul producerii incidentelor de securitate, persoana responsabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și, în comun cu persoanele împuternicite de operator, va întreprinde măsurile necesare în vederea preîntîmpinării dezvoltării și înlăturării incidentului de securitate, în scopul restabilirii securității.

Anual, către 31 ianuarie, DGAMS prezintă Centrului raportul generalizat despre incidentele de securitate a sistemelor informaționale de date cu caracter personal. În baza acestui raport, Centrul întreprinde măsurile ce se impun de Legea cu privire la protecția datelor cu caracter personal.

Secțiunea 10. Protecția tehnică a informației care conține date cu caracter personal

Se exclude prezența necontrolată a persoanelor sau a mijloacelor de transport, precum și instalarea întâmplătoare a antenelor, într-o zonă de 15 metri de la locul amplasării mijloacelor tehnice principale ale sistemului informațional de date cu caracter personal (în continuare – perimetru controlat), în scopul asigurării securității prelucrării datelor cu caracter personal.

Încăperile pentru servere se protejează contra scurgerii informației care conține date de caracter personal din cauza emisiilor electromagnetice prin ecranarea încăperilor sau instalarea sistemelor de bruijă electromagnetică, care se proiectează, realizează și cercetează de întreprinderi specializate în domeniu.

În cazul ecranării încăperilor în care se află mijloace tehnice de prelucrare a datelor cu caracter personal, este asigurată continuitatea conexiunii electrice a materialului tuturor părților ecranului: pereți, tavan, podea, ferestre și uși.

Construcțiile de ecranare trebuie să posede prize de pământ care se amplasează în perimetrul controlat.

Este asigurată protecția informației care conține date cu caracter personal contra scurgerii prin intermediul rețelei electrice, inclusiv încrucișarea rețelelor electrice ale obiectului.

Se exclude sau se limitează instalarea neautorizată a altor dispozitive electrice, radio sau de alt gen în încăperile unde sunt amplasate mijloacele tehnice de prelucrare a datelor cu caracter personal.

Utilajul, liniile căruia au ieșire în afara perimetrului controlat, este instalat la o distanță de cel puțin 3 metri de la mijloacele TI în care sunt prelucrate date cu caracter personal.

V. Dispoziții privind persoana responsabilă de politica de securitate a datelor cu caracter personal

Persoana responsabilă de politica de securitate a datelor cu caracter personal, va fi desemnată persoana care conform fișei postului și/sau ordinului intern, va dispune de competențele funcționale și va avea acces liber la sistemele informaționale de evidență din cadrul DGAMS pentru îndeplinirea funcțiilor sale în scopul implementării și monitorizării respectării prevederilor prezentei Politici.

Persoana responsabilă desemnată, indiferent de funcțiile exercitate, în procesul monitorizării implementării/respectării prevederilor politicii de securitate, se va subordona nemijlocit conducătorului DGAMS sau persoanei care asigură interimatul/atribuțiile funcției.

Persoana responsabilă de politica de securitate a datelor cu caracter personal va asigura procesele de management al securității datelor cu caracter personal (monitorizare, detectare, prevenire și prelucrare), va asigura măsuri tehnice și organizaționale necesare organizării procesului de management al securității datelor cu caracter personal, va elabora procedurile de clasificare a informației care conține date cu caracter personal, va instrui persoanele antrenate în procesul de prelucrare a datelor cu caracter personal în vederea asigurării protecției acestor date și a responsabilităților asumate.

VI. Dezvăluirea datelor cu caracter personal

Dezvăluirea datelor cu caracter personal conținute în sistemele de evidență, prin rețele comunicaționale ori pe alt suport digital de stocare și păstrare, urmează a fi asigurată criptarea acestei informații sau examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat VPN.

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 organizaționale 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 personală, etc.*).

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

Transmiterea transfrontalieră a datelor cu caracter personal este efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecția datelor cu caracter personal, luînd în considerare tratatele internaționale în materie de protecție a datelor cu caracter personal la care fac parte, în baza listei statelor care asigură un nivel adecvat de protecție a datelor cu caracter personal, aprobate de Centrul, publicate în Monitorul Oficial al RM și pe pagina web oficială a Centrului.

Sînt **interzise** operațiunile de dezvăluire a datelor cu caracter personal între DGAMS și alte entități care sunt amplasate geografic în stînga Nistrului, reieșind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părți teritoriale, inclusiv în partea ce ține de conformitatea prelucrării datelor cu caracter personal prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal.

Volumul și categoriile datelor cu caracter personal colectate în scopul ținerii evidenței DGAMS, este limitat la strictul necesar pentru realizarea obiectivelor asumate.

La cererea informației cu caracter personal de către organul de urmărire penală și/sau a instanței de judecată, urmează a fi respectate prevederile art. 91 din Codul Muncii al RM, art. 15 Cod de procedură penală și art. 29 alin. (1) al Legii nr. 133/2011 privind protecția datelor cu caracter personal.

Se explică, că în conformitate cu prevederile art. 157 Cod de procedură penală, documentele în orice formă (*scrisă, audio, video, electronică etc.*) care provin de la persoane oficiale fizice sau juridice dacă în ele sunt expuse ori adevărate circumstanțe care au importanță pentru cauză, pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei.

În acest caz, urmează a fi respectate și prevederile art. 214 alin. (2) Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate și răspândite fără necesitate informație oficială cu accesibilitate limitată.

Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată (*inclusiv operatorii de date cu caracter personal*) au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date.

Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informații o explicație în scris care ar confirma necesitatea furnizării datelor menționate.

Ținând cont de faptul că, la dezvăluirea informației datele cu caracter personal pot fi prejudiciate, accesul la ele poate fi limitat în conformitate cu prevederile art.8 al Legii nr. 148/2023 privind accesul la informațiile de interes public.

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

Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecție speciale tehnice și de program și nu au instalate programe licențiate, programe antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului este *interzisă*.

Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este *interzisă*.

Totodată, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredințate doar persoanei responsabile de politica de securitate desemnate din cadrul DGAMS.

Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia, este asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie.

Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este *interzisă*.

VIII. Răspunderea pentru asigurarea securității datelor cu caracter personal

Conducătorul DGAMS în calitate de operator/persoana împuternicită de operator care dispun de acces la sistemele de evidență a datelor cu caracter personal/persoanele terțe, pentru nerespectarea dispozițiilor Politicii de securitate poartă răspundere civilă, contravențională conform art. 74¹ Cod contravențional al RM și/sau penală, după caz.

Conducătorii subdiviziunilor structurale ale DGAMS conectate la sistemele de evidență a datelor cu caracter personal dispun măsurile necesare în vederea instituirii și menținerii unui nivel suficient de securitate a datelor cu caracter personal.

Utilizatorul/beneficiarul și persoana care a interceptat informația din sistemele de evidență a datelor cu caracter personal poartă răspundere pentru asigurarea securității și protecției informației obținute, neexecutarea sau executarea necorespunzătoare a cerințelor prevăzute în prezenta Politică.

IX. Dispoziții finale

DGAMS, IDNO 1007601010541, are sediul înregistrat în mun. Chișinău, str. București nr. 35, Republica Moldova.

Operatorul (DGAMS), persoanele împuternicite de către operator și persoanele responsabile vor asigura protecția acestora conform cerințelor și reglementărilor din prezenta Politică, care se aduce la cunoștința angajaților implicați în procesul de prelucrare a datelor cu caracter personal, înaintea

acordării accesului la prelucrarea datelor cu caracter personal și la operarea modificărilor odată cu necesitatea asigurării nivelului adecvat de protecție a datelor cu caracter personal, sub semnătură, de către Direcția resurse umane, în termen de 10 zile lucrătoare de la data aprobării acesteia.

Politica poate fi revizuită/ajustată la necesitate, dar nu mai rar decât *odată la doi ani*, ca rezultat al modificărilor legislației sau reevaluării componentelor acesteia și se aprobă de către conducătorul DGAMS.

CATEGORIILE DE DATE CU CARACTER PERSONAL

1. Datele cu caracter personal, care direct sau indirect identifică o persoană fizică, în special prin referire la un număr de identificare (cod personal), la unul sau mai multe elemente specifice proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale, se împart în două categorii: obișnuite și speciale.
2. Categoria specială a datelor cu caracter personal o constituie informația care dezvăluie originea rasială sau etnică, convingerile politice, religioase, privind starea de sănătate sau viața intimă, precum și cele privind condamnările penale ale unei persoane fizice.
3. Categoria obișnuită o constituie informația care dezvăluie:
 - 1) numele și prenumele;
 - 2) sexul;
 - 3) data și locul nașterii;
 - 4) cetățenia;
 - 5) IDNP;
 - 6) imaginea;
 - 7) vocea;
 - 8) situația familială;
 - 9) situația militară;
 - 10) datele de geolocalizare/datele de trafic;
 - 11) porecla/pseudonimul;
 - 12) datele personale ale membrilor de familie;
 - 13) datele din permisul de conducere;
 - 14) datele din certificatul de înmatriculare;
 - 15) situația economică și financiară;
 - 16) datele privind bunurile deținute;
 - 17) datele bancare;
 - 18) semnătura;
 - 19) datele din actele de stare civilă;
 - 20) numărul dosarului de pensie;
 - 21) codul personal de asigurării sociale (CPAS);
 - 22) codul asigurării medicale (CPAM);
 - 23) numărul de telefon/fax;
 - 24) numărul de telefon mobil;
 - 25) adresa (domiciliului/sediului);
 - 26) adresa e-mail;
 - 27) profesia și/sau locul de muncă;
 - 28) formarea profesională — diplome studii;
 - 29) obiceiurile/preferințele/comportamentul;
 - 30) caracteristicile fizice.

4. În cazul prelucrării categoriei obișnuite de date cu caracter personal, DGAMS include în politica de securitate a datelor cu caracter personal și implementează cerințele stabilite pentru nivelul unu de securitate a sistemelor informaționale de date cu caracter personal – (N-1).

CATEGORIILE OPERAȚIUNILOR DE PRELUCRARE A DATELOR CU CARACTER PERSONAL, SUSCEPTIBILE DE A PREZENTA RISCURI SPECIALE PENTRU DREPTURILE ȘI LIBERTĂȚILE PERSOANELOR

Prezintă riscuri speciale pentru drepturile și libertățile persoanelor următoarele categorii ale operațiunilor de prelucrare a datelor cu caracter personal:

1) adaptarea, modificarea, dezvăluirea prin transmitere, difuzare sau în orice alt mod, a datelor cu caracter personal legate de originea rasială sau etnică, de convingerile politice, religioase, de apartenență la un partid politic sau o organizație religioasă, a datelor cu caracter personal privind starea de sănătate sau viața intimă, precum și a datelor cu caracter personal referitoare la condamnările penale, măsurile de constrângere, sancțiunile disciplinare sau contravenționale;

2) operațiunile de prelucrare a datelor genetice, biometrice și a datelor care permit localizarea geografică a persoanelor prin intermediul rețelelor de comunicații electronice;

3) operațiunile de prelucrare a datelor cu caracter personal prin mijloace electronice, avînd ca scop evaluarea unor aspecte de personalitate, precum și competența profesională, credibilitatea, comportamentul etc.;

4) operațiunile de prelucrare a datelor cu caracter personal prin mijloace electronice în cadrul unor sisteme de evidență, avînd ca scop analizarea solvabilității, a situației economico-financiare, a faptelor susceptibile de a atrage răspunderea disciplinară, contravențională sau penală a persoanelor fizice;

5) operațiunile de prelucrare a datelor cu caracter personal menționate la subpunctele 1) și 2) din prezenta anexă, colectate prin intermediul Internetului sau mesageriei electronice.

DECLARAȚIE DE CONFIDENȚIALITATE
din data de _____

În conformitate cu prevederile Legii nr.133 din 18.07.11 „Privind protecția datelor cu caracter personal”, Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010, subsemnatul (a)

(nume, prenume)

(funcția)

(instituția)

confirm, că sunt conștient de gradul de securitate a documentelor care conțin datele cu caracter personal, de riscurile aferente utilizării neadecvate acestora și mă angajez:

1. să respect condițiile impuse pentru protejarea informației primite de la Administratorul SIA prezente în actuala Politică;
2. să păstrez în deplină confidențialitate respectiva informație;
3. să nu divulg către terți informația de care voi lua cunoștință în urma examinării documentelor vizate;
4. să nu utilizez această informație în alte scopuri decât cele anunțate la momentul solicitării.

Prezenta declarație este întocmită în 2 (două) exemplare, câte un exemplar pentru fiecare parte.

(nume, prenume)

(semnătura)