APROBAT
Consiliul Național pentru Determinarea
Determinarea Dizabilității și Capacității de M
Director general Ludmila
„01" iunie

REGULAMENT

de securitate a datelor cu caracter personal

în cadrul Consiliului Național

pentru Determinarea Dizabilității și Capacității de Muncă

Chișinău 2014

I. DISPOZIȚII GENERALE

1. Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale și mecanice de date cu caracter personal au drept scop stabilirea regulilor de implementare de către Consiliul Național pentru Determinarea Dizabilității și Capacității de Muncă (în continuare - CNDDCM) a măsurilor tehnice și organizatorice necesare pentru asigurarea securității, confidențialității și integrității datelor cu caracter personal prelucrate în cadrul sistemelor informaționale și mecanice de date cu caracter personal și/sau registrelor ținute manual, în conformitate cu prevederile Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal și Legii nr. 71-XVI din 22 martie 2007 cu privire la registre și Convenției pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiată la Strasbourg la 28 ianuarie 1981, publicată în European Treaty Series, nr. 108, ratificată de Republica Moldova prin Hotărîrea Parlamentului nr. 483-XIV din 2 iulie 1999.

2. În sensul prezentului regulament, se definesc următoarele noțiuni:

- **regulament de securitate a datelor cu caracter personal**: este un document, elaborat de către CNDDCM (deținătorul de date cu caracter personal), care oferă o descriere precisă a măsurilor de securitate și trăsăturilor de protecție selectate pentru securitatea datelor, ținîndu-se cont de potențialele pericole pentru datele cu caracter personal prelucrate și riscurile reale la care sînt expuse acestea;
- **date cu caracter personal**: constituie 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. **De exemplu:** *numele, prenumele, anul nașterii, domiciliul, numărul de identificare de stat (IDNP), imaginile foto și video - reprezintă date cu caracter personal care se referă la o persoană fizică identificată direct.*
- **categorii speciale de date cu caracter personal:** constituie datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum și cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancțiunile contravenționate. **De exemplu:** *informația conținută în: certificatele medicale/ rapoartele de determinare a dizabilității și capacității de muncă/ rapoartele de expertiză medico-legală, în cazierul judiciar, în anexa la buletinul de identitate (ștampilele „Referendum 2016 Votăm” deoarece în anumite circumstanțe pot cu celeritate reflecta anumite convingeri politice) etc. De asemenea, informația referitoare la persoanele aflate în spitale, oficii pentru bătrîni sau deținute pe baza unui mandat de arest pînă la pronunțarea sentinței judecătorești, referitoare la persoanele condamnate la închisoare, la cele care execută o sancțiune contravențională sub formă de arest, aflate în instituțiile penitenciare, reprezintă categorii speciale de date cu caracter personal.*
- **prelucrarea datelor cu caracter personal**: constituie 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.

Prelucrarea datelor cu caracter personal se efectuează cu consimțământul subiectului datelor cu caracter personal. Consimțământul privind prelucrarea datelor cu caracter personal poate fi retras în orice moment de către subiectul datelor cu caracter personal. Retragerea consimțământului nu poate avea efect retroactiv.

În cazul incapacității de exercițiu sau al capacității de exercițiu limitate a subiectului datelor cu caracter personal, consimțământul privind prelucrarea datelor cu caracter personal se acordă, în formă scrisă, de către reprezentantul lui legal.

În cazul decesului subiectului datelor cu caracter personal, consimțământul privind prelucrarea datelor sale se acordă, în formă scrisă, de către succesorii acestuia, dacă un astfel de consimțământ nu a fost dat de subiectul datelor cu caracter personal în timpul vieții.

Consimțământul subiectului datelor cu caracter personal nu este cerut în cazurile în care prelucrarea este necesară pentru:

a) executarea unui contract la care subiectul datelor cu caracter personal este parte sau pentru luarea unor măsuri înaintea încheierii contractului, la cererea acestuia;

b) îndeplinirea unei obligații care îi revine operatorului conform legii;

c) protejarea vieții, integrității fizice sau a sănătății subiectului datelor cu caracter personal;

d) executarea sarcinilor de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este investit operatorul sau terțul căruia îi sînt dezvăluite datele cu caracter personal;

e) realizarea unui interes legitim al operatorului sau al terțului căruia îi sînt dezvăluite datele cu caracter personal, cu condiția ca acest interes să nu prejudicieze interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal;

f) scopuri statistice, de cercetare istorică sau științifică, cu condiția ca datele cu caracter personal să rămînă anonime pe toată durata prelucrării.

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/reşedinţei);
26) adresa e-mail;
27) datele genetice;
28) datele biometrice şi antropometrice;
29) datele dactiloscopice;
30) profesia şi/sau locul de muncă;
31) formarea profesională – diplome – studii;
32) obişnuinţele/preferinţele/comportamentul;
33) caracteristicile fizice.

- **Categoria specială a datelor cu caracter personal** o constituie informaţia care dezvăluie originea rasială sau etnică, convingerile politice, religioase, privind starea de sănătate sau viaţa intimă, precum şi cele privind condamnările penale ale unei persoane fizice.

- **Prelucrarea categoriilor speciale de date cu caracter personal:** Prelucrarea categoriilor speciale de date cu caracter personal este interzisă, cu excepţia cazurilor în care:

a) subiectul datelor cu caracter personal şi-a dat consimţământul. În cazul incapacităţii de exerciţiu sau al capacităţii de exerciţiu limitate a subiectului datelor cu caracter personal, prelucrarea categoriilor speciale de date cu caracter personal se efectuează numai cu obţinerea consimţământului în formă scrisă al reprezentantului lui legal;

b) prelucrarea este necesară pentru îndeplinirea obligaţiilor sau drepturilor specifice ale operatorului în domeniul dreptului muncii, cu respectarea garanţiilor prevăzute de lege şi ţinându-se cont de faptul că o eventuală dezvăluire către un terţ a datelor cu caracter personal prelucrate în acest scop poate fi efectuată numai dacă există o obligaţie legală a operatorului în acest sens;

c) prelucrarea este necesară pentru protecţia vieţii, integrităţii fizice sau a sănătăţii subiectului datelor cu caracter personal ori a altei persoane, în cazul în care subiectul datelor cu caracter personal se află în incapacitate fizică sau juridică de a-şi da consimţământul;

d) prelucrarea este efectuată în contextul activităţilor legitime de către asociaţii obşteşti, partide şi alte organizaţii social-politice, de către sindicate, asociaţii de patronat, organizaţii filozofice sau religioase, organizaţii cooperatiste necomerciale, cu condiţia ca prelucrarea să se refere numai la membrii acestora sau la persoanele cu care acestea au contacte permanente în legătură cu scopurile lor şi cu condiţia ca datele să nu fie dezvăluite terţilor fără consimţământul subiecţilor datelor cu caracter personal;

e) prelucrarea se referă la date făcute publice în mod voluntar şi manifest de către subiectul datelor cu caracter personal;

f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiţie al subiectului datelor cu caracter personal;

g) prelucrarea este necesară în scopul asigurării securităţii statului, cu condiţia ca aceasta să se efectueze cu respectarea drepturilor subiectului datelor cu caracter personal şi a celorlalte garanţii prevăzute de prezenta lege.

Prezintă riscuri speciale pentru drepturile şi libertăţile persoanelor următoarele categorii de operaţiuni 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 apartenența 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 constrîngere, 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 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 ale minorilor în scopuri comerciale (activităților de marketing direct);

6) operațiunile de prelucrare a datelor cu caracter personal menționate în prezentul reulament, precum și datele cu caracter personal ale minorilor, colectate prin intermediul Internetului sau mesageriei electronice.

- **operator**: constituie acea 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. **De exemplu:** *în toate cazurile cînd se va reglementa printr-un act normativ scopurile și procedurile de colectare, stocare și prelucrare în continuare a cărorva date cu caracter personal în sisteme de evidență automatizate, manuale ori mixte, se va constitui în calitate de operator al acestor date.*
- **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. **De exemplu:** *atunci cînd angajatul prelucrează datele cu caracter personal în conformitate cu instrucțiunile aprobate de CNDDCM.*
- **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. În calitate de sistem de evidență a datelor cu caracter personal se constituie inclusiv dar nu se limitează la, bazele de date, sistemele informaționale și informatice în care sînt stocate și prelucrate automatizat sau manual date cu caracter personal. **De exemplu:** *modele clasice ale sistemelor de evidență a datelor cu caracter personal reprezintă: Registrul de evidență a angajaților CNDDCM sau a numerelor telefoanelor corporative ale angajaților, Registrul de evidență al vizitatorilor, Registrul de evidență a petițiilor și altor adresări, informațiile personalizate referitoare la instruirea specializată a angajaților ori a altor subiecți implicați în procesul instructiv etc., alte serii structurate de date cu caracter personal, cum ar fi: imaginile video colectate printr-un sistem de supraveghere video instalat în incinta sau pe perimetrul [illegible] procuraturii etc.;*

- **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;
- **autentificare**: verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;
- **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;
- **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 datelor cu caracter personal în starea în care se aflau pînă la momentul pierderii sau distrugerii acestora;
- **tehnologie informaţională ((TI) eng. informational technology)**: 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;
- **stocare**: păstrarea pe orice fel de suport a datelor cu caracter personal.

II. CERINȚELE GENERALE

1. Măsurile de protecție a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a sistemului informațional și mecanic de date cu caracter personal și vor fi efectuate neîntrerupt de către persoanele responsabile angajate în cadrul CNDDCM.

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

3. Măsurile de protecție a datelor cu caracter personal prelucrate în sistemele informaționale și mecanice de date cu caracter personal se înfăptuiesc ținîndu-se cont de necesitatea asigurării confidențialității acestor măsuri.

4. Înfăptuirea oricăror măsuri și lucrări cu folosirea resurselor informaționale și mecanice ale deținătorului de date cu caracter personal este interzisă în cazurile în care nu sînt adoptate și implementate măsuri corespunzătoare de protecție a datelor cu caracter personal.

5. Sînt supuse protecției toate resursele informaționale ale deținătorilor de date cu caracter personal, care conțin date cu caracter personal, inclusiv:

1) 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.

6. Protecția datelor cu caracter personal în sistemele informaționale și mecanice de date cu caracter personal este asigurată în scopul:

1) preîntîmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;

2) preîntîmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;

3) respectării cadrului normativ de folosire a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;

4) asigurării caracterului complet, integru, veridic al datelor cu caracter personal în rețelele telecomunicaționale și resurselor informaționale;

5) păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal.

7. Protecția datelor cu caracter personal prelucrate în sistemele informaționale și mecanice se efectuează prin următoarele metode:

1) preîntîmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;

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

3) preîntîmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program;

4) preîntîmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor angajați ai deținătorului de date cu caracter personal, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program.

8. 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, inclusiv cu utilizarea măsurilor organizaţionale, tehnice şi de regim.

9. Preîntîmpinarea accesului neautorizat la informaţiile care conţin date cu caracter personal şi circulă sau se păstrează în mijloace tehnice este asigurată prin metoda folosirii mijloacelor speciale tehnice şi de program, cifrării acestor informaţii, inclusiv prin măsurile organizaţionale şi de regim.

10. Ordinea de acces la informaţia care conţine date cu caracter personal, prelucrată în cadrul sistemelor informaţionale şi mecanice, se stabileşte de către deţinătorul de date cu caracter personal, în conformitate cu prevederile legislaţiei.

11. Toate persoanele implicate în procesul desfăşurării activităţilor în domeniu, care prelucrează date cu caracter personal, urmează a fi supuşi unei declaraţii de confidenţialitate, care, după caz, poate fi inclusă în contractele de muncă, avînd calitate de clauză contractuală, sau în fişele postului, cu menţiunea expresă despre răspunderea civilă, contravenţională ori penală pentru încălcarea acesteia.

III. REGULAMENTUL DE SECURITATE A DATELOR CU CARACTER PERSONAL

1. Prezentul regulament de securitate a datelor cu caracter personal se revizuieşte cel puţin o dată în an ca rezultat al modificărilor sau reevaluării componentelor acesteia şi aprobată prin Ordinul Consiliul Naţional pentru Determinarea Dizabilităţii şi Capacităţii de Muncă.

2. Prevederile regulamentului de securitate va fi adus la cunoştinţă utilizatorilor şi altor angajaţi ai CNDDCM.

3. Prin Ordinul Consiliului nr.15 din "02" iunie 2014 este numit responsabil de elaborarea, implementarea şi monitorizarea respectării prevederilor regulamentului de securitate a datelor cu caracter personal dna Nelea Cojocari.

4. Măsurile de securitate emise sunt stabilite conform regulamentelor de securitate ale fiecărui sistem care prelucrează date cu caracter personal. În acest sens în cadrul CNDDCM sînt create 2 sisteme: sistemul informational Universal Acounting şi unul mecanic în CNDDCM

5. Mecanismul de punere în aplicare a măsurilor de securitate este prevăzut de prezenta politică de securitate.

6. Nomenclatorul datelor cu caracter personal prelucrate în cadrul CNDDCM este stabilit de Regulamentul de securitate al fiecărui sistem, care prelucrează date cu caracter personal.

7. Lista nominală a utilizatorilor, autorizaţi să acceseze datele cu caracter personal este stabilită prin Ordinul Consiliului.

8. Descrierea detaliată a criteriilor, în conformitate cu care sînt accesibile datele cu caracter personal, prelucrate în registrul ţinut manual, este prevăzută în Regulamentul politicii de securitate a datelor cu caracter personal al CNDDCM

9. Documentaţia tehnică cu privire la controalele de securitate este ţinută sub formă de registre de persoana responsabilă, numită prin Ordinul Consiliului pentru fiecare sistem informaţional în parte.

10. Orarul controalelor de securitate este stabilit de către persoana numită responsabilă, în conformitate cu regulamentul de securitate al fiecărui Sistem care prelucrează date cu caracter personal.

11. Rapoartele despre incidentele de securitate sunt înregistrate în registrele respective de către persoanele responsabile. Fiecare incident urmează a fi adus la cunoştinţa con-

CNDDCM în mod de urgență, pentru a putea fi identificată procedura de soluționare a incidentului.

IV.Drepturile subiecților de date cu caracter personal

1. 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 informații, exceptînd cazul în care el deține deja informațiile 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;*
- *existența drepturilor la informare și de acces la datele colectate;*
- *de intervenție asupra datelor* (în special de a rectifica, actualiza, bloca sau șterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora) *și de opoziție, precum și condițiile în care aceste drepturi pot fi exercitate;*

Dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația și posibilitatea de a lua cunoștință cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum și împotriva altor erori comise la înscrierea datelor despre sine.

În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alți subiecți, conținute în actele procesuale (*materialele cauzei*), cu excepția cazurilor în care solicitanții își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal.

2. Dezvăluirea prin transmitere, diseminare sau în orice alt mod a datelor cu caracter personal prelucrate în scopul înfăptuirii justiției urmează a fi interzisă, cu excepția cazurilor cînd subiectul de date cu caracter personal și-a dat consimțămîntul, cînd informația este depersonalizată ori cînd legea ori tratatul internațional prevede expres dreptul destinatarului sau al terțului în acest sens. În acest caz, legea specială sau tratatul internațional trebuie să conțină în mod obligatoriu garanții privind protecția drepturilor subiectului datelor cu caracter personal.

3. Aplicarea excepțiilor și restricțiilor realizării de către subiecții de date cu caracter personal a drepturilor sale, urmează a fi făcute în strictă conformitate cu prevederile art. 15 al Legii privind protecția datelor cu caracter personal.

V. Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate în cazul activității în domeniu

1. Stocarea și păstrarea datelor cu caracter personal consemnate în documentele procedurale cît și în materialele de control, urmează a fi restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate instituționale aprobate.

2. 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, inclusiv

antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului - urmează a fi interzisă.

3. Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu urmează a fi interzisă. De exemplu: *în cazurile în care angajatul se concediază, iar informația acumulată rămîne păstrată pe purtătorul magnetic intern al dispozitivului, acesta va avea în calculatorul personal serii structurate de date cu caracter personal colectate în procesul exercitării activităților ce țin de procedurile DDCM ori de alt gen, iar în cazul defectării persoana care efectuează reparația acestor utilaje poate, fără careva eforturi, să copie informațiile stocate în calculator, ambele situații constituinduse ca grave incidente de securitate. În context, aplicarea principiilor privind protecția datelor cu caracter personal, necesită a fi reglementate prin ordinele și dispozițiile superiorilor, cu verificarea periodică a încăperilor și a utilajului din dotarea angajaților. Mai mult, accesul la computerele din dotare urmează a fi protejat/restricționat prin crearea profilurilor de utilizatori, iar drepturile de administrator să fie încredințate doar persoanei responsabile pentru implementarea politicii de securitate desemnate din cadrul instituției.*

VI. SECURITATEA MEDIULUI FIZIC ȘI A TEHNOLOGIILOR INFORMAȚIONALE FOLOSITE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Autorizarea accesului fizic.

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

2. Accesul în camera de servere este permisă doar personalului IT. Personalului străin are acces în această încăpere doar sub stricta supraveghere a unui specialist IT. Toate operațiunile de acces la servere sau alte mijloace tehnice sau software se face de personalul IT al CNSDM.

Administrarea și monitorizarea accesului fizic.

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

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

3. Registrele de monitorizare se păstrează minimum un an, la expirarea căruia acestea se lichidează, iar datele și documentele ce se conțin în registrul supus lichidării se transmit în arhivă.

4. Încăperile unde sînt instalate sistemele informaționale de date cu caracter personal se echipează cu sisteme de control al accesului și supraveghere video în scopul urmăririi accesului persoanelor în aceste spații.

5. În procesul monitorizării se utilizează mijloace de supraveghere și alarmă în regim real de timp a tuturor cazurilor de acces autorizat și/sau neautorizat.

6. Sînt utilizate mijloace automatizate care asigură identificarea cazurilor de acces neautorizat și inițierea acțiunilor de blocare a accesului.

7. Toate fișele personale ale fiecărui angajat, inclusiv carnetele de muncă sînt păstrate în safeu metallic, ocrotit împotriva incendiilor.

Securitatea sediilor/oficiilor/birourilor şi mijloacelor de prelucrare a datelor cu caracter personal.

1. Perimetrul de securitate se determină concret şi clar. Perimetrul clădirii sau încăperii în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal trebuie să fie integru din punct de vedere fizic.

2. Pereţii exteriori ai încăperilor trebuie să fie rezistenţi, intrările echipate cu lacăte, mijloace de control al accesului, semnalizare etc.

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

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

5. Uşile şi ferestrele se încuie în cazul în care în încăpere lipsesc angajaţii.

6. Agendele şi/sau cărţile de telefoane în care se conţin indicii despre locul amplasării mijloacelor de prelucrare a datelor cu caracter personal nu vor fi accesibile persoanelor străine.

7. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal trebuie să răspundă necesităţii asigurării securităţii acestora contra accesului nesancţionat, furturilor, incendiilor, inundaţiilor şi altor posibile riscuri.

8. 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 deţinătorului de date cu caracter personal.

9. Utilajul de rezervă şi purtătorii de informaţii care conţin date cu caracter personal se păstrează în locuri care permit evitarea distrugerilor sau deteriorărilor cu rezultat al calamităţilor în sediul/oficiul/biroul de bază.

Controlul vizitatorilor.

1. Vizitatorii încăperilor unde sînt amplasate sisteme informaţionale şi mecanice de date cu caracter personal vor fi supravegheaţi în încăperile unde au acces. În birourile cu acces interzis aceştia pot intra doar sub supravegherea personalului autorizat.

2. În cazul depistării persoanelor cu acces interzis în birourile cu acces limitat, acestia vor fi invitaţi să părăsească în mod cît mai urgent. Incidentul va fi adus la cunoştinţa personalului IT şi persoanei responsabile de regulamentul de securitate a datelor cu caracter personal.

3. Accesul vizitatorilor se înregistrează în registre, care se păstrează minimum un an. La expirarea termenului de un an, registrele sînt lichidate, iar datele şi documentele ce se conţin în registrul supus lichidării se transmit în arhivă.

Securitatea electroenergetică.

Se asigură securitatea echipamentului electric utilizat pentru menţinerea funcţionalităţii sistemelor informaţionale şi mecanice de date cu caracter personal, a cablurilor electrice, inclusiv protecţia acestora contra deteriorărilor şi conectărilor nesancţionate. În cazul apariţiei situaţiilor excepţionale, de avarie sau de forţă majoră, trebuie asigurată posibilitatea deconectării electricităţii la sistemele informaţionale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

Securitatea cablurilor de reţea.

Cablurile de reţea, prin care se efectuează operaţiuni de prelucrare a datelor cu caracter personal, sînt protejate contra conectărilor nesancţionate sau deteriorărilor. Cablurile de tensiune sunt separate de cele comunicaţionale pentru a exclude bruiajul. Specialiştii

CNDDCM efectuază controale, nu mai rar decît o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de rețea.

Asigurarea securității antiincendiare a sistemelor informaționale de date cu caracter personal.

CNDDCM dispune de mijloace de asigurare a securității antiincendiare sediilor/oficiilor/birourilor unde sînt amplasate sisteme informaționale și mecanice de date cu caracter personal și mijloace de prelucrare a datelor cu caracter personal.

Controlul instalării și scoaterii componentelor TI.

Se exercită 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, evitîndu-se folosirea funcțiilor standarde de nimicire.

Măsurile generale de administrare a securității informaționale

În cazul neutilizării temporare a purtătorilor de informație pe suport de hîrtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri, dulapuri metalice sau arhiva instituției care se încuie. Computerele, terminalele de acces și imprimantele sînt 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. Accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate este interzis și controlat. 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 Consiliului. Scoaterea și introducerea mijloacelor de prelucrare a datelor cu caracter personal din/în perimetrul de securitate se înregistrează.

VII. IDENTIFICAREA ȘI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAȚIONAL DE DATE CU CARACTER PERSONAL

Identificarea și autentificarea utilizatorului

1. Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale și mecanice de date cu caracter personal și a proceselor executate în numele acestor utilizatori. Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică și mecanică, administratorii de rețea, programatorii și administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului) care nu conține semnalmentele nivelului de accesibilitate al utilizatorului pentru confirmarea ID-ului utilizatorului sînt utilizate parole precum și semnării declarației de confidențialitate a personalului care asigură susținerea mecanică). 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 în mod automat în decursul a două săptămîni de la ultimul acces sau în mod individual imediat la momentul întroducerii modificării în raportul de muncă.

2. Se utilizează autentificarea multifactorială, care include parole complexe, cu includerea simbolurilor, literelor, cifrelor în combinație complex. În mod obligatoriu fiecare pa

conține una sau mai multe litere scrise cu majusculă. Parola nu va conține inițialele sau datele care pot caracteriza o anumită persoană (data de naștere, adresă, poreclă etc.).

Identificarea și autentificarea echipamentului.

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

Administrarea identificatorilor utilizatorilor.

Administrarea identificatorilor utilizatorilor include:

- identificarea univocă a fiecărui utilizator;
- verificarea autenticității fiecărui utilizator;
- obținerea autorizației de la persoana responsabilă pentru eliberarea ID-ului utilizatorului doar în cazul semnării declarației de confidențialitate și trecerii procedurii de instruire;
- garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;
- dezactivarea contului de utilizator după o perioadă inactivă, stabilită în timp (2 săptămîni);
- executarea copiilor de arhivă a ID-urilor utilizatorilor.

Asigurarea conexiunii bilaterale în cazul introducerii informației de autentificare a utilizatorilor

Se asigură conexiunea bilaterală a deținătorului de date cu caracter personal cu utilizatorul în momentul trecerii de către acesta a procedurilor de autentificare, care nu compromit mecanismul de autentificare.

Utilizarea parolelor în procesul asigurării securității informaționale

Se respectă regulile de asigurare a securității informaționale în cazul alegerii și folosirii parolelor care includ:

- păstrarea confidențialității 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;
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

Administrarea parolelor utilizatorilor.

Se folosește 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. Este asigurată păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o perioada de un an) și prevenirea folosirii repetate a acestora. La momentul introducerii, parolele nu se reflectă în clar pe monitor. Parolele se păstrează în formă cifrată, utilizîndu-se algoritmul criptografic unilateral (funcția hash).

VIII. ADMINISTRAREA ACCESULUI UTILIZATORILOR

Administrarea accesului.

Se implementează mecanisme de înregistrare și evidență a persoanelor care au acces sau participă la operațiunile de prelucrare a datelor cu caracter personal și care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare a datelor cu caracter personal.

Administrarea conturilor de acces (account-urilor).

Este efectuată administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Sînt folosite mijloace automatizate de suport în scopul administrării conturilor de acces. Acţiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea unei perioade stabilite în timp (5 zile de inactivitate a conturilor). Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

Acordarea accesului

Este autorizat accesul la sistemele informaţionale şi mecanice de date cu caracter personal în conformitate cu prezentul regulament de securitate persoanei responsabile stabilită prin Ordinul CNDDCM.

Revizuirea drepturilor de acces ale utilizatorilor.

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

Repartizarea obligaţiilor şi învestirea cu minimul de drepturi şi competenţe.

Repartizarea obligaţiilor subiecţilor care asigură funcţionarea sistemelor informaţionale şi mecanice de date cu caracter personal este efectuată prin intermediul învesturii cu drepturi/competenţe corespunzătoare de acces, prin Ordinul Consiliului întocmit în acest sens. Utilizatorii sistemelor informaţionale şi mecanice de date cu caracter personal se învestesc doar cu acele drepturi/competenţe, care sînt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

Informaţii de avertizare

Înainte de acordarea accesului în sistem, utilizatorii sînt informaţi despre faptul că folosirea sistemelor informaţionale şi mecanice de date cu caracter personal este controlată şi că folosirea neautorizată a acestora se urmăreşte în conformitate cu legislaţia.

Blocarea sesiunii de lucru.

Sesiunea de lucru în sistemul informaţional, destinat prelucrării datelor cu caracter personal, se blochează automat, după maximum 5 minute de perioadă 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 şi autentificare.

Controlul administrării accesului.

Se efectuează controlul acţiunilor utilizatorului în vederea evaluării corectitudinii şi conformării operaţiunilor şi acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

Marcarea documentelor.

Informaţia ieşită din sistem, care conţine date cu caracter personal, se marchează, indicîndu-se prescripţii pentru prelucrarea ulterioară şi răspîndirea acesteia, inclusiv indicîndu-se numărul de identificare unic al deţinătorului de date cu caracter personal.

Accesul de la distanţă.

Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal trebuie securizate (utilizîndu-se VPN, criptarea, cifrarea etc.), precum şi sînt documentate, supuse monitorizării şi controlului. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de persoana responsa

din cadrul CNDDCM și este permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

Limitarea folosirii tehnologiilor fără fir.

Accesul fără fir la sistemele informaționale de date cu caracter personal este documentat, supus monitorizării și controlului. 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 personalul IT al CNDDCM.

Administrarea accesului echipamentului portativ și mobil

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 personalul IT al CNDDCM.

IX. PROTECȚIA SISTEMELOR INFORMAȚIONALE ȘI COMUNICAȚIILOR ÎN CARE SÎNT PRELUCRATE DATE CU CARACTER PERSONAL

Divizarea programelor applicative.

Se asigură separarea posibilităților funcționale ale utilizatorului de posibilitățile funcționale de gestionare a sistemelor informaționale și mecanice de date cu caracter personal.

Izolarea funcțiilor de securitate.

Se asigură izolarea funcțiilor de securitate de funcțiile care nu se atribuie la securitatea sistemelor informaționale și mecanice de date cu caracter personal.

Informația restantă.

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

Protecția contra refuzului în serviciu.

Se asigură protecția sistemelor informaționale și mecanice de date cu caracter personal sau limitate posibilitățile de realizare a atacurilor de diferite tipuri, inclusiv DOS (denial of service) - „refuz în serviciu".

Prioritățile resurselor.

Este asigurată posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităților, a folosirii resurselor informaționale și mecanice în care sînt prelucrate date cu caracter personal.

Protecția perimetrului sistemelor informaționale în care sînt prelucrate date cu caracter personal.

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 informaționale. Amplasarea resurselor general accesibile se asigură în spațiile special destinate a rețelei de calcul cu interfețele fizice de rețea. Este asigurată imposibilitatea accesului din exterior a utilizatorilor la rețeaua internă în care se prelucrează date cu caracter personal.

Asigurarea integrității datelor cu caracter personal transmise.

Se asigură integritatea datelor cu caracter personal transmise, utilizîndu-se mijloacele de protecție criptografică.

Asigurarea confidențialității datelor cu caracter personal transmise.

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

X. AUDITUL SECURITĂȚII ÎN SISTEMELE INFORMAȚIONALE DE DATE CU CARACTER PERSONAL.

Generarea înregistrărilor de audit în sistemele informaționale și mecanice de date cu caracter personal.

Responsabilul de administrarea sistemului este obligat să întocmească următoarele proceduri obligatorii de audit al sistemului:

- Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:

a) data și timpul tentativei intrării/ieșirii;

b) ID-ul utilizatorului;

c) rezultatul tentativei de intrare/ieșire – pozitivă sau negativă.

- Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative și proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:

a) data și timpul tentativei de pornire;

b) denumirea/identificatorul programului aplicativ sau procesului;

c) ID-ul utilizatorului;

d) rezultatul tentativei de pornire – 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:

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

b) denumirea (identificatorul) aplicației sau procesului;

c) ID-ul utilizatorului;

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

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

f) rezultatul tentativei de obținere a accesului (executare a operațiunii) – pozitivă sau negativă.

- Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:

a) data și timpul modificării competențelor;

b) ID-ul administratorului care a efectuat modificările;

c) 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:

a) data și timpul eliberării;

b) denumirea informației și căile de acces la aceasta;

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

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

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

Prelucrarea rezultatelor auditului securității în sistemele informaționale de date cu caracter personal.

În caz de deranjament al auditului securității în sistemele informaționale de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informată persoana responsabilă de politica de securitate a datelor cu caracter personal și întreprinse măsuri în vederea restabilirii capacității de lucru a sistemului de audit.

Monitorizarea, analiza și generarea rapoartelor de audit a securității în sistemele informaționale de date cu caracter personal.

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

Protejarea datelor de audit a securității în sistemele informaționale de date cu caracter personal

Rezultatele auditului securității în sistemele informaționale și mecanice de date cu caracter personal, care reprezintă operațiuni de prelucrare a datelor cu caracter personal și mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidențialității și integrității acestora.

Păstrarea datelor de audit a securității în sistemele informaționale de date cu caracter personal

Durata stocării rezultatelor auditului securității în sistemele informaționale de date cu caracter personal se justifică în regulamentul de securitate a datelor cu caracter personal, dar în orice caz acest termen nu este mai mic de **2 ani**, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care investigările sau procesele judiciare se prelungesc, rezultatele auditului se păstrează pe toată durata acestora.

XI. ASIGURAREA INTEGRITĂȚII INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL ȘI A TEHNOLOGIILOR INFORMAȚIONALE

Înlăturarea deficiențelor de soft destinat prelucrării datelor cu caracter personal.

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

Asigurarea protecției contra programelor dăunătoare (virușilor).

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

2. Se asigură administrarea centralizată a mecanismelor de protecție contra programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal.

Tehnologiile și mijloacele de constatare a intruziunilor

Se utilizează tehnologii și mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaționale și mecanice de date cu caracter personal.

constatarea atacurilor, inclusiv care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaționale și mecanice.

Asigurarea integrității soft-urilor și informației

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.

Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de 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).

XII. COPIILE DE REZERVĂ ȘI RESTABILIREA INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL, ȘI IT

Copiile de rezervă ale informației care conține date cu caracter personal

Copiile de siguranță a informațiilor care conțin date cu caracter personal și soft-urile folosite pentru prelucrările automatizate a datelor cu caracter personal, sunt efectuate odată la 24 ore, fiind păstrate cel puțin 1 an în locuri sigure cu acces limitat (safeu). 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.

XIII. GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR INFORMAȚIONALE DE DATE CU CARACTER PERSONAL

Instructajul de reacționare la incidentele de securitate a sistemelor informaționale de date cu caracter personal.

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

Prelucrarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal.

În cazul depistării unui incident de securitate, este asigurat mecanismul de informare neîntîrziată a conducerii CNDDCM. Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor și restabilirea securității.

Monitorizarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal.

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

2. Sînt utilizate mijloace automatizate pentru urmărirea incidentelor de securitate a sistemelor informaționale de date cu caracter personal, colectarea și analiza informației despre aceste incidente.

Prezentarea rapoartelor despre incidentele de securitate a sistemelor informaționale de date cu caracter personal

Anual, către 31 ianuarie, persoana responsabilă de regulamentul de [illegible] Centrului Național pentru Protecția Datelor cu Caracter Persoanl raportul [illegible] incidentele de securitate a sistemelor informaționale de date cu caracter [illegible]