Republica Moldova

GUVERNUL

HOTĂRÎRE Nr. 1123
din 14.12.2010

privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal

Publicat : 24.12.2010 în Monitorul Oficial Nr. 254-256 art Nr : 1282

În temeiul alin. (2) art. 14 din Legea nr.17-XVI din 15 februarie 2007 cu privire la protecţia datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2007, nr.107-111, art.468), cu modificările şi completările ulterioare, Guvernul HOTĂRĂŞTE:

1. Se aprobă Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal (se anexează).

2. Deţinătorii de date cu caracter personal vor întreprinde măsurile necesare privind implementarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal, în termen de 12 luni de la intrarea în vigoare a prezentei Hotărîri.

PRIM-MINISTRU **Vladimir FILAT**

Contrasemnează:
Ministrul tehnologiilor informaţionale şi comunicaţiilor **Alexandru Oleinic**

nr. 1123. Chişinău, 14 decembrie 2010.

Aprobate
prin Hotărîrea Guvernului
nr.1123 din 14 decembrie 2010

CERINŢELE
faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal

I. DISPOZIŢII GENERALE

1. Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal (în continuare – Cerinţe) au drept scop stabilirea regulilor minime de implementare de către deţinătorii de date cu caracter personal a măsurilor tehnice şi organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale de date cu caracter personal şi/sau registrelor

ținute manual, în conformitate cu prevederile Legii nr.17-XVI din 15 februarie 2007 cu privire la protecția datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2007, nr.107-111, art.468) şi ale Legii nr. 71-XVI din 22 martie 2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314).

2. Prezentele Cerințe creează cadrul necesar aplicării Convenției pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiate la Strasbourg la 28 ianuarie 1981, publicate în European Treaty Series, nr. 108, ratificate de Republica Moldova prin Hotărîrea Parlamentului nr. 483-XIV din 2 iulie 1999.

3. În sensul prezentelor Cerințe, se definesc următoarele noțiuni:

autentificare – verificarea identificatorului atribuit subiectului de acces, confirmarea autenticității;

control de securitate – acțiuni întreprinse de către deținătorii de date cu caracter personal sau Centrul Național pentru Protecția Datelor cu Caracter Personal (în continuare – Centrul) în vederea verificării şi/sau asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaționale şi/sau registrelor ținute manual, în conformitate cu prezentele Cerințe;

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

identificare – atribuirea unui identificator subiecților şi obiectelor de acces şi/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

integritate – certitudinea, necontradictorialitatea şi actualitatea informației care conține date cu caracter personal, protecția ei de distrugere şi modificare neautorizată;

mijloace de protecție criptografică a informației care conține date cu caracter personal – mijloace tehnice, de program şi tehnico-aplicative, sisteme şi complexe de sisteme ce realizează algoritmi de conversie criptografică a informației care conține date cu caracter personal, destinate să asigure integritatea şi confidențialitatea informației în procesul de prelucrare, depozitare şi 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 şi față de drepturile şi libertățile persoanelor, stabilit conform Cerințelor, elaborat şi actualizat corespunzător nivelului dezvoltării tehnologice şi costurilor implementării acestor măsuri (N - 1 sau N - 2);

politica de securitate a datelor cu caracter personal – document, elaborat de către deținătorul de date cu caracter personal, care oferă o descriere precisă a măsurilor de securitate şi trăsăturilor de protecție selectate pentru securitatea datelor, ținîndu-se cont de potențialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sînt expuse acestea;

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

persoana responsabilă de politica de securitate a datelor cu caracter personal – persoana responsabilă de funcționarea corespunzătoare a sistemului complex de protecție a informației care conține date cu caracter personal, precum şi de elaborarea, implementarea şi 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 şi 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 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 informațională ((TI) eng. informational technology) – totalitatea metodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informației care conține date cu caracter personal şi 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 şi aplicației de utilizare a resursei informaționale sau din momentul pornirii resursei informaționale şi pînă la momentul opririi acestora;

sistem informațional de date cu caracter personal – totalitatea resurselor şi tehnologiilor informaționale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informație care conține date cu caracter personal;

stocare – păstrarea pe orice fel de suport a datelor cu caracter personal.

II. CERINȚE GENERALE

4. Măsurile de protecție a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare şi exploatare a sistemului informațional de date cu caracter personal şi vor fi efectuate neîntrerupt de către toți deținătorii de date cu caracter personal.

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

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

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

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

1) suporturile magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale şi baze de date;

2) sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date şi alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare şi multiplicare a documentelor şi alte mijloace tehnice de prelucrare a informației.

9. Protecția datelor cu caracter personal în sistemele informaționale 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 şi resursele informaționale;

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

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

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

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

1) preîntîmpinarea conexiunilor neautorizate la rețelele telecomunicaționale şi 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 şi de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic şi de program;

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

11. 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.

12. 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.

13. Preîntîmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor antivirus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă.

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

III. POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

15. Fiecare deţinător de date cu caracter personal, reieşind din specificul activităţii, elaborează şi organizează implementarea prevederilor documentului care stabileşte politica de securitate a datelor cu caracter personal, inclusiv procedurile şi măsurile legate de realizarea acestei politici, cu aplicarea soluţiilor practice cu un nivel de detalizare şi complexitate proporţional, în partea ce ţine de identificarea şi autentificarea utilizatorilor; de reacţionare la incidentele de securitate; de protecţie a TI şi comunicaţiilor; de asigurare a integrităţii informaţiei care conţine date cu caracter personal şi TI; de administrare a accesului; de audit şi asigurare a evidenţei, luînd în considerare:

1) categoria datelor cu caracter personal prelucrate şi a operaţiunilor de prelucrare efectuate asupra lor (conform anexelor nr.1 şi nr.2 la prezentele Cerinţe);

2) dimensiunea deţinătorului de date cu caracter personal, în funcţie de numărul angajaţilor, numărul subdiviziunilor administrative, amplasarea geografică a subdiviziunilor sau filialelor etc., inclusiv numărul persoanelor care pot accesa datele cu caracter personal;

3) formele de ţinere a registrelor în care sînt prelucrate date cu caracter personal (manuală, electronică sau mixtă);

4) complexitatea sistemelor informaţionale de date cu caracter personal şi programelor de aplicaţii implicate în procesul de prelucrare a datelor;

5) riscurile la care este expus deţinătorul de date cu caracter personal sau persoanele ale căror date cu caracter personal sînt prelucrate, starea de dezvoltare tehnologică în acest domeniu şi costul măsurilor de implementare.

16. Politica 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 la cel mai înalt nivel al ierarhiei persoanelor responsabile ale deţinătorului de date cu caracter personal.

Pentru ca politica de securitate a datelor cu caracter personal să fie cunoscută tuturor, acest document este adus la cunoştinţă utilizatorilor şi altor angajaţi ai deţinătorului de date cu caracter personal, în limitele competenţelor funcţionale şi nivelului de acces acordat.

17. Deţinătorul de date cu caracter personal numeşte o persoană responsabilă de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, subordonată nemijlocit conducătorului instituţiei, care nu va avea alte responsabilităţi incompatibile cu sarcinile funcţiei de implementare a politicii.

18. Persoana responsabilă de politica de securitate a datelor cu caracter personal va dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici.

19. Persoana responsabilă de politica de securitate a datelor cu caracter personal asigură definirea clară a diferitelor responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al

intereselor personale sau alte împrejurări.

20. Deținătorii de date cu caracter personal întreprind următoarele acțiuni:

1) definesc clar responsabilitățile şi procesele de management al securității datelor cu caracter personal, cu integrarea lor corespunzătoare în structura organizațională şi de funcționare generală;

2) asigură măsuri tehnice şi organizaționale necesare organizării procesului de management al securității datelor cu caracter personal;

3) elaborează procedurile de clasificare a informației care conține date cu caracter personal astfel încît să fie posibil de întocmit un nomenclator şi toate datele cu caracter personal care sînt prelucrate să fie localizate, indiferent de tipul purtătorului de date;

4) instruiesc persoanele implicate în procesul de prelucrare a datelor cu caracter personal în vederea îndeplinirii de către acestea a atribuțiilor funcționale şi asumării responsabilităților de securitate a datelor cu caracter personal, inclusiv asupra confidențialității acestora.

21. Documentația referitoare la politica de securitate a datelor cu caracter personal este centralizată, completă, actualizată cu regularitate şi conține cel puțin următoarele elemente:

1) identitatea persoanei responsabile de politica de securitate;

2) măsurile de securitate;

3) mecanismul de punere în aplicare a măsurilor de securitate;

4) nomenclatorul datelor cu caracter personal prelucrate, a localizării acestora şi a operațiunilor efectuate asupra lor;

5) lista nominală a utilizatorilor, autorizați să acceseze datele cu caracter personal;

6) configurarea sistemului informațional de date cu caracter personal şi a rețelei;

7) descrierea detaliată a criteriilor, în conformitate cu care sînt accesibile datele cu caracter personal prelucrate în registrul ținut manual;

8) documentația tehnică cu privire la controalele de securitate;

9) orarul controalelor de securitate;

10) măsurile de detectare a cazurilor de acces şi/sau de prelucrare neautorizată a datelor cu caracter personal;

11) rapoarte despre incidentele de securitate.

IV. SECURITATEA MEDIULUI FIZIC ŞI A TEHNOLOGIILOR INFORMAȚIONALE FOLOSITE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Secțiunea 1
Autorizarea accesului fizic

22. Pentru categoria N-1

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 şi doar în timpul orelor de program, conform listei şi însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare, cartele cu microprocesoare).

Conducătorii deținătorilor de date cu caracter personal elaborează şi aprobă listele de acces, care se revizuiesc nu mai rar decît o dată în lună şi însemnele care autorizează accesul.

23. Suplimentar pentru categoria N-2

Accesul se efectuează în baza cartelelor de identificare, cartelelor cu microprocesoare sau altor tehnologii.

Secțiunea 2
Administrarea şi monitorizarea accesului fizic

24. Pentru categoria N-1

Se efectuează administrarea şi monitorizarea accesului fizic 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.

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

25. Suplimentar pentru categoria N-2

Încăperile unde sînt instalate sistemele informaţionale de date cu caracter personal se echipează cu sisteme de control al accesului şi supraveghere video în scopul urmăririi accesului persoanelor în aceste spaţii.

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

Sînt utilizate mijloace automatizate care asigură identificarea cazurilor de acces neautorizat şi iniţierea acţiunilor de blocare a accesului.

Secţiunea 3
Securitatea sediilor/oficiilor/birourilor şi mijloacelor de prelucrare a datelor cu caracter personal

26. Pentru categoria N-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.

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

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.

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

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

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.

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.

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.

Purtătorii de informaţii şi mijloacele de prelucrare a datelor cu caracter personal scoase din încăperile aflate în perimetrul de securitate nu trebuie lăsate fără supraveghere în locuri publice.

27. Suplimentar pentru categoria N-2

Se implementează sisteme de constatare a intruziunilor pentru uşile exterioare şi ferestrele amplasate în locuri accesibile.

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

Secţiunea 4
Controlul vizitatorilor

28. Pentru categoria N-1

Trebuie asigurat controlul accesului fizic al vizitatorilor în încăperile unde sînt amplasate sistemele informaţionale de date cu caracter personal.

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.

29. Suplimentar pentru categoria N-2

Vizitatorii sistemelor informaţionale de date cu caracter personal trebuie să fie însoţiţi de persoane împuternicite în asemenea scop, cu exercitarea în paralel a controlului asupra acţiunilor acestora.

Secțiunea 5
Securitatea electroenergetică

30. Pentru categoria N-1

Se asigură securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor şi conectărilor nesancționate.

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.

Trebuie prevăzute surse autonome de alimentare cu energie electrică de scurtă durată, care sînt folosite pentru terminarea corectă a sesiunii de lucru a sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică.

31. Suplimentar pentru categoria N-2

Sînt prevăzute şi asigurate surse de alimentare cu energie electrică de lungă durată, care sînt folosite în cazul deconectării pentru perioade îndelungate şi necesității continuării îndeplinirii de către sistemele informaționale de date cu caracter personal a sarcinilor funcționale stabilite.

Secțiunea 6
Securitatea cablurilor de rețea

32. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Cablurile de tensiune trebuie separate de cele comunicaționale pentru a exclude bruiajul.

Deținătorii de date cu caracter personal efectuează controale, nu mai rar decît o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de rețea.

Secțiunea 7
Asigurarea securității antiincendiare a sistemelor informaționale de date cu caracter personal

33. Pentru categoria N-1

Se prevăd mijloace de asigurare a securității antiincendiare a sediilor/oficiilor/birourilor unde sînt amplasate sistemele informaționale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

34. Suplimentar pentru categoria N-2

Se implementează sisteme automatizate de depistare/semnalizare şi stingere a incendiilor în sediile/oficiile/birourile unde sînt amplasate sistemele informaționale de date cu caracter personal şi mijloacele de prelucrare a datelor cu caracter personal.

Secțiunea 8
Controlul instalării şi scoaterii componentelor TI

35. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Se exercită controlul şi evidența instalării şi scoaterii mijloacelor de program, mijloacelor tehnice şi celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal. Informațiile, care conțin date cu caracter personal şi care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu şi se nimicesc prin metode sigure, evitîndu-se folosirea funcțiilor standarde de nimicire.

Secțiunea 9
Măsurile generale de administrare a securității informaționale

36. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Computerele, terminalele de acces şi imprimantele sînt deconectate la terminarea sesiunilor de lucru.

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

Trebuie administrat accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia 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 deținătorului de date cu caracter personal.

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

V. IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAȚIONAL DE DATE CU CARACTER PERSONAL

Secțiunea 1
Identificarea şi autentificarea utilizatorului

37. Pentru categoria N-1

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

Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii şi administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmentele nivelului de accesibilitate al utilizatorului.

Pentru confirmarea ID-ului utilizatorului sînt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice şi individuale ale persoanei.

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

38. Suplimentar pentru categoria N-2

Se utilizează autentificarea multifactorială (complexă), care include parole şi mijloace fizice speciale de acces cu memorie ori cartele cu microprocesoare sau parole şi mijloace biometrice de autentificare.

Secțiunea 2
Identificarea şi autentificarea echipamentului

39. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 3
Administrarea identificatorilor utilizatorilor

40. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Administrarea identificatorilor utilizatorilor include:

1) identificarea univocă a fiecărui utilizator;

2) verificarea autenticității fiecărui utilizator;

3) obținerea autorizației de la persoana responsabilă pentru eliberarea ID-ului utilizatorului;

4) garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;

5) dezactivarea contului de utilizator după o perioadă inactivă, stabilită în timp (inacțiune în perioada de maximum 2 luni);

6) executarea copiilor de arhivă a ID-urilor utilizatorilor.

Secțiunea 4
Administrarea mijloacelor de autentificare

41. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Deținătorii de date cu caracter personal determină procedurile administrative, care reglementează procesul distribuirii şi ridicării mijloacelor de autentificare a utilizatorilor, inclusiv acțiunile în cazul pierderii/compromiterii sau defecțiunii acestora.

După instalarea sistemului, se schimbă informațiile de autentificare a utilizatorilor utilizate standard.

Secțiunea 5
Asigurarea conexiunii bilaterale în cazul introducerii informației de autentificare a utilizatorilor

42. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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 compromite mecanismul de autentificare.

Secțiunea 6
Utilizarea parolelor în procesul asigurării securității informaționale

43. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

1) păstrarea confidențialității parolelor;

2) interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia;

3) modificarea parolelor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri a sistemului sau parolei;

4) 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 şi nu sînt compuse integral din grupuri de cifre sau litere;

5) modificarea parolelor peste intervale de maximum 3 luni;

6) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

Secțiunea 7
Administrarea parolelor utilizatorilor

44. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

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

Se asigură blocarea accesului după trei tentative greşite de autentificare.

Este asigurată păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o perioada de un an) şi 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).

VI. ADMINISTRAREA ACCESULUI UTILIZATORILOR

Secțiunea 1
Administrarea accesului

45. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 2
Administrarea conturilor de acces (account-urilor)

46. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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.

Acțiunea conturilor de acces a utilizatorilor temporari, care prelucrează date cu caracter personal, încetează automat la expirarea unei perioade stabilite în timp (pentru fiecare tip de cont de acces în parte).

Sînt dezactivate automat, după o perioadă de maximum trei luni, conturile de acces ale utilizatorilor

neactivi, care prelucrează date cu caracter personal.

Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acțiunii conturilor de acces.

Secțiunea 3

Acordarea accesului

47. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Este autorizat accesul la sistemele informaționale de date cu caracter personal în conformitate cu politica de administrare a accesului stabilită de deținătorul de date cu caracter personal.

Accesul la funcțiile de securitate ale sistemelor informaționale de date cu caracter personal şi la datele acestora este acordat doar persoanelor responsabile indicate expres în politica de securitate a deținătorului de date cu caracter personal.

Secțiunea 4

Revizuirea drepturilor de acces ale utilizatorilor

48. Pentru toate categoriile sistemelor informaționale 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 şase luni) şi după oricare schimbare de statut al utilizatorului.

Secțiunea 5

Administrarea fluxurilor informaționale

49. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Se autorizează de către deținătorii de date cu caracter personal realizarea fluxurilor informaționale în procesul transmiterii acestora în interiorul şi în afara sistemelor informaționale de date cu caracter personal.

Secțiunea 6

Repartizarea obligațiilor şi învestirea cu minimul de drepturi şi competențe

50. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Repartizarea obligațiilor subiecților care asigură funcționarea sistemelor informaționale de date cu caracter personal este efectuată prin intermediul învestirii cu drepturi/competențe corespunzătoare de acces, printr-un act administrativ al conducerii deținătorului de date cu caracter personal.

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

Secțiunea 7

Informații de avertizare

51. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 8

Blocarea sesiunii de lucru

52. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Sesiunea de lucru în sistemul informațional, destinat prelucrării datelor cu caracter personal, se blochează (la solicitarea utilizatorului sau automat, după maximum 15 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.

Secțiunea 9

Controlul administrării accesului

53. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Se efectuează controlul acțiunilor utilizatorului în vederea evaluării corectitudinii şi conformării operațiunilor şi acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

Secțiunea 10
Marcarea documentelor

54. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Informația ieşită din sistem, care conține date cu caracter personal, se marchează, indicîndu-se prescripții pentru prelucrarea ulterioară şi răspîndirea acesteia, inclusiv indicîndu-se numărul de identificare unic al deținătorului de date cu caracter personal.

Secțiunea 11
Accesul de la distanță

55. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Toate metodele de acces de la distanță la sistemele informaționale 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 distanță la sistemele informaționale de date cu caracter personal se autorizează de persoanele responsabile ale deținătorilor de date cu caracter personal şi permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

Secțiunea 12
Limitarea folosirii tehnologiilor fără fir

56. Pentru toate categoriile sistemelor informaționale de date cu caracter personal se stabilesc limitări şi se elaborează reguli de folosire a tehnologiilor fără fir care permit accesul la sistemele informaționale de date cu caracter personal.

Accesul fără fir la sistemele informaționale de date cu caracter personal este documentat, supus monitorizării şi 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 persoanele responsabile ale deținătorului de date cu caracter personal.

Secțiunea 13
Administrarea accesului echipamentului portativ şi mobil

57. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Se stabilesc limitări şi se elaborează reguli de folosire a echipamentului portativ şi mobil care permit accesul la sistemele informaționale de date cu caracter personal.

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

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

VII. PROTECȚIA SISTEMELOR INFORMAȚIONALE ŞI COMUNICAȚIILOR ÎN CARE SÎNT PRELUCRATE DATE CU CARACTER PERSONAL

Secțiunea 1
Divizarea programelor aplicative

58. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 2
Izolarea funcțiilor de securitate

59. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 3
Informația restantă

60. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 4

Protecția contra refuzului în serviciu

61. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 5

Prioritățile resurselor

62. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 6

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

63. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Se efectuează monitorizarea permanentă şi 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.

Secțiunea 7

Asigurarea integrității datelor cu caracter personal transmise

64. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 8

Asigurarea confidențialității datelor cu caracter personal transmise

65. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

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

Secțiunea 1

Generarea înregistrărilor de audit în sistemele informaționale de date cu caracter personal

66. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Deținătorii de date cu caracter personal organizează generarea înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului.

Secțiunea 2

Lista evenimentelor înregistrate de sistemul de audit a securității în sistemele informaționale de date cu caracter personal

67. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

a) data şi timpul tentativei intrării/ieşirii;

b) ID-ul utilizatorului;
c) rezultatul tentativei de intrare/ieşire – pozitivă sau negativă.
2) Este efectuată înregistrarea tentativelor de pornire/terminare a sesiunii de lucru a programelor aplicative şi proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor şi statutul obiectelor de acces conform următorilor parametri:
a) data şi timpul tentativei de pornire;
b) denumirea/identificatorul programului aplicativ sau procesului;
c) ID-ul utilizatorului;
d) rezultatul tentativei de pornire – pozitivă sau negativă.
3) Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații şi procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
a) data şi 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 fişier, număr etc.);
e) tipul operațiunii solicitate (citire, înregistrare, ştergere etc.);
f) rezultatul tentativei de obținere a accesului (executare a operațiunii) – pozitivă sau negativă.
4) Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului şi statutului obiectelor de acces, conform următorilor parametri:
a) data şi timpul modificării competențelor;
b) ID-ul administratorului care a efectuat modificările;
c) ID-ul utilizatorului şi competențele acestuia sau specificarea obiectelor de acces şi statutul nou al acestora.
5) Se efectuează înregistrarea ieşirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților şi statutul obiectelor de acces, conform următorilor parametri:
a) data şi timpul eliberării;
b) denumirea informației şi 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) şi rezultatul eliberării – pozitiv sau negativ.

Secțiunea 3
Prelucrarea rezultatelor auditului securității în sistemele informaționale de date cu caracter personal

68. Pentru toate categoriile sistemelor 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 şi întreprinse măsuri în vederea restabilirii capacității de lucru a sistemului de audit.

Secțiunea 4
Monitorizarea, analiza şi generarea rapoartelor de audit a securității în sistemele informaționale de date cu caracter personal

69. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 5
Protejarea datelor de audit a securității în sistemele informaționale de date cu caracter personal

70. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 6
Păstrarea datelor de audit a securității în sistemele informaționale de date cu caracter personal

71. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Durata stocării rezultatelor auditului securității în sistemele informaționale de date cu caracter personal se justifică în politica 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.

IX. ASIGURAREA INTEGRITĂȚII INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL ŞI A TEHNOLOGIILOR INFORMAȚIONALE

Secțiunea 1
Înlăturarea deficiențelor de soft destinat prelucrării datelor cu caracter personal

72. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 2
Asigurarea protecției contra programelor dăunătoare (viruşilor)

73. Pentru categoria N-1

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

74. Suplimentar pentru categoria N-2

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

Secțiunea 3
Tehnologiile şi mijloacele de constatare a intruziunilor

75. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 4
Asigurarea integrității soft-urilor şi informației

76. Pentru toate categoriile sistemelor informaționale de date cu caracter personal.

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

Soft-urile destinate prelucrării datelor cu caracter personal şi informația care conține date cu caracter personal, accesul la care se efectuează prin intermediul sistemelor de acces public, sînt securizate prin metoda folosirii semnăturii digitale.

Secţiunea 5
Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

77. Pentru toate categoriile sistemelor informaţionale de date cu caracter personal

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

X. COPIILE DE REZERVĂ ŞI RESTABILIREA INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI IT

Secţiunea 1
Copiile de rezervă ale informaţiei care conţine date cu caracter personal

78. Pentru categoria N-1

Reieşind din volumul prelucrărilor efectuate, individual, se stabileşte de către deţinătorul de date cu caracter personal intervalul de timp în care se execută copiile de siguranţă a informaţiilor care conţin date cu caracter personal şi 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 informaţii şi soft-urile de bază.

Copiile de siguranţă se testează în scopul verificării siguranţei purtătorilor de informaţii şi integrităţii informaţiei care conţine date cu caracter personal.

Procedurile de restabilire a copiilor de siguranţă se actualizează şi se testează cu regularitate, în scopul asigurării eficacităţii acestora.

79. Suplimentar pentru categoria N-2

Copiile de siguranţă se păstrează în cutii metalice cu sigiliu aplicat şi stocate în afara zonei de amplasare a informaţiei care conţine date cu caracter personal de soft-urile de bază sau, dacă este posibil, în încăperi din altă clădire.

Se identifică potenţialele probleme de acces în locurile de păstrare a copiilor de siguranţă în cazul defectului sau avariei şi se determină acţiunile concrete pentru restabilirea căilor de acces.

Secţiunea 2
Serviciile telecomunicaţionale de rezervă

80. Pentru categoria N-2

Se identifică serviciile telecomunicaţionale de bază şi de rezervă, inclusiv se soluţionează întrebările privind folosirea serviciilor telecomunicaţionale de rezervă în scopul restabilirii accesibilităţii serviciilor de bază ale sistemelor informaţionale de date cu caracter personal.

Furnizorii serviciilor telecomunicaţionale de bază şi de rezervă urmează a fi diferiţi pentru a nu fi supuşi pericolelor comune.

XI. CONTROALELE DE SECURITATE A SISTEMELOR INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

81. Deţinătorii de date cu caracter personal verifică cu regularitate, cel puţin o dată pe an, îndeplinirea măsurilor tehnice şi/sau organizaţionale luate pentru detectarea unor disfuncţionalităţi în ceea ce priveşte folosirea în procesul prelucrării datelor cu caracter personal a sistemelor de telecomunicaţii şi/sau efectuarea îmbunătăţirilor, în caz de necesitate.

82. Controalele de securitate sînt actualizate de fiecare dată cînd deţinătorul de date cu caracter personal este reorganizat sau îşi schimbă infrastructura.

83. În scopul verificării nivelului de protecţie a sistemelor informaţionale de date cu caracter personal, precum şi în scopul preîntîmpinării unor eventuale cazuri de acces ilicit sau întîmplător asupra acestor sisteme informaţionale, depistării locurilor slabe în mecanismele de protejare a acestora, Centrul întreprinde periodic controale de securitate, inclusiv cu efectuarea unor măsuri tehnice speciale pentru simularea unui model de accesare a sistemelor informaţionale de date cu caracter personal.

84. Rezultatele controalelor efectuate de Centru sînt puse imediat la dispoziţia deţinătorului de date cu caracter personal, nivelul de protecţie a sistemelor informaţionale de date cu caracter personal a căruia a

servit obiect al controlului, cu prescrierea, în caz de necesitate, a acțiunilor necesare de a fi întreprinse în vederea asigurării securității prelucrării datelor cu caracter personal.

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

Secțiunea 1
Instructajul de reacționare la incidentele de securitate a sistemelor informaționale de date cu caracter personal

85. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

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

Secțiunea 2
Prelucrarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal

86. Pentru categoria N-1

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

Prelucrarea incidentelor include depistarea, analiza, preîntîmpinarea dezvoltării, înlăturarea lor şi restabilirea securității.

87. Suplimentar pentru categoria N-2

Trebuie utilizate mijloace automatizate pentru susținerea procesului de prelucrare a incidentelor de securitate a sistemelor informaționale de date cu caracter personal.

Secțiunea 3
Monitorizarea incidentelor de securitate a sistemelor informaționale de date cu caracter personal

88. Pentru categoria N-1

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

89. Suplimentar pentru categoria N-2

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

Secțiunea 4
Prezentarea rapoartelor despre incidentele de securitate a sistemelor informaționale de date cu caracter personal

90. Pentru toate categoriile sistemelor informaționale de date cu caracter personal

Anual, către 31 ianuarie, deținătorii de date cu caracter personal 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.

XIII. PROTECȚIA TEHNICĂ A INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL

91. Pentru categoria N-2

Este exclusă prezența necontrolată a persoanelor sau a mijloacelor de transport, precum şi instalarea întîmplătoare a antenelor, într-o zonă de minimum 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 cu caracter personal din cauza emisiilor electromagnetice prin ecranarea încăperilor sau instalarea sistemelor de bruiaj electromagnetic, care se proiectează, realizează şi cercetează de întreprinderi specializate în

domeniu.

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

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

Trebuie asigurată protecția informației care conține date cu caracter personal contra scurgerii prin intermediul rețelei electrice, inclusiv încrucişarea rețelelor electrice ale obiectului cu instalarea filtrelor de protecție care să blocheze (bruieze) semnalul.

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

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

XIV. SPECIFICUL CERINȚELOR DE SECURITATE ÎN CAZUL FORMEI MANUALE DE ȚINERE A REGISTRELOR ÎN CARE SÎNT PRELUCRATE DATE CU CARACTER PERSONAL

92. Prevederile prezentelor Cerințe, cu excepția pct.11-13, 23, 25, 27, 30-32, 35, 37-44, 46, 49, 51-53, 55-68, 72-77, 80, 87-89 şi 91, se aplică corespunzător de către deținătorii de date cu caracter personal în cazul formei manuale de ținere a registrelor în care sînt prelucrate seriile structurate de date cu caracter personal, accesibile conform criteriilor centralizate sau descentralizate, ori repartizate conform criteriilor funcționale sau geografice.

93. Totodată, înregistrările de audit a securității registrelor ținute manual în care sînt prelucrate date cu caracter personal, trebuie să conțină:

1) numele şi prenumele utilizatorului;

2) numele fişei accesate (pagina şi inscripția din registru);

3) numărul înregistrărilor efectuate;

4) tipul de acces;

5) data accesului (an, lună, zi);

6) timpul (ora, minuta) şi durata accesului.

Anexa nr.1
la Cerințele față de asigurarea securității
datelor cu caracter personal la prelucrarea
acestora în cadrul sistemelor informaționale
de date cu caracter personal

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: obişnuite şi 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 şi cele privind condamnările penale ale unei persoane fizice.

3. Categoria obişnuită o constituie informația care dezvăluie:

1) numele şi prenumele;

2) sexul;

3) data şi locul naşterii;

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 şi 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/reşedinței);
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) obişnuințele/preferințele/comportamentul;
33) caracteristicile fizice.

4. În cazul prelucrării categoriei obişnuite de date cu caracter personal, deținătorii de date cu caracter personal includ în politica de securitate a datelor cu caracter personal şi implementează cerințele stabilite pentru nivelul unu de securitate a sistemelor informaționale de date cu caracter personal – **(N-1).**

5. În cazul prelucrărilor categoriei speciale de date cu caracter personal, deținătorii de date cu caracter personal, suplimentar cerințelor stabilite pentru nivelul unu de securitate, includ în politica de securitate a datelor cu caracter personal şi implementează cerințele stabilite pentru nivelul doi de securitate a sistemelor informaționale de date cu caracter personal – **(N-2).**

Anexa nr.2
la Cerințele față de asigurarea securității
datelor cu caracter personal la prelucrarea
acestora în cadrul sistemelor informaționale
de date cu caracter personal

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

1. Prezintă riscuri speciale pentru drepturile şi 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 apartenența la un partid politic sau o organizație religioasă, a datelor cu caracter personal privind starea de sănătate sau viața intimă, precum şi a datelor cu caracter personal referitoare la condamnările penale, măsurile de

constrîngere, sancțiunile disciplinare sau contravenționale;

2) operațiunile de prelucrare a datelor genetice, biometrice şi 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 la subpunctele 1) şi 2) din prezenta anexă, precum şi datele cu caracter personal ale minorilor, colectate prin intermediul Internetului sau mesageriei electronice.

2. În cazul prelucrărilor de date cu caracter personal prin orice operațiune sau set de operațiuni indicate la pct.1 al prezentei anexe, deținătorii de date cu caracter personal includ în politica de securitate a datelor cu caracter personal şi implementează cerințele stabilite pentru nivelul doi de securitate a sistemelor informaționale de date cu caracter personal – **(N-2).**