APROB:
Director al Serviciului Național
Unic pentru Apelurile de Urgență 112
I. BOBROC
„13” iulie 2018

POLITICA DE SECURITATE

a prelucrării datelor cu caracter personal

a Instituției Publice “Serviciul Național Unic pentru Apelurile de Urgență 112”

Coordonat:
Vicedirector
Constantin GORINCIOI
„13” 07 2018

Șef DTICE
Bohdan BONDAR
„13” 07 2018

Șef
Serviciul juridic
Silvia DONII
„13” 07 2018

Elaborat:
Inginer securitate informației
DTICE
Alexandru TVERDOHLEB
„13” 07 2018

Politica de securitate a prelucrării datelor cu caracter personal			
Data aprobării	13.07.2018	**Tipul documentului**	De uz intern
Responsabili	Inginer Securitatea Informației	**Cross-Referințe**	1. Politica Securității Informaționale al Serviciului 112
Versiunea	Final		
Aprobat	Director Serviciul 112		
Termen de revizuire	Fiecare 1 an	**Anexe**	Anexa 1 – ACORD privind prelucrarea datelor cu caracter personal

Data	Versiunea	Comentariu	Autor
2016	Final ver. 1	Înregistrată la CNPDCP al RM	T. Cristea
26.06.2018	RC 1	Reperfectată conform cerințelor noi	A. Tverdohleb
10.07.2018	Final	Ajustată la Politica de securitate a DCP al MEI	A. Tverdohleb

I. Dispoziții generale

1. Prelucrarea datelor cu caracter personal constituie o procedură complexă care implică un șir de măsuri tehnice și organizatorice, coordonate la nivel înalt având drept scop asigurarea protecției drepturilor libertăților fundamentale ale persoanelor fizice. Asigurarea protecției datelor cu caracter personal se realizează prin crearea unui sistem de evidență securizat și prin respectarea proceselor operaționale de prelucrare a datelor cu caracter personal.
2. Politica de securitate a prelucrării datelor cu caracter personal (în continuare - Politica), este elaborată în conformitate cu prevederile Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal, cât și a prevederilor Hotărârii Guvernului nr.1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.
3. Scopul Politicii este de a asigura nivelul maxim de protecție a datelor cu caracter personal, prin aplicarea corespunzătoare a legislației naționale cu referire la protecția datelor și confidențialitatea acestora, și cuprinde un set de reglementări care determină modul de colectare, administrare, protejare distribuire a datelor cu caracter personal în cadrul Instituției Publice "Serviciul Național Unic pentru Apelurile de Urgență 112" (*în continuare* - Serviciul 112).
4. Prevederile Politicii se aplică tuturor angajaților Serviciului 112 care sunt implicați direct sau indirect în procesul de colectare, prelucrare si păstrare a datelor cu caracter personal precum asupra persoanelor fizice și juridice de

drept public şi de drept privat (petiţionari, candidaţi la funcţie, parteneri, stagiari, persoane împuternicite, etc.).

5. In sensul prezentei Politici, datele cu caracter personal reprezintă orice informaţie referitoare la angajaţii Serviciului 112 şi la sistemul de salarizare al acestora, precum datele persoanelor fizice şi juridice de drept public şi de drept privat care sunt colectate prelucrate în scopul realizării competenţelor funcţionale ale Serviciului 112, si care se referă la numărul de identificare sau elementele specifice identităţii fizice, fiziologice, psihice, economice, culturale sau sociale.
6. Datele cu caracter personal care fac obiectul prelucrării în cadrul Serviciului 112 sunt:
   1) prelucrate în mod corect conform prevederilor cadrului legal aferent în vigoare;
   2) colectate numai în scopuri determinate, explicite legitime, iar prelucrarea ulterioară nu este incompatibilă cu aceste scopuri;
   3) adecvate, pertinente neexcesive prin raportare la scopul în care sunt colectate;
   4) exacte şi actualizate, iar datele inexacte sau incomplete din punctul de vedere al scopului pentru care sunt colectate ulterior prelucrate fiind şterse sau rectificate;
   5) stocate într-o formă care să permită identificarea subiecţilor datelor cu caracter personal pe o perioadă care nu va depăşi durata necesară atingerii scopurilor pentru care sunt colectate şi ulterior prelucrate.

II. Cerinţe generale pentru prelucrarea, stocarea şi utilizarea datelor cu caracter personal

7. Politica are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii datelor cu caracter personal şi vizează toţi angajaţii Serviciului 112.
   1) **Integritatea** presupune totalitatea măsurilor şi procedurilor utilizate pentru asigurarea caracterului complet, integru, veridic al datelor cu caracter personal în vederea preîntâmpinării conexiunilor neautorizate la reţelele resurselor informaţionale care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program.
   2) **Disponibilitatea** asigurată prin administrarea eficientă a datelor cu caracter personal şi care presupune: accesarea, obţinerea şi divulgarea datelor în conformitate cu legislaţia în vigoare.

3) **Confidențialitatea** presupune protecția datelor prin excluderea accesului neautorizat la datele cu caracter personal prelucrate, preîntâmpinarea scurgerii informației transmise prin canale de legătură.

8. Subiecții datelor cu caracter personal prelucrate în cadrul Serviciului 112 sunt:
   1) Angajații Serviciului 112;
   2) Angajații Serviciilor Specializate de Urgență;
   3) Subiecții datelor cu caracter personal – apelanți și/sau victime vizate în cadrul situațiilor de urgență;
   4) Persoane fizice și juridice terțe ale Serviciului 112;

9. Măsurile de protecție a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a sistemelor informaționale de date cu caracter personal și se efectuează neîntrerupt de către Serviciul 112.
10. Protecția datelor cu caracter personal în cadrul sistemelor informaționale ale Serviciului 112 este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.
11. Sunt supuse protecției toate resursele informaționale ale Serviciului 112, care conțin date cu caracter personal, inclusiv:
    1) suporturile magnetice, optice, laser sau alte suporturi electronice de informație, masive informaționale și baze de date;
    2) 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 alte mijloace tehnice de prelucrare a informației.
12. Protecția datelor cu caracter personal în sistemele informaționale de date cu caracter personal ale Serviciului 112 este asigurată în scopul:
    1) preîntâmpinării scurgerii informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la această informație;
    2) preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele de telecomunicații 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 de telecomunicații și resursele informaționale;
    5) păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal.

13. Protecția datelor cu caracter personal prelucrate în sistemele informaționale ale Serviciului 112 se efectuează prin următoarele metode:
    1) preîntâmpinarea conexiunilor neautorizate la rețelele de telecomunicații și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin intermediul acestor rețele;
    2) excluderea accesului neautorizat la datele cu caracter personal prelucrate;
    3) preîntâmpinarea acțiunilor intenționate cu utilizarea mijloacelor tehnice si de program, care pot cauza distrugerea și/sau modificarea datelor cu caracter personal sau provoca defecțiuni ale complexului tehnic și de program;
    4) preîntâmpinarea oricăror acțiuni (intenționate/neintenționate) a utilizatorilor interni și/sau externi, precum a altor angajați ai Serviciului 112, care pot cauza distrugerea și/sau modificarea datelor cu caracter personal sau provoca defecțiuni ale complexului tehnic și de program;.
14. Preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin intermediul canalelor de legătură, este asigurată prin folosirea metodelor de criptare a acestei informații, inclusiv cu utilizarea măsurilor organizaționale, tehnice și de limitare.
15. Preîntâmpinarea accesului neautorizat la informațiile care conțin date cu caracter personal circulante sau păstrate de mijloace tehnice este asigurată prin utilizarea mijloacelor tehnice și de program speciale, metodelor de criptare, precum și prin aplicarea măsurilor organizaționale și celor tehnice și de limitare.
16. Preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin folosirea mijloacelor de protecție tehnice și de program speciale, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de rezervă.

III. Categoriile de date cu caracter personal prelucrate și operațiunile de prelucrare, efectuate asupra acestora

17. În cadrul Serviciului 112 este prelucrată categoria obișnuită de date cu caracter personal cum ar fi:
    1) numele, prenumele, patronimicul;
    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;
11) datele personale ale membrilor de familie;
12) datele din permisul de conducere;
13) situația economică și financiară;
14) datele bancare;
15) semnătura;
16) datele din actele de stare civilă;
17) codul personal de asigurării sociale (CPAS);
18) codul asigurării medicale (CPAM);
19) numărul de telefon/fax;
20) numărul de telefon mobil;
21) adresa (domiciliului/reședinței);
22) adresa e-mail;
23) profesia și/sau locul de muncă;
24) formarea profesională – diplome – studii;
25) caracteristicile fizice.

18. În cadrul Serviciului 112 nu sunt înregistrate și nu sunt prelucrate categoriile speciale de date cu caracter personal: datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale.
19. Datele cu caracter personal colectate și prelucrate în cadrul sistemelor informaționale ale Serviciului 112 nu fac obiectul transferurilor transfrontaliere.
20. Procesul de prelucrare a datelor cu caracter personal include următoarele operațiuni:
    1) colectarea de la subiecți a datelor conform cerințelor;
    2) înregistrarea în sistemele informaționale/resursele informaționale a datelor conform domeniilor de aplicare;
    3) organizarea procesului de lucru cu datele colectate și asigurarea confidențialității acestora;
    4) stocarea datelor;
    5) păstrarea și arhivarea datelor conform legislației în vigoare.
21. Restabilirea, modificarea, actualizarea datelor conform noilor circumstanțe, precum extragerea, utilizarea, transmiterea datelor cu caracter personal la

cerere se realizează doar prin respectarea prevederilor legale în vigoare, fără a leza drepturile subiecților datelor cu caracter personal.

22. Se interzice blocarea, ștergerea sau distrugerea intenționată a datelor, cu excepția persoanelor care dețin dreptul de acces și prelucrare a datelor cu caracter personal.

IV. Sistemele de evidență a datelor cu caracter personal și complexitatea sistemelor informaționale

23. În cadrul Serviciului 112 se definesc următoarele sisteme de evidentă a datelor cu caracter personal:
    1) Evidența și managementul angajaților;
    2) Evidență contabilă și salarizare;
    3) Managementul și arhivarea documentelor;
    4) Managementul control-acces.
24. Colectarea și prelucrarea datelor cu caracter personal în cadrul sistemului de „Evidența și managementul angajaților":
    1) Procesul de colectare prelucrare a datelor cu caracter personal în cadrul sistemului „Evidența managementul angajaților" se realizează de Serviciul resurse umane care are responsabilitatea de a participa la elaborarea, implementarea și monitorizarea respectării prevederilor Politicii la nivelul acestui sistem. Responsabilitatea acestei subdiviziuni se extinde asupra datelor cu caracter personal a tuturor angajaților Serviciului 112.
    2) Resursele informaționale din cadrul sistemului „Evidenta managementul angajaților" sunt ținute manual pentru evidența datelor cu privire la personal, includ:
        a. Registrul de evidență a livretelor militare;
        b. Registrul privind evidența carnetelor de muncă;
        c. Registrul privind evidența polițelor de asigurări medicale;
        d. Registrul contractelor individuale de muncă;
        e. Registrul cererilor și solicitărilor de date cu caracter personal;
        f. Registru de evidentă a certificatelor medicale.
25. Colectarea și prelucrarea datelor cu caracter personal în cadrul sistemului „Evidenta contabilă și salarizare"
    1) Procesul de colectare și prelucrare a datelor cu caracter personal în cadrul sistemului „Evidentă contabilă și salarizare" se realizează de Serviciul finanțe și evidență contabilă care are responsabilitatea de a participa la elaborarea, implementarea si monitorizarea respectării prevederilor Politicii la nivelul sistemului de evidentă contabilă și salarizare.

2) Resursele informaționale din cadrul sistemului „Evidentă contabilă și salarizare" sunt în formă electronică:
   a. Program contabil de ținere a evidenței contabile, inclusiv programul de salarizare;
   b. Serviciul electronic e-Docplat – executarea on-line a plăților trezoreriale;
   c. Serviciul electronic e-Achiziții – înregistrarea contractelor de achiziții publice în Registrul de Stat al Achizițiilor Publice.
   d. Serviciul electronic e-Raportare – raportarea on-line a dărilor de seamă pentru CNAS și CNAM;
   e. Serviciul electronic servicii.fisc.md – raportarea on-line a dărilor de seamă pentru Inspectoratul Fiscal și CNAM.
3) Programul de salarizare reprezintă o bază de date informațională automatizată care include date cu caracter personal (numele, prenumele angajatului, IDNP, CPAS, persoanele care se află la întreținere, adresa). Conform datelor incluse este calculat salariul în mod individual pentru fiecare angajat și este păstrată informația pentru toate persoanele angajate.
   Sarcinile de bază ale programului constau în formarea bazei de date (introducerea și stocarea datelor privind salarizarea personalului), actualizarea periodică și exploatarea (procesarea, sistematizarea, generalizarea, furnizarea și analiza datelor).
   Datele cu caracter personal sunt prelucrate conform legislației în vigoare și se raportează lunar Inspectoratului Fiscal, Casei Teritoriale de Asigurări Sociale a sectorului.

26. Colectarea și prelucrarea datelor cu caracter personal în cadrul sistemului de „Management și arhivarea documentelor":
    1) Procesul de colectare și prelucrare a datelor cu caracter personal în cadrul sistemului „Managementul și arhivarea documentelor" se realizează de Serviciul secretariat și arhivă care are responsabilitatea de a participa la elaborarea, implementarea și monitorizarea respectării prevederilor Politicii la nivelul acestui sistem.
    2) Scopul prelucrării informațiilor ce conțin date cu caracter personal în sistemul de evidență privind „Managementul și arhivarea documentelor", constă în ducerea evidenței corespondenței de intrare și ieșire, conform Regulilor de întocmire a documentelor organizatorice și de dispoziție și Instrucțiunii-tip cu privire la ținerea lucrărilor de secretariat în organele administrației de specialitate și ale autoadministrării locale ale Republicii Moldova, aprobate prin Hotărârea Guvernului nr. 618 din 05.10.1993.
    3) Datelor cu caracter personal prelucrate în cadrul sistemului de „Management și arhivarea documentelor" includ: nume, prenume,

patronimicul, IDNP, semnătura, numărul de telefon mobil/fix, adresa e-mail, domiciliu.

27. Colectarea și prelucrarea datelor cu caracter personal în cadrul sistemului de „Management control-acces":
    1) Procesul de colectare și prelucrare a datelor cu caracter personal în cadrul sistemului „Managementul control-acces" se realizează de Secția asigurare tehnică și aplicativă a Direcției tehnologia informațională și comunicații electronice, care are responsabilitatea de a participa la elaborarea, implementarea monitorizarea respectării prevederilor Politicii la nivelul acestui sistem.
    2) Sistemul electronic de gestiune control-acces al Serviciului 112 include date cu caracter personal ale angajaților Serviciului 112, angajaților Serviciilor Specializate de Urgență și ale vizitatorilor (numele, prenumele, patronimicul, data nașterii, imaginea, numărul de telefon/fax, numărul de telefon mobil, adresa (domiciliului/reședinței), adresa e-mail, profesia și/sau locul de muncă), necesare pentru identificarea persoanelor cu drept de acces la Serviciul 112.

V. Formele de ținere a registrelor în care sunt prelucrate date cu caracter personal

28. In cadrul Serviciului 112 înregistrarea datelor cu caracter personal se efectuează în cadrul sistemelor informaționale de date cu caracter personal și a registrelor ținute manual.
29. Prelucrarea datelor cu caracter personal se realizează prin mijloace mixte cu respectarea cerințelor legale în condiții, care să asigure securitatea, confidențialitatea și respectarea drepturilor subiecților datelor cu caracter personal.
30. Registrele în formă manuală sunt: Registrul de evidență a livretelor militare, Registrul privind evidența carnetelor de muncă, Registrul privind evidența polițelor de asigurări medicale, Registrul contractelor individuale de muncă, Registrul cererilor și solicitărilor de date cu caracter personal, Registru de evidentă a certificatelor medicale, Registrul de evidentă a corespondentei de intrare/ieșire.
31. Registrele în formă electronică sunt: Programul contabil de tinere a evidenței contabile, inclusiv programul de salarizare, Registrul electronic a dosarelor corespondentei de intrare/ieșire, Registrul electronic de achiziții publice, Sistemul electronic de gestiune control-acces al Serviciului 112.
32. Computatoarele unde se află registrele electronice sunt protejate prin intermediul parolei de acces.

33. Tinerea registrelor se realizează conform măsurilor tehnice de protecție și conform legislației in vigoare.
34. Permisiunea de acces prin autentificare se acordă doar persoanei responsabile de protecția datelor cu caracter personal.
35. La nivelul fiecărei subdiviziuni structurale documentele, listele, mapele ce conțin date cu caracter personal se păstrează în dulapuri, safeuri sau în birouri cu acces limitat. Dreptul de acces la informația ce conține date cu caracter personal fiind deținut doar de persoanele responsabile de prelucrarea acestor date doar în limita competentelor funcționale.

VI. Atribuțiile și responsabilitățile subdiviziunilor a persoanelor responsabile de prelucrarea datelor cu caracter personal

36. Persoanele responsabile de prelucrarea datelor cu caracter personal din cadrul Serviciului 112 dețin următoarele atribuții și responsabilități:
    1) cunosc și aplică prevederile actelor normative din domeniul prelucrării datelor cu caracter personal, precum și ale prezentei Politici;
    2) oferă subiecților datelor cu caracter personal informații referitoare la drepturile lor;
    3) prelucrează doar datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu;
    4) asigură caracterul complet, integru, veridic al datelor cu caracter personal;
    5) preîntâmpină scurgerea informației care conține date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
    6) preîntâmpină distrugerea, modificarea, copierea, blocarea neautorizată a datelor cu caracter personal în rețelele și resursele informaționale;
    7) păstrează confidențialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/baze de date prin care sunt gestionate date cu caracter personal;
    8) respectă măsurile de securitate a datelor cu caracter personal;
    9) respectă cadrul normativ de folosire a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;
    10) informează conducerea Serviciului 112 despre situațiile care pot duce la o diseminare neautorizată de date cu caracter personal sau despre situațiile în care au fost accesate/prelucrate date cu caracter personal prin încălcarea normelor legale, despre care au luat cunoștință.
37. Persoanele responsabile vor prelucra date cu caracter personal doar în cazul când subiectul datelor cu caracter personal și-a dat consimțământul (conform modelului din anexa nr. 1), precum și în cazul când prelucrarea este prevăzută în mod expres de legislația în vigoare.

38. Accesul la datele cu caracter personal este acordat de către persoanele responsabile:
    1) conducerii Serviciului 112, care poate solicita date cu caracter personal pentru orice angajat al Serviciului 112;
    2) șefilor subdiviziunilor structurale ale Serviciului 112, care pot solicita date cu caracter personal pentru angajații din subordine;
    3) angajaților, care pot solicita datele personale pentru propriile necesități;
    4) terților, în cazul acțiunilor de prevenire, investigare a infracțiunilor în scopul apărării naționale, al securității statului și menținerii ordinii publice, al protecției drepturilor libertăților subiectului datelor cu caracter personal. Datele sunt transmise în baza demersului organelor abilitate și conform acceptului conducătorului Serviciului 112.
39. Notificările privind accesul și transmiterea datelor cu caracter personal subiecților datelor cu caracter personal terților, se face prin înregistrare în Registrul cererilor solicitărilor de date cu caracter personal gestionat de persoanele responsabile de gestionarea sistemelor de date cu caracter personal.
40. Persoana responsabilă din cadrul Direcției tehnologia informațională și comunicații electronice, în comun cu subdiviziunile care prelucrează date cu caracter personal în cadrul Serviciului 112:
    1) elaborează/actualizează documentele aferente procesului de prelucrare a datelor cu caracter personal;
    2) realizează inventarierea anuală a sistemelor de evidentă a datelor cu caracter personal;
    3) notifică Centrul National pentru Protecția Datelor cu Caracter Personal privind prelucrarea datelor cu caracter personal, în baza notificărilor a informației prezentate de subdiviziunile Serviciului 112;
    4) prezintă rapoarte cu privire la incidentele de securitate.
41. Subdiviziunile structurale ale Serviciului 112, înainte de a prelucra date cu caracter personal destinate să servească unui scop, sunt obligate să informeze despre inițierea procesului de prelucrare a datelor, în mod formalizat, Direcția tehnologia informațională și comunicații electronice, prin specificarea: scopului a temeiului legal al prelucrării, categoriilor de date cu caracter personal supuse prelucrării și a persoanei responsabile de prelucrarea datelor în cauză.
42. Șefii subdiviziunilor structurale ale Serviciului 112 poartă responsabilitatea pentru informația prezentată și/sau pentru neprezentarea informației cu privire la prelucrarea datelor cu caracter personal în cadrul subdiviziunii.

VII. Securitatea datelor cu caracter personal

43. În procesul prelucrării categoriei obișnuite de date cu caracter personal, Serviciul 112 se axează pe prezenta Politică și implementează cerințele stabilite pentru nivelul unu de securitate a sistemelor informaționale de date cu caracter personal (N-1) conform Hotărârii Guvernului nr. 1123 din 14 decembrie 2010 „Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal".
44. Măsurile de securitate întreprinse în cadrul Serviciului 112 privind protecția datelor cu caracter personal sunt stabilite astfel încât să asigure un nivel adecvat de securitate a datelor cu caracter personal procesate. Serviciul 112 îndeplinește cerințele de securitate a datelor cu caracter personal și garantează protejarea informației și sistemelor informatice de accesul neautorizat, folosirea, dezvăluirea, întreruperea, modificarea sau distrugerea accidentală sau ilegală a datelor cu caracter personal.
45. Securitatea mediului fizic a tehnologiilor informaționale folosite în procesul de prelucrare a datelor cu caracter personal.
    1) Se asigură restricția accesului în spațiul unde sunt amplasate registrele manuale și sistemul informațional de date cu caracter personal.
    2) Se admite dreptul de acces doar persoanelor care dețin dreptul de colectare și prelucrare a datelor cu caracter personal și doar în timpul orelor de program.
    3) Se admite ca computerul împreună cu serverul de acces la sistem să fie amplasat în loc cu acces limitat pentru persoanele străine.
    4) Se asigură controlul permanent al accesului în perimetrul sălii, unde sunt amplasate mijloacele de prelucrare a datelor cu caracter personal.
    5) Cazurile de încălcare a regimului de acces în sălile cu registre manuale și sisteme informaționale de prelucrare a datelor cu caracter personal sunt raportate conducerii Serviciului 112.
    6) Persoana responsabilă de prelucrarea datelor cu caracter personal asigură controlul accesului fizic al vizitatorilor în încăperile unde sunt amplasate registrele manuale și sistemele informaționale de date cu caracter personal. Accesul vizitatorilor se înregistrează în Registrul privind accesul la obiectele protejate a vizitatorilor, care se păstrează minimum un an.
    7) Se asigură securitatea echipamentului electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate.

8) Informația pe suport de hârtie care conține date cu caracter personal se păstrează în safeu metalic care va fi încuiat permanent.
9) Se deconectează computerele, terminalele de acces și imprimantele la finisarea sesiunilor de lucru.
10) Se încuie ușile și ferestrele în cazul în care în încăpere lipsesc angajații.
11) Se supune controlului permanent accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoanele neautorizate.
12) Scoaterea registrelor manuale și informației pe suport de hârtie ce conține date cu caracter personal din încăperile aflate în perimetrul de securitate este interzisă, cu excepția cazurilor existenței unei permisiuni scrise a conducerii Serviciului 112, cu efectuarea înregistrărilor corespunzătoare. În cazul când mijloacele de prelucrare a datelor cu caracter personal sunt scoase în afara perimetrului de securitate, acestea nu trebuie lăsate fără supraveghere.
13) Este asigurată protecția rețelelor de comunicații, prin intermediul cărora sunt efectuate operațiuni de prelucrare a datelor cu caracter personal, contra conectărilor nesancționate sau deteriorărilor. Acestea sunt verificate de către persoanele responsabile cu o periodicitate stabilită.
14) Sunt prevăzute mijloace de asigurare a securității antiincendiare a birourilor unde sunt amplasate registrele manuale și sistemele informaționale de date cu caracter personal.
15) Se exercită controlul și evidenta instalării și scoaterii din uz a mijloacelor program și celor tehnice, utilizate la prelucrarea datelor cu caracter personal.
16) Suporții de informații ce conțin date cu caracter personal nu trebuie lăsate la îndemâna persoanelor neautorizate și la necesitate sunt transcrise și/sau distruse prin metode sigure.
17) Suporții de informații (pe hârtie sau electronici) care conțin date cu caracter personal, se păstrează în safeuri sau dulapuri metalice care se încuie.
18) Se asigură securitatea punctelor de primire/expediere a corespondenței și accesului neautorizat la aparatele fax și copiatoare.

46. Identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal:
1) Utilizatorii (inclusiv cei cu drepturi privilegiate) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmentele nivelului de accesibilitate al utilizatorului. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole, bazate pe caracteristici unice și individuale ale persoanei.

2) 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, sau drepturile de acces ale utilizatorului au fost modificate, sau utilizatorul a abuzat de credențialele oferite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, accesul este revocat sau suspendat de către Serviciul 112.
3) Este asigurată confidențialitatea parolelor prin aplicarea Politicii protecției prin parole ale Serviciului 112.

47. Administrarea accesului utilizatorilor:
1) Este asigurată înregistrarea și evidența persoanelor cu drept de acces, participante la prelucrarea datelor cu caracter personal, ce permite identificarea accesării neautorizate a datelor cu caracter personal.
2) Este monitorizată conectarea utilizatorilor la sistemele informaționale ce conțin date cu caracter personal conform graficului de lucru. Utilizarea ilegală a datelor cu caracter personal se urmărește și se pedepsește în conformitate cu legislația în vigoare.
3) Este efectuat controlul acțiunilor utilizatorilor în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de prelucrare a datelor cu caracter personal.
4) Accesul la distanta la sistemelor informaționale de prelucrare a datelor cu caracter personal este securizat, documentat, supus monitorizării și controlului. Persoanele responsabile prelucrarea datelor cu caracter personal din cadrul Serviciului 112 autorizează metodele de acces și utilizatorii, cărora li este necesar accesul la distanță, pentru îndeplinirea obiectivelor stabilite.
5) Se permite accesul la sistemele informaționale de prelucrare a datelor cu caracter personal al Serviciului 112 cu folosirea echipamentului portativ și/sau mobil, doar cu autorizarea persoanei responsabile de prelucrarea datelor cu caracter personal. Utilizarea dispozitivelor mobile este documentată, monitorizată și controlată.

48. Protecția sistemelor informaționale comunicațiilor în care sunt prelucrate date cu caracter personal:
1) Este asigurată combaterea tentativelor dezvăluirii neautorizate sau intenționate a informației care conține date cu caracter personal, prin intermediul resurselor informaționale general accesibile.
2) Este asigurată protecția sistemelor informaționale de prelucrare a datelor cu caracter personal al Serviciului 112 sau limitate posibilitățile de realizare a atacurilor de diferite tipuri, prin monitorizarea permanentă și controlul

comunicațiilor la perimetrul exterior al acestor sisteme, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaționale.

3) Este asigurată imposibilitatea accesului din exterior a utilizatorilor la rețeaua internă în care se prelucrează date cu caracter personal.
4) Este asigurată integritatea datelor cu caracter personal transmise, utilizându-se mijloacele de protecție criptografică.

49. Controlul securității în sistemele informaționale de date cu caracter personal :

1) Sunt organizate verificări permanente de către Serviciul 112 în vederea depistării tentativelor de intrare/ieșire a utilizatorului în sistem; 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; tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal (ex: data și timpul tentativei, ID-ul utilizatorului, scopul și rezultatul tentativei).
2) Este efectuată înregistrarea modificărilor drepturilor de acces (competențelor) a utilizatorului și statutului obiectelor de acces (data și timpul modificării competențelor; ID-ul administratorului care a efectuat modificările; ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora).
3) Este efectuată înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.). Se înregistrează: data și timpul eliberării; denumirea informației și căile de acces la aceasta; specificarea dispozitivului care a eliberat informația; ID-ul utilizatorului, care a solicitat informația; volumul documentului eliberat (numărul paginilor, a filelor, copiilor) și rezultatul eliberării – pozitiv sau negativ.
4) Este efectuată monitorizarea permanentă și analiza înregistrărilor în urma controalelor securității în sistemele informaționale de prelucrare a datelor cu caracter personal, în scopul depistării activităților suspecte de utilizare a acestora, cu întocmirea raportului referitor la cazurile depistării unor astfel de activități și întreprinderea acțiunilor de înlăturare a deficiențelor și sancționare a persoanelor responsabile pentru astfel de cazuri.
5) Rapoartele efectuate în urma controalelor securității în sistemele informaționale de date cu caracter personal se păstrează minimum doi ani și pot servi în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare.

50. Asigurarea integrității informației care conține date cu caracter personal și a tehnologiilor informaționale :

1) Este asigurată identificarea și înlăturarea deficiențelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corectărilor și pachetelor de reînnoire a acestor soft-uri.
2) Este asigurată 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.
3) Este asigurată testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de prelucrare a datelor cu caracter personal (automat la pornirea sistemului și lunar la solicitarea utilizatorului autorizat în acest scop).
4) Sunt rezervate informațiile care conțin date cu caracter personal și soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, reieșind din volumul prelucrărilor efectuate și nu mai rar de o dată în an, care se păstrează în locuri protejate.
5) Este informat neîntârziat conducerea Serviciului 112 despre incidentele de securitate informațională produse în cadrul sistemelor informaționale de prelucrare a datelor cu caracter personal ale Serviciului 112. Aceste incidente urmează a fi investigate prin: depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea consecințelor și restabilirea nivelului de securitate.

VIII. Riscurile de securitate a datelor cu caracter personal

51. Serviciul 112 și/sau subiecții datelor cu caracter personal sunt supuși riscului de modificare, deteriorare, pierdere a datelor în urma:
    1) conexiunilor neautorizate la rețelele de comunicații electronice cu scopul interceptării datelor cu caracter personal transmise prin aceste rețele;
    2) accesului neautorizat la datele cu caracter personal prelucrate;
    3) acțiunilor ale complexelor hardware și software, care poate condiționa distrugerea, modificarea datelor cu caracter personal sau pot produce defecțiuni ale complexului sistemului informațional de prelucrare a datelor cu caracter personal;
    4) acțiunilor utilizatorilor interni și/sau externi ai sistemelor informaționale, care condiționează distrugerea, modificarea datelor cu caracter personal sau pot produce defecțiuni ale complexului de prelucrare.
52. Aceste riscuri pot fi înlăturate și/sau diminuate respectând următoarele:
    1) Restricționarea accesului în birourile și spațiile unde sunt amplasate registrele manuale și sistemele informaționale de prelucrarea a date cu caracter personal. Computerele, serverele, alte terminale de acces vor fi amplasate în locuri cu acces restricționat și vor avea un nivel adecvat de

protecție. Ușile și ferestrele se vor încuia în cazul în care în încăpere lipsesc angajații. Agendele și/sau cărțile de telefoane în care se conțin indicii despre locul amplasării mijloacelor de prelucrare a datelor cu caracter personal nu vor fi accesibile persoanelor neautorizate.

2) Utilizarea metodelor de criptare a acestor informații, inclusiv cu utilizarea măsurilor organizaționale, tehnice și limitare acces, preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal prin metoda folosirii mijloacelor speciale de protecție hardware și software, inclusiv a software licențiat, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de rezervă.
3) Monitorizarea permanentă și controlul comunicațiilor la perimetrul exterior al sistemelor informaționale de prelucrare a datelor cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaționale.
4) Restricționarea accesului din exterior a utilizatorilor la rețeaua internă în care se prelucrează date cu caracter personal, concomitent asigurând-se integritatea și confidențialitatea datelor cu caracter personal.
5) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal va trebui să răspundă necesităților asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

53. Serviciul 112 efectuează controale, în scopul verificării cazurilor de conectare neautorizată la cablurile de rețea.
54. Se vor prevedea mijloace de asigurare a securității antiincendiare a birourilor unde sunt amplasate registrele manuale și sistemele informaționale de date cu caracter personal.

IX. Raportarea incidentelor de securitate a datelor cu caracter personal

55. Utilizatorii și administratorii sistemelor informaționale de prelucrare a datelor cu caracter personal, în cazul apariției incidentelor legate de încălcarea securității informaționale, sunt obligați să comunice neîntârziat persoanei responsabile din cadrul Direcției tehnologii informaționale și comunicații electronice despre incidentul apărut. Persoana responsabilă va investiga cazul, va întreprinde măsurile necesare pentru înlăturarea incidentului, va informa conducerea Serviciului 112 și în termen de 72 de ore de la producerea incidentului va raporta către Centrul Național pentru Protecția Datelor cu Caracter Personal.
56. Incidentele de securitate informațională în cadrul sistemelor de evidență a datelor cu caracter personal vor fi urmărite și documentate în regim permanent de către persoana responsabilă din cadrul Direcției tehnologii informaționale și

comunicații electronice, prin utilizarea mijloacelor automatizate de urmărire a incidentelor, care anual, până la data de 31 ianuarie, va perfecta raportul privind incidentele de securitate informațională la prelucrarea datelor cu caracter personal, aprobat de către conducerea Serviciului 112, și care urmează a fi expediat în adresa Centrului Național pentru Protecția Datelor cu Caracter Personal.

57. Persoana responsabilă de gestionarea incidentelor de securitate informațională și înregistrarea sistemelor de evidență a datelor cu caracter personal ale Serviciului 112 în Centrul Național pentru Protecția Datelor cu Caracter Personal se desemnează Inginerul securității informației, care este numit prin ordinul Directorului Serviciului 112.

X. Marcarea documentelor ce conțin date cu caracter personal

58. Toată informația care se intenționează a fi dezvăluită, și care conține date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidență al operatorilor de date cu caracter personal.
Model Atenție! Documentul conține date cu caracter personal, prelucrate în cadrul sistemului de evidentă nr. 000000X-00X, înregistrat în Registrul de evidentă al operatorilor de date cu caracter personal www.registru.datepersonale.md. Prelucrarea ulterioară a acestor date poate fi efectuată numai în condițiile prevăzute de Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal.

XI. Dispoziții Finale

59. Prezenta Politica este un document public și accesibil tuturor părților interesate.
60. Prezenta Politică va fi revizuită de cel puțin o dată pe an sau la necesitate, și este aprobată de către Directorul Serviciului 112.
61. Încălcarea prevederilor prezentei Politici poate atrage răspundere disciplinară și contravențională.

Anexa nr. 1

ACORD
privind prelucrarea datelor cu caracter personal

Subsemnatul/a:

Numele	
Prenumele	
IDNP	
Seria buletinului de identitate	
Data eliberării buletinului de identitate	
Adresa	

sunt informat cu prevederile art. 12 din Legea nr. 133-XVI din 8 iulie 2011 privind protecția datelor cu caracter personal și îmi exprim consimțământul cu privire la prelucrarea datelor cu caracter personal de către colaboratorii Serviciului resurse umane a datelor mele cu caracter personal, care sunt oferite de către mine, în legătură cu apariția raporturilor de serviciu/muncă, precum și să colecteze și să prelucreze datele mele pe durata raporturilor de serviciu/muncă.

Confirm că mi s-au adus la cunoștință drepturile mele prevăzute în art. 12-18 din Legea privind protecția datelor cu caracter personal (dreptul de a fi informat, dreptul de acces, de intervenție, de opoziție, precum și de a mă adresa în instanța de judecată, în contextul prelucrării efectuate asupra datelor cu caracter personal ce mă vizează).

Am luat cunoștință de faptul că datele cu caracter personal vor fi prelucrate cu respectarea regimului de securitate confidențialitate, în conformitate cu prevederile Legii privind protecția datelor cu caracter personal Hotărârii Guvernului nr. 1123 din 14 decembrie 2010 „Privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal"

Dacă datele cu caracter personal furnizate sunt incorecte sau vor suferi modificări (schimbare domiciliu, statut civil, etc.) mă oblig să informez în scris Serviciul Resurse umane, în timp util.

Prezentul acord intră în vigoare de la data semnării acestuia va fi valabil până la depunerea în scris a unei solicitări de retragere a consimțământului pentru colectarea, verificarea prelucrarea datelor cu caracter personal în scopul prevăzut în acord.

Numele, prenumele	**Semnătura:**
	Data:

Prezentul acord a fost întocmit în două exemplare, câte unul pentru fiecare Parte.

Am primit un exemplar	**Semnătura**