CENTRUL NAŢIONAL PENTRU PROTECŢIA DATELOR
CU CARACTER PERSONAL AL REPUBLICII MOLDOVA

MD-2004, mun. Chişinău, str. Serghei Lazo, 48, tel: (+373-22) 820801, 811807, fax: 820807, www.datepersonale.md

ORDIN nr.

mai 2013 **mun. Chişinău**

Cu privire la aprobarea Instrucţiunilor privind prelucrarea datelor cu caracter personal în sectorul poliţienesc

În temeiul art.20 alin. (1) lit. c) al Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal, Capitolului II, art. 3 lit. e^2) al Regulamentului Centrului Naţional pentru Protecţia Datelor cu Caracter Personal, structurii, efectivului - limită şi a modului de finanţare a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal, aprobat prin Legea nr. 182-XVI din 10 iulie 2008,

ORDON:

1. Se aprobă Instrucţiunile privind prelucrarea datelor cu caracter personal în sectorul poliţienesc (se anexează).
2. Se recomandă Procuraturii Generale luarea în considerare a Instrucţiunilor în cadrul adaptării procedurilor de prelucrare a datelor cu caracter personal de către autorităţile care exercită activităţi în sectorul poliţienesc, la principiile statuate de legislaţia care reglementează domeniul protecţiei datelor cu caracter personal.
3. Direcţia juridică şi relaţii cu publicul, de comun cu Direcţia evidenţă şi control, vor asigura plasarea Instrucţiunilor privind prelucrarea datelor cu caracter personal în sectorul poliţienesc pe pagina web oficială a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova (www.datepersonale.md).

Vitalie PANIŞ
Director

Anexă
la ordinul directorului Centrului
Național pentru Protecția Datelor cu
Caracter Personal al Republicii Moldova
nr. ____ din __ mai 2013

INSTRUCȚIUNI
privind prelucrarea datelor cu caracter personal în sectorul polițienesc

PREAMBUL

Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova (Centrul), conștient de progresul tehnologiilor informaționale şi de trecerea la metode automatizate de prelucrare a datelor cu caracter personal;

în vederea prevenirii operațiunilor neautorizate de prelucrare a datelor cu caracter personal stocate în sistemele de eviden□ă automatizate sub aspectul consultării, extragerii şi utilizării acestora excesiv scopurilor declarate;

ținînd cont de incidentele de securitate constatate de Centru, cum ar fi: anexarea la materialele dosarelor penale ori contraven□ionale a fişelor personale extrase din Registrul de stat al popula□iei sau a copiilor buletinelor de identitate □i a fi□elor de înso□ire la acestea în care sînt consemnate date cu caracter personal ce nu sînt necesare pentru aceste procese (*date cu caracter personal care vizează copiii, culoarea ochilor, grupa sanguină, înăl□imea, informa□ia privind starea familială, informa□ie despre participarea la alegeri, na□ionalitatea etc*); nerespectarea regimului de confiden□ialitate □i de securitate a prelucrării datelor cu caracter personal prin dezvăluirea neautorizată a conținutului interceptărilor convorbirilor telefonice efectuate în cadrul urmăririi penale; accesul neautorizat în perimetrul de securitate al organelor de urmărire penală care condi□ionează ulterior accesul neautorizat la datele cu caracter personal; consultarea informa□iei stocată în resursele informaționale principale de stat în absen□a temeiurilor legale pentru efectuarea unor asemenea operațiuni etc.,

ținînd cont de faptul:

- că schimbul de date cu caracter personal în cadrul cooperării organelor polițienești, în conformitate cu principiul disponibilității informației, ar trebui sprijinit prin norme clare, care să sporească încrederea reciprocă între autoritățile competente, să asigure protecția informațiilor relevante şi respectarea drepturilor fundamentale ale persoanelor fizice;
- că este necesar să fie precizate obiectivele de protecție a datelor cu caracter personal în cadrul activităților polițienești şi instituite norme care ar asigura ca orice informație colectată este prelucrată în mod legal şi în conformitate cu principiile fundamentale privind calitatea datelor;
- că orice acțiune de dezvăluire a datelor cu caracter personal, inclusiv care nu se referă la activitatea în materie penală, contravențională şi, după caz, civilă,

trebuie să respecte drepturile fundamentale şi libertățile persoanelor interesate, inclusiv dreptul la protecția datelor cu caracter personal;

luînd în considerare importanța şi rolul procurorilor în sistemul justiției penale, inclusiv faptul că calitatea activităților procuraturii reflectă direct nivelul democrației într-un stat de drept iar asigurarea unui proces echitabil şi buna funcționare a sistemului de justiție penală poate fi realizată doar cu condiția îndeplinirii de către toți actorii competenți a atribuțiilor în mod corect, consecvent şi rapid, respectînd şi protejînd demnitatea umană şi drepturile omului;

apreciind că Procuraturii Generale îi revine rolul de garant în ceea ce priveşte transpunerea în practică a caracterului imperativ al legisla□iei procesual-penale prin controlul corespunderii acțiunilor procesuale prevederilor Codului de procedură penală, ale altor acte normative, precum şi ale actelor internaționale, inclusiv prin metoda emiterii instrucțiunilor metodologice şi de reglementare în probleme ce țin de aspectele de aplicare a legislației şi de eficiența activității de combatere şi de prevenire a criminalității, -

a elaborat prezentele Instrucțiuni privind prelucrarea datelor cu caracter personal în sectorul polițienesc.

I. DISPOZIȚII GENERALE

1. Instrucțiunile privind prelucrarea datelor cu caracter personal în sectorul polițienesc (Instrucțiunile) au fost elaborate fără a atinge sfera de competență a Procuraturii Generale, □inîndu-se cont de prevederile Convenției pentru apărarea drepturilor omului şi a libertăților fundamentale; Conven□iei pentru protec□ia persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal; Regulilor de la Havana, adoptate de Congresul al optulea al Națiunilor Unite privind prevenirea criminalității şi tratamentul infractorilor; Recomandarea 1604 (2003) a Adunării Parlamentare a Consiliului Europei privind rolul procuraturii în societate democratică guvernată în baza principiului supremației Legii; Codului de procedură penală al Republicii Moldova; Codului contravențional al Republicii Moldova; Legii privind protecția datelor cu caracter personal; Legii cu privire la Procuratură; Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010; Regulamentului Registrului de evidență a operatorilor de date cu caracter personal, aprobat prin Hotărîrea Guvernului nr. 296 din 15 mai 2012; Regulamentului Procuraturii Generale, aprobat prin ordinul Procurorului General nr. 52/3 din 21 iunie 2010; Codului de etică a procurorului, aprobat prin Hotărîrea Consiliului Superior al Procurorilor nr. 12-3d228/11 din 04 octombrie 2011.

2. Instrucțiunile pot servi în calitate de linii directorii în scopul aducerii operațiunilor de prelucrare a datelor cu caracter personal efectuate de procurori şi entitățile implicate în activitatea polițienească în conformitate cu principiile statuate de

Convenția pentru protec□ia persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal, Legea privind protecția datelor cu caracter personal şi bunele practici în domeniu.

3. No□iunile utilizate în text:

- date cu caracter personal: orice informație referitoare la o persoană fizică identificată sau identificabilă (*subiect al datelor cu caracter personal*). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale. **De exemplu:** numele, prenumele, anul naşterii, domiciliul, numărul de identificare de stat (IDNP), imaginile foto şi video - reprezintă date cu caracter personal care se referă la o persoană fizică identificată direct. În procesul efectuării urmăririi penale, de la persoana fizică pot fi colectate □i alte date cu caracter personal, precum semnătura aplicată la întocmirea unor acte/proiecte, amprente papilare, etc. Totodată, declarațiile făcute de participanții la proces şi consemnate în procesele verbale de audiere, de asemenea, reprezintă date cu caracter personal care vizează persoanele audiate ori persoane terțe identificate sau identificabile implicate în comiterea unei fapte prejudiciabile.

- categorii speciale de date cu caracter personal: datele care dezvăluie originea rasială sau etnică a persoanei, convingerile ei politice, religioase sau filozofice, apartenența socială, datele privind starea de sănătate sau viața sexuală, precum şi cele referitoare la condamnările penale, măsurile procesuale de constrîngere sau sancțiunile contravenționale. **De exemplu:** informația conținută în: certificatele medicale/rapoartele de expertiză medico-legală, în cazierul judiciar, în anexa la buletinul de identitate (*ştampilele „Referendum 2010 ”alegeri”, deoarece în anumite circumstanțe pot cu celeritate reflecta anumite convingeri politice*) etc. De asemenea, informa□ia referitoare la persoanele aflate în spitale, aziluri pentru bătrîni ori deținute pe baza unui mandat de arest pînă la pronunțarea sentinței judecătoreşti, referitoare la persoanele condamnate la închisoare, la cele care execută o sancțiune contravențională sub formă de arest, aflate în instituțiile penitenciare, reprezintă categorii speciale de date cu caracter personal.

- **prelucrarea datelor cu caracter personal**: orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi: colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ştergerea sau distrugerea.

- operator: persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabileşte scopurile şi mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare. **De exemplu:** în toate cazurile cînd Procuratura Generală va reglementa printr-un act normativ departamental scopurile □i procedurile de colectare, stocare şi prelucrare în

continuare a cărorva date cu caracter personal în sisteme de evidență automatizate, manuale ori mixte, se va constitui în calitate de operator al acestor date.

- persoană împuternicită de către operator: persoana fizică sau persoana juridică de drept public ori de drept privat, inclusiv autoritatea publică şi subdiviziunile ei teritoriale, care prelucrează date cu caracter personal în numele şi pe seama operatorului, pe baza instrucțiunilor primite de la operator. **De exemplu:** procuraturile teritoriale/specializate sînt persoane împuternicite atunci cînd prelucrează datele cu caracter personal în conformitate cu instrucțiunile aprobate de Procuratura Generală.

- sistem de evidență a datelor cu caracter personal: orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice. În calitate de sistem de evidență a datelor cu caracter personal se constituie inclusiv dar nu se limitează la, bazele de date, sistemele informaționale şi informatice în care sînt stocate şi prelucrate automatizat sau manual date cu caracter personal. **De exemplu:** modele clasice ale sistemelor de evidență a datelor cu caracter personal reprezintă: Registrul de evidență a angajaților procuraturii sau a numerelor telefoanelor corporative ale angajaților Procuraturii, Registrul de eviden□ă al vizitatorilor; Registrul de eviden□ă a peti□iilor □i altor adresări, informa□iile personalizate referitoare la instruirea specializată a angajaților procuraturii ori a altor subiecți implicați în procesul instrucțional, etc., alte serii structurate de date cu caracter personal, cum ar fi: imaginile video colectate printr-un sistem de supraveghere video instalat în incinta sau pe perimetrul sediului procuraturii etc.;

- depersonalizarea datelor: modificarea datelor cu caracter personal astfel încît detaliile privind circumstanțele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile;

- activitate polițienească: totalitatea acțiunilor/inacțiunilor întreprinse de către autorită□ile de drept (*poli□iene□ti*), în vederea prevenirii/combaterii/investigării faptelor prejudiciabile (*infrac□iuni □i contraven□ii*) şi menținerii ordinii publice.

II. PROCEDURI ORGANIZATORICE ŞI TEHNICE NECESAR A FI RESPECTATE

4. Entită□ilor implicate în procesul desfăşurării activității penale ori contravenționale urmează a le fi atribuite, în dependență de rolul pe care îl au, calitatea de operator ori persoană împuternicită de operator, în conformitate cu noțiunile statuate de art. 3 al Legii privind protecția datelor cu caracter personal şi pct. 3 al prezentelor Instrucțiuni. Aceasta va permite delimitarea clară a competen□elor □i repartizarea adecvată a drepturilor şi obligațiilor în cadrul operațiunilor de prelucrare a datelor cu caracter personal.

5. Toate persoanele implicate în procesul desfăşurării activităților specificate în pct. 4, care prelucrează date cu caracter personal, inclusiv angajații procuraturii, urmează a fi supu□i unei declarații de confidențialitate, care, după caz, poate fi inclusă

în contractele de muncă, avînd calitate de clauză contractuală, sau în fişele postului, cu mențiunea expresă despre răspunderea civilă, contraven□ională ori penală pentru încălcarea acesteia.

6. Urmează a fi elaborată □i implementată politica de securitate a datelor cu caracter personal în conformitate cu prevederile Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobată prin Hotărîrea Guvernului nr. 1123 din 14 decembrie 2010 (Cerințe), care ar acoperi aspecte ce vizează inclusiv: procedurile şi măsurile legate de realizarea politicii de securitate, cu aplicarea soluțiilor practice cu un nivel de detaliere şi complexitate proporțional; identificarea şi autentificarea utilizatorilor învesti□i cu drepturi de acces la sistemele informaționale de date cu caracter personal; modalită□ile de reacționare la incidentele de securitate; de protecție a tehnologiei informa□iei şi comunicațiilor; de asigurare a integrității informației care conține date cu caracter personal; de administrare a accesului la datele cu caracter personal prelucrate; de audit în sistemele informaționale □i de eviden□ă a datelor cu caracter personal, etc**.**

7. Politica de securitate instituțională urmează să conțină reglementări care ar asigura protecția datelor cu caracter personal prelucrate în cadrul sistemelor de eviden□ă deținute, în special prin următoarele metode:

- preîntîmpinarea conexiunilor neautorizate la rețelele comunicaționale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele, în special în procesul dezvăluirii prin transmitere a datelor cu caracter personal între entită□ile abilitate cu diferite competen□e în procesul desfăşurării activităților de prelucrare a datelor cu caracter personal în cadrul acțiunilor de prevenire şi investigare a infracțiunilor, punerii în executare a sentințelor de condamnare şi al altor acțiuni din cadrul procedurii penale sau contravenționale;

- excluderea accesului neautorizat la datele cu caracter personal prelucrate în cadrul sistemelor de eviden□ă prin metoda implementării procedurilor de identificare şi autentificare a utilizatorilor; prin repartizarea obligațiilor şi învestirea cu minim de drepturi şi competențe a celor implica□i în procesul de gestionare a sistemelor de eviden□ă a datelor cu caracter personal; prin asigurarea integrității resurselor informaționale (*date şi programe*);

- preîntîmpinarea acțiunilor speciale tehnice şi de program care pot condiționa distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic şi de program, a soft-urilor destinate prelucrării datelor cu caracter personal, prin metoda folosirii mijloacelor de protecție speciale tehnice şi de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-urilor şi efectuarea periodică a copiilor de siguranță;

- preîntîmpinarea acțiunilor intenționate şi/sau neintenționate a utilizatorilor interni şi/sau externi, precum şi a altor angajați, care condiționează distrugerea, modificarea datelor cu caracter personal prelucrate în cadrul sistemelor de eviden□ă sau defecțiuni în lucrul complexului tehnic şi de program;

- preîntîmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, prin folosirea metodelor de cifrare (*criptare*) a acestei informații;

- stabilirea exactă a ordinii □i procedurilor de acces la informația care conține date cu caracter personal, prelucrată în cadrul sistemelor informaționale □i de eviden□ă instituite, atît pentru utilizatorii interni cît □i pentru cei externi;

- organizarea generării înregistrărilor de audit a securității în sistemele informaționale □i de eviden□ă a datelor cu caracter personal pentru a fi posibil acumularea probatoriului în cazurile investigării eventualelor operațiuni de acces/tentativă de acces neautorizat, a operațiunilor de modificare, extragere, blocare, ştergere sau distrugere a datelor cu caracter personal prelucrate în aceste sisteme de evidență.

8. În cazul dezvăluirii formatului electronic al datelor cu caracter personal conținute în dosarele penale, contraven□ionale şi/sau civile, în listele contabile cu datele angajaților şi alte documente care vizează angaja□ii, prin rețele comunicaționale ori pe alt suport digital de stocare şi păstrare, urmează a fi asigurată criptarea acestei informa□ii sau examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat VPN. Accesul fără fir la sistemele de evidență a datelor cu caracter personal urmează a fi permis □i autorizat doar în cazul utilizării mijloacelor criptografice de protecție a informației. Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieşind din posibilitățile tehnice asigurate de destinatar şi operator, precum şi în corespundere cu măsurile organizatorice şi tehnice implementate de părți. În cazul în care re□elele comunica□ionale prezintă riscuri pentru confidențialitatea şi securitatea datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere (*expediere poştală cu aviz recomandat, înmînarea personală, etc.*).

9. Dezvăluirea prin transmitere a datelor cu caracter personal prin re□ele comunica□ionale ce nu corespund Cerințelor, (*spre exemplu: expedierea informa□iei prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.*) urmează a fi interzisă.

10. Urmează a fi interzise operațiunile de dezvăluire a datelor cu caracter personal între procuratură ori autorită□ile care exercită activități în sectorul poliţienesc ale Republicii Moldova către entită□ile amplasate geografic în stînga Nistrului □i care refuză să se supună juridic legislației Republicii Moldova, reie□ind din considerentul că la moment nu există posibilitatea exercitării unui control efectiv asupra acestei părți teritoriale, inclusiv în partea ce □ine de conformitatea prelucrării datelor cu caracter personal prevederilor Legii privind protecția datelor cu caracter personal. **De exemplu:** la 04 ianuarie 2013, în rezultatul examinării plîngerii unui grup de persoane, Centrul a emis decizia privind suspendarea operațiunilor de prelucrare a datelor cu caracter personal, prin care a cerut Ministerului Afacerilor Interne suspendarea oricăror operațiuni de dezvăluire către autoritățile neconstituționale din raioanele administrative aflate în stînga Nistrului, a datelor cu caracter personal, prelucrate în calitate de operator ori destinatar, pînă la momentul înregistrării obligatorii de către aceste entități în conformitate cu prevederile art.23 şi 34 alin.(4) ale Legii privind protecția datelor cu

caracter personal şi implementarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărîrea Guvernului nr.1123 din 14 decembrie 2010. Ulterior, această decizie a servit ca temei pentru emiterea de către Judecătoria Centru a unei hotărîri, prin care instanța a constatat încălcarea dreptului la viață privată şi a legislației privind protecția datelor cu caracter personal prin metoda transmiterii datelor cu caracter personal către autoritățile şi entitățile din stînga Nistrului a Republicii Moldova, care acționează în afara cîmpului legal na□ional, obligînd Ministerul Afacerilor Interne să achite prejudicii morale şi materiale în sumă de peste 180 mii lei. Mai mult, prin Hotărîrea Consiliului Superior al Magistraturii din 10 aprilie 2012, cu privire la demersul Ministrului Justiției, referitor la opinia asupra adresării viceprim-ministrului, pe marginea abordării unor probleme de natură juridică s-a constatat că citat: *„... orice act emis de autoritățile autoproclamate din această parte a Republicii Moldova, contravin din capul locului Constituției, faptul referindu-se în egală măsură şi asupra oricăror hotărîri, decizii, sentințe pronunțate de judecătoriile instituite în regiunea dată ilegal. Astfel, Consiliul consideră ca fiind inacceptabile orice colaborări, conlucrări în aspect juridic şi propuneri de soluții juridice cu structurile din regiunea transnistreană.*”.

11. Procedura dezvăluirii prin transmitere a datelor cu caracter personal stocate pe suport de hîrtie, inclusiv în cazul desfăşurării activității de investigații peste hotarele Republicii Moldova, urmează a fi reglementată prin act normativ institu□ional, luîndu-se în considerare necesitatea asigurării unui nivel adecvat de protecție a datelor cu caracter personal, utilizînd inclusiv canalele diplomatice. Transmiterea transfrontalieră a datelor cu caracter personal urmează a fi efectuată în strictă corespundere cu prevederile art. 32 al Legii privind protecția datelor cu caracter personal, în special în cazurile cînd tratatul internațional în baza căruia se efectuează transmiterea nu conține garanții privind protecția drepturilor subiectului de date cu caracter personal.

12. Volumul şi categoria datelor cu caracter personal colectate în scopul prevenirii şi investigării infracțiunilor, punerii în executare a sentințelor de condamnare şi al altor acțiuni din cadrul procedurii penale sau contravenționale, necesită a fi limitate la strictul necesar pentru realizarea scopurilor declarate.

13. Procuratura Generală (*după caz procuraturile teritoriale/specializate*), urmează să reglementeze explicit, în conformitate cu prevederilor art. 15 şi 212 Cod de procedură penală, procedura de acces la materialele dosarelor a martorilor, bănuiților, învinuiților, victimelor, părților vătămate, părților civile şi civilmente responsabile, a apărătorilor sau persoanelor împuternicite, în vederea neadmiterii dezvăluirii neautorizate a datelor cu caracter personal, inclusiv urmează să interzică efectuarea neautorizată a înregistrărilor foto şi video în perimetrul de securitate a procuraturii, precum şi folosirea mijloacelor tehnice ascunse, □inîndu-se cont de necesitatea asigurării regimului de confiden□ialitate □i securitate a prelucrării datelor cu caracter personal, prevăzut de art.29 □i 30 ale Legii privind protec□ia datelor cu caracter personal, precum şi pct. 26 din Cerințe. **De exemplu*:*** acțiuni de genul înregistrării video, în procesul luării cunoştinței cu materialele dosarului penal nr. 2010038002 şi materialului de control nr. 18 pr/13, cu ulterioara dezvăluire a materialelor video în

spațiul internet pe http://curajtv.play.md/ şi http://www.youtube.com/watch?v=QnFGqTumx8Q), urmează a fi excluse *per se*.

14. În cazul în care, avocatul sau persoana împuternicită solicită să ia cunoştință cu materialele cauzei, aceştia urmează a fi informați în scris despre obligațiile ce le revin în conformitate cu prevederile art. 15 Cod de procedură penală, art. 29 şi 30 ale Legii privind protecția datelor cu caracter personal, inclusiv despre răspunderea prevăzută de art. 74^1 Cod contravențional şi/ori art. 315 Cod penal.

15. Procuratura şi alte entități care exercită activități în sectorul polițienesc urmează să revizuiască clauzele contractelor încheiate cu Întreprinderea de Stat Centrul Resurselor Informaționale de Stat „Registru", în vederea acoperirii în totalitate a prevederilor statuate de art. 4 alin. (1) lit. a), b,) c,) d) şi e) al Legii privind protecția datelor cu caracter personal. În acest sens, persoanele autorizate urmează a avea acces doar la acele categorii şi volum de date cu caracter personal stocate în resursele informaționale principale de stat, care au legătură directă cu scopul pentru care sînt accesate sau colectate. Astfel, accesul individualizat la fiecare categorie în parte, va exclude posibilitatea prelucrării unui volum excesiv de date ce vizează subiecții ori în alte scopuri decît cele prevăzute inițial. **De exemplu:** s-a constatat că în 80 % de cazuri ofițerii de urmărire penală sau procurorii consultă Registrul de stat al populației în scopul identificării locului de domiciliu al martorilor □i altor participan□i la proces pentru a-i cita la audieri. În acest caz celelalte date care în prezent sînt accesibile (*numele, prenumele copiilor, părinților, soților, grupa sangvină, înălțimea, culoarea ochilor, proprietăți etc.*), nu sînt necesare scopului propus inițial.

16. Procurorii, anterior ini□ierii procedurilor de autorizare de către judecătorii de instruc□ie a măsurilor speciale de investigație, urmează să dea o apreciere proporționalității ingerinței admise în viața privată a persoanei în raport cu scopul urmărit şi, să decidă, pe propria răspundere, dacă este necesar restrîngerea unor drepturi şi libertăți ale persoanei, în special a dreptului la viață privată. În cadrul procesului de luare a deciziei privind ini□ierea procedurilor de autorizare sau în cadrul procesului de autorizare a efectuării unei activități speciale de investigație, reprezentanții autorității abilitate şi competente urmează să țină cont de prevederile art. 4 alin. (1) al Legii privind protecția datelor cu caracter personal care statuează că datele cu caracter personal care fac obiectul prelucrării trebuie să fie adecvate, pertinente şi neexcesive în ceea ce priveşte scopul pentru care sînt colectate şi/ sau prelucrate ulterior. Anume acest principiu de protecție a datelor cu caracter personal, coroborat cu prevederile art. 15 □i 132^1 alin. (3) Cod de procedură penală, urmează a fi aplicat de fiecare dată cînd este decisă oportunitatea aplicării unei măsuri speciale de investigație. **De exemplu**: este relevantă situația pe care o sesizează frecvent Centrului operatorii de telefonie mobilă, cînd în cadrul unui dosar penal pornit pe faptul furtului unui telefon mobil, acestora li se solicită datele cu caracter personal ce vizează abonații care au apelat sau au fost apelați de pe acest telefon, utilizînd codul IMEI, informa□ie, care poate fi consemnată pe zeci sau chiar sute de pagini, real fiind utilizate de către solicitan□i doar informațiile privind abonații care au telefonat sau au fost telefonați cel mai des, acestea limitîndu-se doar la cîteva persoane, care după audiere pot contribui la identificarea bănuitului. În aceste situații, volumul datelor cu caracter personal prelucrate „la pachet" este excesiv, iar

ingerința în viața privată a persoanelor în raport cu scopul declarat, aparent, este nejustificată.

17. Datele cu caracter personal stocate în Registrul de stat al populației şi alte resurse informaționale principale de stat, urmează a fi consultate doar în cazul în care această acțiune este motivată şi întemeiată din punct de vedere legal, iar extragerea fişelor personale din sistemul/ele automatizat/e, urmează a fi efectuată doar în cazuri excepționale, urmînd ca fişa extrasă să nu fie stocată pe un termen ce depăşeşte realizarea scopurilor propuse. În continuare, la realizarea scopului pentru care au fost extrase, fişele personale urmează a fi distruse în baza unei decizii adoptate în acest sens. În aceeaşi ordine de idei, urmează a fi reglementat distinct regimul de confidențialitate şi securitate a datelor cu caracter personal consemnate în fişele personale extrase. Urmează ca pe perioada necesară desfăşurării urmăririi penale acestea să fie păstrate separat într-un alt fişier şi să nu fie anexate la materialele dosarului penal, precum şi să nu fie aduse la cunoştință părților, cu excepția persoanei vizate. Se explică că extragerea fi□elor persoanelor care nu sînt participan□i la procesul penal în vederea utilizării fotografiilor consemnate în aceste acte pentru realizarea ac□iunii procesuale prevăzute de art.111 alin.(6) Cod de procedură penală - prezentarea spre recunoa□tere, este inadmisibilă □i încalcă flagrant principiile prevăzute de art.4 alin.(1) lit.b) al Legii privind protec□ia datelor cu caracter personal, inclusiv prevederile art.74[1] alin.(4) Cod contraven□ional.

18. Urmează a fi revizuite categoriile de date cu caracter personal care sînt colectate şi incluse în actele procesuale întocmite de către procurori sau de către ofițerii de urmărire penală, astfel încît acestea să nu fie excesive în raport cu dispozițiile art. 15 Cod de procedură penală. **De exemplu**: în procesul-verbal de audiere a martorilor trebuie indicat doar numele, prenumele şi adresa acestora, reieşind din prevederile art. 105 Cod de procedură penală. Concomitent, procesul-verbal urmează a fi întocmit cu respectarea prevederilor art. 260 Cod de procedură penală, în care sînt stipulate expres elementele ce trebuie să cuprindă procesul-verbal. Astfel, colectarea categoriilor de date cu caracter personal ce nu se regăsesc în prevederile articolului menționat supra, urmează a fi interzise ori motivate în scris în procesul-verbal, în conformitate cu prevederile art. 15 alin. (3) Cod de procedură penală.

19. Urmează a fi întreprinse ac□iuni în vederea excluderii cazurilor de folosire, de către procurori ori reprezentan□ii autorită□ilor care exercită activități în sectorul polițienesc, a situa□iei de serviciu □i a resurselor publice pentru a verifica dacă se află sau nu în vizorul altor organe de drept. **De exemplu**: Centrul a constatat mai multe cazuri cînd factori de decizii de nivel mediu, solicitau de la Î.S.„CRIS„Registru" informa□ii din auditul sistemelor informa□ionale privind entită□ile □i utilizatorii autoriza□i care au efectuat opera□iunile de consultare □i extragere a fi□elor personale a unor colaboratori de poli□ie din subordine, inclusiv a procurorilor. Scopul pentru care se solicitau aceste informa□ii în unul din cazuri - „necesitatea apărută în cadrul urmăririi penale la o cauză pornită în baza art.284 Cod penal (*crearea □i conducerea unei organiza□ii criminale*)", nu era unul real. În final se dorea să se afle dacă informa□ia ce viza procurorul □i angaja□ii Ministerului Afacerilor Interne care cercetau această crimă era consultată de către alte entită□i sub pretextul planării

eventualului pericol de punere a acesteia la dispozi□ia persoanelor suspecte. În acest caz, însă, informa□ia putea fi solicitată doar de Procuratura Generală în cadrul unei proceduri penale, care s-ar referi concret la fapte de pregătire ori tentativă de comitere a unor infrac□iuni în privin□a procurorului care conduce urmărirea penală ori a colaboratorilor poli□iei implica□i în procedurile de investigare □i urmărire penală a infrac□iunii prevăzute de art.284 Cod penal.

20. Se explică că în conformitate cu prevederile art.157 Cod de procedură penală, documentele în orice formă (*scrisă, audio, video, electronică etc.*) care provin de la persoane oficiale fizice sau juridice dacă în ele sînt expuse ori adeverite circumstanțe care au importanță pentru cauză, (*inclusiv informa□ia stocată în auditul sistemelor informa□ionale □i de eviden□ă*), pot fi solicitate printr-un demers al organului de urmărire penală în cadrul urmăririi penale sau în procesul judecării cauzei. În acest caz, însă, urmează a fi respectate prevederile art.214 Cod de procedură penală, care stipulează că în cursul procesului penal nu pot fi administrate, utilizate şi răspîndite fără necesitate informație oficială cu accesibilitate limitată. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată (*inclusiv operatorii de date cu caracter personal*) au dreptul să se convingă de faptul că aceste date se colectează pentru procesul penal respectiv, iar în caz contrar să refuze de a comunica sau de a prezenta date. Persoanele cărora organul de urmărire penală sau instanța le solicită să comunice sau să prezinte informație oficială cu accesibilitate limitată au dreptul să primească în prealabil de la persoana care solicită informații o explicație în scris care ar confirma necesitatea furnizării datelor menționate.

21. Urmează a □ine cont de faptul că în conformitate cu prevederile art.8 al Legii privind accesul la informa□ie, datele cu caracter personal fac parte din categoria informației oficiale cu accesibilitate limitată, accesul la care se realizează în conformitate cu prevederile legislației privind protecția datelor cu caracter personal.

22. Anumite date cu caracter personal prelucrate în sistemele informa□ionale □i de eviden□ă *(amprente digitale, semnătura olografă, etc.*) pot fi colectate □i utilizate într-un proces penal ori contraven□ional în calitate de mostre necesare pentru cercetarea comparativă doar cu respectarea prevederilor art.art.157-156, 260-261 Cod de procedură penală □i art.4 al Legii privind protec□ia datelor cu caracter personal, prin emiterea ordonan□elor motivate □i întocmirea proceselor verbale corespunzătoare. **De exemplu**: Centrul a constatat în cazuri concrete că ac□iunile de solicitare „la pachet”, printr-un simplu demers a organului de urmărire penală, a amprentelor digitale colectate de Î.S.„CRIS „Registru” în procesul perfectării pa□apoartelor biometrice, contravin normelor procesual-penale □i principiilor de protec□ie a datelor cu caracter personal.

III. Drepturile subiecților de date cu caracter personal

23. În cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.15 Cod de procedură penală □i art.12 al Legii privind protec□ia datelor cu caracter personal, persoanei necesită a-i fi

furnizate următoarele informații, exceptînd cazul în care el deține deja informațiile respective:

- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (*denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de eviden□ă al operatorilor de date cu caracter personal*);

- privind scopul concret al prelucrării datelor cu caracter personal colectate;

- privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal; existența drepturilor la informare □i de acces la datele colectate; de intervenție asupra datelor (*în special de a rectifica, actualiza, bloca sau şterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora*) şi de opoziție, precum □i condițiile în care aceste drepturi pot fi exercitate; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informa□ia.

24. Subiecților de date cu caracter personal urmează a le fi asigurat dreptul de acces □i posibilitatea de a lua cunoştință cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluderii sau includerii incorecte a unor date, precum şi împotriva altor erori comise la înscrierea datelor despre sine. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alți subiecți, conținute în actele procesuale (*materialele cauzei*), cu excep□ia cazurilor în care solicitan□ii î□i realizează un interes legitim care nu prejudiciază interesele sau drepturile şi libertățile fundamentale ale subiectului datelor cu caracter personal, ori în cazurile expres prevăzute de art. 293 alin. (1) Cod de procedură penală.

25. Dreptul de informare urmează a fi asigurat de către operatorul datelor cu caracter personal (*procurori sau autorită□ile ce exercită activități în sectorul polițienesc*) tuturor persoanelor supuse măsurilor speciale de investigație prevăzute de art. 132^2 alin. (1) lit. b), c) e), g) şi n) Cod de procedură penală, inclusiv colateral, cu excepția cazului în care informarea persoanelor vizate se dovedeşte a fi imposibilă sau ar implica eforturi disproporționate. Actualmente, în pofida gravității ingerinței, persoanele cu care contactează subiectul supus măsurii speciale de investigație şi care, de asemenea, se constituie în calitate de subiect al datelor cu caracter personal colectate şi prelucrate fără consimțămîntul său de către entitățile ce efectuează activitatea specială de investigație - nu sînt informați despre aceasta. Astfel, persoana este privată de posibilitatea realizării drepturilor sale în calitate de subiect a datelor cu caracter personal. **De exemplu:** în cazul în care locuința persoanei bănuite în comiterea unei fapte prejudiciabile este supusă măsurii speciale de investigație - supravegherea şi înregistrarea audio-video, subiecții care au contactat/comunicat prin intermediul rețelei telefonice sau au intrat în domiciliul persoanei nominalizate, urmează a fi informați obligatoriu în termenele şi în condițiile prevăzute de art. 132^5 Cod de procedură penală. În acest sens sînt relevante unele constatări ale Cur□ii Europene pentru Drepturile Omului în cauza *Amann versus Elveția,* care a statuat că trebuie să fie reglementat în

detaliu cazul persoanelor supravegheate "fortuit" ca "participante necesare" într-o convorbire telefonică înregistrată de autorități pe baza respectivelor prevederi legale.

26. În cazul plasării datelor cu caracter personal, prelucrate în sistemele de evidență interne, prin intermediul paginii web oficiale a procuraturii sau a organelor de urmărire penală, urmează a fi instituite soluții tehnice necesare pentru excluderea accesului nerestricționat la acestea, fiind asigurate măsurile tehnice de program, specializate în securitatea informației, măsuri de protecție în vederea confirmării neechivoce a identității subiectului de date cu caracter personal, care îşi realizează dreptul de acces sau rectificare, prin excluderea accesului neautorizat la aceste date. **De exemplu**: în cazul instituirii rubricii intitulate „Interpelările şi întrebările deputaților" pe pagina oficială a Procuraturii Generale http://www.procuratura.md/md/ID/, aceasta s-a constituit ca un instrument important în vederea informării publicului larg □i asigurării transparenței decizionale în activitatea organelor procuraturii. Cu toate acestea, în prima perioadă de func□ionare a rubricii nominalizate, informa□ia a fost dezvăluită cu încălcarea principiilor de protec□ie a datelor cu caracter personal, fără a fi depersonalizată, fapt care a determinat interven□ia Centrului.

27. În cazul realizării de către subiectul de date cu caracter personal a dreptului de interven□ie, datele inexacte urmează a fi actualizate prin rectificare sau ştergere, ca bază servind doar surse legale (*acte de identitate, de stare civilă, resurse informaționale principale de stat etc.*), modificarea urmînd a fi efectuată în toate sistemele informa□ionale □i de evidență gestionate.

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

29. Aplicarea excepțiilor şi restricțiilor realizării de către subiecții de date cu caracter personal a drepturilor sale, urmează a fi făcute în strictă conformitate cu prevederile art. 15 al Legii privind protecția datelor cu caracter personal □i 132^5 Cod de procedură penală.

IV. Stocarea, păstrarea şi distrugerea datelor cu caracter personal prelucrate în cazul activității polițienești

30. Stocarea □i păstrarea datelor cu caracter personal consemnate în documentele procedurale cît şi în materialele de control, urmează a fi efectuată în strictă conformitate cu prevederile art.211-214 Cod de procedură penală, Procuraturii Generale, procuraturilor teritoriale/specializate şi organelor de urmărire penală revenindu-le dreptul de a decide asupra finalită□ii acestora luînd în considerație prevederile art. 4 alin. (1) lit. e) şi art. 11 ale Legii privind protecția datelor cu caracter personal.

31. Accesul în spațiile unde sînt amplasate sistemele informaționale □i de eviden□ă a datelor cu caracter personal urmează a fi restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate institu□ionale aprobate.

32. Stocarea □i păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de eviden□ă, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecție speciale tehnice şi de program □i nu au instalate programe licențiate, programe antivirus, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță □i de efectuare a auditului - urmează a fi interzisă.

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

34. Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul şi care permite reproducerea acestuia, urmează a fi asigurat prin plasarea acestora în safeuri sau dulapuri metalice care se încuie şi se sigilează. Accesul la safeuri şi dulapuri metalice urmează a fi monitorizat, prin ținerea unui registru de evidență. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului urmează a fi interzisă.