INSTRUCŢIUNI nr. 27 din 3 februarie 2010
privind măsurile de natură organizatorică şi tehnică pentru asigurarea securităţii prelucrărilor de date cu caracter personal efectuate de către structurile/unităţile Ministerului Administraţiei şi Internelor

Având în vedere dispoziţiile Legii nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare, ale Legii nr. 238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice,

ţinând cont de faptul că dispoziţiile Legii nr. 238/2009 şi, în consecinţă, dispoziţiile corespunzătoare cuprinse în prezentul act normativ se aplică exclusiv în cazul prelucrărilor de date cu caracter personal efectuate în cursul activităţilor de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice,

în temeiul art. 7 alin. (4) din Ordonanţa de urgenţă a Guvernului nr. 30/2007 privind organizarea şi funcţionarea Ministerului Administraţiei şi Internelor, aprobată cu modificări prin Legea nr. 15/2008, cu modificările şi completările ulterioare,

ministrul administraţiei şi internelor emite următoarele instrucţiuni:

TITLULUL I
Măsuri organizatorice

CAP. I
Dispoziţii generale

ART. 1
Prezentele instrucţiuni se aplică activităţilor de prelucrare a datelor cu caracter personal efectuate de structurile şi unităţile Ministerului Administraţiei şi Internelor, denumit în continuare MAI, în calitatea acestora de operatori sau împuterniciţi ai operatorilor.

ART. 2
(1) La nivelul MAI, prelucrarea datelor cu caracter personal se realizează cu respectarea regulilor generale şi speciale prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare, de Legea nr. 238/2009 privind reglementarea prelucrării datelor cu caracter personal de către structurile/unităţile Ministerului Administraţiei şi Internelor în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice, a prevederilor deciziilor şi instrucţiunilor cu caracter normativ emise de Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare Autoritatea naţională de supraveghere, a prevederilor prezentelor instrucţiuni şi a procedurilor proprii elaborate de operatori potrivit legii.

(2) Operatorii şi împuterniciţii acestora utilizează sisteme de evidenţă şi/sau mijloace automate şi neautomate de prelucrare a datelor cu caracter personal cu aplicarea principiilor respectării drepturilor omului, legalităţii, necesităţii, confidenţialităţii şi proporţionalităţii şi numai dacă, prin utilizarea acestora, este asigurată protecţia datelor prelucrate.

(3) În cadrul activităţii de prelucrare a datelor cu caracter personal, operatorii şi împuterniciţii acestora se supun activităţilor de control prealabil sau de investigare efectuate de Autoritatea naţională de supraveghere şi, la cerere, acordă acesteia sprijin deplin pentru exercitarea atribuţiilor sale.

ART. 3

(1) Au calitatea de operator structurile şi unităţile MAI, precum şi MAI, dacă:

a) stabilesc scopul şi mijloacele de prelucrare a datelor cu caracter personal; sau

b) scopul şi mijloacele de prelucrare a datelor cu caracter personal sunt stabilite printr-un act normativ sau în baza unui act normativ; sau

c) sunt desemnate ca operator printr-un/în baza unui act normativ.

(2) Au calitatea de împuterniciţi ai operatorului structurile care prelucrează date cu caracter personal pe seama operatorului.

(3) Are calitatea de utilizator al datelor cu caracter personal, denumit în continuare utilizator, personalul operatorului sau al împuternicitului acestuia ale cărui atribuţii de serviciu presupun operaţiuni de prelucrare a datelor cu caracter personal.

CAP. II

Organizarea activităţii de prelucrare a datelor cu caracter personal în MAI

ART. 4

(1) La nivelul fiecărei structuri/unităţi a MAI, centrale sau teritoriale, care are calitatea de operator, funcţionează o structură specializată în domeniul protecţiei datelor cu caracter personal, denumită în continuare structură responsabilă cu protecţia datelor cu caracter personal. În cadrul acestei structuri este obligatoriu ca cel puţin o persoană să aibă specializare IT.

(2) Prin derogare de la prevederile alin. (1), pentru structurile/unităţile MAI care au un număr de cel mult 500 de înregistrări ori interogări pe zi sau care au un număr de până la 30 de utilizatori ori gestionează numai în mod sporadic date cu caracter personal, se desemnează o persoană ca responsabil cu protecţia datelor cu caracter personal, în directa subordonare a conducătorului operatorului. Personalul care urmează să ocupe o astfel de funcţie trebuie să aibă cunoştinţe IT.

ART. 5

Structurile/unităţile MAI, în calitate de operator, au în principal următoarele obligaţii:

a) să notifice Autoritatea naţională de supraveghere potrivit art. 22 din Legea nr. 677/2001, cu modificările şi completările ulterioare;

b) să asigure informarea persoanelor vizate şi să respecte drepturile acestora;

c) să ia măsurile necesare pentru a asigura securitatea prelucrării datelor cu caracter personal;

d) să elaboreze Proceduri privind măsurile de protecţie a persoanelor cu privire la prelucrarea datelor cu caracter personal, denumite în continuare proceduri proprii, conform legislaţiei şi normelor interne în domeniul standardizării în vigoare la nivelul MAI;

e) să întocmească şi să transmită, anual, Autorităţii naţionale de supraveghere raportul de activitate privind protecţia persoanelor în privinţa prelucrării datelor cu caracter personal;

f) să pună la dispoziţia Oficiului Responsabilului cu Protecţia Datelor Personale, denumit în continuare Oficiu, în condiţiile legii, prin intermediul structurii responsabile/responsabilului cu protecţia datelor cu caracter personal şi la solicitarea reprezentanţilor acestuia, informaţiile şi documentele în legătură cu prelucrarea datelor cu caracter personal pe care le deţin, în vederea exercitării atribuţiilor de coordonare, îndrumare şi monitorizare a aplicării unitare a legislaţiei în domeniul protecţiei persoanelor cu privire la prelucrarea datelor cu caracter personal.

ART. 6

(1) Conducătorii operatorului au următoarele atribuţii principale:

a) stabilesc scopul şi mijloacele de prelucrare a datelor cu caracter personal atunci când acestea sunt necesare pentru exercitarea unor competenţe legale;

b) numesc/stabilesc responsabilul/structura responsabilă cu protecţia datelor personale;

c) asigură elaborarea procedurilor proprii şi, după avizarea acestora de către Oficiu, le aprobă;

d) asigură implementarea şi veghează la respectarea normelor procedurale în materia prelucrării datelor cu caracter personal de către utilizatori;

e) asigură desfăşurarea pregătirii de specialitate şi instruirea utilizatorilor în acest domeniu;

f) dispun măsuri de completare sau, după caz, de modificare a fişei posturilor utilizatorilor;

g) analizează şi dispun în ceea ce priveşte suspendarea sau revocarea dreptului de acces al utilizatorilor la sisteme de evidenţă a datelor cu caracter personal, în condiţiile legii;

h) informează Oficiul în legătură cu orice încălcare a normelor de protecţie a datelor cu caracter personal de natură a prejudicia drepturile persoanei vizate, cu privire la măsurile dispuse pentru identificarea persoanei responsabile şi limitarea efectelor unei diseminări neautorizate a datelor, precum şi cu privire la situaţiile în care au fost emise recomandări sau aplicate sancţiuni de către Autoritatea naţională de supraveghere sau când aceasta a dispus efectuarea unui control prealabil ori a unor investigaţii;

i) analizează periodic activitatea responsabilului/structurii responsabile cu protecţia datelor cu caracter personal.

(2) Conducătorii împuterniciţilor operatorului au atribuţiile prevăzute la alin. (1) lit. b), d)-g) şi i); în cazul în care este incidentă una dintre situaţiile prevăzute la alin. (1) lit. h), conducătorii împuterniciţilor au obligaţia de a informa operatorul.

ART. 7

(1) Responsabilul/Structura responsabilă cu protecţia datelor cu caracter personal se subordonează nemijlocit conducătorului operatorului sau, după caz, împuternicitului acestuia, şi are următoarele atribuţii principale:

a) coordonează elaborarea şi implementarea procedurilor proprii, pe care le supune aprobării conducerii operatorului;

b) elaborează ghidul pentru exercitarea drepturilor de către persoana vizată;

c) consiliază conducerea operatorului sau a împuternicitului acestuia şi sprijină instruirea personalului care prelucrează date cu caracter personal referitoare la normele şi regulile de protecţie a datelor cu caracter personal;

d) informează operativ conducerea operatorului sau a împuternicitului acestuia despre vulnerabilităţile şi riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal al structurii şi propune măsuri pentru înlăturarea acestora;

e) coordonează şi monitorizează activitatea personalului pe linia protecţiei datelor cu caracter personal la nivelul operatorului sau al împuternicitului acestuia şi propune conducerii operatorului sau, după caz, a împuternicitului, în condiţiile legii, măsuri privind modificarea, suspendarea ori revocarea drepturilor de acces în situaţiile prevăzute la art. 10 şi 11, după caz;

f) efectuează, prin sondaj, verificări privind modul de aplicare a măsurilor legale de protecţie a datelor cu caracter personal, întocmeşte rapoarte şi face propuneri pentru remedierea deficienţelor constatate, pe care le înaintează spre aprobare conducerii operatorului sau, după caz, a împuternicitului;

g) asigură relaţionarea, solicită asistenţă de specialitate şi participă la convocările şi activităţile organizate de Oficiu în domeniul prelucrării datelor cu caracter personal;

h) coordonează soluţionarea cererilor persoanelor vizate;

i) ţine evidenţa cererilor persoanelor vizate.

(2) Atribuţiile specifice responsabilului/personalului din cadrul structurii responsabile cu protecţia datelor cu caracter personal se stabilesc prin fişa postului.

ART. 8

(1) Utilizatorii au următoarele obligaţii specifice:

a) să cunoască şi să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal, precum şi normele interne în materie emise la nivelul MAI;

b) să informeze persoana vizată atunci când datele cu caracter personal sunt colectate direct de la aceasta, în condiţiile legii, cu privire la: identitatea operatorului, scopul în care se face prelucrarea datelor, destinatarii sau categoriile de destinatari ai datelor, obligativitatea furnizării tuturor datelor cerute şi consecinţele refuzului de a le pune la dispoziţie, drepturile prevăzute de lege, în special drepturile de acces, de intervenţie asupra datelor şi de opoziţie, condiţiile în care pot fi exercitate aceste drepturi, respectiv să ofere orice alte informaţii a căror furnizare este impusă prin dispoziţii ale Autorităţii naţionale de supraveghere, ţinând seama de specificul prelucrării;

c) să prelucreze numai datele cu caracter personal necesare îndeplinirii atribuţiilor de serviciu şi să acorde sprijin responsabilului/structurii responsabile cu protecţia datelor cu caracter personal pentru realizarea activităţilor specifice ale acestuia/acesteia;

d) să păstreze confidenţialitatea 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;

e) să respecte măsurile de securitate, precum şi celelalte reguli stabilite de operator, inclusiv cele stabilite prin proceduri proprii;

f) să informeze de îndată conducerea operatorului sau, după caz, a împuternicitului şi responsabilul/structura responsabilă cu protecţia datelor cu caracter personal despre împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal sau despre o situaţie în care au fost accesate/prelucrate date cu caracter personal prin încălcarea normelor legale, despre care a luat la cunoştinţă.

(2) Pentru fiecare utilizator, fişa postului se completează în mod corespunzător cu atribuţiile prevăzute la alin. (1).

ART. 9

(1) Înainte de începerea activităţilor de prelucrare a datelor cu caracter personal, utilizatorul trebuie să semneze o declaraţie pe propria răspundere privind respectarea normelor de protecţie a acestor date, conform modelului prevăzut în anexa nr. 1.

(2) Utilizatorul poate prelucra date cu caracter personal doar pe perioada în care ocupă funcţia respectivă.

(3) Operatorii pot permite, în condiţiile legii, prelucrarea datelor cu caracter personal de către funcţionarii unui alt operator din afara ori din cadrul MAI, pe perioada necesară îndeplinirii unor atribuţii de serviciu. În acest sens, este obligatorie încheierea unui protocol de cooperare între operatori care să prevadă că prelucrarea datelor cu caracter personal se face cu respectarea drepturilor persoanelor vizate, respectiv condiţiile de securitate stabilite de către operatorul care gestionează sau administrează sistemul de evidenţă a datelor cu caracter personal.

ART. 10

Extinderea sau restrângerea atribuţiilor de prelucrare a datelor cu caracter personal se dispune de operator atunci când utilizatorul se află în una dintre următoarele situaţii:

a) la modificarea raporturilor de muncă;

b) la modificarea atribuţiilor privind prelucrarea datelor cu caracter personal, prevăzute în fişa postului.

ART. 11

(1) Dreptul de acces al utilizatorului la sistemul de evidenţă a datelor cu caracter personal se suspendă pe perioada în care acesta se află în una dintre următoarele situaţii:

a) urmează un curs sau o specializare cu scoatere din program, pentru o perioadă mai mare de 3 luni;

b) se află în concediu fără plată, concediu medical, concediu pentru creşterea sau îngrijirea copilului minor, pentru o perioadă mai mare de 3 luni;

c) se află în concediu de maternitate sau concediu pentru incapacitate temporară de muncă;

d) pe perioada cercetării administrative, în situaţia în care faţă de utilizator se efectuează cercetări referitoare la prelucrarea datelor cu caracter personal cu încălcarea dispoziţiilor legale.

e) alte cazuri prevăzute de lege.

(2) La propunerea responsabilului/structurii responsabile cu protecţia datelor cu caracter personal, conducătorul operatorului dispune revocarea contului unic de către administratorul aplicaţiei atunci când utilizatorul se află în una dintre următoarele situaţii:

a) la încetarea raporturilor de muncă/de serviciu;

b) a intervenit o modificare a raporturilor de muncă/de serviciu, iar noile atribuţii nu impun accesul la date cu caracter personal.

ART. 12

(1) La nivelul Oficiului se constituie Registrul de evidenţă a operatorilor din cadrul Ministerului Administraţiei şi Internelor, al cărui model este prevăzut în anexa nr. 2.

(2) La nivelul operatorilor se constituie Registrul de evidenţă a sistemelor de evidenţă a datelor cu caracter personal. Sistemele informatice de la nivelul structurilor/unităţilor MAI care prelucrează date cu caracter personal ţin evidenţa automată a utilizatorilor.

(3) Registrele prevăzute la alin. (1) şi (2) se pot constitui, după caz, şi în format electronic.

ART. 13

(1) Planurile anuale de pregătire continuă la nivelul operatorilor trebuie să conţină teme privind cunoaşterea legislaţiei naţionale şi a acquis-lui comunitar în materia prelucrării datelor cu caracter personal, precum şi teme specifice privind riscurile pe care le comportă prelucrarea datelor şi măsurile minime de securitate, în funcţie de specificul activităţii fiecărui operator.

(2) Pregătirea utilizatorilor se realizează în perioada tutelei profesionale.

(3) Periodic se realizează instructaje cu utilizatorii pentru cunoaşterea procedurilor specifice de lucru instituite la nivelul fiecărui operator.

(4) Instructajele se efectuează în mod obligatoriu la modificarea cadrului legal în materie, iar prelucrarea incidentelor se va realiza cu întregul personal al operatorului.

(5) Utilizatorii trebuie să fie instruiţi periodic cu privire la riscurile generate de vulnerabilităţi şi ameninţări informatice.

CAP. III
Notificarea

ART. 14

(1) Operatorii notifică Autoritatea naţională de supraveghere cu cel puţin 30 de zile calendaristice înainte de efectuarea primei prelucrări, în condiţiile prevăzute de art. 22 din Legea nr. 677/2001, cu modificările şi completările ulterioare.

(2) În situaţia în care operatorul efectuează mai multe categorii de prelucrări, iar acestea nu au acelaşi scop sau scopuri corelate, notificarea prevăzută la alin. (1) se face separat pentru fiecare dintre aceste prelucrări.

(3) Notificarea Autorităţii naţionale de supraveghere se realizează pe baza formularului tipizat al notificărilor prevăzute de Legea nr. 677/2001, cu modificările şi completările ulterioare, aprobat prin Decizia preşedintelui Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 95/2008 privind stabilirea formularului tipizat al notificărilor prevăzute de Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.

(4) Notificarea prelucrării datelor cu caracter personal prin sisteme de evidenţă întocmite în anumite cazuri numai pentru perioada necesară realizării unor activităţi de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice se face cu respectarea regulilor prevăzute la alin.

(1)-(3), numai dacă prelucrarea nu a făcut obiectul unei notificări anterioare.

ART. 15

(1) Structurile şi unităţile MAI cu personalitate juridică care se încadrează în una dintre situaţiile prevăzute la art. 3 alin. (1) şi care prelucrează date cu caracter personal incluse în categoria celor pentru care notificarea este obligatorie conform legii se notifică la Autoritatea naţională de supraveghere prin şeful/conducătorul structurii/unităţii ca reprezentant legal, pentru prelucrările efectuate de operator direct sau prin împuternicit.

(2) Structurile şi unităţile M.A.I. fără personalitate juridică care se încadrează în una dintre situaţiile prevăzute la art. 3 alin. (1) şi care prelucrează date cu caracter personal incluse în categoria celor pentru care notificarea este obligatorie conform legii se notifică la Autoritatea naţională de supraveghere, prin şeful/conducătorul structurii/unităţii ca reprezentant legal, menţionând la denumirea operatorului titulatura structurii MAI care are personalitate juridică şi căreia i se subordonează sau titulatura MAI pentru structurile din aparatul central al ministerului, urmată de titulatura structurii/unităţii MAI interesate.

(3) Notificarea prevăzută la alin. (2) se face numai cu avizul structurii MAI care are personalitate juridică, în subordinea căreia se află structura/unitatea MAI interesată sau, pentru structurile din aparatul central al MAI, numai cu avizul Oficiului.

ART. 16

(1) Notificarea prelucrării datelor cu caracter personal de către structurile/unităţile MAI se efectuează în formă simplificată în situaţiile prevăzute de Decizia preşedintelui Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 91/2006 privind cazurile în care este permisă notificarea simplificată a prelucrării datelor cu caracter personal.

(2) Notificarea prelucrării datelor cu caracter personal de către structurile/unităţile MAI se poate efectua în formă simplificată şi în alte cazuri stabilite prin decizii ale Autorităţii naţionale de supraveghere.

ART. 17

(1) Numărul de înregistrare a notificării comunicat de Autoritatea naţională de supraveghere structurilor/unităţilor MAI se menţionează în orice document prin care se colectează, stochează sau dezvăluie date cu caracter personal.

(2) Începerea operaţiunilor de prelucrare se realizează numai după împlinirea termenului de 5 zile de la data notificării, dacă Autoritatea naţională de supraveghere nu dispune efectuarea unui control prealabil sau după comunicarea rezultatului favorabil al controlului şi emiterea deciziei.

ART. 18

(1) Notificarea nu este necesară în situaţia prevăzută la art. 22 alin. (2) din Legea nr. 677/2001, cu modificările şi completările ulterioare, precum şi în situaţiile prevăzute de Decizia preşedintelui Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 90/2006 privind cazurile în care nu este necesară notificarea prelucrării unor date cu caracter personal şi Decizia preşedintelui Autorităţii Naţionale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 100/2007 privind stabilirea cazurilor în care nu este necesară notificarea prelucrării unor date cu caracter personal.

(2) Notificarea prelucrării datelor cu caracter personal de către structurile/unităţile MAI nu este necesară în alte cazuri prevăzute de lege sau stabilite prin decizii ale Autorităţii naţionale de supraveghere.

ART. 19

(1) Transferul de date cu caracter personal către un alt stat se face, în condiţiile legii, numai după notificarea prealabilă a Autorităţii naţionale de supraveghere.

(2) Notificarea Autorităţii naţionale de supraveghere prevăzută la alin. (1) nu este necesară dacă transferul datelor se face în baza prevederilor unei legi speciale sau ale unui acord internaţional ratificat de România.

CAP. IV
Prelucrarea datelor cu caracter personal

ART. 20

(1) Operatorii şi împuterniciţii acestora prelucrează date cu caracter personal care pot face ulterior obiectul unui sistem de evidenţă, automat sau neautomat, ori care sunt destinate să fie incluse într-un asemenea sistem, în mod distinct, pentru realizarea activităţilor de prevenire, cercetare şi reprimare a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice, pentru scopuri administrative proprii ori pentru scopuri de administraţie publică, după caz, conform specificului activităţii.

(2) Structura/Unitatea MAI care, în calitate de operator, prelucrează date cu caracter personal prin împuterniciţi trebuie să încheie un contract sau, după caz, un document de cooperare cu instituţia ori autoritatea publică sau entitatea de drept privat care prelucrează datele pe seama sa.

(3) Documentul prevăzut la alin. (2) trebuie să conţină obligaţiile împuternicitului de a acţiona doar în baza instrucţiunilor primite de la operator, precum şi de a aplica măsurile tehnice şi organizatorice adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii ori accesului neautorizat, în special dacă prelucrarea respectivă presupune transferul de date on-line, precum şi împotriva oricărei alte forme de prelucrare ilegală.

ART. 21

Prelucrarea datelor cu caracter personal se poate realiza prin mijloace automate sau neautomate în cadrul unor operaţiuni ori seturi de operaţiuni, fără a fi limitate la acestea, după cum urmează:

a) colectarea - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale şi din orice sursă;

b) înregistrarea - consemnarea datelor cu caracter personal într-un sistem de evidenţă automat ori neautomat, care poate fi registru, fişier automat, bază de date sau orice altă formă de evidenţă organizată, structurată ori ad-hoc sau într-un text, înşiruire de date ori document, indiferent de modalitatea în care se înscriu datele;

c) organizarea - ordonarea, structurarea sau sistematizarea datelor cu caracter personal, conform unor criterii prestabilite, potrivit atribuţiilor legale ale operatorului, în scopul eficientizării/optimizării activităţilor de prelucrare a acestora;

d) stocarea - păstrarea pe orice fel de suport a datelor cu caracter personal culese, inclusiv prin efectuarea copiilor de siguranţă;

e) adaptarea - transformarea datelor cu caracter personal colectate iniţial, conform criteriilor prestabilite şi scopurilor pentru care au fost colectate;

f) modificarea - actualizarea, completarea, schimbarea, corectarea ori refacerea datelor cu caracter personal, în scopul menţinerii caracteristicilor de exactitate, realitate, actualitate;

g) extragerea - scoaterea unei părţi din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat şi distinct de prelucrarea iniţială;

h) consultarea - examinarea, vizualizarea, interogarea ori cercetarea datelor cu caracter personal, fără a fi limitate la acestea, în scopul efectuării unei operaţiuni sau set de operaţiuni de prelucrare ulterioară;

i) utilizarea - folosirea datelor cu caracter personal, în tot sau în parte, de către şi în interiorul operatorului, împuterniciţilor operatorului ori destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;

j) dezvăluirea - a face disponibile date cu caracter personal către terţi prin comunicare, transmitere, diseminare sau în orice alt mod;

k) alăturarea - adăugarea, alipirea sau anexarea unor date cu caracter personal la cele deja existente, pe care nu le modifică;

l) combinarea - îmbinarea, unirea sau asamblarea unor date cu caracter personal separate iniţial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;

m) blocarea - întreruperea prelucrării datelor cu caracter personal;

n) ştergerea - eliminarea sau înlăturarea, în tot sau în parte, a datelor cu caracter personal din evidenţe sau înregistrări, prin împlinirea termenului de păstrare, la atingerea scopului pentru care au fost introduse, caducitatea, inexistenţa, inexactitatea;

o) transformarea - operaţiunea efectuată asupra datelor cu caracter personal având ca scop anonimizarea ori utilizarea acestora în scopuri exclusiv statistice;

p) distrugerea - aducerea la stare de neîntrebuinţare, în condiţiile legii, definitivă şi irecuperabilă, prin mijloace mecanice sau termice, a suportului fizic pe care au fost prelucrate date cu caracter personal.

ART. 22

(1) Prelucrarea datelor cu caracter personal se realizează de către operatori şi împuterniciţi ai acestora în exercitarea atribuţiilor expres stabilite printr-un act normativ sau atunci când acesta prevede constituirea unor sisteme de evidenţă la nivel naţional/teritorial, în scopul realizării unor activităţi/servicii de interes public.

(2) Colectarea datelor cu caracter personal se poate face direct de la persoana vizată sau prin surse specifice, care pot fi, dar fără a se limita la: activitatea proprie a operatorului sau a împuterniciţilor acestuia, consultarea directă a unor sisteme de evidenţă a datelor cu caracter personal constituite de alţi operatori ori schimbul de date şi informaţii cu alţi operatori, naţionali sau internaţionali, cu respectarea drepturilor persoanelor vizate şi instituirea unor măsuri adecvate de securitate a prelucrărilor.

(3) Informarea persoanei vizate se realizează în condiţiile şi cu excepţiile prevăzute de lege, cu privire la cel puţin următoarele informaţii:

a) identitatea operatorului, a împuternicitului acestuia şi, dacă este cazul, numărul atribuit de Autoritatea naţională de supraveghere;

b) scopul în care se face prelucrarea datelor cu caracter personal;

c) destinatarii sau categoriile de destinatari ai datelor;

d) dacă furnizarea tuturor datelor cerute este obligatorie şi consecinţele refuzului de a le furniza;

e) existenţa drepturilor persoanei vizate, în special a drepturilor de acces, de intervenţie asupra datelor şi de opoziţie, precum şi condiţiile de exercitare a acestor drepturi;

f) orice alte informaţii a căror furnizare este impusă prin decizii/instrucţiuni ale Autorităţii naţionale de supraveghere, ţinând seama de specificul prelucrării.

(4) Stocarea datelor cu caracter personal se realizează în condiţiile stabilite prin actul normativ care reglementează scopul prelucrării şi potrivit regulilor generale de arhivare a documentelor.

ART. 23

(1) Operatorii şi împuterniciţii acestora prelucrează date cu caracter personal în scopuri de organizare, gestiune economico-financiară şi administrativă privind proprii angajaţi şi membrii de familie ai acestora, în cadrul activităţii de management resurse umane, asigurarea asistenţei medicale sau pentru desfăşurarea unor activităţi cultural-artistice, jurnalistice ori sportive.

(2) Operatorii şi împuterniciţii acestora care prelucrează date cu caracter personal cu ocazia organizării unor concursuri sau examene stabilesc condiţiile concrete de asigurare a securităţii prelucrărilor, precum şi de informare a persoanelor vizate privind drepturile acestora. Datele cu caracter personal astfel prelucrate se şterg sau se distrug după realizarea scopului în care au fost prelucrate. Stocarea acestor date pentru o perioadă mai mare decât cea necesară realizării scopului se poate efectua numai pentru interes statistic, după ce au fost transformate în date anonime.

(3) Supravegherea prin mijloace audio şi/sau video, fixe sau mobile, a unor spaţii publice perimetrale ori adiacente propriilor sedii, precum şi a spaţiilor interioare ale acestora constituie o prelucrare a datelor cu caracter personal doar dacă aceasta este însoţită de un sistem de stocare a datelor care permite identificarea ulterioară, prin orice mijloace, a persoanei vizate. În acest caz este obligatorie avertizarea personalului propriu şi a publicului privind existenţa sistemului de supraveghere, precum şi informarea acestuia privind identitatea operatorului, scopul prelucrării, categoriile de date prelucrate, destinatarii datelor sau alte date suplimentare, după caz, conform legii. Instalarea acestor mijloace se realizează astfel încât, pe cât posibil, să nu fie vizualizat interiorul altor imobile sau căile de acces la acestea, aflate în zona adiacentă echipamentelor de supraveghere.

CAP. V
Dezvăluirea datelor cu caracter personal

ART. 24

(1) Datele cu caracter personal se pot comunica între operatori şi împuterniciţii acestora sau între operatori sau împuterniciţi ai

acestora şi alte instituţii ori organisme publice sau entităţi de drept public sau privat în una dintre următoarele situaţii:

a) dacă persoana vizată şi-a dat consimţământul expres şi neechivoc pentru comunicarea datelor sale;

b) fără consimţământul persoanei vizate în cazurile prevăzute de art. 5 alin. (2) din Legea nr. 677/2001, cu modificările şi completările ulterioare;

c) în cazul prelucrării datelor cu caracter personal în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice, în condiţiile prevăzute de art. 6 din Legea nr. 238/2009.

(2) Comunicarea datelor cu caracter personal în situaţiile prevăzute la alin. (1) se poate face dacă este îndeplinită una dintre următoarele condiţii:

a) comunicarea se efectuează pe baza unui contract sau, după caz, a unui document de cooperare care trebuie să cuprindă cel puţin: numărul de înregistrare a notificării, temeiul legal al prelucrării şi scopul acesteia, termenul maxim de prelucrare, drepturile şi obligaţiile părţilor, modalităţile de asigurare a securităţii prelucrărilor şi de respectare a drepturilor persoanei vizate, precum şi menţiunea că datele pot fi utilizate doar de structura beneficiară şi numai în scopul pentru care au fost solicitate;

b) comunicarea se efectuează în baza unei solicitări scrise, care trebuie să cuprindă temeiul legal, scopul prelucrării şi datele solicitate, precum şi, dacă este cazul, numărul atribuit beneficiarului de Autoritatea naţională de supraveghere.

(3) Comunicarea datelor cu caracter personal de către operatori şi împuterniciţii acestora se poate face şi on-line, cu respectarea dispoziţiilor alin. (1) şi (2) şi asigurarea securităţii sistemelor de comunicaţii a datelor cu caracter personal.

(4) Datele cu caracter personal asupra cărora persoanele vizate au exercitat şi li s-a recunoscut dreptul de opoziţie nu pot face obiectul prelucrării.

(5) Comunicarea de date cu caracter personal se poate efectua şi din oficiu, în condiţiile legii.

ART. 25

(1) Cererile pentru comunicarea datelor cu caracter personal adresate operatorilor şi împuterniciţilor acestora trebuie să conţină datele de identificare a solicitantului, precum şi motivarea şi scopul cererii, conform prevederilor legale sau obligaţiilor cuprinse în tratate la care România este parte.

(2) Cererile care nu conţin elementele prevăzute la alin. (1) se restituie pentru completare, iar cele care nu se încadrează în condiţiile prevăzute de lege sau de tratatele la care România este parte se resping, menţionându-se motivele pentru care comunicarea datelor cu caracter personal nu este posibilă.

(3) Înainte de comunicarea datelor cu caracter personal, operatorii şi împuterniciţii acestora verifică dacă acestea sunt exacte şi, dacă este cazul, actualizate.

(4) În situaţia în care se constată că au fost transmise date incorecte sau neactualizate, operatorii au obligaţia de a informa destinatarii respectivelor date asupra neconformităţii acestora, cu menţionarea datelor care au fost modificate.

(5) La comunicarea datelor cu caracter personal operatorii şi împuterniciţii acestora atenţionează destinatarii asupra interdicţiei de a prelucra datele pentru alte scopuri decât cele specificate în cererea de comunicare.

CAP. VI
Transferul de date cu caracter personal

ART. 26
(1) Datele cu caracter personal gestionate de operatori pot fi transferate către instituţiile competente ale altor state sau organisme de cooperare poliţienească şi judiciară internaţională, în condiţiile legii, fără autorizarea Autorităţii naţionale de supraveghere, numai dacă există o prevedere legală expresă în legislaţia naţională sau comunitară ori într-un tratat ratificat de România.

(2) Operatorii pot transmite date cu caracter personal către instituţiile competente ale altor state sau organisme de cooperare poliţienească şi judiciară din state non-UE numai dacă legislaţia statului în cauză prevede un nivel de protecţie cel puţin egal cu cel oferit de legea română sau organizaţia asigură un nivel adecvat de protecţie pentru prelucrarea datelor, cu respectarea condiţiei prevăzute la art. 29 alin. (3) din Legea nr. 677/2001, cu modificările şi completările ulterioare.

(3) Transmiterea de date cu caracter personal către instituţiile competente ale altor state sau către organisme de cooperare poliţienească şi judiciară din state non-UE a căror legislaţie nu prevede un nivel de protecţie cel puţin egal cu cel oferit de legea română poate fi efectuată numai cu autorizarea Autorităţii naţionale de supraveghere, în condiţiile prevăzute la art. 29 alin. (4) din Legea nr. 677/2001, cu modificările şi completările ulterioare.

(4) În cazul prelucrărilor efectuate în activităţile de prevenire, cercetare şi combatere a infracţiunilor, precum şi de menţinere şi asigurare a ordinii publice, transmiterea de date cu caracter personal către instituţiile prevăzute la alin. (1)-(3) este întotdeauna permisă dacă transferul este necesar pentru prevenirea unui pericol grav şi iminent asupra vieţii, integrităţii corporale sau sănătăţii unei persoane ori a proprietăţii acesteia, precum şi pentru combaterea unei infracţiuni grave prevăzute de lege, cu respectarea legii române.

ART. 27
(1) Transferul de date cu caracter personal către entităţi de drept public sau privat, altele decât cele prevăzute la art. 26, se face în condiţiile legii române şi numai cu autorizarea Autorităţii naţionale de supraveghere.

(2) Autorizarea Autorităţii naţionale de supraveghere prevăzută la alin. (1) nu este necesară în situaţiile în care datele urmează să fie folosite exclusiv în scopuri jurnalistice, literare sau artistice, au fost făcute publice în mod manifest de către persoana vizată sau sunt strâns legate de calitatea de persoană publică a persoanei vizate ori de caracterul public al faptelor în care este implicată.

(3) În cadrul documentului pe baza căruia se realizează transferul datelor cu caracter personal, se menţionează drepturile recunoscute persoanelor vizate, precum şi condiţiile necesare asigurării confidenţialităţii datelor. În acest sens, operatorii avertizează beneficiarii datelor cu caracter personal privind obligativitatea utilizării acestora conform scopurilor specificate în documentele care stau la baza transferului.

(4) Datele cu caracter personal asupra cărora persoanele vizate au exercitat şi li s-a recunoscut dreptul de opoziţie nu pot face obiectul transferului.

(5) Datele cu caracter personal transferate altor organisme publice, entităţi de drept privat sau autorităţi străine nu pot fi folosite pentru alte scopuri decât cele specificate în cererea de comunicare a datelor cu caracter personal.

ART. 28

Transferul datelor cu caracter personal către un alt stat este întotdeauna permis în condiţiile art. 30 din Legea nr. 677/2001, cu modificările şi completările ulterioare, cu notificarea prealabilă a Autorităţii naţionale de supraveghere.

CAP. VII
Măsuri de asigurare a exercitării drepturilor persoanelor vizate

ART. 29

(1) Informarea persoanei vizate se face în condiţiile art. 12 din Legea nr. 677/2001, cu modificările şi completările ulterioare.

(2) Operatorii şi împuterniciţii acestora dispun măsuri pentru existenţa, în spaţiile accesibile publicului, a mijloacelor de informare a persoanelor vizate care să cuprindă drepturile conferite de lege, precum şi a ghidului pentru exercitarea drepturilor de către persoana vizată; ghidul trebuie să conţină detalierea drepturilor persoanei vizate, dar şi modalitatea practică pentru depunerea cererilor de către persoana vizată, structurile responsabile cu analizarea acestora, datele de contact ale acestor structuri şi modalitatea de transmitere a răspunsurilor; ghidul se afişează, după caz, şi pe pagina de internet a operatorului.

(3) Operatorii afişează, după caz, pe pagina de internet formulare-tip de cereri pentru exercitarea drepturilor de către persoana vizată.

(4) Exercitarea drepturilor persoanei vizate poate fi limitată doar în condiţiile prevăzute la art. 16 alin. (1) din Legea nr. 677/2001, cu modificările şi completările ulterioare, sau, respectiv, la art. 11 din Legea nr. 238/2009.

(5) În orice situaţie, persoana vizată trebuie să fie informată cu privire la dreptul de a se adresa Autorităţii naţionale de supraveghere sau instanţei de judecată.

(6) Operatorii ţin evidenţa cazurilor în care, în aplicarea dispoziţiilor art. 16 din Legea nr. 677/2001, cu modificările şi completările ulterioare, a fost limitată exercitarea drepturilor persoanei vizate. Operatorii informează anual Autoritatea naţională de supraveghere cu privire la cazurile apărute şi modul de soluţionare a acestora.

ART. 30

În cadrul procedurilor proprii operatorii stabilesc modalităţile prin care, în exercitarea dreptului de acces la date, la cererea persoanei vizate, comunică informaţiile prevăzute de lege, atunci când prelucrează date cu caracter personal care o privesc pe aceasta. Comunicarea se efectuează în termen de cel mult 15 zile de la data primirii cererii, cu excepţiile prevăzute de lege.

ART. 31

(1) Exercitarea dreptului de acces se face gratuit o singură dată pe an.

(2) Pentru toate celelalte situaţii când drepturile prevăzute de lege nu pot fi exercitate în mod gratuit, structurile/unităţile MAI stabilesc, potrivit art. 5 lit. b), măsuri adecvate pentru asigurarea unui nivel rezonabil al cheltuielilor, în sarcina persoanei vizate.

(3) Cuantumul cheltuielilor se rezumă la acoperirea costurilor suportate de operator.

ART. 32

(1) Dreptul de intervenţie al persoanei vizate se exercită în condiţiile art. 14 din Legea nr. 677/2001, cu modificările şi completările ulterioare.

(2) Persoana vizată se poate adresa operatorului printr-o cerere scrisă, datată şi semnată.

(3) În termen de 15 zile de la primirea cererii, operatorul comunică persoanei vizate măsurile luate, după caz.

ART. 33

(1) În exercitarea dreptului de opoziţie, persoana vizată se poate adresa operatorului, prin cerere motivată, cu respectarea condiţiilor prevăzute de art. 15 alin. (3) din Legea nr. 677/2001, cu modificările şi completările ulterioare.

(2) În termen de 15 zile de la primirea cererii, operatorul comunică persoanei vizate măsurile luate, precum şi terţul căruia i-au fost dezvăluite anterior datele cu caracter personal, după caz, cu respectarea eventualei opţiuni a solicitantului privind comunicarea la o anumită adresă, care poate fi şi de poştă electronică, sau printr-un serviciu de corespondenţă care să asigure că predarea i se va face numai personal.

(3) Dreptul de opoziţie nu poate fi exercitat pentru prelucrările prevăzute de lege.

ART. 34

Orice persoană are dreptul de a nu fi supusă unei decizii individuale de către structurile/unităţile MAI şi de a se adresa Autorităţii naţionale de supraveghere sau justiţiei, potrivit legii.

ART. 35

(1) Operatorul informează persoana vizată asupra procedurii de primire a cererilor, prin afişare la sediu, publicare pe pagina WEB sau prin alte mijloace.

(2) În cazul cererilor transmise fără a fi îndeplinite condiţiile prevăzute de lege, solicitantul va fi informat în scris cu privire la condiţiile de exercitare a drepturilor prevăzute de Legea nr. 677/2001, cu modificările şi completările ulterioare.

(3) Odată cu soluţionarea cererii, se aduce la cunoştinţa persoanelor vizate că au dreptul de a se adresa Autorităţii naţionale de supraveghere sau justiţiei pentru apărarea drepturilor garantate de lege.

TITLUL II
Măsuri tehnice

CAP. I
Utilizatorii datelor cu caracter personal

ART. 36

(1) Pentru fiecare utilizator, administratorul aplicaţiei stabileşte un cont unic care să permită atât identificarea, cât şi configurarea categoriilor de prelucrări la care are dreptul, asigurând totodată şi jurnalizarea operaţiunilor efectuate.

(2) Identificarea în sistem a utilizatorului se poate realiza prin:

a) introducerea unui cod de identificare de la tastatură - user name -, însoţită de introducerea unei parole;

b) folosirea unei cartele inteligente - smart card - sau a unei cartele magnetice;

c) mijloace biometrice: amprenta dactiloscopică, amprenta vocală, angiografia retiniană sau prin alte mijloace;

d) certificat digital pe suport extern de memorie, token.

(3) Operatorii stabilesc modalitatea concretă de identificare şi autentificare folosită, în funcţie de importanţa datelor cu caracter personal deţinute, volumul acestora, numărul de utilizatori, frecvenţa interogărilor şi operaţiunile de prelucrare, precum şi măsurile de protecţie fizică a locaţiei.

(4) Codurile de identificare, parolele sau cartelele sunt unice, personale şi netransmisibile. Se interzice folosirea lor în comun de către mai mulţi utilizatori.

(5) Parolele trebuie să aibă minimum 6 caractere alfanumerice - cifre şi litere -, iar introducerea acestora nu trebuie să fie afişată în clar pe ecran.

(6) Parolele se schimbă ori de câte ori este nevoie, dar cel puţin o dată la 3 luni pentru utilizatori şi la 6 luni pentru administratorii aplicaţiei.

(7) La generarea contului unic utilizatorul primeşte în scris parola şi codul de identificare. Utilizatorul are obligaţia să schimbe parola în următoarele situaţii:

a) la prima accesare a contului unic;

b) în cazurile prevăzute de alin. (6);

c) ori de câte ori apreciază ca fiind necesar pentru asigurarea securităţii prelucrării datelor cu caracter personal.

(8) Administratorul sistemului de evidenţă a datelor cu caracter personal ia măsurile necesare pentru activarea unui mesaj de avertizare după a treia introducere greşită a parolei şi blocarea contului la a cincea introducere greşită. Mesajul pentru utilizator va cuprinde următorul text: "Atenţie, aţi introdus greşit parola de 3 ori. La a 5-a introducere greşită, contul va fi blocat. Vă rugăm să reverificaţi codul şi parola." După cea de-a cincea introducere greşită a parolei, pe ecran va fi afişat următorul mesaj: "Atenţie! Contul este blocat. Vă rugăm să contactaţi administratorul aplicaţiei."

ART. 37

(1) Cartela de acces sau tokenul în timpul programului de lucru se păstrează permanent asupra utilizatorului. În afara programului de lucru, cartela de acces sau tokenul se păstrează în fişet/casetă metalic/metalică încuiat/încuiată şi sigilat/sigilată la care are acces numai utilizatorul acesteia.

(2) Se interzice transcrierea/păstrarea parolei, respectiv a cartelei sau tokenului, la vedere sau în alt mod decât cel prevăzut mai sus ori diseminarea/transmiterea acestora către alte persoane.

(3) Documentele care conţin coduri de identificare şi parole de acces vor fi arhivate numai dacă acestea nu se mai află în uz.

(4) Conducătorul operatorului dispune măsuri astfel încât conturile de utilizator să fie suspendate sau revocate imediat pentru personalul aflat în situaţiile prevăzute la art. 11.

(5) Utilizatorul aflat în una dintre situaţiile prevăzute la art. 11 are obligaţia de a preda cartela de acces responsabilului/structurii responsabile cu protecţia datelor cu caracter personal.

(6) După încetarea situaţiilor prevăzute la art. 10, operatorul dispune reactivarea contului de utilizator.

(7) Aplicaţia de gestiune a bazelor de date trebuie configurată astfel încât să asigure dezactivarea automată a codurilor de identificare şi a cartelelor care nu au fost folosite o perioadă de

până la 6 luni; acestea sunt menţinute în istoricul de utilizatori, după caz, de către administratorul aplicaţiei.

(8) La apariţia unei situaţii de modificare a competenţelor sau raporturilor de serviciu, operatorii stabilesc modalităţi concrete de revocare/suspendare a conturilor de acces, astfel încât prelucrarea datelor cu caracter personal să se facă numai de către personalul autorizat şi numai în exercitarea atribuţiilor de serviciu ale acestora.

(9) Revocarea/Suspendarea conturilor de acces se va face numai de către administratorul aplicaţiei.

(10) Fiecare operator permite accesul utilizatorilor la sisteme de evidenţă a datelor cu caracter personal neautomate numai pe baza unei liste nominale aprobate de conducătorul/şeful acestuia.

(11) Elaborarea şi actualizarea listei se asigură de către responsabilul/structura responsabilă cu protecţia datelor cu caracter personal, în baza comunicărilor făcute pe linie de resurse umane.

(12) Pentru accesul personalului la sistemele de evidenţă a datelor cu caracter personal deţinute de alţi operatori, conturile de utilizator se vor obţine în baza solicitării scrise şi motivate a structurii/unităţii interesate sau pe baza unor protocoale încheiate în acest sens.

ART. 38

(1) Conducătorul operatorului stabileşte fiecărui utilizator tipurile de acces şi operaţiunile permise acestuia, strict necesare pentru îndeplinirea atribuţiilor de serviciu.

(2) Cu ocazia proiectării, întreţinerii, actualizării aplicaţiilor de gestiune a bazelor de date, se interzice accesul programatorilor/personalului de întreţinere a sistemelor informatice la orice fel de date cu caracter personal deţinute/create/accesate de personalul din structura/unitatea respectivă. În aceste situaţii, se pun la dispoziţia programatorilor/personalului de întreţinere numai date anonime.

(3) Pentru cazuri excepţionale, numai pe durata intervenţiei şi circumstanţiat limitativ la datele strict necesare, persoanele care asigură suportul tehnic pot avea acces la datele cu caracter personal numai în prezenţa unui utilizator desemnat de operator. În această situaţie, răspunderea pentru păstrarea confidenţialităţii datelor aparţine persoanelor în cauză, sens în care trebuie să semneze un angajament de confidenţialitate.

(4) Conducătorii operatorului desemnează utilizatorii care au ca atribuţii de serviciu ştergerea sau distrugerea datelor cu caracter personal.

ART. 39

(1) În cadrul operatorului sau al împuterniciţilor acestuia, operaţiunile de colectare, introducere, modificare şi actualizare a datelor cu caracter personal se fac numai de personalul anume desemnat de către conducătorii acestora.

(2) Conducătorii operatorilor sau ai împuterniciţilor acestora dispun măsurile necesare care să permită identificarea utilizatorului care a introdus, modificat sau actualizat datele, precum şi a datei şi orei efectuării operaţiunilor. Datele şterse sau modificate vor fi păstrate separat o perioadă de timp stabilită de operator, după care se distrug sau se şterg.

ART. 40

(1) Bazele de date cu caracter personal deţinute/create şi programele folosite de operatori sau de împuterniciţii acestora sunt salvate, prin copii de siguranţă, la un interval de timp stabilit de

conducătorii operatorului sau ai împuterniciților acestuia, în funcție de mărimea, volumul și importanța acestor baze de date, care nu poate depăși 6 luni. Operatorii și împuterniciții acestora țin evidența copiilor de siguranță.

(2) Conducătorii operatorului sau ai împuterniciților acestuia desemnează utilizatori care trebuie să aibă ca atribuție de serviciu și executarea copiilor de siguranță ale bazelor de date deținute/create și ale programelor folosite.

(3) Conducătorii operatorului sau ai împuterniciților acestuia dispun măsurile necesare pentru stocarea copiilor de siguranță în camere special amenajate sau în fișete metalice, sigilate. Accesul în încăperea special amenajată se acordă numai personalului anume desemnat și se consemnează într-un registru special. În exercitarea atribuțiilor legale, Autoritatea națională de supraveghere are acces la copiile de siguranță.

(4) Conducătorii operatorilor sau ai împuterniciților acestuia pot institui măsuri suplimentare de siguranță, precum sisteme de monitorizare video, atât pentru accesul în încăpere, cât și pentru operațiunile derulate cu această ocazie, după caz.

ART. 41

(1) Accesul în încăperile în care se află echipamente care prelucrează date cu caracter personal este strict limitat la utilizatorii desemnați de conducătorii operatorului sau ai împuterniciților acestuia și numai pentru îndeplinirea atribuțiilor de serviciu.

(2) În cazul în care nu se poate restricționa accesul în aceste încăperi, echipamentele se securizează cu chei sau cartele magnetice.

(3) Aplicațiile informatice care gestionează date cu caracter personal trebuie prevăzute cu facilitatea închiderii automate a sesiunii de lucru dacă utilizatorul nu acționează asupra datelor afișate pe ecran o perioadă de timp de până la 5 minute, stabilită în funcție de operațiile care trebuie executate.

(4) Terminalele de acces folosite în relația cu publicul se poziționează astfel încât datele afișate să fie vizualizate numai de utilizatori. Aceste terminale de acces trebuie să aibă setată funcția "screen saver" la o temporizare de maximum 5 minute, iar dacă acest lucru nu este posibil din punct de vedere tehnic, după trecerea intervalului de timp menționat, datele afișate trebuie ascunse.

ART. 42

(1) Pentru prelucrările efectuate în sistemele de evidență automate, aplicația trebuie să înregistreze orice accesare într-un fișier de acces, denumit în continuare log. Stocarea acestor informații se face într-un fișier de acces general sau în fișiere separate pentru fiecare utilizator, după caz.

(2) Informațiile înregistrate în log vor fi:

a) codul de identificare a utilizatorului și a stației de lucru folosite;

b) numele fișierului accesat;

c) numărul înregistrărilor efectuate;

d) tipul de acces;

e) motivul prelucrării datelor cu caracter personal care trebuie să permită identificarea documentului/situației concrete care a stat la baza și a justificat prelucrarea datelor;

f) codul operației executate sau programul folosit;

g) data accesului - an, lună, zi;

h) timpul - ora, minutul, secunda.

(3) Aplicaţia înregistrează orice încercare de acces neautorizat, iar responsabilul/structura responsabilă cu protecţia datelor cu caracter personal are obligaţia de a verifica împrejurările producerii acesteia, luând măsurile ce se impun.

(4) Logurile se păstrează cel puţin 2 ani, în funcţie de necesitatea asigurării disponibilităţii datelor pentru operator, corelat cu importanţa şi volumul de date stocate. La acoperirea capacităţii de stocare, logurile vor fi transferate şi păstrate pe suport amovibil în condiţiile prevăzute pentru copiile de siguranţă.

(5) Pentru ţinerea evidenţei operaţiunilor de consultare a datelor cu caracter personal conţinute în sisteme de evidenţă neautomate-manuale, operatorul sau împuterniciţii acestuia instituie Registrul de consultare/multiplicare a documentelor din sistemul de evidenţă, conform modelului prevăzut în anexa nr. 3.

(6) Declanşarea unei investigaţii a cărei finalizare depăşeşte termenul stabilit de operator, conform alin. (5), atrage prelungirea perioadei de păstrare.

(7) Logurile pot fi accesate, respectiv consultate.

(8) Se interzice orice prelucrare de date cu caracter personal care nu este motivată strict de îndeplinirea unei atribuţii de serviciu a utilizatorului.

ART. 43

(1) Conducătorii operatorului sau ai împuterniciţilor acestuia care prelucrează date cu caracter personal dispun luarea măsurilor tehnice adecvate pentru identificarea eventualelor disfuncţionalităţi în ceea ce priveşte funcţionarea sistemelor de comunicaţii.

(2) Responsabilul/Structura responsabilă cu protecţia datelor cu caracter personal efectuează periodic, prin sondaj, controlul autentificărilor şi tipurilor de acces, precum şi respectarea măsurilor de securitate specifice sistemelor de comunicaţii folosite pentru transmiterea acestor date.

(3) Rezultatul controlului, eventualele disfuncţionalităţi identificate, precum şi măsurile de remediere a acestora se consemnează într-un raport care se supune aprobării conducătorului/şefului structurii/unităţii respective.

(4) Conducătorii operatorului sau ai împuterniciţilor acestuia dispun măsurile necesare de securitate a sistemului de comunicaţii pentru înlăturarea posibilităţii de diseminare neautorizată sau interceptare a transmisiilor de date. În acest scop se poate folosi inclusiv transmisia criptată a datelor cu caracter personal.

(5) Folosirea sistemelor de comunicaţii pentru transmiterea datelor cu caracter personal se realizează numai dacă prin această metodă se asigură gradul de operativitate impus de specificul activităţii desfăşurate de structurile implicate.

ART. 44

(1) Conducătorii operatorului sau ai împuterniciţilor acestuia dispun măsurile necesare în vederea instituirii şi menţinerii unui nivel suficient de securitate a prelucrării datelor cu caracter personal, care vor consta cel puţin în:

a) interzicerea instalării de către personalul MAI a altor programe software în afara celor configurate de personalul autorizat, pentru îndeplinirea atribuţiilor de serviciu;

b) configurarea porturilor de acces la mediile de stocare pentru fiecare staţie de lucru şi a comenzilor care permit salvarea sau listarea documentelor, în mod adecvat, pentru categoriile de operaţiuni efectuate de fiecare utilizator, în strictă legătură cu îndeplinirea atribuţiilor de serviciu ale acestuia;

c) implementarea unor aplicaţii automate de contracarare a vulnerabilităţilor şi ameninţărilor informatice şi de securitate a sistemelor informatice.

(2) În timpul activităţii, monitoarele de lucru trebuie să afişeze mesaje de avertizare privind obligativitatea păstrării confidenţialităţii datelor cu caracter personal prelucrate.

ART. 45

(1) Conducătorii operatorului sau ai împuterniciţilor acestuia desemnează utilizatorii cu drept de imprimare a extraselor din sistemele de evidenţă a datelor cu caracter personal sau a altor documente care includ astfel de date, inclusiv de multiplicare, în strictă corelare cu îndeplinirea atribuţiilor de serviciu ale acestora.

(2) Toate documentele care conţin date cu caracter personal se înregistrează şi urmează regulile de păstrare, procesare, multiplicare, transport, transmitere, distrugere şi arhivare stabilite prin acte normative interne.

(3) Documentele elaborate de structurile/unităţile MAI, care conţin date cu caracter personal, se marchează după cum urmează:

a) în cadrul documentului se menţionează numărul atribuit notificării de către Autoritatea naţională de supraveghere;

b) în subsolul fiecărei pagini, cu excepţia documentelor clasificate, se inserează următorul text: "Document care conţine date cu caracter personal protejate de prevederile Legii nr. 677/2001!".

(4) Marcajul prevăzut la alin. (3) lit. b) este obligatoriu inclusiv în cazul prelucrărilor de date cu caracter personal în situaţii pentru care, potrivit legii, notificarea nu este necesară.

ART. 46

Procedurile proprii elaborate de operatori trebuie să cuprindă:

a) modalităţi de administrare a conturilor de utilizator;

b) modalităţi de control al accesului în zonele în care se prelucrează date cu caracter personal;

c) modalităţi de asigurare a confidenţialităţii, integrităţii şi disponibilităţii datelor cu caracter personal;

d) modalităţi privind securitatea transmisiilor de date şi accesul securizat la aceste mijloace de transmitere a datelor.

CAP. II
Dispoziţii finale

ART. 47

(1) Structurile/Unităţile MAI care procesează date cu caracter personal au obligaţia să transmită Oficiului, anual, până la 31 decembrie, o analiză cu privire la activitatea desfăşurată în domeniul prelucrării datelor cu caracter personal.

(2) Structurile/Unităţile MAI care procesează date cu caracter personal trebuie să pună la dispoziţia Oficiului, în condiţiile legii, informaţiile, documentele sau actele pe care le deţin pentru îndeplinirea atribuţiilor ce îi revin în domeniul protecţiei datelor cu caracter personal.

ART. 48

Prezentele instrucţiuni sunt aplicabile unităţilor aparatului central al MAI şi unităţilor, instituţiilor şi structurilor aflate în subordinea ministerului, în conformitate cu statutul şi relaţia acestora cu ministerul, stabilite prin dispoziţii legale şi în măsura în care nu contravin acestora.

ART. 49

Nerespectarea dispoziţiilor prezentelor instrucţiuni atrage, potrivit legii, răspunderea disciplinară, civilă, materială sau penală, după caz.

ART. 50

(1) Prezentele instrucţiuni intră în vigoare în termen de 90 de zile de la data publicării în Monitorul Oficial al României, Partea I.

(2) Procedurile proprii prevăzute la art. 5 lit. d) şi ghidul pentru exercitarea drepturilor de către persoana vizată prevăzut la art. 29 alin. (2) se elaborează în termen de 90 de zile de la intrarea în vigoare a prezentelor instrucţiuni.

(3) Anexele nr. 1-3 fac parte integrantă din prezentele instrucţiuni.

Ministrul administraţiei
şi internelor,
Vasile Blaga

Bucureşti, 3 februarie 2010.
Nr. 27.

ANEXA 1

DECLARAȚIE

Subsemnatul/Subsemnata, ..., născut(ă) în localitatea ....., la data de ....., fiul (fiica) lui ..... și al(a) ....., angajat/angajată al(a) ....., în funcția de ....., cu domiciliul în ....., declar pe propria răspundere că am luat cunoștință de prevederile legale referitoare la protecția datelor cu caracter personal și consimt să păstrez confidențialitatea datelor cu caracter personal a căror prelucrare o efectuez în condițiile legii, în virtutea atribuțiilor de serviciu, inclusiv după încetarea activităților de prelucrare a acestor date.

Cunosc faptul că încălcarea normelor legale privind protecția datelor cu caracter personal atrage răspunderea administrativă, disciplinară, materială, civilă ori penală, în raport cu gravitatea faptei, potrivit legii.

Data .....

Semnătura .....

Dată în prezența

.....

(numele și prenumele responsabilului/persoanei din structura responsabilă cu protecția datelor personale)

.....

ANEXA 2

REGISTRUL DE EVIDENȚĂ

a operatorilor din cadrul Ministerului Administrației și Internelor

Nr. crt.	Denumirea structurii/ unității MAI	Responsabilul/ Șeful compartimentului (date de contact)	Denumirea sistemului de evidență	Data și numărul de înregistrare a notificării	Scopul prelucrării/ Baza legală	Sursa de colectare	Operațiunile de prelucrare care se efectuează	Tipul de evidență utilizat (automat/ neautomat)	Nr. și data procedurii proprii	Obs

ANEXA 3

REGISTRUL DE CONSULTARE/MULTIPLICARE
a documentelor din ....., deţinut de .....denumirea sistemului (serviciu/birou etc.) de evidenţă)

Nr. crt.	Emitentul şi numărul de înregistrare a cererii de consultare/multiplicare	Data şi ora consultării	Şeful/Conducătorul structurii/unităţii care a aprobat consultarea/multiplicarea	Gradul, numele şi prenumele persoanei care consultă	Denumirea documentului consultat/nr. file	Semnătura de primire a documentului consultat	Semnătura de restituire	Denumirea documentului multiplicat/nr. file	Nr. adresei prin care a fost expediat documentul multiplicat	Obs.