

## **INSTRUCTIUNI nr. 27 din 3 februarie 2010**

privind masurile de natura organizatorica si tehnica pentru asigurarea securitatii prelucrarilor de date cu caracter personal efectuate de catre structurile/unitatile Ministerului Administratiei si Internelor

**EMITENT:** MINISTERUL ADMINISTRATIEI SI INTERNELOR

**PUBLICAT ÎN:** MONITORUL OFICIAL nr. 98 din 12 februarie 2010

Având în vedere dispozițiile [Legii nr. 677/2001](#) pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare, ale [Legii nr. 238/2009](#) privind reglementarea prelucrării datelor cu caracter personal de către structurile/unitățile Ministerului Administrației și Internelor în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, ținând cont de faptul că dispozițiile [Legii nr. 238/2009](#) și, în consecință, dispozițiile corespunzătoare cuprinse în prezentul act normativ se aplică exclusiv în cazul prelucrărilor de date cu caracter personal efectuate în cursul activităților de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, în temeiul [art. 7 alin. \(4\) din Ordonanța de urgență a Guvernului nr. 30/2007](#) privind organizarea și funcționarea Ministerului Administrației și Internelor, aprobată cu modificări prin [Legea nr. 15/2008](#), cu modificările și completările ulterioare,

ministrul administrației și internelor emite următoarele instrucțiuni:

### TITLULUL I

#### Măsuri organizatorice

#### CAP. I

##### Dispoziții generale

#### ART. 1

Prezentele instrucțiuni se aplică activităților de prelucrare a datelor cu caracter personal efectuate de structurile și unitățile Ministerului Administrației și Internelor, denumit în continuare MAI, în calitatea acestora de operatori sau împuterniciți ai operatorilor.

#### ART. 2

(1) La nivelul MAI, prelucrarea datelor cu caracter personal se realizează cu respectarea regulilor generale și speciale prevăzute de [Legea nr. 677/2001](#) pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare, de [Legea nr. 238/2009](#) privind reglementarea prelucrării datelor cu caracter personal de către structurile/unitățile Ministerului Administrației și Internelor în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, a prevederilor deciziilor și instrucțiunilor cu caracter

normativ emise de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare Autoritatea națională de supraveghere, a prevederilor prezentelor instrucțiuni și a procedurilor proprii elaborate de operatori potrivit legii.

(2) Operatorii și împuterniciții acestora utilizează sisteme de evidență și/sau mijloace automate și neautomate de prelucrare a datelor cu caracter personal cu aplicarea principiilor respectării drepturilor omului, legalității, necesității, confidențialității și proporționalității și numai dacă, prin utilizarea acestora, este asigurată protecția datelor prelucrate.

(3) În cadrul activității de prelucrare a datelor cu caracter personal, operatorii și împuterniciții acestora se supun activităților de control prealabil sau de investigare efectuate de Autoritatea națională de supraveghere și, la cerere, acordă acesteia sprijin deplin pentru exercitarea atribuțiilor sale.

#### ART. 3

(1) Au calitatea de operator structurile și unitățile MAI, precum și MAI, dacă:

- a) stabilesc scopul și mijloacele de prelucrare a datelor cu caracter personal; sau
- b) scopul și 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 împuterniciți 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 atribuții de serviciu presupun operațiuni de prelucrare a datelor cu caracter personal.

#### CAP. II

Organizarea activității de prelucrare a datelor cu caracter personal în MAI

#### ART. 4

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

(2) Prin derogare de la prevederile alin. (1), pentru structurile/unitățile 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 protecția datelor cu caracter personal, în directă subordonare a conducătorului operatorului. Personalul care urmează să ocupe o astfel de funcție trebuie să aibă cunoștințe IT.

#### ART. 5

Structurile/unitățile MAI, în calitate de operator, au în principal următoarele obligații:

- a) să notifice Autoritatea națională de supraveghere potrivit [art. 22 din](#)

[Legea nr. 677/2001](#), cu modificările și completările ulterioare;

b) să asigure informarea persoanelor vizate și 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 protecție a persoanelor cu privire la prelucrarea datelor cu caracter personal, denumite în continuare proceduri proprii, conform legislației și normelor interne în domeniul standardizării în vigoare la nivelul MAI;

e) să întocmească și să transmită, anual, Autorității naționale de supraveghere raportul de activitate privind protecția persoanelor în privința prelucrării datelor cu caracter personal;

f) să pună la dispoziția Oficiului Responsabilului cu Protecția Datelor Personale, denumit în continuare Oficiu, în condițiile legii, prin intermediul structurii responsabile/responsabilului cu protecția datelor cu caracter personal și la solicitarea reprezentanților acestuia, informațiile și documentele în legătură cu prelucrarea datelor cu caracter personal pe care le dețin, în vederea exercitării atribuțiilor de coordonare, îndrumare și monitorizare a aplicării unitare a legislației în domeniul protecției persoanelor cu privire la prelucrarea datelor cu caracter personal.

#### ART. 6

(1) Conducătorii operatorului au următoarele atribuții principale:

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

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

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

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

e) asigură desfășurarea pregătirii de specialitate și instruirea utilizatorilor în acest domeniu;

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

g) analizează și dispun în ceea ce privește suspendarea sau revocarea dreptului de acces al utilizatorilor la sisteme de evidență a datelor cu caracter personal, în condițiile legii;

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

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

(2) Conducătorii împuterniciților operatorului au atribuțiile prevăzute la alin. (1) lit. b), d)-g) și i); în cazul în care este incidentă una dintre situațiile prevăzute la alin. (1) lit. h), conducătorii împuterniciților au

obligatia de a informa operatorul.

#### ART. 7

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

a) coordonează elaborarea și 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 și sprijină instruirea personalului care prelucrează date cu caracter personal referitoare la normele și regulile de protecție a datelor cu caracter personal;

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

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

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

g) asigură relaționarea, solicită asistență de specialitate și participă la convocările și activitățile organizate de Oficiu în domeniul prelucrării datelor cu caracter personal;

h) coordonează soluționarea cererilor persoanelor vizate;

i) ține evidența cererilor persoanelor vizate.

(2) Atribuțiile specifice responsabilului/personalului din cadrul structurii responsabile cu protecția datelor cu caracter personal se stabilesc prin fișa postului.

#### ART. 8

(1) Utilizatorii au următoarele obligații specifice:

a) să cunoască și să aplice prevederile actelor normative din domeniul prelucrării datelor cu caracter personal, precum și 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 condițiile 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 și consecințele refuzului de a le pune la dispoziție, drepturile prevăzute de lege, în special drepturile de acces, de intervenție asupra datelor și de opoziție, condițiile în care pot fi exercitate aceste drepturi, respectiv să ofere orice alte informații a căror furnizare este impusă prin dispoziții ale Autorității naționale de supraveghere, ținând seama de specificul prelucrării;

c) să prelucereze numai datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin responsabilului/structurii responsabile cu protecția datelor cu caracter personal pentru realizarea activităților specifice ale acestuia/acesteia;

d) să păstreze confidențialitatea datelor prelucrate, a contului de utilizator, a parolei/codului de acces la sistemele informatice/baze de date prin care sunt gestionate date cu caracter personal;

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

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

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

#### ART. 9

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

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

(3) Operatorii pot permite, în condițiile legii, prelucrarea datelor cu caracter personal de către funcționarii unui alt operator din afara ori din cadrul MAI, pe perioada necesară îndeplinirii unor atribuții 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 condițiile de securitate stabilite de către operatorul care gestionează sau administrează sistemul de evidență a datelor cu caracter personal.

#### ART. 10

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

a) la modificarea raporturilor de muncă;

b) la modificarea atribuțiilor privind prelucrarea datelor cu caracter personal, prevăzute în fișa postului.

#### ART. 11

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

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 creșterea 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 situația în care față de

utilizator se efectuează cercetări referitoare la prelucrarea datelor cu caracter personal cu încălcarea dispozițiilor legale.

e) alte cazuri prevăzute de lege.

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

a) la încetarea raporturilor de muncă/de serviciu;

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

#### ART. 12

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

(2) La nivelul operatorilor se constituie Registrul de evidență a sistemelor de evidență a datelor cu caracter personal. Sistemele informatice de la nivelul structurilor/unităților MAI care prelucrează date cu caracter personal țin evidența automată a utilizatorilor.

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

#### ART. 13

(1) Planurile anuale de pregătire continuă la nivelul operatorilor trebuie să conțină teme privind cunoașterea legislației naționale și a acquis-ului comunitar în materia prelucrării datelor cu caracter personal, precum și teme specifice privind riscurile pe care le comportă prelucrarea datelor și măsurile minime de securitate, în funcție de specificul activității fiecărui operator.

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

(3) Periodic se realizează instructaje cu utilizatorii pentru cunoașterea 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 instruiți periodic cu privire la riscurile generate de vulnerabilități și amenințări informatice.

### CAP. III

#### Notificarea

#### ART. 14

(1) Operatorii notifică Autoritatea națională de supraveghere cu cel puțin 30 de zile calendaristice înainte de efectuarea primei prelucrări, în condițiile prevăzute de [art. 22 din Legea nr. 677/2001](#), cu modificările și completările ulterioare.

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

(3) Notificarea Autorității naționale de supraveghere se realizează pe baza formularului tipizat al notificărilor prevăzute de [Legea nr. 677/2001](#),



cu modificările și completările ulterioare, aprobat prin Decizia președintelui Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal nr. 95/2008 privind stabilirea formularului tipizat al notificărilor prevăzute de [Legea nr. 677/2001](#) pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date.

(4) Notificarea prelucrării datelor cu caracter personal prin sisteme de evidență întocmite în anumite cazuri numai pentru perioada necesară realizării unor activități de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și 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 și unitățile MAI cu personalitate juridică care se încadrează în una dintre situațiile prevăzute la art. 3 alin. (1) și care prelucrează date cu caracter personal incluse în categoria celor pentru care notificarea este obligatorie conform legii se notifică la Autoritatea națională de supraveghere prin șeful/conducătorul structurii/unității ca reprezentant legal, pentru prelucrările efectuate de operator direct sau prin împuternicit.

(2) Structurile și unitățile M.A.I. fără personalitate juridică care se încadrează în una dintre situațiile prevăzute la art. 3 alin. (1) și care prelucrează date cu caracter personal incluse în categoria celor pentru care notificarea este obligatorie conform legii se notifică la Autoritatea națională de supraveghere, prin șeful/conducătorul structurii/unității ca reprezentant legal, menționând la denumirea operatorului titulatura structurii MAI care are personalitate juridică și căreia i se subordonează sau titulatura MAI pentru structurile din aparatul central al ministerului, urmată de titulatura structurii/unității 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/unitățile MAI se efectuează în formă simplificată în situațiile prevăzute de Decizia președintelui Autorității Naționale 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/unitățile MAI se poate efectua în formă simplificată și în alte cazuri stabilite prin decizii ale Autorității naționale de supraveghere.

#### ART. 17

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

(2) Începerea operațiunilor de prelucrare se realizează numai după împlinirea termenului de 5 zile de la data notificării, dacă Autoritatea națională de supraveghere nu dispune efectuarea unui control prealabil sau

după comunicarea rezultatului favorabil al controlului și emiterea deciziei.

#### ART. 18

(1) Notificarea nu este necesară în situația prevăzută la [art. 22 alin. \(2\) din Legea nr. 677/2001](#), cu modificările și completările ulterioare, precum și în situațiile prevăzute de Decizia președintelui Autorității Naționale 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 și Decizia președintelui Autorității Naționale 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/unitățile MAI nu este necesară în alte cazuri prevăzute de lege sau stabilite prin decizii ale Autorității naționale de supraveghere.

#### ART. 19

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

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

### CAP. IV

#### Prelucrarea datelor cu caracter personal

#### ART. 20

(1) Operatorii și împuterniciții acestora prelucrează date cu caracter personal care pot face ulterior obiectul unui sistem de evidență, automat sau neautomat, ori care sunt destinate să fie incluse într-un asemenea sistem, în mod distinct, pentru realizarea activităților de prevenire, cercetare și reprimare a infracțiunilor, precum și de menținere și asigurare a ordinii publice, pentru scopuri administrative proprii ori pentru scopuri de administrație publică, după caz, conform specificului activității.

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

(3) Documentul prevăzut la alin. (2) trebuie să conțină obligațiile împuternicitului de a acționa doar în baza instrucțiunilor primite de la operator, precum și de a aplica măsurile tehnice și 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 și 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 operațiuni ori seturi de operațiuni, fără a fi limitate la acestea, după cum urmează:

- a) colectarea - strângerea, adunarea ori primirea datelor cu caracter personal prin orice mijloace legale și din orice sursă;
- b) înregistrarea - consemnarea datelor cu caracter personal într-un



sistem de evidență automat ori neautomat, care poate fi registru, fișier automat, bază de date sau orice altă formă de evidență organizată, structurată ori ad-hoc sau într-un text, înșiruire 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 atribuțiilor legale ale operatorului, în scopul eficientizării/optimizării activităților de prelucrare a acestora;

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

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

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

g) extragerea - scoaterea unei părți din categoria specifică de date cu caracter personal, în scopul utilizării acesteia, separat și distinct de prelucrarea inițială;

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

i) utilizarea - folosirea datelor cu caracter personal, în tot sau în parte, de către și în interiorul operatorului, împuterniciților 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 terți 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 inițial, într-o formă nouă, pe baza unor criterii prestabilite, pentru scopuri anume determinate;

m) blocarea - întreruperea prelucrării datelor cu caracter personal;

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

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

p) distrugerea - aducerea la stare de neîntrebuințare, în condițiile legii, definitivă și 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 și împuterniciți ai acestora în exercitarea atribuțiilor expres stabilite printr-un act normativ sau atunci când acesta prevede constituirea unor sisteme de evidență la nivel național/teritorial, în scopul realizării unor activități/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 împuterniciților acestuia, consultarea directă a unor sisteme de evidență a datelor cu caracter personal constituite de alți operatori ori schimbul de date și informații cu alți operatori, naționali sau internaționali, cu respectarea drepturilor persoanelor vizate și instituirea unor măsuri adecvate de securitate a prelucrărilor.

(3) Informarea persoanei vizate se realizează în condițiile și cu excepțiile prevăzute de lege, cu privire la cel puțin următoarele informații:

- a) identitatea operatorului, a împuternicitului acestuia și, dacă este cazul, numărul atribuit de Autoritatea națională 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 și consecințele refuzului de a le furniza;
- e) existența drepturilor persoanei vizate, în special a drepturilor de acces, de intervenție asupra datelor și de opoziție, precum și condițiile de exercitare a acestor drepturi;
- f) orice alte informații a căror furnizare este impusă prin decizii/instrucțiuni ale Autorității naționale de supraveghere, ținând seama de specificul prelucrării.

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

#### ART. 23

(1) Operatorii și împuterniciții acestora prelucrează date cu caracter personal în scopuri de organizare, gestiune economico-financiară și administrativă privind proprii angajați și membrii de familie ai acestora, în cadrul activității de management resurse umane, asigurarea asistenței medicale sau pentru desfășurarea unor activități cultural-artistice, jurnalistice ori sportive.

(2) Operatorii și împuterniciții acestora care prelucrează date cu caracter personal cu ocazia organizării unor concursuri sau examene stabilesc condițiile concrete de asigurare a securității prelucrărilor, precum și de informare a persoanelor vizate privind drepturile acestora. Datele cu caracter personal astfel prelucrate se șterg 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 și/sau video, fixe sau mobile, a unor spații publice perimetrice ori adiacente propriilor sedii, precum și a spațiilor interioare ale acestora constituie o prelucrare a datelor cu caracter personal doar dacă aceasta este însoțită 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 și a publicului privind existența sistemului de supraveghere, precum și 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 și împuterniciții acestora sau între operatori sau împuterniciți ai acestora și alte instituții ori organisme publice sau entități de drept public sau privat în una dintre următoarele situații:

a) dacă persoana vizată și-a dat consimțământul expres și neechivoc pentru comunicarea datelor sale;

b) fără consimțământul persoanei vizate în cazurile prevăzute de [art. 5 alin. \(2\) din Legea nr. 677/2001](#), cu modificările și completările ulterioare;

c) în cazul prelucrării datelor cu caracter personal în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, în condițiile prevăzute de [art. 6 din Legea nr. 238/2009](#).

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

a) comunicarea se efectuează pe baza unui contract sau, după caz, a unui document de cooperare care trebuie să cuprindă cel puțin: numărul de înregistrare a notificării, temeiul legal al prelucrării și scopul acesteia, termenul maxim de prelucrare, drepturile și obligațiile părților, modalitățile de asigurare a securității prelucrărilor și de respectare a drepturilor persoanei vizate, precum și mențiunea că datele pot fi utilizate doar de structura beneficiară și 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 și datele solicitate, precum și, dacă este cazul, numărul atribuit beneficiarului de Autoritatea națională de supraveghere.

(3) Comunicarea datelor cu caracter personal de către operatori și împuterniciții acestora se poate face și on-line, cu respectarea dispozițiilor alin. (1) și (2) și asigurarea securității sistemelor de comunicații a datelor cu caracter personal.

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

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

#### ART. 25

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

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

nu este posibilă.

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

(4) În situația în care se constată că au fost transmise date incorecte sau neactualizate, operatorii au obligația de a informa destinatarii respectivelor date asupra neconformității acestora, cu menționarea datelor care au fost modificate.

(5) La comunicarea datelor cu caracter personal operatorii și împuterniciții acestora atenționează destinatarii asupra interdicției 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 instituțiile competente ale altor state sau organisme de cooperare polițienească și judiciară internațională, în condițiile legii, fără autorizarea Autorității naționale de supraveghere, numai dacă există o prevedere legală expresă în legislația națională sau comunitară ori într-un tratat ratificat de România.

(2) Operatorii pot transmite date cu caracter personal către instituțiile competente ale altor state sau organisme de cooperare polițienească și judiciară din state non-UE numai dacă legislația statului în cauză prevede un nivel de protecție cel puțin egal cu cel oferit de legea română sau organizația asigură un nivel adecvat de protecție pentru prelucrarea datelor, cu respectarea condiției prevăzute la [art. 29 alin. \(3\) din Legea nr. 677/2001](#), cu modificările și completările ulterioare.

(3) Transmiterea de date cu caracter personal către instituțiile competente ale altor state sau către organisme de cooperare polițienească și judiciară din state non-UE a căror legislație nu prevede un nivel de protecție cel puțin egal cu cel oferit de legea română poate fi efectuată numai cu autorizarea Autorității naționale de supraveghere, în condițiile prevăzute la [art. 29 alin. \(4\) din Legea nr. 677/2001](#), cu modificările și completările ulterioare.

(4) În cazul prelucrărilor efectuate în activitățile de prevenire, cercetare și combatere a infracțiunilor, precum și de menținere și asigurare a ordinii publice, transmiterea de date cu caracter personal către instituțiile prevăzute la alin. (1)-(3) este întotdeauna permisă dacă transferul este necesar pentru prevenirea unui pericol grav și iminent asupra vieții, integrității corporale sau sănătății unei persoane ori a proprietății acesteia, precum și pentru combaterea unei infracțiuni grave prevăzute de lege, cu respectarea legii române.

#### ART. 27

(1) Transferul de date cu caracter personal către entități de drept public sau privat, altele decât cele prevăzute la art. 26, se face în condițiile legii române și numai cu autorizarea Autorității naționale de supraveghere.

(2) Autorizarea Autorității naționale de supraveghere prevăzută la alin.

(1) nu este necesară în situațiile 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 menționează drepturile recunoscute persoanelor vizate, precum și condițiile necesare asigurării confidențialității 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 și li s-a recunoscut dreptul de opoziție nu pot face obiectul transferului.

(5) Datele cu caracter personal transferate altor organisme publice, entități de drept privat sau autorități 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 condițiile [art. 30 din Legea nr. 677/2001](#), cu modificările și completările ulterioare, cu notificarea prealabilă a Autorității naționale de supraveghere.

### CAP. VII

Măsuri de asigurare a exercitării drepturilor persoanelor vizate

#### ART. 29

(1) Informarea persoanei vizate se face în condițiile [art. 12 din Legea nr. 677/2001](#), cu modificările și completările ulterioare.

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

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

(4) Exercițarea drepturilor persoanei vizate poate fi limitată doar în condițiile prevăzute la [art. 16 alin. \(1\) din Legea nr. 677/2001](#), cu modificările și completările ulterioare, sau, respectiv, la [art. 11 din Legea nr. 238/2009](#).

(5) În orice situație, persoana vizată trebuie să fie informată cu privire la dreptul de a se adresa Autorității naționale de supraveghere sau instanței de judecată.

(6) Operatorii țin evidența cazurilor în care, în aplicarea dispozițiilor [art. 16 din Legea nr. 677/2001](#), cu modificările și completările ulterioare, a

fost limitată exercitarea drepturilor persoanei vizate. Operatorii informează anual Autoritatea națională de supraveghere cu privire la cazurile apărute și modul de soluționare a acestora.

#### ART. 30

În cadrul procedurilor proprii operatorii stabilesc modalitățile prin care, în exercitarea dreptului de acces la date, la cererea persoanei vizate, comunică informațiile 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 excepțiile prevăzute de lege.

#### ART. 31

(1) Exercițarea dreptului de acces se face gratuit o singură dată pe an.  
(2) Pentru toate celelalte situații când drepturile prevăzute de lege nu pot fi exercitate în mod gratuit, structurile/unitățile 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 intervenție al persoanei vizate se exercită în condițiile [art. 14 din Legea nr. 677/2001](#), cu modificările și completările ulterioare.  
(2) Persoana vizată se poate adresa operatorului printr-o cerere scrisă, datată și 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 opoziție, persoana vizată se poate adresa operatorului, prin cerere motivată, cu respectarea condițiilor prevăzute de [art. 15 alin. \(3\) din Legea nr. 677/2001](#), cu modificările și completările ulterioare.  
(2) În termen de 15 zile de la primirea cererii, operatorul comunică persoanei vizate măsurile luate, precum și terțul căruia i-au fost dezvăluite anterior datele cu caracter personal, după caz, cu respectarea eventualei opțiuni a solicitantului privind comunicarea la o anumită adresă, care poate fi și de poștă electronică, sau printr-un serviciu de corespondență care să asigure că predarea i se va face numai personal.  
(3) Dreptul de opoziție 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/unitățile MAI și de a se adresa Autorității naționale de supraveghere sau justiției, potrivit legii.

#### ART. 35

(1) Operatorul informează persoana vizată asupra procedurii de primire a cererilor, prin afișare la sediu, publicare pe pagina WEB sau prin alte mijloace.  
(2) În cazul cererilor transmise fără a fi îndeplinite condițiile prevăzute de lege, solicitantul va fi informat în scris cu privire la condițiile de exercitare a drepturilor prevăzute de [Legea nr. 677/2001](#), cu modificările și completările ulterioare.  
(3) Odată cu soluționarea cererii, se aduce la cunoștința persoanelor



vizate că au dreptul de a se adresa Autorității naționale de supraveghere sau justiției pentru apărarea drepturilor garantate de lege.

## TITLUL II Măsuri tehnice

### CAP. I

#### Utilizatorii datelor cu caracter personal

##### ART. 36

(1) Pentru fiecare utilizator, administratorul aplicației stabilește un cont unic care să permită atât identificarea, cât și configurarea categoriilor de prelucrări la care are dreptul, asigurând totodată și jurnalizarea operațiunilor efectuate.

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

- a) introducerea unui cod de identificare de la tastatură - user name -, însoțită 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 și autentificare folosită, în funcție de importanța datelor cu caracter personal deținute, volumul acestora, numărul de utilizatori, frecvența interogărilor și operațiunile de prelucrare, precum și măsurile de protecție fizică a locației.

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

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

(6) Parolele se schimbă ori de câte ori este nevoie, dar cel puțin o dată la 3 luni pentru utilizatori și la 6 luni pentru administratorii aplicației.

(7) La generarea contului unic utilizatorul primește în scris parola și codul de identificare. Utilizatorul are obligația să schimbe parola în următoarele situații:

- 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 securității prelucrării datelor cu caracter personal.

(8) Administratorul sistemului de evidență a datelor cu caracter personal ia măsurile necesare pentru activarea unui mesaj de avertizare după a treia introducere greșită a parolei și blocarea contului la a cincea introducere greșită. Mesajul pentru utilizator va cuprinde următorul text: "Atenție, ați introdus greșit parola de 3 ori. La a 5-a introducere greșită, contul va fi blocat. Vă rugăm să reverificați codul și parola." După cea de-a cincea introducere greșită a parolei, pe ecran va fi afișat următorul mesaj: "Atenție! Contul este blocat. Vă rugăm să contactați administratorul aplicației."

## 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 fișet/casetă metalic/metalică încuiat/încuiată și 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 conțin coduri de identificare și 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 situațiile prevăzute la art. 11.

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

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

(7) Aplicația de gestiune a bazelor de date trebuie configurată astfel încât să asigure dezactivarea automată a codurilor de identificare și a cartelelor care nu au fost folosite o perioadă de până la 6 luni; acestea sunt menținute în istoricul de utilizatori, după caz, de către administratorul aplicației.

(8) La apariția unei situații de modificare a competențelor sau raporturilor de serviciu, operatorii stabilesc modalități concrete de revocare/suspendare a conturilor de acces, astfel încât prelucrarea datelor cu caracter personal să se facă numai de către personalul autorizat și numai în exercitarea atribuțiilor de serviciu ale acestora.

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

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

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

(12) Pentru accesul personalului la sistemele de evidență a datelor cu caracter personal deținute de alți operatori, conturile de utilizator se vor obține în baza solicitării scrise și motivate a structurii/unității interesate sau pe baza unor protocoale încheiate în acest sens.

## ART. 38

(1) Conducătorul operatorului stabilește fiecărui utilizator tipurile de acces și operațiunile permise acestuia, strict necesare pentru îndeplinirea atribuțiilor de serviciu.

(2) Cu ocazia proiectării, întreținerii, actualizării aplicațiilor de gestiune a bazelor de date, se interzice accesul programatorilor/personalului de întreținere a sistemelor informatice la orice fel de date cu caracter personal deținute/create/accesate de personalul din structura/unitatea respectivă. În aceste situații, se pun la dispoziția programatorilor/personalului de întreținere numai date anonime.

(3) Pentru cazuri excepționale, numai pe durata intervenției și circumstanțiat limitativ la datele strict necesare, persoanele care asigură suportul tehnic pot avea acces la datele cu caracter personal numai în prezența unui utilizator desemnat de operator. În această situație, răspunderea pentru păstrarea confidențialității datelor aparține persoanelor în cauză, sens în care trebuie să semneze un angajament de confidențialitate.

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

#### ART. 39

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

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

#### ART. 40

(1) Bazele de date cu caracter personal deținute/create și programele folosite de operatori sau de împuterniciții acestora sunt salvate, prin copii de siguranță, 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) Aplicația înregistrează orice încercare de acces neautorizat, iar responsabilul/structura responsabilă cu protecția datelor cu caracter personal are obligația de a verifica împrejurările producerii acesteia, luând măsurile ce se impun.

(4) Logurile se păstrează cel puțin 2 ani, în funcție de necesitatea asigurării disponibilității datelor pentru operator, corelat cu importanța și volumul de date stocate. La acoperirea capacității de stocare, logurile vor fi transferate și păstrate pe suport amovibil în condițiile prevăzute pentru copiile de siguranță.

(5) Pentru ținerea evidenței operațiunilor de consultare a datelor cu caracter personal conținute în sisteme de evidență neautomate-manuale, operatorul sau împuterniciții acestuia instituie Registrul de consultare/multiplicare a documentelor din sistemul de evidență, conform modelului prevăzut în anexa nr. 3.

(6) Declanșarea unei investigații a cărei finalizare depășește 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 atribuții de serviciu a utilizatorului.

#### ART. 43

(1) Conducătorii operatorului sau ai împuterniciților acestuia care prelucrează date cu caracter personal dispun luarea măsurilor tehnice adecvate pentru identificarea eventualelor disfuncționalități în ceea ce privește funcționarea sistemelor de comunicații.

(2) Responsabilul/Structura responsabilă cu protecția datelor cu caracter personal efectuează periodic, prin sondaj, controlul autentificărilor și

tipurilor de acces, precum și respectarea măsurilor de securitate specifice sistemelor de comunicații folosite pentru transmiterea acestor date.

(3) Rezultatul controlului, eventualele disfuncționalități identificate, precum și măsurile de remediere a acestora se consemnează într-un raport care se supune aprobării conducătorului/șefului structurii/unității respective.

(4) Conducătorii operatorului sau ai împuterniciților acestuia dispun măsurile necesare de securitate a sistemului de comunicații pentru înlăturarea posibilității 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 comunicații pentru transmiterea datelor cu caracter personal se realizează numai dacă prin această metodă se asigură gradul de operativitate impus de specificul activității desfășurate de structurile implicate.

#### ART. 44

(1) Conducătorii operatorului sau ai împuterniciților acestuia dispun măsurile necesare în vederea instituirii și menținerii unui nivel suficient de securitate a prelucrării datelor cu caracter personal, care vor consta cel puțin în:

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

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

c) implementarea unor aplicații automate de contracarare a vulnerabilităților și amenințărilor informatice și de securitate a sistemelor informatice.

(2) În timpul activității, monitoarele de lucru trebuie să afișeze mesaje de avertizare privind obligativitatea păstrării confidențialității datelor cu caracter personal prelucrate.

#### ART. 45

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

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

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

a) în cadrul documentului se menționează numărul atribuit notificării de către Autoritatea națională de supraveghere;

b) în subsolul fiecărei pagini, cu excepția documentelor clasificate, se inserează următorul text: "Document care conține 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 situații pentru care, potrivit legii, notificarea nu este necesară.

#### ART. 46

Procedurile proprii elaborate de operatori trebuie să cuprindă:

- a) modalități de administrare a conturilor de utilizator;
- b) modalități de control al accesului în zonele în care se prelucrează date cu caracter personal;
- c) modalități de asigurare a confidențialității, integrității și disponibilității datelor cu caracter personal;
- d) modalități privind securitatea transmisiilor de date și accesul securizat la aceste mijloace de transmitere a datelor.

#### CAP. II

##### Dispoziții finale

#### ART. 47

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

(2) Structurile/Unitățile MAI care procesează date cu caracter personal trebuie să pună la dispoziția Oficiului, în condițiile legii, informațiile, documentele sau actele pe care le dețin pentru îndeplinirea atribuțiilor ce îi revin în domeniul protecției datelor cu caracter personal.

#### ART. 48

Prezentele instrucțiuni sunt aplicabile unităților aparatului central al MAI și unităților, instituțiilor și structurilor aflate în subordinea ministerului, în conformitate cu statutul și relația acestora cu ministerul, stabilite prin dispoziții legale și în măsura în care nu contravin acestora.

#### ART. 49

Nerespectarea dispozițiilor prezentelor instrucțiuni atrage, potrivit legii, răspunderea disciplinară, civilă, materială sau penală, după caz.

#### ART. 50

(1) Prezentele instrucțiuni 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) și 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 instrucțiuni.

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

Ministrul administrației  
și internele,  
Vasile Blaga

București, 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 .....

Data 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

\*Font 9\*

Nr. crt.	Denumirea structurii/unității MAI (date de contact)	Responsabilul/Șeful compartimentului (date de contact)	Denumirea sistemului/evidență a notificărilor	Data și numărul înregistrării legale	Scopul/prelucrare	Sursa de preluare/Baza de date	Operațiunile utilizate (automat/neautomat)	Tipul de evidență (proceduri proprii)	Nr. și data Obs

## ANEXA 3

REGISTRUL DE CONSULTARE/MULTIPLICARE

a documentelor din ....., deținut de .....  
 (denumirea sistemului (serviciu/birou etc.)  
 de evidență)

\*Font 9\*

Nr. crt.	Emitentul și numărul de înregistrare a cererii de consultare/multiplicare	Data și ora conșulării	Șeful/Conducătorul structurii care a aprobat conșularea/multiplicarea	Gradul, și prenumele persoanei care consultă	Denumirea documentului primire a documentului multiplicat	Semnătura de restituire a file expediat documentului	Semnătura documentului multipliat/nr. fost expediat documentului	Denumirea adresei prin care a	Nr. Obs.

CTCE Piatra Neamă