



MONITORUL OFICIAL

AL

ROMÂNIEI

Anul 193 (XXXVII) — Nr. 744

PARTEA I
LEGI, DECRETE, HOTĂRĂRI ȘI ALTE ACTE

Vineri, 8 august 2025

SUMAR

Nr.

Pagina

DECIZII ALE CURȚII CONSTITUȚIONALE

Decizia nr. 66 din 25 februarie 2025 referitoare la excepția de neconstituționalitate a dispozițiilor art. 2 lit. b) și d) și ale art. 6 alin. (1) lit. b) și d) din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor....

2–5

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

112. — Instrucțiuni ale viceprim-ministrului, ministrul afacerilor interne, privind măsurile de natură organizatorică și tehnică pentru asigurarea securității prelucrărilor de date cu caracter personal efectuate de către structurile/unitățile/instituțiile Ministerului Afacerilor Interne

6–16

DECIZII ALE CURȚII CONSTITUȚIONALE

CURTEA CONSTITUȚIONALĂ

DECIZIA Nr. 66

din 25 februarie 2025

referitoare la excepția de neconstituționalitate a dispozițiilor art. 2 lit. b) și d) și ale art. 6 alin. (1) lit. b) și d) din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor

Marian Enache	— președinte
Mihaela Ciochină	— judecător
Cristian Deliorga	— judecător
Dimitrie-Bogdan Licu	— judecător
Gheorghe Stan	— judecător
Livia Doina Stanciu	— judecător
Varga Attila	— judecător
Ionița Cochintu	— magistrat-asistent

Cu participarea reprezentantului Ministerului Public, procuror Ioana-Codruța Dărăngă.

1. Pe rol se află soluționarea excepției de neconstituționalitate a dispozițiilor art. 2 lit. b) și d) și ale art. 6 din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor, excepție ridicată de Societatea Alfa Beta — S.R.L. din Constanța în Dosarul nr. 31.065/212/2018/a1 al Judecătoriei Constanța — Secția civilă și care formează obiectul Dosarului Curții Constituționale nr. 537D/2020.

2. La apelul nominal se constată lipsa părților. Procedura de înștiințare este legal îndeplinită.

3. Cauza fiind în stare de judecată, președintele Curții acordă cuvântul reprezentantului Ministerului Public, care pune concluzii de respingere a excepției de neconstituționalitate ca neîntemeiată, întrucât normele criticate nu au un caracter echivoc și nu încalcă principiul egalității în drepturi, deoarece nu instituie regimuri diferite de răspundere contravențională pentru operatorii economici care utilizează practici comerciale înșelătoare, iar, în ceea ce privește dispozițiile art. 45 din Constituție, arată că acestea au fost invocate în mod formal, fără o motivare concretă din partea autoarei excepției de neconstituționalitate.

CURTEA,

având în vedere actele și lucrările dosarului, constată următoarele:

4. Prin Încheierea din 7 ianuarie 2020, pronunțată în Dosarul nr. 31.065/212/2018/a1, **Judecătoria Constanța — Secția civilă a sesizat Curtea Constituțională cu excepția de neconstituționalitate a dispozițiilor art. 2 lit. b) și d) și ale art. 6 din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor**, excepție ridicată de Societatea Alfa Beta — S.R.L. din Constanța într-o cauză având ca obiect soluționarea unei plângeri formulate împotriva unui proces-verbal de constatare și sancționare a unei contravenții întemeiate pe dispozițiile Legii nr. 363/2007.

5. În motivarea excepției de neconstituționalitate se susține, în esență, că dispozițiile criticate utilizează noțiunea de „comercianți” și include în această categorie și persoanele juridice care prestează activități comerciale privind vânzarea

en détail a mărfurilor produse și ambalate de către producători, respectiv de către alți comercianți, fără a face deosebirea între calitatea acestora din urmă, care procedează la etichetarea produselor în scop comercial pe baza strategiei de marketing, și cei care realizează revânzarea mărfurilor respective și care nu au posibilitatea reambalării produselor ambalate de către un alt comerciant/producător sau a eliminării de pe ambalaje a mențiunilor respective. Prin urmare, aceste aspecte conferă textului legal un caracter echivoc și imprecis și, în contextul interpretării și aplicării acestui text, rămâne la discreția autorităților administrative să decidă referitor la răspunderea ce poate fi atrasă din punctul de vedere al protecției consumatorilor în ceea ce privește cele două categorii comercianți — vânzători și producători —, care vor interpreta subiectiv dispozițiile criticate, conducând la încălcarea atât a egalității în drepturi, cât și a libertății economice.

6. **Judecătoria Constanța — Secția civilă** opinează că excepția de neconstituționalitate este neîntemeiată, nefiind încălcate prevederile constituționale menționate în susținerea acesteia, întrucât Legea nr. 363/2007 este o lege specială, ce reglementează combaterea practicilor incorecte ale comercianților în relația cu consumatorii și are ca scop armonizarea reglementărilor naționale cu legislația europeană privind protecția consumatorilor, astfel că în cuprinsul noțiunii de „comerciant” intră inclusiv operatorul economic care realizează vânzare *en détail*. Astfel, textele legale criticate nu au un caracter echivoc și imprecis, iar faptul că legiuitorul nu a instituit regimuri diferite de răspundere contravențională în privința diferiților operatori economici care utilizează practici comerciale înșelătoare, astfel cum sunt acestea definite prin dispozițiile art. 6 din Legea nr. 363/2007, nu este contrar principiilor constituționale referitoare la egalitatea în drepturi și libertatea economică. De altfel, și Curtea Europeană a Drepturilor Omului a statuat că statele beneficiază de o anumită marjă de apreciere în a decide dacă și în ce măsură diferențele dintre diversele situații similare justifică un tratament juridic diferit, iar scopul acestei marje variază în funcție de anumite circumstanțe, de domeniu și de context (spre exemplu, Hotărârea din 28 noiembrie 1984, pronunțată în Cauza *Rasmussen împotriva Danemarcei*, paragraful 40).

7. Potrivit dispozițiilor art. 30 alin. (1) din Legea nr. 47/1992, încheierea de sesizare a fost comunicată președinților celor două Camere ale Parlamentului, Guvernului și Avocatului Poporului, pentru a-și exprima punctele de vedere asupra excepției de neconstituționalitate.

8. **Guvernul**, având în vedere jurisprudența Curții Constituționale în materia principiilor menționate în susținerea excepției de neconstituționalitate, apreciază că: (i) dispozițiile criticate îndeplinesc criteriile de calitate a legii și nu se poate reține nici încălcarea prevederilor art. 16 din Constituție, întrucât nu există elemente din care să rezulte că includerea mai multor categorii de profesioniști din lanțul de producție sau de distribuție în noțiunea de „comerciant” ar afecta principiul egalității în

drepturi, cu atât mai mult cu cât Legea nr. 363/2007 transpune în legislația națională o serie de instrumente europene în domeniul protecției consumatorilor, astfel că, din aceste perspective, excepția de neconstituționalitate este neîntemeiată; (ii) raportat la dispozițiile constituționale ale art. 45, excepția de neconstituționalitate este inadmisibilă, nefiind motivată pretinsa încălcare a acestor norme.

9. Președinții celor două Camere ale Parlamentului și Avocatul Poporului nu au comunicat punctele lor de vedere cu privire la excepția de neconstituționalitate.

CURTEA,

examinând încheierea de sesizare, punctul de vedere al Guvernului, raportul întocmit de judecătorul-raportor, concluziile procurorului, dispozițiile legale criticate, raportate la prevederile Constituției, precum și Legea nr. 47/1992, reține următoarele:

10. Curtea Constituțională a fost legal sesizată și este competentă, potrivit dispozițiilor art. 146 lit. d) din Constituție, precum și ale art. 1 alin. (2), ale art. 2, 3, 10 și 29 din Legea nr. 47/1992, să soluționeze excepția de neconstituționalitate.

11. **Obiectul excepției de neconstituționalitate**, astfel cum reiese din încheierea de sesizare, îl constituie dispozițiile art. 2 lit. b) și d) și ale art. 6 din Legea nr. 363/2007 privind combaterea practicilor încorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor, publicată în Monitorul Oficial al României, Partea I, nr. 899 din 28 decembrie 2007. Având în vedere motivarea excepției de neconstituționalitate și dispozițiile legale care au constituit temeiul emiterii procesului-verbal de constatare și sancționare a unor contravenții contestat, Curtea reține ca obiect al excepției art. 2 lit. b) și d) și art. 6 alin. (1) lit. b) și d) din Legea nr. 363/2007, care au următorul cuprins:

— Art. 2 lit. b) și d): „În sensul prezentei legi, termenii și expresiile de mai jos au următoarele semnificații: (...)

b) *comerciant* — orice persoană fizică sau juridică care, în practicile comerciale ce fac obiectul prezentei legi, acționează în cadrul activității sale comerciale, industriale sau de producție, artisanale ori liberale, precum și orice persoană care acționează în același scop, în numele sau pe seama acesteia; (...)

d) *practici ale comercianților în relația cu consumatorii*, denumite în continuare *practici comerciale* — orice acțiune, omisiune, comportament, demers sau prezentare comercială, inclusiv publicitate și comercializare, efectuate de un comerciant, în strânsă legătură cu promovarea, vânzarea sau furnizarea unui produs consumatorilor;”;

— Art. 6 alin. (1) lit. b) și d): „(1) O practică comercială este considerată ca fiind acțiune înșelătoare dacă aceasta conține informații false sau, în orice situație, inclusiv în prezentarea generală, induce în eroare sau este susceptibilă să inducă în eroare consumatorul mediu, astfel încât, în ambele ipoteze, fie îl determină, fie este susceptibilă a-l determina pe consumator să ia o decizie de tranzacționare pe care altfel nu ar fi luat-o, chiar dacă informațiile sunt, în fapt, corecte în raport cu unul sau mai multe dintre următoarele elemente: (...)

b) *principalele caracteristici ale produsului*, cum ar fi: disponibilitatea, avantajele, riscurile, fabricarea, compoziția, accesoriile, asistența acordată după vânzare și instrumentarea reclamațiilor, modul și data fabricației sau prestării, livrarea, capacitatea de a corespunde scopului, utilizarea, cantitatea, specificațiile, originea geografică sau comercială, rezultatele care se pot obține din utilizarea sa, rezultatele și caracteristicile esențiale ale testelor sau controalelor efectuate asupra produsului; (...)

d) *prețul sau modul de calcul al prețului ori existența unui avantaj specific al prețului*;”.

12. În susținerea neconstituționalității acestor dispoziții legale sunt invocate prevederile constituționale ale art. 1 alin. (5)

privind principiul legalității (în componenta privind calitatea legii), ale art. 16 — *Egalitatea în drepturi* și ale art. 45 — *Libertatea economică*.

13. Examinând excepția de neconstituționalitate, Curtea constată că prin Legea nr. 363/2007 se reglementează combaterea practicilor încorecte ale comercianților în relația cu consumatorii, în acord cu reglementările europene privind protecția consumatorilor, iar dispozițiile criticate în mod concret fac parte din titlul I: *Definirea și interzicerea unor practici comerciale incorecte*, capitolul I: *Dispoziții generale* prin care se stabilește semnificația noțiunilor și expresiilor „comerciant” și „practici ale comercianților în relația cu consumatorii”, denumite practici comerciale, și capitolul II: *Practici comerciale incorecte*, care, potrivit art. 4 alin. (3), sunt, în special, cele (i) înșelătoare, în sensul prevederilor art. 6 și 7, și (ii) agresive, în sensul prevederilor art. 8 și 9 din aceeași lege.

14. Având în vedere acest context legislativ, autoarea excepției de neconstituționalitate consideră că normele criticate ar fi neconstituționale și contrare principiilor legalității, în componenta privind calitatea legii, egalității și libertății economice, întrucât noțiunea de „comerciant” este înțeleasă în sens larg, vizând și persoanele juridice care prestează activități comerciale în regim en détail, deși acestea nu ar avea nicio implicare în ceea ce privește mărfurile produse sau comercializate angro de alți comercianți și, cu toate acestea, persoanele respective ar intra sub incidența contravențiilor prevăzute de textele criticate — respectiv practici comerciale înșelătoare care, prin informații false sau prin prezentarea generală, induc în eroare consumatorul cu privire la principalele caracteristici ale produsului sau prețul/modul de calcul al prețului ori existența unui avantaj specific al prețului. Acest aspect ar conduce autoritățile îndrituite cu efectuarea controlului, constatarea și sancțiunea contravențiilor prevăzute de Legea nr. 363/2007 să aplice în mod arbitrar legea și, prin urmare, ar avea drept consecință atragerea răspunderii contravenționale în materia protecției consumatorilor în mod subiectiv.

15. În ceea ce privește principiul legalității, în componenta privind calitatea legii, invocat în susținerea excepției de neconstituționalitate, Curtea a stabilit că cerința de claritate a legii vizează caracterul neechivoc al obiectului reglementării, cea de precizie se referă la exactitatea soluției legislative alese și a limbajului folosit, în timp ce previzibilitatea legii privește scopul și consecințele pe care le antrenează, respectiv faptul că actul normativ trebuie să fie suficient de precis și clar pentru a putea fi aplicat, iar accesibilitatea, din punct de vedere formal, are în vedere aducerea la cunoștința publică a actelor normative de rang infraconstituțional și intrarea în vigoare a acestora, care se realizează prin publicarea în Monitorul Oficial al României, Partea I (a se vedea, în acest sens, spre exemplu, Decizia nr. 363 din 7 mai 2015, publicată în Monitorul Oficial al României, Partea I, nr. 495 din 6 iulie 2015, paragrafele 16-20 și 26). Prin urmare, o lege îndeplinește condițiile calitative impuse atât de Constituție, cât și de Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, numai dacă norma este enunțată cu suficientă precizie pentru a permite cetățeanului să își adapteze conduita în funcție de aceasta, astfel încât, apelând la nevoie la consiliere de specialitate în materie, el să fie capabil să prevadă, într-o măsură rezonabilă, fața de circumstanțele speței, consecințele care ar putea rezulta dintr-o anumită faptă și să își corecteze conduita. Având în vedere principiul generalității legilor, Curtea reține că poate să fie dificil să se redacteze legi de o precizie totală și o anumită suplețe, suplețe care nu trebuie să afecteze însă previzibilitatea legii (Decizia Curții Constituționale nr. 363 din 7 mai 2015, paragrafele 16-18, precum și jurisprudența Curții Europene a Drepturilor Omului cu privire la care se reține, spre exemplu, Hotărârea din 15 noiembrie 1996, pronunțată în Cauza *Cantoni*

împotriva Franței, paragraful 29). De asemenea, instanța de contencios constituțional a avut în vedere Hotărârea din 24 mai 2007, pronunțată de Curtea Europeană a Drepturilor Omului în Cauza *Dragotoniu și Militaru-Pidhorni împotriva României*, paragraful 35, prin care s-a statuat că semnificația noțiunii de „previzibilitate” depinde într-o mare măsură de conținutul textului despre care este vorba, de domeniul pe care îl acoperă, precum și de numărul și calitatea destinatarilor săi. Previzibilitatea legii nu se opune ideii ca persoana în cauză să fie determinată să recurgă la îndrumări clare pentru a putea evalua, într-o măsură rezonabilă în circumstanțele cauzei, consecințele ce ar putea rezulta dintr-o anumită faptă. La fel se întâmplă și cu profesioniștii, obișnuiți să dea dovadă de o mare prudență în exercitarea activității lor. Astfel, se poate aștepta ca aceștia să acorde o atenție specială evaluării riscurilor pe care aceasta le prezintă.

16. Cu privire la noțiunea de „comerciant”, Curtea observă că Ordonanța Guvernului nr. 99/2000 privind comercializarea produselor și serviciilor de piață, republicată în Monitorul Oficial al României, Partea I, nr. 603 din 31 august 2007, stabilește principiile generale privind desfășurarea activității comerciale și reglementează dezvoltarea rețelei de distribuție a produselor și serviciilor de piață cu respectarea principiilor liberei concurențe, protecției vieții, sănătății, securității și intereselor economice ale consumatorilor, precum și a mediului. La art. 4 sunt definite anumite noțiuni specifice, respectiv: (i) *consumator* — orice persoană fizică sau grup de persoane fizice constituite în asociații, care cumpără, dobândește, utilizează ori consumă produse sau servicii în afara activității profesionale; (ii) *comerciant* — persoana fizică sau juridică autorizată să desfășoare activități de comercializare a produselor și serviciilor de piață; (iii) *comerț cu ridicata/de gros* — activitatea desfășurată de comercianții care cumpără produse în cantități mari în scopul revânzării acestora în cantități mai mici altor comercianți sau utilizatori profesionali și colectivi; (iv) *comerț cu amănuntul/de détail* — activitatea desfășurată de comercianții care vând produse, de regulă, direct consumatorilor pentru uzul personal al acestora; (v) *comerț de tip cash and carry/formă de comerț cu autoservire pe bază de legitimație de acces* — activitatea desfășurată de comercianții care vând mărfuri prin sistemul de autoservire către persoane juridice, persoane fizice autorizate, asociații familiale autorizate conform legii și persoane fizice înregistrate în baza de date a vânzătorului, în scopul revânzării și/sau prelucrării, precum și al utilizării acestora ca produse consumabile, păstrând regimul diferențiat de preț tip angro/en détail.

17. De asemenea, cu referire la noțiunea de „comerciant”, Legea nr. 71/2011 pentru punerea în aplicare a Legii nr. 287/2009 privind Codul civil, publicată în Monitorul Oficial al României, Partea I, nr. 409 din 10 iunie 2011, în capitolul I: „Dispoziții generale”, la art. 6, prevede că: (i) în cuprinsul actelor normative aplicabile la data intrării în vigoare a Codului civil, referirile la comercianți se consideră a fi făcute la persoanele fizice sau, după caz, la persoanele juridice supuse înregistrării în registrul comerțului, potrivit prevederilor art. 1 din Legea nr. 26/1990 privind registrul comerțului, republicată, cu modificările și completările ulterioare, precum și cu cele aduse prin această lege; (ii) dispozițiile anterioare nu se aplică termenului „comerciant” prevăzut în: a) Legea nr. 84/1998 privind mărcile și indicațiile geografice, republicată; b) Legea pomiculturii nr. 348/2003, republicată, cu modificările ulterioare; c) Legea nr. 321/2009 privind comercializarea produselor alimentare, cu modificările și completările ulterioare; d) orice alte acte normative în care termenul „comerciant” are un înțeles specific dispozițiilor cuprinse în aceste din urmă acte normative;

(iii) în legislația privind protecția drepturilor consumatorilor, termenul „comerciant” se înlocuiește cu cel de „profesionist”. De asemenea, art. 3 din Codul civil, cu denumirea marginală *Aplicarea generală a Codului civil*, stabilește că (i) dispozițiile acestui cod se aplică și raporturilor dintre profesioniști, precum și raporturilor dintre aceștia și orice alte subiecte de drept civil; (ii) sunt considerați profesioniști toți cei care exploatează o întreprindere; (iii) constituie exploatarea unei întreprinderi exercitarea sistematică, de către una sau mai multe persoane, a unei activități organizate ce constă în producerea, administrarea ori înstrăinarea de bunuri sau în prestarea de servicii, indiferent dacă are sau nu un scop lucrativ.

18. Or, ținând seama de cadrul legislativ mai sus redat și de dispozițiile criticate, Curtea observă că acestea din urmă includ și comercianții *en détail* și reglementează, în mod clar și precis, conduita pe care trebuie să o urmeze subiecții ce se află în ipoteza normei legale, respectiv comercianții/profesionistii nu pot practica activități comerciale înșelătoare, în caz contrar, persoanelor care se află în ipoteza normei — persoane care sunt profesioniști în domeniul comerțului — li se poate atrage răspunderea contravențională. De asemenea, acestea sunt accesibile, întrucât, după caz, au fost aduse la cunoștință publică prin publicarea în Monitorul Oficial al României, Partea I, iar între normele legale criticate și care reglementează comercializarea produselor și serviciilor de piață, ale Codului civil și ale altor acte normative care reglementează activitatea comercianților și protecția consumatorilor există atât o conexiune logică pentru a da posibilitatea destinatarilor acestora să determine conținutul domeniului reglementat, cât și o corespondență sub aspectul forței lor juridice. Destinatarii acestora, având în vedere conținutul normativ al prevederilor criticate, pot avea reprezentarea consecințelor nerespectării acestor prevederi legale.

19. În ceea ce privește critica de neconstituționalitate raportată la art. 16 alin. (1) din Constituție, Curtea observă că, potrivit jurisprudenței sale, principiul egalității presupune ca în situații egale să se aplice un tratament juridic egal, fără nicio discriminare pe criterii arbitrare, și, în același timp, presupune și dreptul la diferențiere în tratament juridic, dacă situațiile sunt diferite (Decizia nr. 87 din 25 februarie 2020, publicată în Monitorul Oficial al României, Partea I, nr. 411 din 18 mai 2020, paragraful 25). Față de cele prezentate, având în vedere faptul că principiul egalității în fața legii presupune instituirea unui tratament egal pentru situații care, în funcție de scopul urmărit, nu sunt diferite, nu poate fi reținută critica privind încălcarea principiului egalității, întrucât normele criticate sunt aplicabile deopotrivă tuturor comercianților ce intră sub ipoteza textelor în discuție.

20. În ceea ce privește libertatea economică, Curtea reține că, potrivit art. 45 din Legea fundamentală, accesul liber al persoanei la o activitate economică, libera inițiativă și exercitarea acestora în condițiile legii sunt garantate. Accesul liber la o activitate economică nu exclude, ci, dimpotrivă, implică stabilirea unor limite de exercitare a libertății economice, statul având obligația să impună reguli de disciplină economică, iar legiuitorul având competența să stabilească sancțiunile corespunzătoare pentru nerespectarea acestora (Decizia nr. 362 din 25 martie 2010, publicată în Monitorul Oficial al României, Partea I, nr. 328 din 18 mai 2010). Mai mult, Curtea a învederat că principiul libertății economice nu este un drept absolut al persoanei, ci este condiționat de respectarea limitelor stabilite de lege, limite ce urmăresc asigurarea unei anumite discipline economice ori protejarea unor interese generale, precum și asigurarea respectării drepturilor și intereselor legitime ale tuturor (a se vedea, în acest sens, Decizia nr. 162

din 8 februarie 2011, publicată în Monitorul Oficial al României, Partea I, nr. 272 din 19 aprilie 2011). Astfel, a fi comerciant/profesionist implică nu doar dreptul de a presta o activitate economică în scopul obținerii unei surse de venit, ci și o obligație corelativă față de destinatarul produselor comercializate, care trebuie protejat împotriva eventualelor practici comerciale incorecte. Comerciantul/profesionistul economic *en détail* este cel care, în definitiv, alege produsele pe care le expune vânzării, ceea ce implică în mod necesar din partea sa diligență în respectarea obligațiilor legale impuse vânzătorului.

21. Astfel, accesul liber al persoanelor la o activitate economică se desfășoară în condițiile prestabilite de către legiuitor, în virtutea art. 61 alin. (1) din Constituție, potrivit căruia „*Parlamentul este organul reprezentativ suprem al poporului român și unica autoritate legiuitoare a țării*”, care trebuie să țină seama și de dispozițiile art. 135 din Constituție, potrivit cărora economia României este economie de piață, bazată pe libera inițiativă și concurență, statul având obligația să asigure, printre altele, libertatea comerțului, protecția concurenței loiale, crearea cadrului favorabil pentru valorificarea tuturor factorilor de producție și protejarea intereselor naționale în activitatea economică, financiară și valutară. Or, dispozițiilor constituționale ale art. 45, ale art. 61 alin. (1) și ale art. 135 li se subsumează și prevederile criticate în prezenta cauză, astfel că excepția de neconstituționalitate este neîntemeiată și din această perspectivă.

22. În ceea ce privește celelalte chestiuni înveredate, Curtea observă că acestea țin de interpretarea și aplicarea legii de către autoritățile îndrituite cu efectuarea controlului, constatarea și aplicarea sancțiunilor contravenționale prevăzute de Legea nr. 363/2007, iar, în măsura în care sunt nemulțumiți de modul în care s-a stabilit atragerea răspunderii contravenționale în materia protecției consumatorilor, comercianții, în virtutea art. 16 din Legea nr. 363/2007, pot apela la dispozițiile Ordonanței Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, publicată în Monitorul Oficial al României, Partea I, nr. 410 din 25 iulie 2001, cu excepțiile prevăzute de lege. În acest context,

instanța competentă să soluționeze plângerea, după ce verifică dacă aceasta a fost introdusă în termen, ascultă pe cel care a făcut-o și pe celelalte persoane citate, dacă aceștia s-au prezentat, administrează orice alte probe prevăzute de lege, necesare în vederea verificării legalității și temeiniciei procesului-verbal, și hotărăște asupra sancțiunii, despăgubirii stabilite, precum și asupra măsurii confiscării.

23. Față de această împrejurare, Curtea a reținut că interpretarea legii este operațiunea de stabilire a conținutului și a sensului la care aceasta se referă și este o etapă absolut necesară în vederea aplicării sale corecte la situația de fapt concretă din cauză, instanța de judecată fiind ținută să aplice în acest scop metodele de interpretare a normelor juridice. Instanțele judecătorești interpretează legea, în mod necesar, în procesul soluționării cauzelor cu care au fost investite, interpretarea fiind faza indispensabilă procesului de aplicare a legii. Totodată, Curtea a statuat că, în conformitate cu principiile enunțate în teoria generală a dreptului, norma juridică se interpretează în mod sistematic, prin coroborare cu alte dispoziții normative care țin de aceeași instituție juridică sau de aceeași ramură de drept. Rațiunea procedeei sistematice de interpretare se întemeiază pe natura sistemică a ansamblului normelor de drept, în care normele se află într-o legătură funcțională, caracteristică elementelor unei structuri. Așa fiind, fiecare normă se completează prin celelalte și își dezvoltă în întregul sens în cadrul sistemului de norme care este dreptul. În acest context, norma criticată nu poate fi privită în mod individual, izolat, ci se va interpreta în mod sistematic, prin coroborare cu celelalte prevederi normative din actul în care se regăsește (a se vedea, în acest sens, Decizia nr. 144 din 13 martie 2019, publicată în Monitorul Oficial al României, Partea I, nr. 292 din 16 aprilie 2019, paragraful 68). Așadar, aplicarea și interpretarea legii sunt chestiuni ce țin de resortul exclusiv al instanței de judecată care judecă fondul cauzei, precum și, eventual, al instanțelor de control judiciar, astfel cum rezultă din prevederile coroborate ale art. 126 alin. (1) și (3) din Constituție.

24. Pentru considerentele expuse, în temeiul art. 146 lit. d) și al art. 147 alin. (4) din Constituție, precum și al art. 1-3, al art. 11 alin. (1) lit. A.d) și al art. 29 din Legea nr. 47/1992, cu unanimitate de voturi,

CURTEA CONSTITUȚIONALĂ

În numele legii

DECIDE:

Respinge, ca neîntemeiată, excepția de neconstituționalitate ridicată de Societatea Alfa Beta — S.R.L. din Constanța în Dosarul nr. 31.065/212/2018/a1 al Judecătoriei Constanța — Secția civilă și constată că dispozițiile art. 2 lit. b) și d) și ale art. 6 alin. (1) lit. b) și d) din Legea nr. 363/2007 privind combaterea practicilor incorecte ale comercianților în relația cu consumatorii și armonizarea reglementărilor cu legislația europeană privind protecția consumatorilor sunt constituționale în raport cu criticile formulate.

Definitivă și general obligatorie.

Decizia se comunică Judecătoriei Constanța — Secția civilă și se publică în Monitorul Oficial al României, Partea I.

Pronunțată în ședința din data de 25 februarie 2025.

PREȘEDINTELE CURȚII CONSTITUȚIONALE

MARIAN ENACHE

Magistrat-asistent,
Ionița Cochințu

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

MINISTERUL AFACERILOR INTERNE

INSTRUCȚIUNI

privind măsurile de natură organizatorică și tehnică pentru asigurarea securității prelucrărilor de date cu caracter personal efectuate de către structurile/unitățile/instituțiile Ministerului Afacerilor Interne

Având în vedere prevederile Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), ale Legii nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările ulterioare, precum și ale Legii nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date,

în temeiul prevederilor art. 7 alin. (5) din Ordonanța de urgență a Guvernului nr. 30/2007 privind organizarea și funcționarea Ministerului Afacerilor Interne, aprobată cu modificări prin Legea nr. 15/2008, cu modificările și completările ulterioare,

viceprim-ministrul, ministrul afacerilor interne, emite următoarele instrucțiuni:

TITLUL I

Măsurile organizatorice

CAPITOLUL I

Dispoziții generale

Art. 1. — Prezentele instrucțiuni se aplică activităților de prelucrare a datelor cu caracter personal efectuate de Ministerul Afacerilor Interne, denumit în continuare *MAI*, unitățile, instituțiile și structurile din subordinea/cadrul *MAI*, în calitatea acestora de operatori, operatori asociați sau persoane împuternicite de operatori.

Art. 2. — (1) La nivelul *MAI* prelucrarea datelor cu caracter personal se realizează cu respectarea regulilor generale și speciale prevăzute de:

a) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), denumit în continuare *RGPD*;

b) Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările ulterioare;

c) Legea nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date;

d) deciziile și instrucțiunile cu caracter normativ emise de Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, denumită în continuare *ANSPDCP*;

e) prezentele instrucțiuni.

(2) Operatorii, operatorii asociați și persoanele împuternicite de operatori utilizează sisteme de evidență și/sau mijloace

automate și manuale 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, operatorii asociați și persoanele împuternicite de operatori se supun activităților de control prealabil sau de investigare efectuate de *ANSPDCP*, potrivit legii, și, la cerere, acordă acesteia sprijin deplin pentru exercitarea atribuțiilor sale.

(4) Termenii și expresiile utilizate în prezentele instrucțiuni au semnificațiile prevăzute la art. 4 din *RGPD*, art. 2 din Legea nr. 190/2018, cu modificările ulterioare, respectiv la art. 4 din Legea nr. 363/2018.

Art. 3. — (1) Au calitatea de *operator* unitățile, instituțiile și structurile din subordinea/cadrul *MAI*, precum și *MAI*, pentru prelucrările realizate la nivelul aparatului central, dacă stabilesc scopul și mijloacele de prelucrare a datelor cu caracter personal sau dacă scopul și mijloacele de prelucrare a datelor cu caracter personal sunt stabilite printr-un act normativ sau în baza unui act normativ ori dacă sunt desemnate ca operator printr-un/în baza unui act normativ.

(2) Au calitatea de *operatori asociați* doi sau mai mulți operatori, cu condiția ca cel puțin un operator să fie din cadrul *MAI*, care stabilesc în comun scopurile și mijloacele de prelucrare.

(3) Au calitatea de *persoană împuternicită de operator* unitățile, instituțiile și structurile din subordinea/cadrul *MAI* care prelucrează date cu caracter personal în numele operatorului.

(4) Are calitatea de *utilizator al datelor cu caracter personal*, denumit în continuare *utilizator*, personalul operatorului sau al persoanei împuternicite de operator ale cărui atribuții de serviciu presupun operațiuni de prelucrare a datelor cu caracter personal.

CAPITOLUL II

Organizarea activității de prelucrare a datelor cu caracter personal în *MAI*

Art. 4. — (1) La nivelul fiecărui operator din cadrul *MAI* se desemnează un responsabil cu protecția datelor personale prin

act administrativ. La nivelul aparatului central al MAI, responsabil cu protecția datelor personale este șeful Oficiului Responsabilului cu Protecția Datelor Personale, denumit în continuare *ORPDP*, iar, în lipsa acestuia, lucrătorul din cadrul *ORPDP*, desemnat în acest sens.

(2) Operatorul se asigură că responsabilul desemnat potrivit alin. (1) nu a fost sancționat administrativ sau disciplinar și/sau nu este cercetat referitor la încălcarea dispozițiilor legale privind prelucrarea datelor cu caracter personal.

(3) În funcție de volumul datelor prelucrate, complexitatea operațiunilor de prelucrare și de numărul de utilizatori, operatorul poate înființa o structură/un compartiment specializat(ă) în domeniul protecției datelor cu caracter personal care să sprijine responsabilul în îndeplinirea atribuțiilor legale.

(4) Înființarea structurii/compartimentului prevăzut(e) la alin. (3) se efectuează cu încadrarea în numărul total de posturi și indicatori în finanțare aprobați de MAI.

Art. 5. — (1) MAI și unitățile, instituțiile și structurile aflate în subordinea/în cadrul MAI, în calitate de operator, au în principal următoarele obligații:

a) să asigure informarea persoanelor vizate și să respecte drepturile acestora;

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

c) să întocmească o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor, conform art. 30 din RGPD sau, după caz, conform art. 27 din Legea nr. 363/2018;

d) să elaboreze politici și 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 transmită *ORPDP* anual, până la 31 ianuarie, o analiză cu privire la activitatea desfășurată în domeniul prelucrării datelor cu caracter personal pentru anul precedent, prin intermediul responsabilului/structurii/compartimentului specializat(e) în domeniul protecției datelor cu caracter personal;

f) să pună la dispoziția *ORPDP*, în condițiile legii, și, la solicitarea reprezentanților acestuia, prin intermediul responsabilului/structurii/compartimentului specializat(e) în domeniul protecției datelor cu caracter personal informațiile și documentele în legătură cu prelucrarea datelor cu caracter personal pe care le dețin, precum și orice alte documente pe care le dețin pentru îndeplinirea atribuțiilor ce le revin în domeniul protecției datelor cu caracter personal, cu excepția celor care conțin date cu caracter personal prelucrate în contextul unor activități din domeniul securității naționale;

g) să informeze *ORPDP* cu privire la situațiile de încălcare a securității datelor cu caracter personal;

h) să notifice *ANSPDCP* în cazul încălcării securității datelor cu caracter personal potrivit art. 33 din RGPD sau, după caz, potrivit art. 36 din Legea nr. 363/2018;

i) să asigure informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal potrivit art. 34 din RGPD sau, după caz, potrivit art. 39 din Legea nr. 363/2018;

j) să publice pe site-ul instituției și la avizier datele de contact ale responsabilului cu protecția datelor personale (nume, prenume, telefon de serviciu, adresă de e-mail și fax), ghidul persoanei vizate și formulare privind exercitarea drepturilor în acest domeniu;

k) să identifice și să evalueze riscurile inerente prelucrării datelor cu caracter personal și să implementeze măsuri pentru atenuarea acestor riscuri;

l) să informeze *ANSPDCP* cu privire la situația statistică a măsurilor de omisiune a furnizării de informații/limitare a dreptului de acces al persoanei vizate, adoptate în anul precedent, în conformitate cu art. 15 alin. (8) și art. 17 alin. (6) din Legea nr. 363/2018;

m) să respecte principiile de prelucrare a datelor cu caracter personal specificate la art. 5 din RGPD și art. 5 din Legea nr. 363/2018;

n) să constituie Registrul de evidență a cererilor persoanelor vizate pentru exercitarea drepturilor conferite de prevederile RGPD, precum și de cele ale Legii nr. 363/2018, al cărui model este prevăzut în anexa nr. 1;

o) să comunice datele de contact ale responsabilului cu protecția datelor personale *ANSPDCP*, *ORPDP* și structurilor ierarhic superioare care îi monitorizează activitatea pe linie de protecție a datelor.

(2) Analiza prevăzută la alin. (1) lit. e) va cuprinde cel puțin următoarele:

a) denumirea și datele de contact ale structurii/unității/instituției MAI;

b) datele de contact ale responsabilului cu protecția datelor personale și data numirii în această funcție, dacă la nivelul operatorului există o structură/un compartiment specializat/specializată în domeniul protecției datelor cu caracter personal și dacă responsabilul exercită alte sarcini și atribuții;

c) o descriere a măsurilor tehnice și organizatorice întreprinse;

d) o scurtă descriere a procedurilor proprii prevăzute la alin. (1) lit. d);

e) numărul cererilor de exercitare a drepturilor, defalcat pe fiecare drept în parte;

f) încălcări ale securității datelor cu caracter personal și măsurile întreprinse (notificarea *ANSPDCP*, informarea persoanei vizate, măsuri dispuse etc.), dacă au avut loc;

g) controale și investigații ale *ANSPDCP*, dacă au fost efectuate, și măsurile dispuse cu această ocazie;

h) un extras din planul de pregătire a personalului care să cuprindă temele de pregătire din domeniul protecției datelor cu caracter personal;

i) probleme identificate în aplicarea legislației din domeniul protecției datelor cu caracter personal;

j) activități de automonitorizare a legalității prelucrărilor de date, dacă au fost realizate, iar dacă au fost constatate nereguli, menționarea acestora și a măsurilor dispuse;

k) situația statistică a măsurilor de omisiune a furnizării de informații în conformitate cu art. 15 alin. (8) din Legea nr. 363/2018, precum și a celor de limitare a dreptului de acces, în conformitate cu art. 17 alin. (6) din Legea nr. 363/2018.

Art. 6. — (1) Conducerea operatorului are următoarele atribuții principale:

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

b) desemnează/stabilește responsabilul/structura/compartimentul specializat(ă) în domeniul protecției datelor cu caracter personal;

c) asigură elaborarea procedurilor proprii și, după avizarea acestora de către *ORPDP*, le aprobă. Se exceptează de la avizarea de către *ORPDP* procedurile care stabilesc măsuri de protecție a datelor cu caracter personal prelucrate în contextul unor activități din domeniul securității naționale;

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

g) analizează și dispune 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 *ORPDP* 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 ANSPDCP sau când aceasta a dispus efectuarea unui control prealabil ori a unor investigații;

i) asigură realizarea evidenței tuturor categoriilor de activități de prelucrare a datelor cu caracter personal, precum și actualizarea acesteia;

j) dispune măsuri prin care să se realizeze monitorizarea cu privire la eficacitatea măsurilor de securitate stabilite în vederea asigurării securității datelor personale prelucrate la nivelul structurii;

k) dispune măsuri cu privire la măsurile organizatorice necesare referitoare la monitorizarea internă pentru a asigura legalitatea operațiunilor de prelucrare, respectarea prezentelor instrucțiuni și a legislației din domeniul protecției datelor (automonitorizare);

l) asigură implementarea mecanismelor adecvate pentru obținerea, păstrarea și demonstrarea existenței consimțământului valabil în baza căruia se realizează prelucrări de date în temeiul art. 6 alin. (1) lit. (a) și al art. 9 alin. (2) lit. (a) din RGPD.

(2) Conducerea structurii/instituției/unității care are calitatea de persoană împuternicită de operator are atribuțiile prevăzute la alin. (1) lit. b), d)-g) și i)-j).

(3) În cazul în care este incidentă una dintre situațiile prevăzute la alin. (1) lit. h), conducerea persoanei împuternicite de operator are obligația de a informa și operatorul al cărui împuternicit este.

Art. 7. — (1) Responsabilul cu protecția datelor personale are obligațiile stabilite la art. 38 alin. (3) teza finală și alin. (5) din RGPD și îndeplinește sarcinile stabilite la art. 39 din RGPD și la art. 42 din Legea nr. 363/2018, după caz, precum și următoarele atribuții:

a) elaborează și implementează politici de protecția datelor sau proceduri proprii, pe care le supune aprobării conducerii operatorului, după avizarea acestora de ORPDP;

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

c) informează de îndată conducerea operatorului sau a persoanei împuternicite de operator despre vulnerabilitățile și riscurile semnalate în sistemul de securitate a prelucrării datelor cu caracter personal al structurii/instituției/unității și propune măsuri pentru înlăturarea acestora;

d) coordonează și monitorizează activitatea personalului pe linia protecției datelor cu caracter personal la nivelul operatorului sau al persoanei împuternicite de operator;

e) efectuează, prin sondaj, verificări privind modul de aplicare a măsurilor legale de protecție a datelor cu caracter personal, întocmește documente și formulează propuneri pentru remedierea deficiențelor constatate, pe care le înaintează spre aprobare conducerii operatorului sau, după caz, a persoanei împuternicite de operator;

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

g) coordonează și asigură soluționarea cererilor persoanelor vizate. Informarea persoanei vizate în temeiul art. 12-14 din RGPD se realizează de responsabilul cu protecția datelor prin postarea pe site/la avizier a unei note de informare/a unui material de informare/ghid, însoțită/insoțit de formulare;

h) ține evidența cererilor persoanelor vizate și a cazurilor de limitare în condițiile prevăzute de art. 15, 17 și 18 din Legea nr. 363/2018 sau în condițiile art. 23 din RGPD;

i) păstrează și actualizează evidența întocmită de operator în conformitate cu art. 30 din RGPD sau cu art. 27 din Legea nr. 363/2018, după caz, cu sprijinul structurilor care realizează operațiunile de prelucrare;

j) realizează periodic instruiți în domeniul protecției datelor cu personalul care prelucerează date cu caracter personal din cadrul operatorului;

k) primește sesizările privind încălcările de securitate sau se sesizează din oficiu, desfășoară activități de verificare și propune măsuri conducerii;

l) ține evidența declarațiilor de consimțământ explicit în baza cărora se realizează prelucrări de date în temeiul art. 6 alin. (1) lit. (a) și al art. 9 alin. (2) lit. (a) din RGPD;

m) asistă, la solicitarea ANSPDCP, la efectuarea unor investigații în domeniul protecției datelor cu caracter personal, efectuate la operator sau persoana împuternicită de operator;

n) participă, potrivit competențelor, la solicitarea structurilor cu atribuții de control din cadrul operatorului sau persoanei împuternicite de operator, la activitățile de îndrumare, sprijin și control efectuate la structurile din cadrul operatorului sau persoanei împuternicite de operator, în conformitate cu dispozițiile legale în vigoare;

o) ține documentația aferentă evaluărilor de impact efectuate la nivelul operatorului de date.

(2) Atribuțiile specifice responsabilului/personalului din cadrul structurii/compartimentului specializat(e) în domeniul protecției datelor cu caracter personal se stabilesc prin fișa postului.

Art. 8. — (1) Utilizatorul are 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 prelucreze exclusiv datele cu caracter personal necesare îndeplinirii atribuțiilor de serviciu și să acorde sprijin responsabilului/structurii responsabile cu protecția datelor personale pentru realizarea activităților specifice ale acestuia/acesteia;

c) 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;

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

e) să informeze de îndată conducerea ierarhic superioară a structurii din care face parte și responsabilul/structura responsabilă cu protecția datelor personale cu privire la orice împrejurări de natură a conduce la o diseminare neautorizată de date cu caracter personal, cu privire la situațiile în care au fost accesate/prelucrate date cu caracter personal prin încălcarea normelor legale sau la orice alte situații de încălcare a securității datelor, despre care a luat la cunoștință;

f) să utilizeze numai echipamentele securizate și puse la dispoziție de operator, în vederea diseminării/comunicării de date cu caracter personal.

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

Art. 9. — (1) La începerea activității în cadrul operatorului și înainte de începerea exercitării atribuțiilor specifice funcției îndeplinite, în cazul în care acestea includ activități de prelucrare a datelor cu caracter personal, utilizatorul trebuie să semneze o declarație pe propria răspundere, conform modelului prevăzut în anexa nr. 2, prin care menționează că a luat cunoștință de normele de protecție a acestor date, pe care se obligă să le respecte. Declarația se semnează în prezența responsabilului cu protecția datelor sau, în caz de imposibilitate obiectivă, în prezența șefului nemijlocit, după care se păstrează în format electronic, scanat de către responsabil, și se înaintează, în

original, structurii de resurse umane din cadrul operatorului, în vederea păstrării la dosarul de personal.

(2) Utilizatorul prelucrează date cu caracter personal doar pe perioada în care îndeplinește atribuții care includ activități de prelucrare a datelor cu caracter personal.

(3) Operatorul permite, în condițiile legii, prelucrarea datelor cu caracter personal de către utilizatorii unui alt operator din afara ori din cadrul MAI, pe perioada necesară îndeplinirii unor atribuții de serviciu.

(4) În scopul prevăzut la alin. (3), operatorii încheie un protocol de cooperare/contract, care să prevadă că prelucrarea datelor cu caracter personal se face cu respectarea drepturilor persoanelor vizate, respectiv a condițiilor de securitate stabilite de către operatorul care gestionează sau administrează sistemul de evidență a datelor cu caracter personal.

Art. 10 — Extinderea sau restrângerea atribuțiilor privind prelucrarea datelor cu caracter personal se dispune de către conducerea operatorului ori a persoanei împuternicite de operator atunci când utilizatorul se află în una dintre următoarele situații:

- a) la modificarea raporturilor de muncă/serviciu;
- b) la modificarea atribuțiilor privind prelucrarea datelor cu caracter personal, prevăzute în fișa postului.

Art. 11. — (1) Dreptul de acces al utilizatorului la sistemele de evidență se suspendă pe perioada în care acesta se află în una dintre următoarele situații:

- a) lipsește o perioadă mai mare de 3 luni din unitate;
- b) este cercetat administrativ sau disciplinar referitor la încălcarea dispozițiilor legale privind prelucrarea datelor cu caracter personal.

(2) Conducerea operatorului dispune revocarea contului unic de către administratorul sistemului 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.

(3) Accesul la bazele de date poate fi reacordat numai în urma analizării și înlăturării cauzei/cauzelor care a/au determinat aplicarea măsurilor prevăzute la art. 10.

(4) Analiza prevăzută la alin. (3) se efectuează de către șeful nemijlocit al utilizatorului, care poate consulta în acest sens responsabilul cu protecția datelor.

Art. 12. — (1) La nivelul ORPDP se constituie Registrul de evidență a operatorilor din cadrul MAI, al cărui model este prevăzut în anexa nr. 3.

(2) Operatorii au obligația de a informa ORPDP ori de câte ori datele conținute de registrul prevăzut la alin. (1) suferă modificări.

Art. 13. — (1) Fără a se limita la aceste modalități, instruirea utilizatorilor în domeniul protecției datelor se realizează prin: însușirea temelor incluse în planurile anuale de pregătire continuă, tutela profesională, instruiți organizate de ORPDP sau responsabilul cu protecția datelor desemnat la nivelul operatorului, cursuri organizate de ORPDP sau instituțiile care asigură formarea profesională a personalului MAI.

(2) Planurile anuale de pregătire continuă la nivelul operatorilor și programul perioadei de tutelă profesională trebuie să conțină teme privind legislația națională și legislația europeană în materia prelucrării datelor cu caracter personal, precum și teme specifice privind riscurile pe care le comportă prelucrarea datelor cu caracter personal și măsurile minime de securitate, în funcție de specificul activității fiecărui operator.

(3) Instruirile prevăzute la alin. (1) se realizează periodic sau la modificarea raporturilor de serviciu ale utilizatorului, la modificarea cadrului legal în materie sau când a avut loc o încălcare privind securitatea datelor.

(4) Atunci când a avut loc o încălcare privind securitatea datelor, prelucrarea acestora se realizează cu toți utilizatorii operatorului, pentru a evita producerea unei încălcări similare în viitor.

(5) Instruirile periodice conțin obligatoriu informații cu privire la riscurile generate de vulnerabilități și amenințări informatice.

(6) La finalul instruirilor prevăzute la alin. (1) se pot face evaluări ale gradului de înțelegere a temelor prezentate.

(7) Evaluările de la finalul anului trebuie să conțină obligatoriu și întrebări din domeniul protecției datelor cu caracter personal.

CAPITOLUL III

Prelucrarea datelor cu caracter personal

Art. 14. — (1) Operatorii și persoanele împuternicite de operatori prelucrează date cu caracter personal care pot face ulterior obiectul unui sistem de evidență, automat sau manual, ori care sunt destinate să fie incluse într-un asemenea sistem, în mod distinct, pentru realizarea activităților desfășurate în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor, executării pedepselor, măsurilor educative și de siguranță, precum și menținerii și asigurării ordinii și siguranței publice, pentru scopuri administrative proprii ori pentru scopuri de administrație publică, după caz, conform specificului activității.

(2) Unitățile, instituțiile și structurile aflate în subordinea/în cadrul MAI care, în calitate de operatori, prelucrează date cu caracter personal prin persoane împuternicite 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 în numele ei.

(3) Documentele prevăzute la alin. (2) trebuie să conțină obligațiile prevăzute la art. 28 din RGPD, respectiv la art. 25 din Legea nr. 363/2018, după caz.

(4) Unitățile, instituțiile și structurile aflate în subordinea/în cadrul MAI care au calitatea de operatori asociați, în sensul art. 3 alin. (2), au obligația de a încheia un acord care trebuie să cuprindă cel puțin următoarele elemente:

- a) obligațiile părților pentru asigurarea unei prelucrări legale și echitabile;
- b) categoriile de date care fac obiectul prelucrării, inclusiv modalitatea prin care se asigură respectarea principiului reducerii la minimum a datelor;
- c) operațiunile și procedurile de prelucrare a datelor cu caracter personal;
- d) condițiile în care datele cu caracter personal pot fi comunicate altor persoane fizice sau juridice;
- e) descrierea măsurilor necesare pentru asigurarea securității prelucrărilor;
- f) măsurile necesare a fi instituite pentru asigurarea confidențialității prelucrărilor;
- g) măsurile instituite pentru asigurarea exercitării drepturilor de către persoanele vizate;
- h) punctul de contact unic pentru persoanele vizate.

Art. 15. — Prelucrarea datelor cu caracter personal se poate realiza prin mijloace automate sau manual în cadrul unor operațiuni ori seturi de operațiuni, cum ar fi:

- a) colectarea — strângerea 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 manual, care poate fi registrul, fișier electronic, 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 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) structurarea — utilizarea unor metode sistematice de stocare a informațiilor și datelor într-un sistem de evidență, în așa fel încât ele să poată fi folosite în mod eficient;

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

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

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

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

i) 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;

j) utilizarea — folosirea datelor cu caracter personal, în tot sau în parte, de către și în interiorul operatorului, persoanelor împuternicite de operator ori destinatarului, după caz, inclusiv prin tipărire, copiere, multiplicare, scanare sau orice alte procedee similare;

k) divulgarea prin transmitere, diseminare sau punere la dispoziție în orice alt mod — modalitatea prin care datele cu caracter personal se fac disponibile către terți prin comunicare, transmitere, dezvăluire sau în orice alt mod;

l) alinierea — modalitatea prin care datele sunt aranjate și accesate din memoria sistemului informatic în vederea valorificării ulterioare;

m) 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;

n) restricționarea — marcarea datelor cu caracter personal stocate, cu scopul de a limita prelucrarea viitoare a acestora;

o) 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;

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. 16. — (1) Prelucrarea datelor cu caracter personal se realizează de către operatori și persoane împuternicite de operatori 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 din alte surse, care pot fi, dar fără a se limita la: activitatea proprie a operatorului sau a persoanei împuternicite de operator, 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 art. 13 și 14 din RGPD, respectiv art. 13 și 14 din Legea nr. 363/2018, după caz.

(4) Stocarea datelor cu caracter personal se realizează în condițiile stabilite prin actul normativ care reglementează scopul prelucrării și potrivit legislației arhivistice în vigoare.

Art. 17. — (1) Operatorii și persoanele împuternicite de operatori prelucrează date cu caracter personal în scopuri de organizare, gestiune sau asigurare economico-financiară și administrativă privind proprii angajați și membrii de familie ai acestora, în cadrul activității de management resurse umane, asigurare a asistenței medicale sau pentru desfășurarea unor activități cultural-artistice, jurnalistice ori sportive.

(2) Operatorii și persoanele împuternicite de operatori 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.

(3) Datele cu caracter personal astfel prelucrate se șterg sau se distrug după realizarea scopului în care au fost prelucrate.

(4) Stocarea acestor date pentru o perioadă mai mare decât cea necesară realizării scopului poate avea loc în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare sau în scopuri statistice.

CAPITOLUL IV

Comunicarea datelor cu caracter personal

Art. 18. — (1) Datele cu caracter personal se comunică între operatori și persoanele împuternicite de operatori sau între operatorii sau persoanele împuternicite de operatorii în cauză și alte instituții ori organisme publice sau entități de drept public sau privat în una dintre următoarele situații:

a) în cazurile prevăzute la art. 6 alin. (1) din RGPD;

b) în cazul prelucrării datelor cu caracter personal în scopul realizării activităților de prevenire, descoperire, cercetare, urmărire penală și combatere a infracțiunilor, de executare a pedepselor, măsurilor educative și de siguranță, precum și de menținere și asigurare a ordinii și siguranței publice de către autoritățile competente, în condițiile prevăzute de Legea nr. 363/2018.

(2) Comunicarea datelor cu caracter personal în situațiile prevăzute la alin. (1) se 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: temeiul legal al prelucrării și scopul acesteia, tipurile de date care fac obiectul prelucrării, perioadele de stocare, drepturile și obligațiile părților, măsurile de asigurare a unei prelucrări legale și echitabile și de respectare a drepturilor persoanei vizate, măsurile necesare pentru asigurarea securității prelucrărilor, măsurile necesare a fi instituite pentru asigurarea confidențialității și limitările legate de scop;

b) comunicarea se efectuează în baza unei solicitări scrise, care trebuie să cuprindă temeiul legal, care abilităază persoana/autoritatea solicitantă să prelucreze categoriile de date solicitate în scopul urmărit, scopul prelucrării și datele solicitate.

(3) Comunicarea datelor cu caracter personal de către operatori și persoanele împuternicite de operatori se poate face și online, cu respectarea dispozițiilor alin. (1) și (2) și asigurarea securității sistemelor de comunicații ale 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. 19. — (1) Cererile pentru comunicarea datelor cu caracter personal adresate operatorilor și persoanelor împuternicite de operatori trebuie să conțină datele de identificare ale solicitantului, precum și motivarea și scopul cererii, conform prevederilor legale sau obligațiilor cuprinse în tratate la care România sau Guvernul României 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 sau Guvernul României 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 persoanele împuternicite de operatori 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 persoanele împuternicite de operatori atenționează destinatarii asupra interdicției de a prelucra datele pentru alte scopuri decât cele specificate în cererea de comunicare.

CAPITOLUL V

Măsuri de asigurare a exercitării drepturilor persoanelor vizate

Art. 20. — (1) Exercițarea drepturilor de către persoana vizată se face în conformitate cu prevederile capitolului III din RGPD și, după caz, ale art. 13-18 din Legea nr. 363/2018, iar soluționarea acestora se face potrivit procedurilor proprii ale operatorilor MAI pentru soluționarea cererilor de exercitare a drepturilor de către persoana vizată.

(2) Operatorii și persoanele împuternicite de operatori dispun măsuri pentru ca în spațiile accesibile publicului să existe mijloace de informare a persoanei vizate care să cuprindă drepturile conferite de lege, precum și ghidul pentru exercitarea drepturilor de către persoana vizată.

(3) Ghidul trebuie să conțină detalierea drepturilor persoanei vizate, dar și modalitatea practică pentru depunerea cererilor de către persoana vizată, datele de contact ale operatorului, ale responsabilului cu protecția datelor personale și modalitatea de transmitere a răspunsurilor. Ghidul se afișează, după caz, și pe pagina de internet a operatorului.

(4) Operatorii și persoanele împuternicite de operatori afișează, după caz, pe pagina de internet formulare-tip de cereri pentru exercitarea drepturilor de către persoana vizată.

(5) Exercițarea drepturilor persoanei vizate poate fi limitată în condițiile prevăzute la art. 15, 17 și art. 18 alin. (8) din Legea nr. 363/2018 sau în condițiile art. 23 din RGPD, ținând seama de domeniul în care a avut loc prelucrarea, sau în alte situații prevăzute de lege.

(6) Operatorii și persoanele împuternicite de operatori țin evidența cazurilor prevăzute la alin. (5) și o comunică sub formă statistică, anual, ORPDP, până la 31 ianuarie, pentru anul precedent, în cadrul analizei prevăzute de art. 5 alin. (1) lit. e).

(7) Evidența cazurilor prevăzute la alin. (5) trebuie să cuprindă cel puțin următoarele informații: măsura luată, motivul care a stat la baza măsurii, data în care a fost dispusă măsura și perioada de aplicare a măsurii. În situația omisiunii și limitării parțiale, la încetarea perioadei de aplicare a măsurii, structura care a invocat măsura transmite informațiile aferente prelucrării responsabilului cu protecția datelor în vederea informării persoanei vizate.

(8) Operatorii și persoanele împuternicite de operatori elaborează proceduri interne privind stabilirea modului de soluționare a cererilor persoanelor vizate, inclusiv mecanismul de determinare a perioadei care face obiectul verificărilor în scopul soluționării acestor cereri, conform structurii-cadru prevăzute la anexa nr. 4.

(9) Pentru aparatul central al MAI, obligațiile prevăzute la alin. (2)-(4) se aduc la îndeplinire prin grija ORPDP.

TITLUL II

Măsuri tehnice

Art. 21. — (1) Pentru fiecare utilizator de date cu caracter personal, administratorul sistemului de evidență automat care prelucrează date cu caracter personal stabilește un cont unic de acces în sistem care să permită identificarea, autentificarea și autorizarea operațiunilor, asigurând totodată înregistrarea operațiunilor efectuate.

(2) Identificarea și autentificarea utilizatorului într-un sistem informatic care prelucrează date cu caracter personal se poate realiza prin introducerea unui cod de identificare de la tastatură (nume de utilizator) însoțit de introducerea unei parole și/sau prin utilizarea unui dispozitiv electronic de tip smart card/token însoțit de introducerea unui cod PIN.

(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, aceștia având posibilitatea să opteze, după caz, pentru instituirea unei autentificări multiple, combinând oricare dintre modalitățile prevăzute la alin. (2).

(4) Smartcardurile, tokenurile, codurile de identificare, numele de utilizator, parolele și codurile PIN sunt unice, personale și netransmisibile. Se interzice folosirea lor în comun de către mai mulți utilizatori.

(5) Parolele trebuie să aibă minimum 10 caractere alfanumerice — litere mari, litere mici, cifre, semne și caractere speciale —, iar introducerea acestora nu trebuie să conducă la identificarea lor prin afișarea pe ecran. Se interzice păstrarea parolei la vedere astfel încât să nu fie accesibilă altor persoane.

(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 parola/codul PIN și codul de identificare sau numele de utilizator. 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 informatic care prelucrează date cu caracter personal ia măsurile necesare pentru activarea unui mesaj de avertizare după a patra 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 4 ori. La a cincea introducere greșită, contul va fi blocat”. 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 de sistem.” Aceste măsuri sunt obligatorii și în fazele de proiectare și implementare a sistemelor informatice ce prelucrează date cu caracter personal.

(9) La începutul sesiunii de lucru, interfața grafică a sistemului informatic care prelucrează date cu caracter personal trebuie să afișeze un mesaj de avertizare privind obligativitatea păstrării confidențialității datelor cu caracter personal prelucrate, precum și referitor la auditarea tuturor operațiunilor efectuate de către operator. Mesajul afișat la începutul sesiunii va cuprinde următorul text: „Atenție! Ați accesat un sistem informatic proprietatea MAI care prelucrează date cu caracter personal. Aveți obligativitatea respectării legislației privind prelucrarea datelor cu caracter personal, orice activitate fiind auditată. Nerespectarea acestor norme atrage, potrivit legii, răspunderea disciplinară, civilă sau materială, după caz.”

(10) În situația în care pe sistemul informatic sunt gestionate și informații clasificate, mesajul afișat la începutul sesiunii va cuprinde următorul text: „Atenție! Ați accesat un sistem informatic proprietatea MAI care prelucrează date cu caracter personal și informații clasificate de nivel secrete de serviciu/secrete de stat de nivel secret/strict secret/strict secret de importanță deosebită, după caz. Aveți obligativitatea respectării legislației în vigoare, orice activitate fiind auditată. Nerespectarea acestor norme atrage, potrivit legii, răspunderea disciplinară, civilă sau materială, după caz.”

Art. 22. — (1) În timpul programului de lucru, dispozitivele de autentificare menționate la art. 21 alin. (2), precum și cartelele de acces se păstrează permanent asupra utilizatorului. În afara programului de lucru, dispozitivele de autentificare menționate la art. 21 alin. (2) se păstrează în fișet/casetă metalică încuiat/încuiată și sigilat/sigilată.

(2) Se interzice păstrarea 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, parole de acces și PIN-uri vor fi distruse, cu excepția situațiilor în care legislația în domeniul arhivistic interzice în mod expres acest lucru.

(4) Șeful nemijlocit al utilizatorului informează conducerea operatorului despre incidența situațiilor prevăzute la art. 11.

(5) Ulterior informării prevăzute la alin. (4), conducerea operatorului dispune de îndată măsuri astfel încât conturile de utilizator să fie suspendate sau revocate.

(6) Utilizatorul aflat în una dintre situațiile prevăzute la art. 11 are obligația de a preda dispozitivele de autentificare menționate la art. 21 alin. (2), precum și cartelele de acces structurii emitente.

(7) După încetarea situațiilor prevăzute la art. 11 alin. (1) și (2), operatorul dispune reactivarea contului de utilizator.

(8) Sistemul informatic care prelucrează date cu caracter personal trebuie configurat astfel încât să asigure dezactivarea automată a codurilor de identificare și a cartelelor de acces/smart card/token care nu au fost folosite o perioadă de 4 luni pentru utilizatori, respectiv 6 luni pentru administratorii aplicației; acestea sunt menținute în istoricul de utilizatori.

(9) 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.

(10) Revocarea/Suspendarea manuală a conturilor de utilizator se va face numai de către administratorul sistemului informatic care prelucrează date cu caracter personal sau de către administratorii de utilizatori aferenți.

(11) Fiecare operator permite accesul utilizatorilor la sisteme de evidență a datelor cu caracter personal manuale numai pe baza unei liste nominale aprobate de conducerea operatorului/șeful acestuia, iar responsabilul cu elaborarea și actualizarea listei se desemnează prin dispoziția zilnică a conducerii operatorului.

(12) Pentru accesul personalului la sistemele informatice care prelucrează datele cu caracter personal deținute de alți operatori, conturile de utilizator se obțin în baza solicitării scrise și motivate a structurii/unității/instituției interesate sau pe baza unor protocoale încheiate în acest sens.

Art. 23. — (1) La propunerea șefului nemijlocit al utilizatorului, conducerea operatorului stabilește fiecărui utilizator tipurile de acces și operațiunile permise acestuia, strict necesare pentru îndeplinirea atribuțiilor de serviciu.

(2) Cu ocazia proiectării, întreținerii, actualizării de către dezvoltatorul public/privat a sistemelor informatice care prelucrează datele cu caracter personal, se interzice accesul specialiștilor 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 care asigură suportul tehnic, sens în care trebuie să semneze un angajament de confidențialitate.

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

Art. 24. — (1) În cazul încălcării securității datelor cu caracter personal, conducerea operatorului, raportat la prevederile art. 33 și 34 din RGPD, respectiv art. 36 și 39 din Legea nr. 363/2018, în funcție de scopul în care sunt prelucrate datele, va dispune evaluarea încălcării și notificarea ANSPDCP și/sau informarea persoanei vizate/persoanelor vizate, după caz.

(2) În evaluare va fi implicat responsabilul cu protecția datelor desemnat la nivelul operatorului, o persoană din cadrul structurii/compartimentului unde a avut loc încălcarea securității datelor și, după caz, o persoană din cadrul structurii/compartimentului de IT&C.

(3) Notificarea ANSPDCP și informarea persoanei vizate se vor realiza de către responsabilul cu protecția datelor.

Art. 25. — (1) Datele cu caracter personal prelucrate prin mijloace automatizate folosite de operatori sau de persoanele împuternicite de operatori sunt salvate, prin copii de siguranță, ori de câte ori este nevoie sau la un interval de timp stabilit de conducerea operatorului sau a persoanelor împuternicite de operatori, în funcție de tipul operațiunilor efectuate, mărimea, volumul și importanța acestor sisteme informatice care prelucrează date cu caracter personal, care nu poate depăși 6 luni.

(2) Operatorii și persoanele împuternicite de operatori țin evidența copiilor de siguranță.

(3) Conducerea operatorului sau a persoanei împuternicite de operator desemnează personal tehnic de specialitate care trebuie să aibă ca atribuție de serviciu și executarea copiilor de siguranță ale sistemelor informatice deținute/create, precum și, după caz, ale programelor/aplicațiilor/codului sursă utilizate în prelucrarea datelor cu caracter personal.

(4) Conducerea operatorului sau a persoanei împuternicite de operator dispune 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. Accesul la copiile de siguranță se acordă ANSPDCP, în exercitarea atribuțiilor sale legale.

(5) Copiile de siguranță se vor realiza în mod automat și vor fi stocate pe sisteme dedicate salvării copiilor de siguranță.

(6) Conducerea operatorului sau a persoanei împuternicite de operator poate institui măsuri suplimentare de siguranță, precum sisteme de monitorizare video, atât pentru accesul în încăpere, cât și pentru asigurarea integrității patrimoniului operatorului sau a persoanei împuternicite de operator, după caz.

Art. 26. — (1) Accesul fizic în încăperile în care se află echipamente tip server sau storage care stochează date cu

caracter personal este strict limitat la personalul desemnat de conducerea operatorului sau a persoanei împuternicite de operator 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) Sistemele informatice care prelucrează 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 30 de minute, stabilită în funcție de operațiunile care trebuie executate.

(4) Sistemele informatice care prelucrează date cu caracter personal trebuie prevăzute cu facilitatea închiderii automate a sesiunii de lucru după 120 de minute de la deschiderea sesiunii de lucru.

(5) Terminalele de acces folosite în relația cu publicul se poziționează astfel încât datele afișate să fie vizualizate numai de utilizatori sau să poată fi posibilă aplicarea pe ecranul acestora a unor filtre care să micșoreze unghiul de vizibilitate (filtre de confidențialitate). 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. 27. — (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 cel puțin:

- a) codul de identificare a stației de lucru folosite sau adresa IP și codul/numele utilizatorului, după caz;
- b) categoriile de informații accesate;
- c) tipul operațiunii de prelucrare;
- d) informații care să facă posibilă identificarea motivului prelucrării datelor cu caracter personal care trebuie să permită identificarea documentului/situației concrete care a stat la baza și a justificat prelucrarea datelor;

e) codul operației executate sau programul folosit;

f) data accesului — an, lună, zi, ora, minutul, secunda.

(3) Aplicația înregistrează orice încercare de acces neautorizat, sens în care administratorul sistemului de evidență informează responsabilul/structura responsabilă cu protecția datelor cu caracter personal cu privire la alertă și împreună cu acesta verifică împrejurările producerii alertei, propunând conducerii operatorului măsurile ce se impun.

(4) Fără a aduce atingere regulilor în materie de păstrare a logurilor la nivel național, prevăzute de actele legislative europene și naționale care reglementează instituirea, funcționarea și utilizarea sistemelor de informații respective, logurile se păstrează cel puțin 2 ani, în funcție de necesitatea asigurării disponibilității datelor pentru operator sau persoana împuternicită de 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) Operatorul sau persoana împuternicită de operator instituie mecanisme de ținere a evidenței operațiunilor de consultare a datelor cu caracter personal conținute în sisteme de evidență manuale.

(6) Declanșarea unei investigații a cărei finalizare depășește termenul stabilit de operator, conform alin. (4), atrage prelungirea perioadei de păstrare, dar nu mai mult de 3 ani de la momentul declanșării acesteia.

(7) Informațiile din fișierele *log* sunt accesate în următoarele situații:

a) de către operatorul sau persoana împuternicită de operator care gestionează sistemul de evidență, pentru utilizatorii proprii, în scopul efectuării de autoevaluări/automonitorizări cu privire la legalitatea și la oportunitatea operațiunilor, pentru soluționarea cererilor de acces, pentru cercetări și pentru verificări de ordin administrativ ori de control intern și pentru valorificarea informațiilor, conform destinației sistemului informatic;

b) de către operatorul sau persoana împuternicită de operator care gestionează sistemul de evidență, pentru toți utilizatorii sistemului, pentru soluționarea cererilor de acces;

c) de către operatorul sau persoana împuternicită de operator care gestionează sistemul de evidență, cu privire la utilizatorii altor operatori, la solicitarea acestora adresată în scopul efectuării de autoevaluări/automonitorizări cu privire la legalitatea și la oportunitatea operațiunilor, pentru soluționarea cererilor de acces, pentru cercetări și pentru verificări de ordin administrativ ori de control intern și pentru valorificarea informațiilor, conform destinației sistemului informatic;

d) la solicitarea organelor de urmărire penală de comunicare a datelor informatice, în condițiile stabilite de Codul de procedură penală;

e) la solicitarea instituțiilor și a structurilor cu atribuții speciale conferite prin lege în domeniul asigurării securității naționale, a securității infrastructurii cibernetice a MAI ori în cadrul activităților de informații, de contrainformații și de protecție;

f) la solicitarea ANSPDCP în cadrul exercitării atribuțiilor de investigare și control ale acesteia.

Art. 28. — (1) Conducerea operatorului sau a persoanei împuternicite de operator care prelucrează date cu caracter personal dispune luarea măsurilor tehnice adecvate pentru identificarea eventualelor disfuncționalități în ceea ce privește funcționarea sistemelor informatice care prelucrează date cu caracter personal și/sau sistemelor de comunicații folosite pentru transmiterea datelor.

(2) Responsabilul/Structura responsabilă cu protecția datelor cu caracter personal împreună cu administratorul sistemelor informatice care prelucrează date cu caracter personal efectuează periodic, prin sondaj sau la nevoie, controlul autentificărilor și tipurilor de acces.

(3) Responsabilul/Structura responsabilă cu protecția datelor cu caracter personal împreună cu administratorul de rețea efectuează periodic, prin sondaj sau la nevoie, controlul respectării măsurilor de securitate specifice folosite pentru transmiterea datelor cu caracter personal.

(4) Rezultatul controlului, eventualele disfuncționalități identificate, precum și măsurile de remediere a acestora se consemnează într-un raport care se supune aprobării conducerii operatorului sau a persoanei împuternicite de operator/șefului structurii/unității/instituției respective. Modalitatea de realizare a controlului, precum și conținutul raportului se stabilesc printr-o procedură proprie.

(5) Conducerea operatorului sau a persoanei împuternicite de operator dispune 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.

(6) 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. 29. — Conducerea operatorului sau a persoanei împuternicite de operator dispune 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 și/sau folosirii de către personalul MAI a altor produse 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) securizarea echipamentelor mobile/amovibile, destinate stocării datelor cu caracter personal;

d) implementarea unor produse software/soluții informatice de contracarare a vulnerabilităților și amenințărilor informatice și de securitate a sistemelor informatice;

e) implementarea unor măsuri suplimentare de securitate privind identificarea, prevenirea, partajarea, transferul sau utilizarea într-un mod nesigur/nepotrivit a datelor cu caracter personal;

f) auditarea întregii infrastructuri hardware și software în vederea identificării vulnerabilităților și activității utilizatorilor care pot genera incidente de securitate; de asemenea, se va lua în considerare transmiterea acestora către o soluție de management al evenimentelor și informațiilor de securitate — SIEM.

Art. 30. — (1) Operatorul sau persoana împuternicită de operator se asigură că, atunci când sunt prelucrate date cu caracter personal prin mijloace manuale (documente pe suport hârtie, agende, formulare, date care sunt stocate în mod obișnuit în format electronic, dar au fost tipărite din anumite considerente etc.), sunt luate măsuri de securitate adecvate pentru a preveni accesul neautorizat, pierderea sau distrugerea datelor.

(2) Operatorul sau persoana împuternicită de operator se asigură că mijloacele manuale se păstrează într-un loc sigur unde persoanele neautorizate nu pot avea acces. Prezentele instrucțiuni se aplică, de asemenea, și asupra datelor care sunt stocate în mod obișnuit în format electronic, dar au fost tipărite din anumite considerente, care țin de specificul anumitor activități.

(3) Utilizatorii au obligația ca la terminarea programului de lucru să depoziteze mijloacele manuale care conțin date cu caracter personal în dulapuri sau încăperi închise cu cheie sau cu un alt mecanism de securizare. Mijloacele manuale care vizează cercetarea penală și care conțin date cu caracter personal, precum și cele care conțin date speciale vor fi întotdeauna depozitate în dulapuri închise la finalizarea programului de lucru.

(4) Atunci când folosesc mijloace manuale care conțin date cu caracter personal în încăperi destinate publicului, utilizatorii au obligația să se asigure că datele cu caracter personal nu sunt vizibile altor persoane, cu excepția persoanei vizate de prelucrare, când accesul acesteia la date nu afectează caracterul operativ al măsurilor ce trebuie luate.

(5) Obligația de la alin. (4) vizează și prelucrările realizate de utilizatori în spațiul public.

(6) Documentele elaborate de structurile/unitățile/instituțiile MAI, care conțin date cu caracter personal, se marchează în subsolul fiecărei pagini, cu excepția documentelor clasificate, cu următoarele texte, după caz: „Document care conține date cu caracter personal protejate de prevederile Regulamentului (UE)

2016/679!” sau „Document care conține date cu caracter personal protejate de prevederile Legii nr. 363/2018!”, în funcție de scopul în care sunt prelucrate datele.

(7) Conducerea operatorului sau a persoanei împuternicite de operator stabilește condițiile 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. Extrasele din baza de date vor fi imprimate numai în măsura în care este necesar și proporțional prin raportare la motivul efectuării interogării.

(8) La finalizarea operațiunilor de prelucrare, în situația în care mijloacele manuale au fost înregistrate, acestea vor urma regulile de clasare și arhivare, în conformitate cu legislația specifică acestui domeniu.

(9) În situația în care mijloacele manuale nu au fost înregistrate și scopul prelucrării a fost atins, acestea se distrug prin metode care garantează imposibilitatea reconstruirii acestora (de exemplu, tocător tip cross-cut sau micro-cut, incinerare autorizată etc).

Art. 31. — Procedurile proprii elaborate de operatori, potrivit art. 5 alin. (1) lit. d) și art. 7 alin. (1) lit. a), trebuie să cuprindă, cel puțin:

- a) modalități de administrare a conturilor de utilizator;
- b) modalități de automonitorizare;
- c) modalități de control al accesului în încăperi în care se prelucreză date cu caracter personal;
- d) modalități de asigurare a confidențialității, integrității și disponibilității datelor cu caracter personal;
- e) modalități privind securitatea transmisiilor de date și accesul securizat la aceste mijloace de transmitere a datelor;
- f) modalități de gestionare a riscurilor și incidentelor de securitate;
- g) soluționarea cererilor formulate de către persoana vizată cu privire la prelucrările datelor cu caracter personal;
- h) activitățile desfășurate în cazul încălcării securității datelor cu caracter personal.

Art. 32. — Nerespectarea dispozițiilor prezentelor instrucțiuni poate atrage, potrivit legii, răspunderea disciplinară, civilă sau materială, după caz.

Art. 33. — Pentru sistemele informatice aflate în exploatare, administratorii acestora vor actualiza măsurile tehnice conform prevederilor prezentelor instrucțiuni, în termen de 12 luni de la intrarea lor în vigoare.

Art. 34. — (1) Prezentele instrucțiuni se publică în Monitorul Oficial al României, Partea I, și intră în vigoare în termen de 15 zile de la data publicării.

(2) Anexele nr. 1-4 fac parte integrantă din prezentele instrucțiuni.

(3) La data intrării în vigoare a prezentelor instrucțiuni, Instrucțiunile ministrului administrației și internelor nr. 27/2010 privind măsurile de natură organizatorică și tehnică pentru asigurarea securității prelucrărilor de date cu caracter personal efectuate de către structurile/unitățile Ministerului Afacerilor Interne, publicate în Monitorul Oficial al României, Partea I, nr. 98 din 12 februarie 2010, se abrogă.

(4) Toate trimiterile la Instrucțiunile ministrului administrației și internelor nr. 27/2010 se interpretează ca trimiteri la prezentele instrucțiuni.

p. Viceprim-ministru, ministrul afacerilor interne,

Silviu Nicu Macovei,
secretar de stat

REGISTRU DE EVIDENȚĂ

a cererilor persoanelor vizate pentru exercitarea drepturilor conferite de prevederile Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), precum și de cele ale Legii nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date

Intrare

Nr. curent de intrare	Data înregistrării Anul		Modalitatea de intrare a cererii	Numele, prenumele și adresa (domiciliul) persoanei vizate	Conținutul pe scurt al cererii	Act normativ aplicabil cererii		Termenul de rezolvare
	Luna	Ziua				Regulamentul (UE) 2016/679	Legea nr. 363/2018	

Ieșire

Data ieșirii Anul		Modalitatea de transmitere a răspunsului	Cât a durat rezolvarea		Rezultatul cererii	Unde s-a clasat	Observații (motivul prelungirii termenului etc.)
Luna	Ziua		În termen	Prelungirea termenului			

DECLARAȚIE

Subsemnatul/Subsemnata,, născut(ă) la data de, 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 sau civilă, în raport cu gravitatea faptei, potrivit legii.

Data

Semnătura

Dată în prezența

.....

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

Document care conține date cu caracter personal protejate de prevederile Regulamentului (UE) 2016/679!

REGISTRU DE EVIDENȚĂ**a operatorilor din cadrul Ministerului Afacerilor Interne**

Nr. crt.	Denumirea și datele de contact ale structurii/unității/instituției Ministerului Afacerilor Interne	Responsabilul/Coordonatorul compartimentului (date de contact)	Scopul prelucrării/Baza legală	Datele prelucrate	Categorii de persoane vizate	Destinatari	Măsurile organizatorice și tehnice implementate	Observații

STRUCTURA - CADRU

a procedurii privind soluționarea cererilor formulate de către persoana vizată în exercitarea drepturilor prevăzute de Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) și de Legea nr. 363/2018 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, descoperirii, cercetării, urmăririi penale și combaterii infracțiunilor sau al executării pedepselor, măsurilor educative și de siguranță, precum și privind libera circulație a acestor date

1. Scop

Cuprinde prevederi referitoare la:

- stabilirea unui set unitar de reguli pentru soluționarea cererilor adresate operatorului, formulate de către persoana vizată în exercitarea drepturilor prevăzute de Regulamentul (UE) 2016/679 și de Legea nr. 363/2018;
- asigurarea respectării drepturilor persoanelor vizate în conformitate cu prevederile Regulamentului (UE) 2016/679, precum și ale Legii nr. 363/2018, după caz, în funcție de scopul prelucrării.

2. Domeniu de aplicare

Cuprinde prevederi referitoare la:

- modul în care se organizează și se desfășoară activitatea pentru soluționarea cererilor formulate de către persoana vizată în exercitarea drepturilor prevăzute de Regulamentul (UE) 2016/679 și de Legea nr. 363/2018;
- compartimentul/compartimentele care implementează procedura din cadrul operatorului Ministerului Afacerilor Interne.

3. Documente de referință

Cuprinde enumerarea actelor normative și documentelor cu rol de reglementare.

4. Definiții și abrevieri

Cuprinde prevederi referitoare la termenii relevanți pentru înțelegerea conținutului procedurii, conform definițiilor din actele normative, precum și explicitarea acronimelor utilizate.

5. Descrierea procedurii

Cuprinde prevederi referitoare la:

- scopurile prelucrării de date cu caracter personal de la nivelul operatorului Ministerului Afacerilor Interne;
- enumerarea drepturilor persoanei vizate;
- condițiile privind cererea persoanei vizate — stabilirea naturii juridice a cererii;
- situațiile în care se solicită informații suplimentare pentru a identifica persoana vizată (spre exemplu: solicitarea a venit de pe o adresă de e-mail pseudonimizată, nu sunt atașate copii după un document de identitate, nu este anexată împuternicirea avocațională etc.);
- situațiile în care se refuză cererea (spre exemplu: nu poate să fie identificată persoana vizată, persoana vizată depune cereri cu același conținut repetitiv etc.);
- termenul în care operatorul este obligat să comunice răspunsul persoanei vizate în funcție de scopul și motivele prelucrării datelor;
- mecanismul de determinare a perioadei care face obiectul verificărilor în scopul soluționării acestor cereri;
- modalitatea de depunere a cererii persoanei vizate (la sediul operatorului, înaintată prin poștă ori trimisă la adresa de e-mail a acestuia);
- modalitatea de înregistrare și repartizare a cererilor;
- modalitatea de soluționare a cererilor persoanei vizate și arhivarea documentelor aferente soluționării cererilor.

6. Responsabilități

Cuprinde prevederi referitoare la responsabilitățile personalului implicat în activitatea de primire, înregistrare, repartizare a cererilor, întocmire, avizare și aprobare a răspunsului către persoana vizată, respectiv expedierea acestuia.

7. Dispoziții finale

Cuprinde prevederi referitoare la modul de implementare a procedurii, data intrării în vigoare etc.

8. Anexe

Cuprinde enumerarea tuturor elementelor atașate corpului procedurii: diagrama de proces, formulare, modele de documente etc.

9. Cuprins

Include o listă cu toate elementele componente ale procedurii și numărul paginii pentru fiecare dintre acestea.

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR



„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; 012329
C.I.F. RO427282, IBAN: RO55RNCB0082006711100001 BCR
și IBAN: RO12TREZ7005069XXX000531 DTCPMB (alocat numai persoanelor juridice bugetare)
Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, www.monitoruloficial.ro
Relații cu publicul: șos. Panduri nr. 1, bloc P33, sectorul 5, București; 050651.
Tel. 021.401.00.73, 021.401.00.78/79/83.
Pentru publicări, încărcăți actele pe site, la: <https://www.monitoruloficial.ro>, secțiunea Publicări.

