

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÎRE nr. ____
din _____

**Pentru aprobarea proiectului de lege privind protecția
persoanelor fizice în ceea ce privește prelucrarea datelor
cu caracter personal și privind libera circulație a acestor date**

Guvernul HOTĂRĂȘTE:

Se aprobă și se prezintă Parlamentului spre examinare proiectul de lege privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.

PRIM-MINISTRU

Contrasemnează:

Ministrul Justiției

LEGE
privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date

Prezenta lege transpune Regulamentul Uniunii Europene 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).

Parlamentul adoptă prezenta lege organică

CAPITOLUL I
DISPOZIȚII GENERALE

Articolul 1. Obiect și obiective

- (1) Prezenta lege asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice și în special a dreptului acestora la protecția datelor cu caracter personal.
- (2) Libera circulație a datelor cu caracter personal în interiorul Republicii Moldova nu poate fi restricționată sau interzisă din motive legate de protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.

Articolul 2. Domeniul de aplicare material

- (1) Prezenta lege se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.
- (2) Prezenta lege nu se aplică prelucrării datelor cu caracter personal:
 - a) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;
 - b) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora
- (3) Prezenta lege nu aduce atingere aplicării Legii nr. 284/2004 privind serviciile societății informaționale, în special normelor privind răspunderea furnizorilor de servicii intermediari, prevăzute la art.14-17 din legea menționată.

Articolul 3. Domeniul de aplicare teritorial

- (1) Prezenta lege se aplică prelucrării datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator pe teritoriul Republica Moldova, indiferent dacă prelucrarea are loc sau nu pe teritoriul Republicii Moldova.
- (2) Prezenta lege se aplică prelucrării datelor cu caracter personal ale unor persoane vizate care se află în Republica Moldova de către un operator sau o persoană împuternicită de operator care nu este stabilit(ă) în Republica Moldova, atunci când activitățile de prelucrare sunt legate de:

- a) oferirea de bunuri sau servicii unor astfel de persoane vizate în Republica Moldova, indiferent dacă se solicită sau nu efectuarea unei plăți de către persoana vizată;
- b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Republicii Moldova.

(3) Prezenta lege se aplică prelucrării datelor cu caracter personal de către un operator care nu este stabilit în Republica Moldova, ci într-un loc în care dreptul intern se aplică în temeiul dreptului internațional public.

Articolul 4. Noțiuni

(1) În sensul prezentei legi:

a) date cu caracter personal – reprezintă orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

b) prelucrare – reprezintă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;

c) restricționarea prelucrării – reprezintă marcarea datelor cu caracter personal stocate cu scopul de a limita prelucrarea viitoare a acestora;

d) creare de profiluri – reprezintă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau prevedea aspecte privind performanța la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locul în care se află persoana fizică respectivă sau deplasările acesteia;

e) pseudonimizare – reprezintă prelucrarea datelor cu caracter personal într-un asemenea mod încât acestea să nu mai poată fi atribuite unei anume persoane vizate fără a se utiliza informații suplimentare, cu condiția ca aceste informații suplimentare să fie stocate separat și să facă obiectul unor măsuri de natură tehnică și organizatorică care să asigure neatribuirea respectivelor date cu caracter personal unei persoane fizice identificate sau identificabile;

f) sistem de evidență a datelor – reprezintă orice set structurat de date cu caracter personal accesibile conform unor criterii specifice, fie ele centralizate, descentralizate sau repartizate după criterii funcționale sau geografice;

g) operator – reprezintă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal; atunci când scopurile și mijloacele prelucrării sunt stabilite prin actele normative, operatorul sau criteriile specifice pentru desemnarea acestuia pot fi prevăzute în actele normative.

h) persoană împuternicită de operator – reprezintă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează datele cu caracter personal în numele operatorului;

i) destinatar – reprezintă persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căreia îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Cu toate acestea, autoritățile publice cărora li se pot comunica date cu caracter personal în

cadrul unei anumite anchete în conformitate cu actele normative nu sunt considerate destinatari; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

i) *parte terță* – reprezintă o persoană fizică sau juridică, autoritate publică, agenție sau organism altul decât persoana vizată, operatorul, persoana împuternicită de operator și persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date cu caracter personal;

j) *consimțământ* - al persoanei vizate reprezintă orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate;

k) *cifra de facere mondială* – reprezintă totalul vânzărilor realizate (facturate) pe parcursul unui exercițiu fiscal al operatorului de date;

l) *încălcarea securității datelor cu caracter personal* – reprezintă o încălcare a securității care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

m) *date genetice* – reprezintă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

n) *date biometrice* – reprezintă date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;

o) *date privind sănătatea* – reprezintă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;

p) *reprezentant* – reprezintă o persoană fizică sau juridică stabilită în Republica Moldova sau Spațiul Economic European, desemnată în scris de către operator sau persoana împuternicită de operator în temeiul art. 27, care reprezintă operatorul sau persoana împuternicită în ceea ce privește obligațiile lor respective care le revin în temeiul prezentei legi;

q) *întreprindere* – reprezintă o persoană fizică sau juridică ce desfășoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociații care desfășoară în mod regulat o activitate economică;

r) *grup de întreprinderi* – reprezintă o întreprindere care exercită controlul și întreprinderile controlate de aceasta;

s) *reguli corporatiste obligatorii* – reprezintă politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul Republicii Moldova, în ceea ce privește transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe țări în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună cu excepția țărilor din Spațiul Economic European;

ș) *autoritate de supraveghere* – reprezintă o autoritate publică independentă instituită sau desemnată în temeiul art. 51;

t) *serviciile societății informaționale* – reprezintă un serviciu astfel cum este definit de Legea nr. 284/2004 privind serviciile societății informaționale;

ț) *organizație internațională* – reprezintă o organizație și organismele sale subordonate reglementate de dreptul internațional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe țări sau în temeiul unui astfel de acord.

CAPITOLUL II

PRINCIPII

Articolul 5. Principiile prelucrării datelor cu caracter personal

Datele cu caracter personal sunt:

- a) principiul legalității, echității și transparenței – datele cu caracter personal sunt prelucrate în mod legal, echitabil și transparent față de persoana vizată;
- b) principiul limitării legate de scop – datele cu caracter personal sunt colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale, în conformitate cu art. 70 alin. (1) ;
- c) principiul reducerii la minimum a datelor – datele cu caracter personal sunt adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate;
- d) principiul exactității – datele cu caracter personal sunt exacte și, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere;
- d) principiul limitării legate de stocare – datele cu caracter personal sunt păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu art. 70 alin. (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezenta lege în vederea garantării drepturilor și libertăților persoanei vizate;
- f) principiul integrității și confidențialității – datele cu caracter personal sunt prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare.

(2) Operatorul este responsabil de respectarea alin.(1) și poate demonstra această respectare.

Articolul 6. Legalitatea prelucrării

(1) Prelucrarea este legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:

- a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
- b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
- c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;
- d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
- e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul;

f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil. Lit. (f) nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor.

(2) Pot fi menținute sau introduse dispoziții mai specifice de adaptare a aplicării normelor prezentei legi în ceea ce privește prelucrarea în vederea respectării alin. (1) lit. c) și e) prin definirea unor cerințe specifice mai precise cu privire la prelucrare și a altor măsuri de asigurare a unei prelucrări legale și echitabile, inclusiv pentru alte situații concrete de prelucrare, astfel cum este prevăzut în capitolul VIII.

(3) Temeiul pentru prelucrarea menționată la alin. (1) lit. (c) și (e) trebuie să fie prevăzut în actele normative. Scopul prelucrării este stabilit pe baza respectivului temei juridic sau, în ceea ce privește prelucrarea menționată la alin. (1) lit. (e), este necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcții publice atribuite operatorului. Respectivul temei juridic poate conține dispoziții specifice privind adaptarea aplicării normelor prezentei legi, printre altele: condițiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date care fac obiectul prelucrării; persoanele vizate; entitățile cărora le pot fi divulgate datele și scopul pentru care respectivele date cu caracter personal pot fi divulgate; limitările legate de scop; perioadele de stocare; și operațiunile și procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale și echitabile cum sunt cele pentru alte situații concrete de prelucrare astfel cum sunt prevăzute în capitolul VIII. Actele normative urmăresc un obiectiv de interes public și este proporțional cu obiectivul legitim urmărit.

(4) În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimțământul persoanei vizate sau pe actele normative, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja obiectivele menționate la art. 23 alin.(1), operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, ia în considerare, printre altele:

- a) orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;
- b) contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și operator;
- c) natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, în conformitate cu art. 9, sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni, în conformitate cu art. 10;
- d) posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;
- e) existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.

Articolul 7. Condiții privind consimțământul

(1) În cazul în care prelucrarea se bazează pe consimțământ, operatorul trebuie să fie în măsură să demonstreze că persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal.

(2) În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o

formă care o diferențiază în mod clar de celelalte aspecte, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Nicio parte a respectivei declarații care constituie o încălcare a prezentei legi nu este obligatorie.

(3) Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragera consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragera consimțământului se face la fel de simplu ca acordarea acestuia.

(4) Atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

Articolul 8. Condiții aplicabile în ceea ce privește consimțământul copiilor în legătură cu serviciile societății informaționale

(1) În cazul în care se aplică art. 6 alin. (1) lit. (a), în ceea ce privește oferirea de servicii ale societății informaționale în mod direct unui copil, prelucrarea datelor cu caracter personal ale unui copil este legală dacă copilul are cel puțin vârsta de 14 ani. Dacă copilul are sub vârsta de 14 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de titularul răspunderii părintești asupra copilului.

(2) Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că titularul răspunderii părintești a acordat sau a autorizat consimțământul, ținând seama de tehnologiile disponibile.

(3) Alin. (1) nu afectează dreptul general al contractelor, cum ar fi normele privind valabilitatea, încheierea sau efectele unui contract în legătură cu un copil.

Articolul 9. Prelucrarea de categorii speciale de date cu caracter personal

(1) Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.

(2) Alin. (1) nu se aplică în următoarele situații:

- a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care actele normative prevăd ca interdicția prevăzută la alin.(1) să nu poată fi ridicată prin consimțământul persoanei vizate;
- b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de actele normative ori de un contract colectiv de muncă care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;
- c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de ași

da consimțământul;

- d) prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;
- e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;
- f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;
- g) prelucrarea este necesară din motive de interes public major, în baza actelor normative, care sunt proporționale cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;
- h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul actelor normative sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alin. (3);
- i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul actelor normative, care prevăd măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional;
- j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu art. 70 alin. (1), în baza actelor normative, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate.

(3) (3) Datele cu caracter personal menționate la alin. (1) pot fi prelucrate în scopurile menționate la alin. (2) lit.h) în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul actelor normative sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul actelor normative.

(4) (4) După caz, pot fi menținute sau introduse condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea de date genetice, date biometrice sau date privind sănătatea.

Articolul 10. Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni

Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe în temeiul art. 6 alin. (1) se efectuează numai sub controlul unei autorități de stat, sau atunci când prelucrarea este autorizată de actele normative care prevăd garanții adecvate pentru drepturile și libertățile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat.

Articolul 11. Prelucrarea care nu necesită identificare

(1) În cazul în care scopurile pentru care un operator prelucrează date cu caracter personal nu necesită sau nu mai necesită identificarea unei persoane vizate de către operator, operatorul nu are obligația de a păstra, obține sau prelucra informații suplimentare pentru a identifica persoana vizată în scopul unic al respectării prezentei legi.

(2) Dacă, în cazurile menționate la alin.1 (1) din prezentul articol, operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, art. 15-20 nu se aplică, cu excepția cazului în care persoana vizată, în scopul exercitării drepturilor sale în temeiul respectivelor articole, oferă informații suplimentare care permit identificarea sa.

CAPITOLUL III

DREPTURILE PERSOANEI VIZATE

Secțiunea 1

Transparență și modalități

Articolul 12. Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate

(1) Operatorul ia măsuri adecvate pentru a furniza persoanei vizate orice informații menționate la art. 13 și 14 și orice comunicări în temeiul art. 15-22 și 34 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, în special pentru orice informații adresate în mod specific unui copil. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic. La solicitarea persoanei vizate, informațiile pot fi furnizate verbal, cu condiția ca identitatea persoanei vizate să fie dovedită prin alte mijloace.

(2) Operatorul facilitează exercitarea drepturilor persoanei vizate în temeiul art. 15-22. În cazurile menționate la art. 11 alin. (2), operatorul nu refuză să dea curs cererii persoanei vizate de a-și exercita drepturile în conformitate cu art. 15-22, cu excepția cazului în care operatorul demonstrează că nu este în măsură să identifice persoana vizată.

(3) Operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul art. 15-22, fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Operatorul informează persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care persoana vizată introduce o cerere în format electronic, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția cazului în care persoana vizată solicită un alt format.

(4) Dacă nu ia măsuri cu privire la cererea persoanei vizate, operatorul informează persoana vizată, fără întârziere și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu ia măsuri și la posibilitatea de a depune o plângere în fața unei autorități de supraveghere și de a introduce o cale de atac judiciară.

(5) Informațiile furnizate în temeiul art. 13 și 14 și orice comunicare și orice măsuri luate în temeiul art. 15-22 și 34 sunt oferite gratuit. În cazul în care cererile din partea unei persoane vizate

sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, operatorul poate:

- a) fie să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării sau pentru luarea măsurilor solicitate;
- b) fie să refuze să dea curs cererii.

În aceste cazuri, operatorului îi revine sarcina de a demonstra caracterul vădit nefondat sau excesiv al cererii.

(6) Fără a aduce atingere art. 11, în cazul în care are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la art. 15-21, operatorul poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

(7) Informațiile care urmează să fie furnizate persoanelor vizate în temeiul art. 13 și 14 pot fi furnizate în combinație cu pictograme standardizate pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea trebuie să poată fi citite automat.

(8) Centrul Național pentru Protecția Datelor cu Caracter Personal (în continuare – CNPDCP) este împuternicit să adopte acte în vederea determinării informațiilor care urmează să fie prezentate de pictograme și a procedurilor pentru furnizarea de pictograme standardizate.

Secțiunea 2

Informare și acces la date cu caracter personal

Articolul 13. Informații care se furnizează în cazul în care datele cu caracter personal sunt colectate de la persoana vizată

(1) În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate toate informațiile următoare:

- a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- b) datele de contact ale responsabilului cu protecția datelor, după caz
- c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- d) în cazul în care prelucrarea se face în temeiul art. 6 alin.(1) lit. (f), interesele legitime urmărite de operator sau de o parte terță;
- e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
- f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către țările din Spațiul Economic European sau o țară terță sau o organizație internațională și existența sau absența unei decizii ale CNPDCP privind caracterul adecvat sau, în cazul transferurilor menționate la art. 46 sau 47 sau la art. 49 alin. (1), o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.

(2) În plus față de informațiile menționate la alin. (1), în momentul în care datele cu caracter personal sunt obținute, operatorul furnizează persoanei vizate următoarele informații suplimentare

necesare pentru a asigura o prelucrare echitabilă și transparentă:

- a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- b) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
- c) atunci când prelucrarea se bazează pe art. 6 alin. (1) lit. a) sau pe art.9 alin. (2) lit. a), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
- d) dreptul de a depune o plângere în fața unei autorități de supraveghere;
- e) dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații;
- f) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la art.22 alin. (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(3) În cazul în care operatorul intenționează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu alin. (2).

(4) Alin. (1), (2) și (3) nu se aplică dacă și în măsura în care persoana vizată deține deja informațiile respective.

Articolul 14. Informații care se furnizează în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată

(1) În cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată, operatorul furnizează persoanei vizate următoarele informații:

- a) identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia;
- b) datele de contact ale responsabilului cu protecția datelor, după caz;
- c) scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării;
- d) categoriile de date cu caracter personal vizate;
- e) destinatarii sau categoriile de destinatari ai datelor cu caracter personal, după caz;
- f) dacă este cazul, intenția operatorului de a transfera date cu caracter personal către un destinatar din țările din Spațiul Economic European sau dintr-o țară terță sau o organizație internațională și existența sau absența unei decizii a CNPDCP privind caracterul adecvat sau, în cazul transferurilor menționate la art. 46 sau 47 sau la art. 49 alin. (1), o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție.

(2) Pe lângă informațiile menționate la alin. (1), operatorul furnizează persoanei vizate următoarele informații necesare pentru a asigura o prelucrare echitabilă și transparentă în ceea ce

privește persoana vizată:

- a) perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- b) în cazul în care prelucrarea se face în temeiul art. 6 alin. (1) lit. (f), interesele legitime urmărite de operator sau de o parte terță;
- c) existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării și a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor;
- d) atunci când prelucrarea se bazează pe art. 6 alin.(1) lit. (a) sau pe art. 9 alin. (2) lit. (a), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia;
- e) dreptul de a depune o plângere în fața unei autorități de supraveghere;
- f) sursa din care provin datele cu caracter personal și, dacă este cazul, dacă acestea provin din surse disponibile public;
- g) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la art. 22 alin.(1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată;

(3) Operatorul furnizează informațiile menționate la alin. (1) și (2):

- a) într-un termen rezonabil după obținerea datelor cu caracter personal, dar nu mai mare de o lună, ținându-se seama de circumstanțele specifice în care sunt prelucrate datele cu caracter personal;
- b) dacă datele cu caracter personal urmează să fie utilizate pentru comunicarea cu persoana vizată, cel târziu în momentul primei comunicări către persoana vizată respectivă;
- c) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel mai târziu la data la care acestea sunt divulgate pentru prima oară

(4) În cazul în care operatorul intenționează să prelucrez ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost obținute, operatorul furnizează persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și orice informații suplimentare relevante, în conformitate cu alin. (2).

(5) Alin. (1)-(4) nu se aplică dacă și în măsura în care:

- a) persoana vizată deține deja informațiile;
- b) furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate, în special în cazul prelucrării în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva condițiilor și a garanțiilor prevăzute la art. 70 alin. (1), sau în măsura în care obligația menționată la alin.(1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective. În astfel de cazuri, operatorul ia măsuri adecvate pentru a proteja drepturile, libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului;
- c) obținerea sau divulgarea datelor este prevăzută în mod expres în actele normative sub incidența căruia intră operatorul și care prevede măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate;
- d) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații statutare de secret profesional reglementate de actele normative, inclusiv al unei

obligatii legale de a păstra secretul.

Articolul 15. Dreptul de acces al persoanei vizate

(1) Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:

- a) scopurile prelucrării;
- b) categoriile de date cu caracter personal vizate;
- c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țările Spațiului Economic European sau din țări terțe sau organizații internaționale;
- d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
- e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;
- f) dreptul de a depune o plângere în fața unei autorități de supraveghere;
- g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;
- h) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la art. 22 alin. (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(2) În cazul în care datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională, persoana vizată are dreptul să fie informată cu privire la garanțiile adecvate în temeiul art. 46 referitoare la transfer.

(3) Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent.

(4) Dreptul de a obține o copie menționată la alin. (3) nu aduce atingere drepturilor și libertăților altora.

Secțiunea 3

Rectificare și ștergere

Articolul 16. Dreptul la rectificare

Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.

Articolul 17. Dreptul la ștergerea datelor

(1) Persoana vizată are dreptul de a obține din partea operatorului ștergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate, iar operatorul are obligația de a șterge datele cu caracter personal fără întârzieri nejustificate în cazul în care se aplică unul dintre următoarele motive:

- a) datele cu caracter personal nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;
- b) persoana vizată își retrage consimțământul pe baza căruia are loc prelucrarea, în conformitate cu art. 6 alin. (1) lit. (a) sau cu art. 9 alin. (2) lit. (a), și nu există niciun alt temei juridic pentru prelucrarea;
- c) persoana vizată se opune prelucrării în temeiul art. 21 alin. (1) și nu există motive legitime care să prevaleze în ceea ce privește prelucrarea sau persoana vizată se opune prelucrării în temeiul art. 21 alin. (2);
- d) datele cu caracter personal au fost prelucrate ilegal;
- e) datele cu caracter personal trebuie șterse pentru respectarea unei obligații legale care revine operatorului în temeiul actelor normative sub incidența cărora se află operatorul;
- f) datele cu caracter personal au fost colectate în legătură cu oferirea de servicii ale societății informaționale menționate la art. 8 alin. (1).

(2) În cazul în care operatorul a făcut publice datele cu caracter personal și este obligat, în temeiul alin. (1), să le șteargă, operatorul, ținând seama de tehnologia disponibilă și de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal că persoana vizată a solicitat ștergerea de către acești operatori a oricăror linkuri către datele respective sau a oricăror copii sau reproduceri ale acestor date cu caracter personal.

(3) Alin. (1) și (2) nu se aplică în măsura în care prelucrarea este necesară:

- a) pentru exercitarea dreptului la liberă exprimare și la informare;
- b) pentru respectarea unei obligații legale care prevede prelucrarea în temeiul actelor normative care se aplică operatorului sau pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul;
- c) din motive de interes public în domeniul sănătății publice, în conformitate cu art. 9 alin. (2) lit. h) și i) și alin. (3);
- d) în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu art. 70 alin. (1), în măsura în care dreptul menționat la alin. (1) este susceptibil să facă imposibilă sau să afecteze în mod grav realizarea obiectivelor prelucrării respective;
- e) pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Articolul 18. Dreptul la restricționarea prelucrării

(1) Persoana vizată are dreptul de a obține din partea operatorului restricționarea prelucrării în cazul în care se aplică unul din următoarele cazuri:

- a) persoana vizată contestă exactitatea datelor, pentru o perioadă care îi permite operatorului să verifice exactitatea datelor;
- b) prelucrarea este ilegală, iar persoana vizată se opune ștergerii datelor cu caracter personal, solicitând în schimb restricționarea utilizării lor;
- c) operatorul nu mai are nevoie de datele cu caracter personal în scopul prelucrării, dar persoana vizată i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanță;

d) persoana vizată s-a opus prelucrării în conformitate cu art. 21 alin. (1), pentru intervalul de timp în care se verifică dacă drepturile legitime ale operatorului prevalează asupra celor ale persoanei vizate.

(2) În cazul în care prelucrarea a fost restricționată în temeiul alin. (1), astfel de date cu caracter personal pot, cu excepția stocării, să fie prelucrate numai cu consimțământul persoanei vizate sau pentru constatarea, exercitarea sau apărarea unui drept în instanță sau pentru protecția drepturilor unei alte persoane fizice sau juridice sau din motive de interes public important al Republicii Moldova.

(3) O persoană vizată care a obținut restricționarea prelucrării în temeiul alin. (1) este informată de către operator înainte de ridicarea restricției de prelucrare.

Articolul 19. Obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în conformitate cu art. 16, 17 alin. (1) și 18, cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.

Articolul 20. Dreptul la portabilitatea datelor

(1) Persoana vizată are dreptul de a primi datele cu caracter personal care o privesc și pe care le-a furnizat operatorului într-un format structurat, utilizat în mod curent și care poate fi citit automat și are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele cu caracter personal, în cazul în care:

- a) prelucrarea se realizează în baza consimțământului în temeiul art. 6 alin. (1) lit. a) sau al art. 9 alin. (2) lit. a) sau a unui contract în temeiul art. 6 alin. (1) lit.b);
- b) prelucrarea este efectuată prin mijloace automate

(2) În exercitarea dreptului său la portabilitatea datelor în temeiul alin. (1), persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

(3) Exercițarea dreptului menționat la alin. (1) nu aduce atingere prevederilor art. 17. Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorități oficiale cu care este investit operatorul.

(4) Dreptul menționat la alin. (1) nu aduce atingere drepturilor și libertăților altora.

Secțiunea 4

Dreptul la opoziție și procesul decizional individual automatizat

Articolul 21. Dreptul la opoziție

(1) În orice moment, persoana vizată are dreptul de a se opune, din motive personale, prelucrării în temeiul art. 6 alin. (1) lit. e) sau f) sau al art. 6 alin. (1) a datelor cu caracter personal care o privesc, inclusiv creării de profiluri pe baza respectivelor dispoziții. Operatorul nu mai prelucrează

datele cu caracter personal, cu excepția cazului în care operatorul demonstrează că are motive legitime și imperioase care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanță.

(2) Atunci când prelucrarea datelor cu caracter personal are drept scop marketingul direct, persoana vizată are dreptul de a se opune în orice moment prelucrării în acest scop a datelor cu caracter personal care o privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.

(3) În cazul în care persoana vizată se opune prelucrării în scopul marketingului direct, datele cu caracter personal nu mai sunt prelucrate în acest scop.

(4) Cel târziu în momentul primei comunicări cu persoana vizată, dreptul menționat la alin.(1) și (2) este adus în mod explicit în atenția persoanei vizate și este prezentat în mod clar și separat de orice alte informații.

(5) În contextual utilizării serviciilor societății informaționale și în pofida Legii nr. 284/2004 privind serviciile societății informaționale, persoana vizată își poate exercita dreptul de a se opune prin mijloace automate care utilizează specificații tehnice.

(6) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică sau în scopuri statistice în conformitate cu art. 70 alin. (1), persoana vizată, din motive personale, are dreptul de a se opune prelucrării datelor cu caracter personal care o privesc, cu excepția cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

Articolul 22. Procesul decizional individual automatizat, inclusiv crearea de profiluri

(1) Persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă.

(2) Alin. (1) nu se aplică în cazul în care decizia:

- a) este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator de date;
- b) este autorizată prin actele normative care se aplică operatorului și care prevăd, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate;
- c) are la bază consimțământul explicit al persoanei vizate.

(3) În cazurile menționate la alin. (2) lit. a) și c), operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate, cel puțin dreptul acesteia de a obține intervenție umană din partea operatorului, de a-și exprima punctul de vedere și de a contesta decizia.

(4) Deciziile menționate la alin.(2) nu au la bază categoriile speciale de date cu caracter personal menționate la art. 9 alin. (1), cu excepția cazului în care se aplică art. 9 alin.(2) lit. a) sau g) și în care au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate.

Secțiunea 5

Restricții

Articolul 23. Restricții

(1) Actele normative care se aplică operatorului de date sau persoanei împuternicite de operator pot restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la art. 12-22 și 34, precum și la art.5 în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la art. 12-22, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura:

- a) securitatea națională;
- b) apărarea;
- c) securitatea publică;
- d) prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa securității publice și prevenirea acestora;
- e) alte obiective importante de interes public general ale Republicii Moldova, în special un interes economic sau financiar important al Republicii Moldova, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale;
- f) protejarea independenței judiciare și a procedurilor judiciare;
- g) prevenirea, investigarea, depistarea și urmărirea penală a încălcării eticii în cazul profesiilor reglementate;
- h) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității oficiale în cazurile menționate la lit.(a)-(e) și (g);
- i) protecția persoanei vizate sau a drepturilor și libertăților altora;
- j) punerea în aplicare a pretențiilor de drept civil.

(2) În special, orice măsură legislativă menționată la alin. (1) conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește:

- a) scopurile prelucrării sau ale categoriilor de prelucrare;
- b) categoriile de date cu caracter personal; c) domeniul de aplicare al restricțiilor introduse; d) garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal; e) menționarea operatorului sau a categoriilor de operatori; f) perioadele de stocare și garanțiile aplicabile având în vedere natura, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare;
- g) riscurile pentru drepturile și libertăților persoanelor vizate;
- h) dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției.

CAPITOLUL IV

Operatorul și persoana împuternicită de operator

Secțiunea 1

Obligații generale

Articolul 24. Responsabilitatea operatorului

(1) Ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a garanta și a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu prezenta lege. Respectivale măsuri se revizuiesc și se actualizează dacă este necesar.

(2) Atunci când sunt proporționale în raport cu operațiunile de prelucrare, măsurile menționate la alin.(1) includ punerea în aplicare de către operator a unor politici adecvate de protecție a datelor.

(3) Aderarea la coduri de conduită aprobate, menționate la art. 40, sau la un mecanism de certificare aprobat, menționat la art. 42, poate fi utilizată ca element care să demonstreze respectarea obligațiilor de către operator.

Articolul 25. Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscurile cu grade diferite de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atât în momentul stabilirii mijloacelor de prelucrare, cât și în cel al prelucrării în sine, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare în mod eficient principiile de protecție a datelor, precum reducerea la minimum a datelor, și să integreze garanțiile necesare în cadrul prelucrării, pentru a îndeplini cerințele prezentei legi și a proteja drepturile persoanelor vizate.

(2) Operatorul pune în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura că, în mod implicit, sunt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării. Respectiva obligație se aplică volumului de date colectate, gradului de prelucrare a acestora, perioadei lor de stocare și accesibilității lor. În special, astfel de măsuri asigură că, în mod implicit, datele cu caracter personal nu pot fi accesate, fără intervenția persoanei, de un număr nelimitat de persoane.

(3) Un mecanism de certificare aprobat în conformitate cu art. 42 poate fi utilizat drept element care să demonstreze îndeplinirea cerințelor prevăzute la alin. (1) și (2).

Articolul 26. Operatori asociați

(1) În cazul în care doi sau mai mulți operatori stabilesc în comun scopurile și mijloacele de prelucrare, aceștia sunt operatori asociați. Ei stabilesc într-un mod transparent responsabilitățile fiecăruia în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul prezentei legi, în special în ceea ce privește exercitarea drepturilor persoanelor vizate și îndatoririle fiecăruia de furnizare a informațiilor prevăzute la art. 13 și 14, prin intermediul unui acord între ei, cu excepția cazului și în măsura în care responsabilitățile operatorilor sunt stabilite în actele normative care se aplică acestora. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

(2) Acordul menționat la alin. (1) reflectă în mod adecvat rolurile și raporturile respective ale operatorilor asociați față de persoanele vizate. Esența acestui acord este făcută cunoscută persoanei vizate.

(3) Indiferent de clauzele acordului menționat la alin. (1), persoana vizată își poate exercita drepturile în temeiul prezentei legi cu privire la și în raport cu fiecare dintre operatori.

Articolul 27. Reprezentanții operatorilor sau ai persoanelor împuternicite de operatori care nu își au sediul în Republica Moldova

(1) În cazul în care se aplică art. 3 alin. (2), operatorul sau persoana împuternicită de operator desemnează în scris un reprezentant pentru Republica Moldova.

(2) Obligația prevăzută la alin. (1) nu se aplică:

- a) prelucrării care are un caracter ocazional, care nu include, pe scară largă, prelucrarea unor categorii speciale de date, astfel cum se prevede la art. 9 alin. (1), sau prelucrarea unor date cu caracter personal referitoare la condamnări penale și infracțiuni menționată la art. 10, și care este puțin susceptibilă de a genera un risc pentru drepturile și libertățile persoanelor, ținând cont de natura, contextul, domeniul de aplicare și scopurile prelucrării;
- b) unei autorități sau unui organism public.

(3) Reprezentantul își are sediul în Republica Moldova sau în statele din Spațiul Economic European, unde se află persoanele vizate ale căror date cu caracter personal sunt prelucrate în legătură cu furnizarea de bunuri și servicii sau al căror comportament este monitorizat.

(4) Reprezentantul primește din partea operatorului sau a persoanei împuternicite de operator un mandat prin care autoritățile de supraveghere și persoanele vizate, în special, se pot adresa reprezentantului, în plus față de operator sau persoana împuternicită de operator sau în locul acestora, cu privire la toate chestiunile legate de prelucrarea, în scopul asigurării respectării prezentei legi.

(5) Desemnarea unui reprezentant de către operator sau persoana împuternicită de operator nu aduce atingere acțiunilor în justiție care ar putea fi introduse împotriva operatorului sau persoanei împuternicite de operator înseși.

Articolul 28. Persoana împuternicită de operator

(1) În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezenta lege și să asigure protecția drepturilor persoanei vizate.

(2) Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecții față de aceste modificări.

(3) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic în temeiul actelor normative care au caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoană împuternicită de operator:

- a) prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal efectuate în

condițiile Capitolului V, cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul actelor normative care i se aplică; în acest caz, notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

- b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate;
- c) adoptă toate măsurile necesare în conformitate cu art. 32;
- d) respectă condițiile menționate la alin. (2) și (4) privind recrutarea unei alte persoane împuternicite de operator;
- e) ținând seama de natura prelucrării, oferă asistență operatorului prin măsuri tehnice și organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute în Capitolul III;
- f) ajută operatorul să asigure respectarea obligațiilor prevăzute la art. 32-36, ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator;
- g) la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care actele normative impun stocarea datelor cu caracter personal;
- h) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute în prezentul articol, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea, persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă prezenta lege referitoare la protecția datelor.

(4) În cazul în care o persoană împuternicită de un operator recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, astfel cum se prevede la alin. (3), revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul actelor normative, în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentei legi. În cazul în care această a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor, persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor acestei a doua persoane împuternicite.

(5) Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, menționat în art. 40, sau la un mecanism de certificare aprobat, menționat la art. 42, poate fi utilizată ca element prin care să se demonstreze existența garanțiilor suficiente menționate la alin. (1) și (4).

(6) Fără a aduce atingere unui contract individual încheiat între operator și persoana împuternicită de operator, contractul sau celălalt act juridic menționat la alin. (3) și (4) se poate baza, integral sau parțial, pe clauze contractuale standard menționate în alin. (7) și (8), inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul art. 42 și 43.

(7) CNPDCP poate să adopte clauze contractuale standard pentru aspectele menționate la alin. (3) și (4).

(8) Contractul sau celălalt act juridic menționat la alin. (3) și (4) se formulează în scris, inclusiv în format electronic.

(9) Fără a aduce atingere art. 63, 64 și 65, în cazul în care o persoană împuternicită de operator încălcă prezenta lege, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă.

Articolul 29. Desfășurarea activității de prelucrare sub autoritatea operatorului sau a persoanei împuternicite de operator

Persoana împuternicită de operator și orice persoană care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator care are acces la date cu caracter personal nu le prelucreează decât la cererea operatorului, cu excepția cazului în care actele normative îl obligă să facă acest lucru.

Articolul 30. Evidențele activităților de prelucrare

(1) Fiecare operator și, după caz, reprezentantul acestuia păstrează o evidență a activităților de prelucrare desfășurate sub responsabilitatea lor. Respectiva evidență cuprinde toate următoarele informații:

- a) numele și datele de contact ale operatorului și, după caz, ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor;
- b) scopurile prelucrării;
- c) o descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal;
- d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal, inclusiv destinatarii din țările Spațiului Economic European, țări terțe sau organizații internaționale;
- e) dacă este cazul, transferurile de date cu caracter personal către țările Uniunii Europene sau o țară terță sau o organizație internațională, inclusiv identificarea țărilor Spațiului Economic European și țărilor terțe sau a organizației internaționale respective și, în cazul transferurilor menționate la art. 49 alin. (1), documentația care dovedește existența unor garanții adecvate;
- f) acolo unde este posibil, termenele-limită preconizate pentru ștergerea diferitelor categorii de date;
- g) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate la art. 32 alin. (1).

(2) Fiecare operator și, după caz, persoana împuternicită de operator păstrează o evidență a tuturor categoriilor de activități de prelucrare desfășurate în numele operatorului, care cuprind:

- a) numele și datele de contact ale persoanei sau persoanelor împuternicite de operator și ale fiecărui operator în numele căruia acționează această persoană, precum și ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;
- b) categoriile de activități de prelucrare desfășurate în numele fiecărui operator;
- c) dacă este cazul, transferurile de date cu caracter personal către o țară din Spațiului Economic European, o țară terță sau o organizație internațională, inclusiv identificarea țării terțe sau a organizației internaționale respective și, în cazul transferurilor prevăzute la art. 49 alin. (1), documentația care dovedește existența unor garanții adecvate;
- d) acolo unde este posibil, o descriere generală a măsurilor tehnice și organizatorice de securitate menționate în art. 32 alin. (1).

(3) Prevederile menționate la alin. (1) și (2) se formulează în scris, inclusiv în format electronic.

(4) Operatorul sau persoana împuternicită de acesta, precum și, după caz, reprezentantul operatorului sau al persoanei împuternicite de operator pun evidențele la dispoziția autorității de supraveghere, la cererea acesteia.

(5) Obligațiile menționate la alin. (1) și (2) nu se aplică unei întreprinderi sau organizații cu mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede în art. 9 alin. (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează în art. 10.

Articolul 31. Cooperarea cu autoritatea de supraveghere

Operatorul și persoana împuternicită de operator și, după caz, reprezentantul acestora cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor lor.

Secțiunea 2

Securitatea datelor cu caracter personal

Articolul 32. Securitatea prelucrării

(1) Având în vedere stadiul actual al dezvoltării, costurile implementării și natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul și persoana împuternicită de acesta implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

- a) pseudonimizarea și criptarea datelor cu caracter personal;
- b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continue ale sistemelor și serviciilor de prelucrare;
- c) capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- d) un proces pentru testarea, evaluarea și aprecierea periodice ale eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

Articolul 33. Notificarea autorității de supraveghere în cazul încălcării securității datelor cu caracter personal

(1) În cazul în care are loc o încălcare a securității datelor cu caracter personal, operatorul notifică acest lucru autorității de supraveghere competente în temeiul art.51, fără întârzieri nejustificate și, dacă este posibil, în termen de cel mult 72 de ore de la data la care a luat cunoștință de aceasta, cu excepția cazului în care este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. În cazul în care notificarea nu are loc în termen de 72 de ore, aceasta este însoțită de o explicație motivată din partea autorității de supraveghere în cazul în care.

(2) Persoana împuternicită de operator înștiințează operatorul fără întârzieri nejustificate după ce ia cunoștință de o încălcare a securității datelor cu caracter personal.

(3) Notificarea menționată la alin. (1) cel puțin:

- a) descrie caracterul încălcării securității datelor cu caracter personal, inclusiv, acolo unde este posibil, categoriile și numărul aproximativ al persoanelor vizate în cauză, precum și categoriile și numărul aproximativ al înregistrărilor de date cu caracter personal în cauză;
- b) comunică numele și datele de contact ale responsabilului cu protecția datelor sau un alt punct de contact de unde se pot obține mai multe informații;
- c) descrie consecințele probabile ale încălcării securității datelor cu caracter personal;
- d) descrie măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securității datelor cu caracter personal, inclusiv, după caz, măsurile pentru atenuarea eventualelor sale efecte negative.

(4) Atunci când și în măsura în care nu este posibil să se furnizeze informațiile în același timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

(5) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securității datelor cu caracter personal, care cuprind o descriere a situației de fapt în care a avut loc încălcarea securității datelor cu caracter personal, a efectelor acesteia și a măsurilor de remediere întreprinse. Această documentație permite autorității de supraveghere să verifice conformitatea cu prezentul articol.

Articolul 34. Informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal

(1) În cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul informează persoana vizată fără întârzieri nejustificate cu privire la această încălcare.

(2) În informarea transmisă persoanei vizate prevăzută la alin. (1) se include o descriere într-un limbaj clar și simplu a caracterului încălcării securității datelor cu caracter personal, precum și cel puțin informațiile și măsurile menționate în art. 33 alin. (3) lit. b), c) și d).

(3) Informarea persoanei vizate menționată la alin. (1) nu este necesară în cazul în care oricare dintre următoarele condiții este îndeplinită:

- a) operatorul a implementat măsuri de protecție tehnice și organizatorice adecvate, iar aceste măsuri au fost aplicate în cazul datelor cu caracter personal afectate de încălcarea securității datelor cu caracter personal, în special măsuri prin care se asigură că datele cu caracter personal devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;
- b) operatorul a luat măsuri ulterioare prin care se asigură că riscul ridicat pentru drepturile și libertățile persoanelor vizate menționat la alin. (1) nu mai este susceptibil să se materializeze;
- c) ar necesita un efort disproporționat. În această situație, se efectuează în loc o informare publică sau se ia o măsură similară prin care persoanele vizate sunt informate într-un mod la fel de eficace.

(4) În cazul în care operatorul nu a comunicat deja încălcarea securității datelor cu caracter personal către persoana vizată, autoritatea de supraveghere, după ce a luat în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condițiile menționate la alin. (3) sunt îndeplinite.

Secțiunea 3

Evaluarea impactului asupra protecției datelor și consultarea prealabilă

Articolul 35. Evaluarea impactului asupra protecției datelor

- (1) Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.
- (2) La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.
- (3) Evaluarea impactului asupra protecției datelor menționată la alin. (1) se impune mai ales în cazul:
 - a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;
 - b) prelucrării pe scară largă a unor categorii speciale de date, menționată în art. 9 alin. (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată în art. 10;
 - c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.
- (4) Autoritatea de supraveghere întocmește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, în conformitate cu alin. (1).
- (5) CNPDCP poate, de asemenea, să stabilească și să pună la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor.
- (6) Înainte de adoptarea listelor menționate la alineatele (4) și (5), CNPDCP consultă practica Uniunii Europene în domeniul protecției datelor cu caracter personal în cazul în care aceste liste implică activități de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii către persoane vizate sau monitorizarea comportamentului acestora sau pot afecta în mod substanțial libera circulație a datelor cu caracter personal .
- (7) Evaluarea conține cel puțin:
 - a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;
 - b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;
 - c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alin. (1);
 - d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentei legi, luând în considerare drepturile și interesele legitime

ale persoanelor vizate și ale altor persoane interesate.

(8) La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menționate în art.40, în special în vederea unei evaluări a impactului asupra protecției datelor.

(9) Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

(10) Atunci când prelucrarea în temeiul art. 6 alineatul (1) litera c) sau e) are un temei juridic în actele normative, iar actele normative respective reglementează operațiunea de prelucrare specifică sau setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, alineatele (1)-(7) nu se aplică, cu excepția cazului în care actele normative determină că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.

(11) Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

Articolul 36. Consultarea prealabilă

(1) Operatorul consultă autoritatea de supraveghere înainte de prelucrarea atunci când evaluarea impactului asupra protecției datelor prevăzută la art. 35 indică faptul că prelucrarea ar genera un risc ridicat în absența unor măsuri luate de operator pentru atenuarea riscului.

(2) Atunci când consideră că prelucrarea prevăzută menționată la alin.(1) ar încălca prezenta lege, în special atunci când riscul nu a fost identificat sau atenuat într-o măsură suficientă de către operator, autoritatea de supraveghere oferă consiliere în scris operatorului și, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii de consultare, și își poate utiliza oricare dintre competențele menționate în art. 58. Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Autoritatea de supraveghere informează operatorul și, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când autoritatea de supraveghere a obținut informațiile pe care le-a solicitat în scopul consultării.

(3) Atunci când consultă autoritatea de supraveghere în conformitate cu alin. (1), operatorul îi furnizează acesteia:

- a) dacă este cazul, responsabilitățile respective ale operatorului, ale operatorilor asociați și ale persoanelor împuternicite de operator implicate în activitățile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;
- b) scopurile și mijloacele prelucrării preconizate;
- c) măsurile și garanțiile prevăzute pentru protecția drepturilor și libertăților persoanelor vizate, în conformitate cu prezenta lege;
- d) dacă este cazul, datele de contact ale responsabilului cu protecția datelor;
- e) evaluarea impactului asupra protecției datelor prevăzută în art. 35;

f) orice alte informații solicitate de autoritatea de supraveghere.

(4) Subiecții cu drept de inițiativă legislativă consultă autoritatea de supraveghere în cadrul procesului de pregătire a unei propuneri de măsură legislativă care urmează să fie adoptată de organul legislativ sau a unei măsuri de reglementare întemeiate pe o astfel de măsură legislativă, care se referă la prelucrarea.

(5) În pofida alin. (1), actele normative poate impune operatorilor să se consulte cu autoritatea de supraveghere și să obțină în prealabil autorizarea din partea acesteia în legătură cu prelucrarea de către un operator în vederea îndeplinirii unei sarcini exercitate de acesta în interes public, inclusiv prelucrarea în legătură cu protecția socială și sănătatea publică.

Secțiunea 4

Responsabilul de protecția datelor

Articolul 37. Desemnarea responsabilului de protecția datelor

(1) Operatorul și persoana împuternicită de operator desemnează un responsabil de protecția datelor ori de câte ori:

- a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;
- b) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă; sau
- c) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, menționată în art. 9, sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată în art. 10.

(2) Un grup de întreprinderi poate numi un responsabil de protecția datelor unic, cu condiția ca responsabilul de protecția datelor să fie ușor accesibil din fiecare întreprindere.

(3) În cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, poate fi desemnat un responsabil de protecția datelor unic pentru mai multe dintre aceste autorități sau organisme, luând în considerare structura organizatorică și dimensiunea acestora.

(4) În alte cazuri decât cele menționate la alin. (1), operatorul sau persoana împuternicită de operator ori asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde actele normative solicită acest lucru, desemnează un responsabil cu protecția datelor. Responsabilul de protecția datelor poate să acționeze în favoarea unor astfel de asociații și alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

(5) Responsabilul de protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la art. 39.

(6) Responsabilul de protecția datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să își îndeplinească sarcinile în baza unui contract de

servicii.

(7) Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului de protecția datelor și le comunică autorității de supraveghere.

Articolul 38. Funcția responsabilului cu protecția datelor

(1) Operatorul și persoana împuternicită de operator se asigură că responsabilul de protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

(2) Operatorul și persoana împuternicită de operator sprijină responsabilul de protecția datelor în îndeplinirea sarcinilor menționate la art. 39, asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate.

(3) Operatorul și persoana împuternicită de operator se asigură că responsabilul de protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. Acesta nu este demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul de protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

(4) Persoanele vizate pot contacta responsabilul de protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentei legi.

(5) Responsabilul de protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu actele normative.

(6) Responsabilul de protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.

Articolul 39. Sarcinile responsabilului de protecția datelor

(1) Responsabilul de protecția datelor are cel puțin următoarele sarcini:

- a) informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin în temeiul prezentei legi și al altor dispoziții ale actelor normative referitoare la protecția datelor;
- b) monitorizarea respectării prezentei legi, a altor dispoziții ale actelor normative referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
- c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu art.35;
- d) cooperarea cu autoritatea de supraveghere;
- e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la art. 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

(2) În îndeplinirea sarcinilor sale, responsabilul de protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

Secțiunea 5

Coduri de conduită și certificare

Articolul 40. Coduri de conduită

(1) Se încurajează elaborarea codurilor de conduită menite să contribuie la buna aplicare a prezentei legi, ținând seama de caracteristicile specifice ale diverselor sectoare de prelucrare și de nevoile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.

(2) Asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot pregăti coduri de conduită sau le pot modifica sau extinde pe cele existente, în scopul de a specifica modul de aplicare a prezentei legi, cum ar fi :

- a) prelucrarea în mod echitabil și transparent;
- b) interesele legitime urmărite de operatori în contexte specifice;
- c) colectarea datelor cu caracter personal;
- d) pseudonimizarea datelor cu caracter personal;
- e) informarea publicului și a persoanelor vizate;
- f) exercitarea drepturilor persoanelor vizate;
- g) informarea și protejarea copiilor și modalitatea în care trebuie obținut consimțământul titularilor răspunderii părintești asupra copiilor;
- h) măsurile și procedurile menționate la art. 24 și 25 și măsurile de asigurare a securității prelucrării, menționate la art. 32;
- i) notificarea autorităților de supraveghere cu privire la încălcările securității datelor cu caracter personal și informarea persoanelor vizate cu privire la aceste încălcări;
- j) transferul de date cu caracter personal către țări terțe sau organizații internaționale;
- k) proceduri extrajudiciare și alte proceduri de soluționare a litigiilor pentru soluționarea litigiilor între operatori și persoanele vizate în ceea ce privește prelucrarea, fără a aduce atingere drepturilor persoanelor vizate, în temeiul art. 59 și 60.

(3) La codurile de conduită aprobate în temeiul alin. (5) și care au o valabilitate generală în temeiul alin.(9) pot adera nu numai operatorii sau persoanele împuternicite de operatori care fac obiectul prezentei legi, ci și operatorii sau persoanele împuternicite de operatori care nu fac obiectul prezentei legi în temeiul art.3, în scopul de a oferi garanții adecvate în cadrul transferurilor de date cu caracter personal către țări terțe sau organizații internaționale în condițiile menționate la art. 46 alin. (2) lit. e). Acești operatori sau persoane împuternicite de operatori își asumă angajamente cu caracter obligatoriu și executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanțiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

(4) Codul de conduită prevăzut la alin. (2) cuprinde mecanisme care permit organismului menționat la art.41 alin. (1) să efectueze monitorizarea obligatorie a respectării dispozițiilor acestuia de către operatorii sau persoanele împuternicite de operatori care se angajează să îl aplice, fără a aduce atingere sarcinilor și competențelor autorităților de supraveghere care sunt competente în temeiul art. 51.

(5) Asociațiile și alte organisme menționate la alin.(2) care intenționează să pregătească un cod de conduită sau să modifice sau să extindă un cod existent transmit proiectul de cod, de modificare sau de extindere autorității de supraveghere care este competentă în temeiul art. 51. Autoritatea de supraveghere emite un aviz cu privire la conformitatea cu prezenta lege a proiectului de cod, de modificare sau de extindere și îl aprobă în cazul în care se constată că acesta oferă garanții adecvate suficiente.

(6) În cazul în care proiectul de cod, de modificare sau de extindere este aprobat în conformitate cu alin. (5), autoritatea de supraveghere înregistrează și publică codul.

(7) CNPDCP regroupează toate codurile de conduită, modificările și extinderile aprobate într- un registru și le pune la dispoziția publicului prin mijloace corespunzătoare.

Articolul 41. Monitorizarea codurilor de conduită aprobate

(1) Fără a aduce atingere sarcinilor și competențelor autorității de supraveghere în temeiul articolului 55, monitorizarea respectării unui cod de conduită în temeiul articolului 40 poate fi realizată de un organism care dispune de un nivel adecvat de expertiză în legătură cu obiectul codului și care este acreditat în acest scop de CNPDCP.

(2) Un organism menționat la alineatul (1) poate fi acreditat pentru monitorizarea respectării unui cod de conduită dacă:

- a) a demonstrat CNPDCP, într-un mod satisfăcător, independența și expertiza sa în legătură cu obiectul codului;
- b) a instituit proceduri care îi permit să evalueze eligibilitatea operatorilor și a persoanelor împuternicite de operatori în vederea aplicării codului, să monitorizeze respectarea de către aceștia a dispozițiilor codului și să revizuiască periodic funcționarea acestuia;
- c) a instituit proceduri și structuri pentru tratarea plângerilor privind încălcări ale codului sau privind modul în care codul a fost sau este pus în aplicare de un operator sau o persoană împuternicită de operator, precum și pentru asigurarea transparenței acestor proceduri și structuri pentru persoanele vizate și pentru public; și
- d) a demonstrat CNPDCP, într-un mod satisfăcător, că sarcinile și atribuțiile sale nu creează conflicte de interese

(3) CNPDCP adoptă criteriile pentru acreditarea unui organism menționat la alineatul (1).

(4) Fără a aduce atingere sarcinilor și competențelor CNPDCP competente și dispozițiilor capitolului VII, un organism menționat la alineatul (1) din prezentul articol ia măsuri corespunzătoare, sub rezerva unor garanții adecvate, în cazul încălcării codului de către un operator sau o persoană împuternicită de operator, inclusiv prin suspendarea sau excluderea respectivului operator sau a respectivei persoane din cadrul codului. Organismul în cauză informează CNPDCP cu privire la aceste măsuri și la motivele care le-au determinat.

(5) CNPDCP revocă acreditarea unui organism menționat la alineatul (1) în cazul în care nu mai sunt îndeplinite condițiile pentru acreditare sau măsurile luate de organismul în cauză încalcă prezenta lege.

(6) Prezentul articol nu se aplică prelucrării efectuate de autorități și organisme publice.

Articolul 42. Certificare

(1) Se încurajează, instituirea de mecanisme de certificare în domeniul protecției datelor, precum și de sigilii și mărci în acest domeniu, care să permită demonstrarea faptului că operațiunile de prelucrare efectuate de operatori și de persoanele împuternicite de operatori respectă prezenta lege. Sunt luate în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii.

(2) Mecanismele de certificare din domeniul protecției datelor, sigiliile sau mărcile aprobate în temeiul alin. (5) sunt instituite nu numai pentru a fi respectate de operatorii sau de persoanele împuternicite de operatori care fac obiectul prezentei legi, ci și pentru a demonstra existența unor garanții adecvate oferite de operatorii sau de persoanele împuternicite de operatori care nu fac obiectul prezentei legi, în temeiul art. 3, în cadrul transferurilor de date cu caracter personal către țări terțe sau organizații internaționale în condițiile menționate la art. 46 alin. (2) lit. (f). Acești operatori sau persoane împuternicite de operatori își asumă angajamente cu caracter obligatoriu și executoriu, prin intermediul unor instrumente contractuale sau al altor instrumente obligatorii din punct de vedere juridic, în scopul aplicării garanțiilor adecvate respective, inclusiv cu privire la drepturile persoanelor vizate.

(3) Certificarea este voluntară și disponibilă prin intermediul unui proces transparent.

(4) Certificarea în conformitate cu prezentul articol nu reduce responsabilitatea operatorului sau a persoanei împuternicite de operator de a respecta prezenta lege și nu aduce atingere sarcinilor și competențelor autorităților de supraveghere care sunt competente în temeiul art. 51.

(5) Organismele de certificare menționate la art. 43 sau CNPDCP emit o certificare în temeiul prezentului articol, pe baza criteriilor aprobate de către CNPDCP în temeiul art. 56 alin. (3).

(6) Operatorul sau persoana împuternicită de operator care supune activitățile sale de prelucrare mecanismului de certificare oferă organismului de certificare menționat la art. 43 sau, după caz, CNPDCP toate informațiile necesare pentru desfășurarea procedurii de certificare, precum și accesul la activitățile de prelucrare respective.

(6) Certificarea este eliberată unui operator sau unei persoane împuternicite de operator pentru o perioadă maximă de trei ani și poate fi reînnoită în aceleași condiții, cu condiția ca cerințele relevante să fie îndeplinite în continuare. Certificarea este retrasă, după caz, de către organismele de certificare menționate la art. 43 sau de către CNPDCP în cazul în care nu mai sunt îndeplinite cerințele pentru certificare.

(7) CNPDCP regroupează toate mecanismele de certificare și sigiliile și mărcile de protecție a datelor într-un registru și le pune la dispoziția publicului prin orice mijloc corespunzător.

Articolul 43. Organisme de certificare

(1) Fără a aduce atingere sarcinilor și competențelor CNPDCP, prevăzute la art. 55 și 56, organismele de certificare care dispun de un nivel adecvat de competență în domeniul protecției datelor, după ce informează CNPDCP pentru a-i permite să își exercite competențele în temeiul art. 56 alin. (2) lit. (h), emit și reînnoiesc certificarea. Acreditarea organismelor de certificare se va asigura de către:

a) Centrul Național de Acreditare;

b) dacă au demonstrat Centrul Național de Acreditare, într-un mod satisfăcător, independența și

expertiza sa în legătură cu obiectul certificării;

- c) s-a angajat să respecte criteriile menționate la art. 42 alin. (5) și aprobate de CNPDCP care este competent în temeiul art.51;
- d) a instituit proceduri pentru emiterea, revizuirea periodică și retragerea certificării, a sigiliilor și mărcilor din domeniul protecției datelor
- e) a instituit proceduri și structuri pentru tratarea plângerilor privind încălcări ale certificării sau privind modul în care certificarea a fost sau este pusă în aplicare de un operator sau o persoană împuternicită de operator, precum și pentru asigurarea transparenței acestor proceduri și structuri pentru persoanele vizate și pentru public;
- f) a demonstrat CNPDCP într-un mod satisfăcător, că sarcinile și atribuțiile sale nu creează conflicte de interese.

(2) Acreditarea organismelor de certificare menționate la alin. (1) și (2) se realizează pe baza criteriilor aprobate de către CNPDCP.

(3) Organismele de certificare menționate la alin. (1) sunt responsabile cu realizarea unei evaluări adecvate în vederea certificării sau retragerii acestei certificări, fără a aduce atingere responsabilității operatorului sau a persoanei împuternicite de operator de a respecta prezenta lege. Acreditarea se eliberează pentru o perioadă maximă de cinci ani și poate fi reînnoită în aceleași condiții, cu condiția ca organismul de certificare să îndeplinească cerințele prevăzute în prezentul articol.

(4) Organismele de certificare menționate la alin. (1) transmit CNPDCP motivele acordării sau retragerii certificării solicitate.

(5) Cerințele menționate la alin. (3) și criteriile menționate la art. 42 alin. (5) se publică de către CNPDCP într-o formă ușor de accesat. CNPDCP regroupează toate mecanismele de certificare și sigiliile de protecție a datelor într-un registru și le pune la dispoziția publicului prin orice mijloc corespunzător.

(6) Fără a aduce atingere dispozițiilor Capitolului VII, organismul național de acreditare revocă acreditarea acordată unui organism de certificare în temeiul alin. (1) în cazul în care nu sunt sau nu mai sunt îndeplinite condițiile pentru acreditare sau măsurile luate de organismul de acreditare încalcă prezenta lege.

(7) CNPDCP poate adopta acte de punere în aplicare pentru a stabili standarde tehnice pentru mecanismele de certificare și pentru sigiliile și mărcile din domeniul protecției datelor, precum și mecanisme de promovare și recunoaștere a acelor mecanisme de certificare, sigilii și mărci.

CAPITOLUL V

TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ȚĂRILE DIN SPAȚIUL ECONOMIC EUROPEAN ȘI ȚĂRILE TERȚE SAU ORGANIZAȚII INTERNAȚIONALE

Articolul 44. Principiul general al transferurilor

(1) Orice date cu caracter personal care fac obiectul prelucrării sau care urmează a fi prelucrate

după ce sunt transferate într-o țară a Spațiului Economic European sau o țară terță sau către o organizație internațională pot fi transferate doar dacă, sub rezerva celorlalte dispoziții ale prezentei legi, condițiile prevăzute în prezentul capitol sunt respectate de operator și de persoana împuternicită de operator, inclusiv în ceea ce privește transferurile ulterioare de date cu caracter personal din țara Spațiului Economic European sau țara terță sau de la organizația internațională către o altă țară a Spațiului Economic European sau o țară terță sau către o altă organizație internațională. Toate dispozițiile din prezentul capitol se aplică pentru a se asigura că nivelul de protecție a persoanelor fizice garantat prin prezenta lege nu este subminat.

(2) Transmiterea datelor cu caracter personal către statele din Spațiul Economic European se permite și se realizează, ținând cont de principiul liberei circulații a datelor.

Articolul 45. Transferuri în temeiul unei decizii privind caracterul adecvat al nivelului de protecție

(1) Transferul de date cu caracter personal către o țară terță sau o organizație internațională se poate realiza atunci când CNPDCP a decis că țara terță, un teritoriu ori unul sau mai multe sectoare specificate din acea țară terță sau organizația internațională în cauză asigură un nivel de protecție adecvat. Transferurile realizate în aceste condiții nu necesită autorizări speciale.

(2) Atunci când evaluează caracterul adecvat al nivelului de protecție, CNPDCP ține seama, în special, de următoarele elemente:

- a) statul de drept, respectarea drepturilor omului și a libertăților fundamentale, legislația relevantă, atât generală, cât și sectorială, inclusiv privind securitatea publică, apărarea, securitatea națională și dreptul penal, precum și accesul autorităților publice la datele cu caracter personal, precum și punerea în aplicare a acestei legislații, normele de protecție a datelor, normele profesionale și măsurile de securitate, inclusiv normele privind transferul ulterior de date cu caracter personal către o altă țară terță sau organizație internațională, care sunt respectate în țara terță respectivă sau în organizația internațională respectivă, jurisprudența, precum și existența unor drepturi efective și opozabile ale persoanelor vizate și a unor reparații efective pe cale administrativă și judiciară pentru persoanele vizate ale căror date cu caracter personal sunt transferate;
- b) existența și funcționarea eficientă a uneia sau mai multor autorități de supraveghere independente în țara terță sau sub jurisdicția cărora intră o organizație internațională, cu responsabilitate pentru asigurarea și impunerea respectării normelor de protecție a datelor, incluzând competențe adecvate de asigurare a respectării aplicării, pentru acordarea de asistență și consiliere persoanelor vizate cu privire la exercitarea drepturilor acestora și pentru cooperarea cu autoritățile de supraveghere din statele membre; și
- c) angajamentele internaționale la care a aderat țara terță sau organizația internațională în cauză sau alte obligații care decurg din convenții sau instrumente obligatorii din punct de vedere juridic, precum și din participarea acestora la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal;

d) deciziile Comisiei Europene privind caracterul adecvat al nivelului de protecție.

(3) CNPDCP, după ce evaluează caracterul adecvat al nivelului de protecție, poate decide, printr-un act de punere în aplicare, că o țară terță, un teritoriu sau unul sau mai multe sectoare specificate dintr-o țară terță sau o organizație internațională asigură un nivel de protecție adecvat în sensul alin. (2). Actul de punere în aplicare prevede un mecanism de revizuire periodică, cel puțin o dată la patru ani, care ia în considerare toate evoluțiile relevante din țara terță sau organizația internațională. Actul de punere în aplicare menționează aplicarea geografică și sectorială, și, după

caz, identifică autoritatea sau autoritățile de supraveghere menționate la alin. (2) lit. b) .

(4) CNPDCP monitorizează continuu evoluțiile din țările terțe și de la nivelul organizațiilor internaționale care ar putea afecta funcționarea deciziilor adoptate în temeiul alin. (3) și a deciziilor adoptate în temeiul Legii nr. 133/2011 privind protecția datelor cu caracter personal.

(5) În cazul în care informațiile disponibile dezvăluie, în special în urma revizuirii menționate la alin. (3), că o țară terță, un teritoriu sau un sector specificat din acea țară terță sau o organizație internațională nu mai asigură un nivel de protecție adecvat în sensul alin. (2) , CNPDCP, dacă este necesar, abrogă, modifică sau suspendă, prin intermediul unui act de punere în aplicare, decizia menționată la alin. (3) fără efect retroactiv.

(6)

(6) CNPDCP după caz, de comun cu autoritățile competente din Republica Moldova, inițiază consultări cu țara terță sau organizația internațională în vederea remedierii situației care a stat la baza deciziei luate în conformitate cu alin. (5).

(7) O decizie luată în temeiul alin. (5) nu aduce atingere transferurilor de date cu caracter personal către țara terță, un teritoriu sau unul sau mai multe sectoare specificate din acea țară terță sau către organizația internațională în cauză în conformitate cu art. 46-49.

(8) CNPDCP publică în Monitorul Oficial și pe site-ul său o listă a țărilor terțe, a teritoriilor și sectoarelor specificate dintr-o țară terță și a organizațiilor internaționale în cazul cărora a decis că nivelul de protecție adecvat este asigurat sau nu mai este asigurat.

(9) Deciziile adoptate de CNPDCP în temeiul art. 32 alin. (3) din Legea nr. 133/2011 privind protecția datelor cu caracter personal rămân în vigoare până când sunt modificate, înlocuite sau abrogate de o decizie a CNPDCP adoptată în conformitate cu alin. (3) sau (5).

Articolul 46. Transferuri în baza unor garanții adecvate

(1) În absența unei decizii în temeiul art. 45 alin. (3), operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o țară terță sau o organizație internațională numai dacă operatorul sau persoana împuternicită de operator a oferit garanții adecvate și cu condiția să existe drepturi opozabile și căi de atac eficiente pentru persoanele vizate.

(2) Garanțiile adecvate menționate la alin.(1) pot fi furnizate fără să fie nevoie de nicio autorizație specifică din partea CNPDCP, prin:

- a) un instrument obligatoriu din punct de vedere juridic și executoriu între autoritățile sau organismele publice;
- b) reguli corporatiste obligatorii în conformitate cu art. 47;
- c) clauze standard de protecție a datelor adoptate de CNPDCP;
- d) clauze standard de protecție a datelor adoptate de Comisia Europeană și aprobate de CNPDCP;
- e) un cod de conduită aprobat în conformitate cu art.40, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau
- f) un mecanism de certificare aprobat în conformitate cu art. 42, însoțit de un angajament obligatoriu și executoriu din partea operatorului sau a persoanei împuternicite de operator din

țara terță de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

(3) Sub rezerva autorizării din partea autorității de supraveghere competente, garanțiile adecvate menționate la alin. (1) pot fi furnizate de asemenea, în special, prin:

- a) clauze contractuale între operator sau persoana împuternicită de operator și operatorul, persoana împuternicită de operator sau destinatarul datelor cu caracter personal din țara terță sau organizația internațională;
- b) dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau organismele publice, care includ drepturi opozabile și efective pentru persoanele vizate.

(4) Autorizațiile CNPDCP țin cont de practica Uniunii Europene în domeniul protecției datelor cu caracter personal în cazurile menționate la alin. (3) .

Articolul 47. Reguli corporatiste obligatorii

(1) Ținând cont de practica Uniunii Europene, CNPDCP aprobă reguli corporatiste obligatorii, cu condiția ca acestea:

- a) să fie obligatorii din punct de vedere juridic și să se aplice fiecărui membru vizat al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, inclusiv angajaților acestuia, precum și să fie puse în aplicare de membrii în cauză;
- b) să confere, în mod expres, drepturi opozabile persoanelor vizate în ceea ce privește prelucrarea datelor lor cu caracter personal; și
- c) să îndeplinească cerințele prevăzute la alin.(2).

(2) Regulile corporatiste obligatorii menționate la alin.(1) precizează cel puțin:

- a) structura și datele de contact ale grupului de întreprinderi sau ale grupului de întreprinderi implicate într-o activitate economică comună și ale fiecăruia dintre membrii săi
- b) transferurile de date sau setul de transferuri, inclusiv categoriile de date cu caracter personal, tipul prelucrării și scopurile prelucrării, tipurile de persoane vizate afectate și identificarea țării terțe sau a țărilor terțe în cauză;
- c) caracterul lor juridic obligatoriu, atât pe plan intern, cât și extern;
- d) aplicarea principiilor generale în materie de protecție a datelor, în special limitarea scopului, reducerea la minimum a datelor, perioadele de stocare limitate, calitatea datelor, protecția datelor începând cu momentul conceperii și protecția implicită, temeiul juridic pentru prelucrare, prelucrarea categoriilor speciale de date cu caracter personal, măsurile de asigurare a securității datelor, precum și cerințele referitoare la transferurile ulterioare către organisme care nu fac obiectul regulilor corporatiste obligatorii;
- e) drepturile persoanelor vizate în ceea ce privește prelucrarea și mijloacele de exercitare a acestor drepturi, inclusiv dreptul de a nu face obiectul unor decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, în conformitate cu art. 22, dreptul de a depune o plângere în fața CNPDCP și în fața instanțelor , în conformitate cu art. 61, precum și dreptul de a obține reparații și, după caz, despăgubiri pentru încălcarea regulilor corporatiste obligatorii;
- f) acceptarea de către operator sau de persoana împuternicită de operator, care își are sediul pe teritoriul Republicii Moldova, a răspunderii pentru orice încălcare a regulilor corporatiste obligatorii de către orice membru în cauză care nu își are sediul în Republica Moldova; operatorul sau persoana împuternicită de operator este exonerat(ă) de această răspundere, integral sau parțial, numai dacă dovedește că membrul respectiv nu a fost răspunzător de

- evenimentul care a cauzat prejudiciul;
- g) modul în care informațiile privind regulile corporatiste obligatorii, în special privind dispozițiile menționate la lit. d), e) și f), sunt furnizate persoanelor vizate în completarea informațiilor menționate la art. 13 și 14;
 - h) sarcinile oricărui responsabil cu protecția datelor desemnat în conformitate cu art. 37 sau ale oricărei alte persoane sau entități însărcinate cu monitorizarea respectării regulilor corporatiste obligatorii în cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, a activităților de formare și a gestionării plângerilor;
 - i) procedurile de formulare a plângerilor;
 - j) mecanismele din cadrul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, menite să asigure verificarea conformității cu regulile corporatiste obligatorii. Aceste mecanisme includ auditurile privind protecția datelor și metodele de asigurare a acțiunilor corective menite să protejeze drepturile persoanei vizate. Rezultatele acestor verificări ar trebui să fie comunicate persoanei sau entității menționate la litera h) și consiliului de administrație al întreprinderii care exercită controlul grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună și ar trebui să fie puse la dispoziția CNPDCP, la cerere;
 - k) mecanismele de raportare și înregistrare a modificărilor aduse regulilor și de raportare a acestor modificări către CNPDCP;
 - l) mecanismul de cooperare cu CNPDCP în vederea asigurării respectării regulilor de către orice membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună, în special prin punerea la dispoziția CNPDCP a rezultatelor verificărilor cu privire la măsurile menționate la punctul j);
 - m) mecanismele de raportare către CNPDCP a oricăror cerințe legale impuse unui membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună într-o țară terță care pot avea un efect advers considerabil asupra garanțiilor furnizate prin regulile corporatiste obligatorii;
 - n) formarea corespunzătoare în domeniul protecției datelor a personalului care are un acces permanent sau periodic la date cu caracter personal

(3) CNPDCP poate preciza formatul și procedurile pentru schimbul de informații între operatori, persoanele împuternicite de operatori și CNPDCP pentru regulile corporatiste obligatorii în sensul prezentului articol.

Articolul 48. Transferurile sau divulgările de informații neautorizate de actele normative.

Orice hotărâre a unei instanțe sau a unui tribunal și orice decizie a unei autorități administrative a unei țări terțe care impun unui operator sau persoanei împuternicite de operator să transfere sau să divulge date cu caracter personal poate fi recunoscută sau executată în orice fel numai dacă se bazează pe un acord internațional, cum ar fi un tratat de asistență judiciară reciprocă în vigoare între țara terță solicitantă și Republica Moldova, fără a se aduce atingere altor motive de transfer în temeiul prezentului capitol.

Articolul 49. Derogări pentru situații specifice

(1) În absența unei decizii privind caracterul adecvat al nivelului de protecție în conformitate cu art.45 alin. (3) sau a unor garanții adecvate în conformitate cu art. 46, inclusiv a regulilor corporatiste obligatorii, un transfer sau un set de transferuri de date cu caracter personal către o țară terță sau o organizație internațională poate avea loc numai în una dintre condițiile următoare:

- a) persoana vizată și-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a

fost informată asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru persoana vizată ca urmare a lipsei unei decizii privind caracterul adecvat al nivelului de protecție și a unor garanții adecvate;

- b) transferul este necesar pentru executarea unui contract între persoana vizată și operator sau pentru aplicarea unor măsuri precontractuale adoptate la cererea persoanei vizate;
- c) transferul este necesar pentru încheierea unui contract sau pentru executarea unui contract încheiat în interesul persoanei vizate între operator și o altă persoană fizică sau juridică;
- d) transferul este necesar din considerente importante de interes public;
- e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;
- f) transferul este necesar pentru protejarea intereselor vitale ale persoanei vizate sau ale altor persoane, atunci când persoana vizată nu are capacitatea fizică sau juridică de a-și exprima acordul;
- g) transferul se realizează dintr-un registru care, potrivit actelor normative, are scopul de a furniza informații publicului și care poate fi consultat fie de public în general, fie de orice persoană care poate face dovada unui interes legitim, dar numai în măsura în care sunt îndeplinite condițiile cu privire la consultare prevăzute de actele normative în acel caz specific.

(1) ¹⁾ În cazul în care un transfer nu ar putea să se întemeieze pe o dispoziție prevăzută la art.45 sau 46, inclusiv dispoziții privind reguli corporatiste obligatorii, și nu este aplicabilă niciuna dintre derogările pentru situații specifice prevăzute la primul paragraf din prezentul alineat, un transfer către o țară terță sau o organizație internațională poate avea loc numai în cazul în care transferul nu este repetitiv, se referă doar la un număr limitat de persoane vizate, este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile și libertățile persoanei vizate și operatorul a evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, a prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal. Operatorul informează CNPDCP cu privire la transfer. Operatorul, în plus față de furnizarea informațiilor menționate la art. 13 și 14, informează persoana vizată cu privire la transfer și la interesele legitime majore pe care le urmărește.

(2) Transferul în temeiul alin. (1) lit. g) nu implică totalitatea datelor cu caracter personal sau ansamblul categoriilor de date cu caracter personal cuprinse în registru. Atunci când registrul urmează a fi consultat de către persoane care au un interes legitim, transferul se efectuează numai la cererea persoanelor respective sau în cazul în care acestea vor fi destinatarii.

(3) Alin. (1) lit. a), b) și c) nu se aplică în cazul activităților desfășurate de autoritățile publice în exercitarea competențelor lor publice.

(4) Interesul public prevăzut la alin. (1) lit. d) este recunoscut în actele normative sub incidența căruia intră operatorul.

(5) În absența unei decizii privind caracterul adecvat al nivelului de protecție, actelor normative sau dreptul intern poate, din considerente importante de interes public, să stabilească în mod expres limite asupra transferului unor categorii specifice de date cu caracter personal către o țară terță sau o organizație internațională.

(6) Operatorul sau persoana împuternicită de operator consemnează evaluarea, precum și garanțiile adecvate prevăzute la paragraful al doilea al alin.(1), în evidențele menționate la art.30.

Articolul 50. Cooperarea internațională în domeniul protecției datelor cu caracter personal

(1) În ceea ce privește țările din Spațiul Economic European și țările terțe și organizațiile internaționale, autoritățile de supraveghere iau măsurile corespunzătoare pentru:

- a) elaborarea de mecanisme de cooperare internațională pentru a facilita asigurarea aplicării efective a legislației privind protecția datelor cu caracter personal;
- b) acordarea de asistență internațională reciprocă în asigurarea aplicării legislației din domeniul protecției datelor cu caracter personal, inclusiv prin notificare, transferul plângerilor, asistență în investigații și schimb de informații, sub rezerva unor garanții adecvate pentru protecția datelor cu caracter personal și a altor drepturi și libertăți fundamentale;
- c) implicarea părților interesate relevante în discuțiile și activitățile care au ca scop intensificarea cooperării internaționale în domeniul aplicării legislației privind protecția datelor cu caracter personal;
- d) promovarea schimbului reciproc și a documentației cu privire la legislația și practicile în materie de protecție a datelor cu caracter personal, inclusiv în ceea ce privește conflictele jurisdicționale cu țările din Spațiul Economic European și țările terțe.

CAPITOLUL VI

AUTORITĂȚI DE SUPRAVEGHERE INDEPENDENTE

Secțiunea 1

Statutul independent

Articolul 51. Autoritatea de supraveghere

(1) În calitate de Autoritate de supraveghere se desemnează:

- a) CNPDCP pentru toate cazurile cu excepția situațiilor prevăzute la lit. b);
- b) Consiliul Superior al Magistraturii în cazul prelucrărilor de date cu caracter personal efectuate de către instanțele judecătorești în cadrul exercitării sarcinilor sale judiciare.

(2) Autoritățile de supraveghere indicate la alin. (1), sunt responsabile de monitorizarea aplicării prezentei legi, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea și în vederea facilitării liberei circulații a datelor cu caracter personal

(3) Autoritatea de supraveghere contribuie la aplicarea coerentă a prezentei legi și asigură conlucrarea și cooperarea cu autoritățile de supraveghere din Spațiul Economic European și alte autorități similare.

(4) Autoritatea de supraveghere se conduce de legislația din domeniul protecției datelor cu caracter personal și la necesitate, ia în considerare actele emise de instituțiile Uniunii Europene în domeniul protecției datelor cu caracter personal.

Articolul 52. Independență

(1) Fiecare autoritate de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor sale și exercitarea competențelor sale în conformitate cu prezenta lege.

(2) Membrii sau conducătorii fiecărei autorități de supraveghere, în cadrul îndeplinirii sarcinilor și al exercitării competențelor sale în conformitate cu prezenta lege, rămâne independent de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la o parte

externă.

(3) Membrii sau conducătorii fiecărei autorități de supraveghere se abțin de la a întreprinde acțiuni incompatibile cu atribuțiile lor, iar pe durata mandatului, nu desfășoară activități incompatibile, remunerate sau nu.

(4) Fiecare autoritate de supraveghere beneficiază de resurse umane, tehnice și financiare, de un sediu și de infrastructura necesară pentru îndeplinirea sarcinilor și exercitarea efectivă a competențelor sale, inclusiv a celor care urmează să fie aplicate în contextul asistenței reciproce.

(5) Fiecare

autoritate de supraveghere își selectează personalul propriu și deține personal propriu aflat sub conducerea exclusivă a membrilor sau a conducătorilor autorității de supraveghere respective.

(6) Fiecare autoritate de supraveghere face obiectul unui control financiar din partea Curții de Conturi a Republicii Moldova, care nu aduce atingere independenței sale și că dispune de bugete anuale distincte, publice, care pot face parte din bugetul general de stat sau național.

(7) Autoritatea de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor sale și exercitarea competențelor sale în conformitate cu prezenta lege.

Articolul 53. Condiții generale aplicabile conducerii CNPDCP

(1) CNPDCP este condusă de un director care este numit de Parlamentul Republicii Moldova prin concurs, pentru un mandat de 7 ani, fără dreptul de a fi numit din nou în această funcție consecutiv, care este asistat de 2 adjuncți numiți de directorul CNPDCP. Directorii și directorii adjuncți, trebuie să dețină cetățenia Republicii Moldova, calificări, experiență și competențe necesare, în special în domeniul protecției datelor cu caracter personal nu mai puțin de 5 ani.

(2) Numirea sau încetarea mandatului de director al CNPDCP se dispune de Parlament, cu votul a 3/5 a majorității deputaților aleși din numărul deputaților aleși.

(3) În cazul în care termenul de exercitare a mandatului a expirat, directorul CNPDCP continuă să se afle în exercițiul funcției până la preluarea acestei funcții de către succesorul său, dar nu mai mult de 6 luni.

(4) Prin derogare de la alin. (1), atribuțiile directorului CNPDCP încetează în cazul expirării mandatului, în cazul demisiei sau pensionării.

(5) Directorul și directorii adjuncți ai CNPDCP pot fi demși în condițiile Legii nr. 199/2010 cu privire la statutul persoanelor cu funcție de demnitate publică.

Articolul 54. Norme privind instituirea autorității de supraveghere

(1) Actele normative trebuie să conțină:

a) Instituirea autorității de supraveghere;

b) calificările și condițiile de eligibilitate necesare pentru a fi numit în calitate de membru al autorității de supraveghere;

c) normele și procedurile pentru numirea membrului sau a membrilor autorității de supraveghere;

d) durata mandatului membrului sau membrilor fiecărei autorități de supraveghere, de minimum patru ani;

- e) dacă și de câte ori este eligibil pentru reînnoire mandatul membrului sau membrilor fiecărei autorități de supraveghere;
- f) condițiile care reglementează obligațiile membrului sau membrilor și ale personalului fiecărei autorități de supraveghere, interdicții privind acțiunile, ocupațiile și beneficiile incompatibile cu acestea în cursul mandatului și după încetarea acestuia, precum și normele care reglementează încetarea contractului de angajare.

(2) Membrii, conducătorii și angajații autorităților de supraveghere au obligația, de a respecta atât pe parcursul mandatului sau a raporturilor de muncă, cât și după încetarea acestuia, secretul profesional în ceea ce privește informațiile confidențiale de care au luat cunoștință în cursul îndeplinirii sarcinilor sau al exercitării competențelor lor. Pe durata mandatului/funcțiilor lor, această obligație de păstrare a secretului profesional se aplică în special în ceea ce privește raportarea de către persoane fizice a încălcărilor prezentei legi.

Secțiunea 2

Abilități, sarcini și competențe

Articolul 55. Sarcini

(1) Fără a aduce atingere altor sarcini stabilite în temeiul prezentei legi, autoritatea de supraveghere:

- a) monitorizează și asigură aplicarea prezenta lege;
- b) promovează acțiuni de sensibilizare și de înțelegere în rândul publicului a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare. Se acordă atenție specială activităților care se adresează în mod specific copiilor;
- c) oferă consiliere Parlamentului Republicii Moldova, Guvernului Republicii Moldova și altor instituții și organisme cu privire la măsurile legislative și administrative referitoare la protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea;
- d) promovează acțiuni de sensibilizare a operatorilor și a persoanelor împuternicite de aceștia cu privire la obligațiile care le revin în temeiul prezenta lege;
- e) la cerere, furnizează informații oricărei persoane vizate în legătură cu exercitarea drepturilor sale în conformitate cu prezenta lege și, dacă este cazul, cooperează cu autoritățile de supraveghere din alte state în acest scop;
- f) tratează plângerile depuse de o persoană vizată, un organism, o organizație sau o asociație în conformitate cu art.62 și investighează într-o măsură adecvată obiectul plângerii și informează reclamantul cu privire la evoluția și rezultatul investigației, într-un termen rezonabil, în special dacă este necesară efectuarea unei investigații mai amănunțite sau coordonarea cu o altă autoritate de supraveghere;
- g) cooperează, inclusiv prin schimb de informații, cu alte autorități de supraveghere și își oferă asistență reciprocă pentru a asigura coerența aplicării și respectării prezentei legi;
- h) desfășoară investigații privind aplicarea prezentei legi, inclusiv pe baza unor informații primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică;
- i) monitorizează evoluțiile relevante, în măsura în care acestea au impact asupra protecției datelor cu caracter personal, în special evoluția tehnologiilor informației și comunicațiilor și a practicilor comerciale;
- j) adoptă clauze contractuale standard menționate la art. 28 alin. (8) și la art.46 alin. (2) lit.d);
- k) întocmește și menține la zi o listă în legătură cu cerința privind evaluarea impactului asupra protecției datelor, în conformitate cu art.35 alin.(4).

- l) oferă consiliere cu privire la operațiunile de prelucrare menționate la art. 36 alin. (2);
- m) încurajează elaborarea de coduri de conduită în conformitate cu art. 40 alin.(1), își dă avizul cu privire la acestea și le aprobă pe cele care oferă suficiente garanții, în conformitate cu art. 40 alin. (5);
- n) încurajează stabilirea unor mecanisme de certificare, precum și a unor sigilii și mărci în domeniul protecției datelor în conformitate cu art. 42 alin.(1) și aprobă criteriile de certificare în conformitate cu art.42 alin.(5);
- o) acolo unde este cazul, efectuează o revizuire periodică a certificărilor acordate, în conformitate cu art. 42 alin. (7);
- p) elaborează și publică criteriile de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu art. 41 și a unui organism de certificare în conformitate cu art. 43;
- q) coordonează procedura de acreditare a unui organism de monitorizare a codurilor de conduită în conformitate cu art. 41 și a unui organism de certificare în conformitate cu art. 43;
- r) autorizează clauzele și dispozițiile contractuale menționate la art. 46 alin. (3);
- s) aprobă regulile corporatiste obligatorii în conformitate cu art. 47;
- t) ține cont de practica Uniunii Europene în domeniul protecției datelor cu caracter personal;
- u) menține la zi evidențe interne privind încălcările prezentei legi și măsurile luate, în special avertismentele emise și sancțiunile impuse în conformitate cu art. 56 alin. (2);
- v) îndeplinește orice alte sarcini legate de protecția datelor cu caracter personal.

(2) Autoritatea de supraveghere facilitează depunerea plângerilor menționate la alin.

(1) Lit. f) prin măsuri precum punerea la dispoziție a unui formular de depunere a plângerii care să poată fi completat inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

(3) Îndeplinirea sarcinilor autorității de supraveghere este gratuită pentru persoana vizată și, după caz, pentru responsabilul cu protecția datelor.

(4) În cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, autoritatea de supraveghere poate percepe o taxă rezonabilă, bazată pe costurile administrative, sau poate refuza să le trateze. Sarcina de a demonstra caracterul evident nefondat sau excesiv al cererii revine autorităților de supraveghere.

Articolul 56. Competențe

(1) Autoritatea de supraveghere are următoarele competențe de investigare:

- a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale;
- b) de a efectua investigații sub formă de audituri privind protecția datelor conform Capitolului IX din prezenta lege;
- c) de a efectua o revizuire a certificărilor acordate în temeiul art.42 alin. (7);
- d) de a notifica operatorul sau persoana împuternicită de operator cu privire la presupusa încălcare a prezentei legi;
- e) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale;
- f) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu actele normative;

(2) Fiecare autoritate de supraveghere are toate următoarele competențe corective:

- a) de a emite avertizări în atenția unui operator sau a unei persoane împuternicite de operator cu privire la posibilitatea ca operațiunile de prelucrare prevăzute să încalce dispozițiile prezentei legi;
- b) de a emite muștrări adresate unui operator sau unei persoane împuternicite de operator în cazul în care operațiunile de prelucrare au încălcat dispozițiile prezentei legi;
- c) de a da dispoziții operatorului sau persoanei împuternicite de operator să respecte cererile persoanei vizate de a-și exercita drepturile în temeiul prezentei legi;
- d) de a da dispoziții operatorului sau persoanei împuternicite de operator să asigure conformitatea operațiunilor de prelucrare cu dispozițiile prezentei legi, specificând, după caz, modalitatea și termenul-limită pentru aceasta;
- e) de a obliga operatorul să informeze persoana vizată cu privire la o încălcare a protecției datelor cu caracter personal;
- f) de a impune o limitare temporară sau definitivă, inclusiv o interdicție asupra prelucrării;
- g) de a dispune rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării, în temeiul art. 16, 17 și 18, precum și notificarea acestor acțiuni destinatarilor cărora le-au fost divulgate datele cu caracter personal, în conformitate cu art. 17 alin. (2) și cu art. 19;
- h) de a retrage o certificare sau de a obliga organismul de certificare să retragă o certificare eliberată în temeiul art.42 și 43 sau de a obliga organismul de certificare să nu elibereze o certificare în cazul în care cerințele de certificare nu sunt sau nu mai sunt îndeplinite;
- i) de a impune amenzi administrative în conformitate cu art. 64, în completarea sau în locul măsurilor menționate la prezentul alineat, în funcție de circumstanțele fiecărui caz în parte;
- j) de a dispune suspendarea fluxurilor de date către un destinatar dintr-o țară terță sau către o organizație internațională;

(3) Fiecare autoritate de supraveghere are toate următoarele competențe de autorizare și de consiliere:

- a) de a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă menționată la art. 36;
- b) de a emite avize, din proprie inițiativă sau la cerere, Parlamentului Republicii Moldova, Guvernului Republicii Moldova, altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal;
- c) de a autoriza prelucrarea menționată la art.36 alin. (5), în cazul în care actele normative prevăd o astfel de autorizare prealabilă;
- d) de a emite un aviz și de a aproba proiectele de coduri de conduită, în conformitate cu art. 40 alin. (5);
- e) de a acredita organismele de certificare în conformitate cu art. 43;
- f) de a emite certificări și de a aproba criterii de certificare în conformitate cu art.42 alin.(5);
- g) de a adopta clauzele standard în materie de protecție a datelor menționate la art. 28 alin. (8) și la art. 46 alin. (2) lit. d);
- h) de a autoriza clauzele contractuale menționate la art. 46 alin. (3) lit. a);
- i) de a autoriza acordurile administrative menționate la art. 46 alin. (3) lit. b);
- j) de a aproba reguli corporatiste obligatorii în conformitate cu art.47;
- k) de a emite acte normative necesare pentru aplicarea prevederilor prezentei legi.

(4) Exercițarea competențelor conferite în temeiul prezentului articol face obiectul unor garanții adecvate, inclusiv căi de atac judiciare eficiente și procese echitabile, prevăzute în actele normative.

(5) Autoritatea de supraveghere are competența de a aduce în fața autorităților judiciare cazurile de încălcare a prezentei legi și, după caz, de a iniția sau de a se implica într-un alt mod în proceduri

judiciare, în scopul de a asigura aplicarea dispozițiilor prezentei legi.

(6) Actele normative pot să prevadă faptul că autoritatea de supraveghere are competențe suplimentare, în afara celor menționate la alin. (1), (2) și (3).

Articolul 57. Rapoarte de activitate

(1) Anual, până la data de 1 aprilie, autoritatea de supraveghere prezintă Parlamentului raportul de activitate pentru anul precedent.

(2) Raportul de activitate se publică pe pagina web oficială a autorității de supraveghere.

Articolul 58. Cooperarea autorităților de supraveghere

Autoritatea de supraveghere cooperează cu alte autorități de supraveghere din Spațiul Economic European, după caz, din alte țări terțe.

CAPITOLUL VII

CĂI DE ATAC, RĂSPUNDEREA ȘI SANCTIUNILE

Articolul 59. Dreptul de a depune o plângere la o autoritate de supraveghere

(1) Fără a aduce atingere oricăror alte căi de atac administrative sau judiciare, orice persoană vizată are dreptul de a depune o plângere la o autoritate de supraveghere.

(2) Autoritatea de supraveghere informează reclamantul cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a exercita o cale de atac judiciară în temeiul art. 60.

Articolul 60. Dreptul la o cale de atac judiciară eficientă împotriva unei autorități de supraveghere

(1) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană fizică sau juridică are dreptul de a exercita o cale de atac judiciară eficientă împotriva unei decizii obligatorii din punct de vedere juridic a unei autorități de supraveghere care o vizează.

(2) Fără a aduce atingere oricăror alte căi de atac administrative sau nejudiciare, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care Autoritatea de supraveghere care este competentă în temeiul art. 51 nu tratează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse în temeiul art. 59, prin adresarea directă în instanța de contencios administrativ competentă.

Articolul 61. Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau unei persoane împuternicite de operator

Fără a aduce atingere vreunei căi de atac administrative sau nejudiciare disponibile, inclusiv dreptului de a depune o plângere către autoritate de supraveghere în temeiul art. 59, fiecare persoană vizată are dreptul de a exercita o cale de atac judiciară eficientă în cazul în care consideră că drepturile de care beneficiază în temeiul prezentei legi au fost încălcate ca urmare a prelucrării datelor sale cu caracter personal fără a se respecta prezenta lege.

Articolul 62. Reprezentarea persoanelor vizate

(1) Persoana vizată are dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ, care au fost constituite în mod corespunzător, ale căror obiective statutare sunt de interes public, care sunt active în domeniul protecției drepturilor și libertăților persoanelor vizate în ceea ce privește protecția datelor lor cu caracter personal, să depună plângerea în numele său, să exercite în numele său drepturile menționate la art. 59, 60 și 61, precum și să exercite dreptul de a primi despăgubiri menționat la art. 63 în numele persoanei vizate, dacă acest lucru este prevăzut în actele normative.

(2) Organismele, organizațiile sau asociațiile menționate la alin. (1), independent de mandatul unei persoane vizate, au dreptul de a depune o plângere la autoritatea de supraveghere care este competentă în temeiul art. 59 și de a exercita drepturile menționate la art. 60 și 61, în cazul în care consideră că drepturile unei persoane vizate în temeiul prezentei legi au fost încălcate ca urmare a prelucrării.

Articolul 64. Condiții generale pentru impunerea amenzilor administrative

(1) Autoritatea de supraveghere asigură faptul că impunerea unor amenzi administrative în conformitate cu prezentul articol pentru încălcările prezentei legi menționate la alin. (4), (5) și (6) este, în fiecare caz, eficace, proporțională și disuasivă.

(2) În funcție de circumstanțele fiecărui caz în parte, amenzile administrative sunt impuse în completarea sau în locul măsurilor menționate la art. 56 alin. (2) lit. a)-h) și j). Atunci când se ia decizia dacă să se impună o amendă administrativă și decizia cu privire la valoarea amenzii administrative în fiecare caz în parte, se acordă atenția cuvenită următoarelor aspecte:

- a) natura, gravitatea și durata încălcării, ținându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum și de numărul persoanelor vizate afectate și de nivelul prejudiciilor suferite de acestea;
- b) dacă încălcarea a fost comisă intenționat sau din neglijență;
- c) orice acțiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de persoana vizată;
- d) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ținându-se seama de măsurile tehnice și organizatorice implementate de aceștia în temeiul art. 25 și 32;
- e) eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;
- f) gradul de cooperare cu autoritatea de supraveghere pentru a remedia încălcarea și a atenua posibilele efecte negative ale încălcării;
- g) categoriile de date cu caracter personal afectate de încălcare;
- h) modul în care încălcarea a fost adusă la cunoștința autorității de supraveghere, în special dacă și în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;
- i) în cazul în care măsurile menționate la art. 56 alin. (2) au fost dispuse anterior împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la același obiect, respectarea respectivelor măsuri;
- j) aderarea la coduri de conduită aprobate, în conformitate cu art.40, sau la mecanisme de certificare aprobate, în conformitate cu art. 42;
- k) orice alt factor agravant sau atenuant aplicabil circumstanțelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(3) În cazul în care un operator sau o persoană împuternicită de operator încalcă în mod intenționat sau din neglijență, pentru aceeași operațiune de prelucrare sau pentru operațiuni de prelucrare

conexe, mai multe dispoziții din prezenta lege, cuantumul total al amenzii administrative nu poate depăși suma prevăzută pentru cea mai gravă încălcare.

(4) Pentru încălcările dispozițiilor următoare, în conformitate cu alin. (2), se aplică amenzi administrative de până la 2 000 000 lei sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare:

- a) obligațiile operatorului și ale persoanei împuternicite de operator în conformitate cu art. 8, 11, 25-39, 42 și 43;
- b) obligațiile organismului de certificare în conformitate cu art. 42 și 43;
- c) obligațiile organismului de monitorizare în conformitate cu art. 41 alin. (4).

(5) Pentru încălcările dispozițiilor următoare, în conformitate cu alin. (2), se aplică amenzi administrative de până la 4 000 000 lei sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare:

- a) principiile de bază pentru prelucrare, inclusiv condițiile privind consimțământul, în conformitate cu art. 5, 6, 7 și 9;
- b) drepturile persoanelor vizate în conformitate cu art. 12-22;
- c) transferurile de date cu caracter personal către un destinatar dintr-o țară terță sau o organizație internațională, în conformitate cu art. 44-49;
- d) orice obligații în temeiul actelor normative adoptate în temeiul Capitolului VIII;
- e) nerespectarea unui ordin sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de autoritatea de supraveghere în limitele prevăzute de lege, în temeiul art. 56 alin. (2), sau neacordarea accesului, încălcând art. 56 alin. (1);

(6) Pentru încălcarea unui ordin emis de autoritatea de supraveghere în conformitate cu art. 57 alin. (2) se aplică, în conformitate cu alin. (2), amenzi administrative de până la 4 000 000 lei sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.

(7) Fără a aduce atingere competențelor corective ale autorității de supraveghere menționate la art. 56 alin. (2), sancțiunile prevăzute de prezentul articol se aplică și autorităților publice, conform prezentei legi.

(8) Exercițarea de către autoritatea de supraveghere a competențelor sale în temeiul prezentului articol are loc cu condiția existenței unor garanții procedurale adecvate în conformitate cu actele normative, inclusiv căi de atac judiciare eficiente și dreptul la un proces echitabil.

Articolul 65. Sancțiuni

Prin lege, pot fi stabilite norme privind alte sancțiunile aplicabile în caz de încălcare a prezentei lege, în special pentru încălcări care nu fac obiectul unor amenzi administrative în temeiul art. 64, și iau toate măsurile necesare pentru a garanta faptul că acestea sunt puse în aplicare. Sancțiunile respective sunt eficace, proporționale și disuasive.

CAPITOLUL VIII

DISPOZIȚII REFERITOARE LA SITUAȚII SPECIFICE DE PRELUCRARE

Articolul 66. Prelucrarea și libertatea de exprimare și de informare

(1) Actele normative asigură un echilibru între dreptul la protecția datelor cu caracter personal în temeiul prezentei legi și dreptul la libertatea de exprimare și de informare, inclusiv prelucrarea în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare.

(2) (2) Pentru prelucrarea efectuată în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare, se instituie următoarele derogări de la prezenta lege: capitolul II (principii), capitolul III (drepturile persoanei vizate), capitolul IV (operatorul și persoana împuternicită de operator), capitolul V (transferul datelor cu caracter personal către țări terțe sau organizații internaționale), capitolul VI (autorități de supraveghere independente), capitolul VII (cooperare și coerență) și capitolul IX (situații specifice de prelucrare a datelor) în cazul în care acestea sunt necesare pentru a asigura un echilibru între dreptul la protecția datelor cu caracter personal și libertatea de exprimare și de informare.

Articolul 67. Prelucrarea și accesul public la documente oficiale

Datele cu caracter personal din documentele oficiale deținute de o autoritate publică sau de un organism public sau privat pentru îndeplinirea unei sarcini care servește interesului public pot fi divulgate de autoritatea sau organismul respectiv în conformitate cu actele normative, pentru a stabili un echilibru între accesul public la documente oficiale și dreptul la protecția datelor cu caracter personal în temeiul prezentei legi.

Articolul 68. Prelucrarea unui număr de identificare național

Prelucrarea unui număr de identificare național sau a oricărui alt identificator cu aplicabilitate generală este determinat de actele normative. În acest caz, numărul de identificare național sau orice alt identificator cu aplicabilitate generală este folosit numai în temeiul unor garanții corespunzătoare pentru drepturile și libertățile persoanei vizate în conformitate cu cerințele prezentei legi.

Articolul 69. Prelucrarea în contextul ocupării unui loc de muncă

(1) Prin lege sau prin acorduri colective, pot fi prevăzute norme mai detaliate pentru a asigura protecția drepturilor și a libertăților cu privire la prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al egalității și diversității la locul de muncă, al asigurării sănătății și securității la locul de muncă, al protejării proprietății angajatorului sau a clientului, precum și în scopul exercitării și beneficierii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și pentru încetarea raporturilor de muncă.

(2) Aceste norme includ măsuri corespunzătoare și specifice pentru garantarea demnității umane, a intereselor legitime și a drepturilor fundamentale ale persoanelor vizate, în special în ceea ce privește transparența prelucrării, transferul de date cu caracter personal în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună și sistemele de monitorizare la locul de muncă.

Articolul 70. Garanții și derogări privind prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice

(1) Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice are loc cu condiția existenței unor garanții corespunzătoare, în conformitate cu prezenta lege, pentru drepturile și libertățile persoanelor vizate. Respectivă garanție asigură faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivă măsuri pot include pseudonimizarea, cu condiția ca respectivă scopuri să fie îndeplinite în acest mod. Atunci când respectivă scopuri pot fi îndeplinite printr-o prelucrare ulterioară care nu permite sau nu mai permite identificarea persoanelor vizate, scopurile respective sunt îndeplinite în acest mod.

(2) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică ori în scopuri statistice, actele normative pot să prevadă derogări de la drepturile menționate la art. 15, 16, 18 și 21, sub rezerva condițiilor și a garanțiilor prevăzute la alin. (1), în măsura în care drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

(3) În cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public, actele normative pot să prevadă derogări de la drepturile menționate la art. 15, 16, 18, 19, 20 și 21, sub rezerva condițiilor și a garanțiilor prevăzute la alin. (1), în măsura în care drepturile respective sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

(4) În cazul în care prelucrarea menționată la alin. (2) și (3) servește în același timp și altui scop, derogările se aplică numai prelucrării în scopurile menționate la alineatele respective.

Articolul 71. Obligații privind păstrarea confidențialității

Pot fi adoptate norme specifice pentru a stabili competențele autorității competente, prevăzute la art. 56 alin. (1) lit. e) și f), în legătură cu operatori sau cu persoane împuternicite de operatori care, în temeiul actelor normative, au obligația de a păstra secretul profesional sau alte obligații echivalente de confidențialitate, în cazul în care acest lucru este necesar și proporțional pentru a stabili un echilibru între dreptul la protecția datelor cu caracter personal și obligația păstrării confidențialității. Respectivă norme se aplică doar în ceea ce privește datele cu caracter personal pe care operatorul sau persoana împuternicită de operator le-a primit în urma sau în contextul unei activități care intră sub incidența acestei obligații de păstrare a confidențialității.

Articolul 72. Normele existente în domeniul protecției datelor pentru biserici și asociații religioase

(1) În cazul în care, bisericile și asociațiile sau comunitățile religioase aplică, la data intrării în vigoare a prezentei legi, un set cuprinzător de norme de protecție a persoanelor fizice cu privire la prelucrare, aceste norme pot continua să se aplice, cu condiția să fie aliniate la prezenta lege.

(2) Bisericele și asociațiile religioase care aplică un set cuprinzător de norme în conformitate cu alin. (1) sunt supuse supravegherii din partea CNPDCP.

Capitolul IX DEPUEREA PLÂNGERILOR ȘI MODUL DE EFECTUARE A INVESTIGAȚIILOR

Articolul 73. Cerințe pentru depunerea plângerii

(1) Plângerea poate fi înaintată pe suport de hârtie cu aplicarea semnăturii olografe sau în format electronic în corespundere cu Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere.

(2) Plângerea trebuie să cuprindă:

a) numele, prenumele persoanei vizate, semnătura, adresa de domiciliu sau adresa electronică, după caz, alte date de contact, împuternicirile legale ale reprezentantului;

b) specificarea într-un mod cât mai detaliat posibil a faptelor și circumstanțelor care stau la baza faptei deplânse autorității de supraveghere în raport cu cerințele prezentei legi;

c) dacă se cunosc: informații cu privire la identitatea operatorului sau a persoanei împuternicite de operator, dacă obiectul cererii a fost sau se examinează de o instanță de judecată sau de alte entități competente, realizarea drepturilor persoanei vizate, alte informații relevante cauzei.

Articolul 74. Investigația

(1) Investigația reprezintă activitatea desfășurată de colectare și administrare a informațiilor, privind legalitatea prelucrărilor de date și a măsurilor de protecție asigurate, prevăzute de actele normative.

(2) Investigațiile sunt de 2 tipuri: planificate sub formă de audit sau inopinate, în ambele cazuri cu sau fără ieșirea la fața locului. Planificarea investigațiilor sub formă de audituri se va realiza conform metodologiei și criteriilor aprobate prin act normativ emis de CNPDCP.

(3) Investigația începe odată cu înregistrarea plângerii sau din oficiu în baza notei motivate, cu excepția cazurilor când același obiect cu aceleași părți a fost examinat anterior.

(4) La efectuarea investigației, CNPDCP are în vedere prioritar posibilitatea efectuării acesteia prin solicitare directă de la persoana investigată a documentației și a altor informații sau prin alte metode care fac posibilă obținerea unor astfel de date. Doar în cazul insuficienței documentației și informației deținute pentru a stabili respectarea legislației de către persoana supusă investigației sau reieșind din tipul investigației și analiza riscurilor, CNPDCP va realiza investigația la fața locului. În cazul solicitărilor directe de informații fără ieșirea la fața locului, în demersurile adresate, CNPDCP va specifica datele indicate la alin. (5) cu excepția celor indicate la lit. a).

(5) Delegația de efectuare a investigației cu ieșirea la fața locului va conține cel puțin:

a) numărul și data emiterii;

b) date de identificare a CNPDCP;

c) trimitere la prevederile legale, în baza căruia este realizată investigația;

d) tipul investigației și temeiul inițierii lui;

e) date despre inspector/i (nume, prenume, funcția deținută);

f) date despre persoana supusă controlului (denumirea/numele persoanei; în cazul persoanei juridice codul fiscal; sediul/adresa subdiviziunii controlate și codul acesteia, după caz, alte date de

contact);

g) obiectul controlului;

h) scopul, aspectele ce urmează a fi verificate și după caz, respectarea cerințelor prezentei legi și actelor normative ale CNPDCP;

i) data începerii controlului și durata preconizată a acestuia.

(6) Delegația privind efectuarea investigației cu ieșirea la fața locului se aduce la cunoștință sub semnătură persoanei, entității supuse investigației, sau reprezentantului legal. În cazul refuzului primirii și semnării delegației se întocmește un act, în prezența unui martor. Prezența martorului nu este necesară în cazul înregistrării refuzului prin mijloace video și audio.

(7) Inspectorii de protecție a datelor în limita împuternicirilor ce rezultă din alin. (4) și (5) au următoarele drepturi:

a) să dispună de acces și să examineze informațiile și sistemele de evidență care conțin date personale, soluțiile software și suporturile hardware, datele cu caracter personal și orice mijloace sau documente legate de obiectul și scopul investigației, indiferent de echipamentul și/sau suportul pe care sunt stocate datele personale;

b) să aibă acces în orice spații și încăperi, aflate în proprietatea sau folosința persoanelor vizate în cadrul investigației;

c) să solicite și să primească informațiile, documentele și explicațiile solicitate în termenul stabilit, care trebuie să fie rezonabil dar nu mai mare de 15 zile. Termenul poate fi prelungit la solicitarea motivată a persoanei investigate;

d) să audieze și să solicite persoanei, supuse investigației sau reprezentantului legal, sau altor persoane care pot oferi CNPDCP informațiile necesare pentru soluționarea unei cereri în legătură cu prelucrarea datelor cu caracter personal în cadrul investigației și, după caz, de a înregistra, răspunsurile acestora, inclusiv prin mijloace audio, video sau prin alte mijloace, cu informarea prealabilă a persoanei supuse investigației;

e) să solicite și să primească informațiile referitoare la obiectul și scopul investigației, stocate pe calculatoare sau alte dispozitive electronice, într-o formă care să permită ridicarea și transportarea acestora, precum și să fie lizibile;

f) să solicite sprijinul subdiviziunilor abilitate ale organelor de ocrotire a normelor de drept, în cadrul efectuării investigației care sunt obligate să acorde asistența necesară angajaților CNPDCP. La efectuarea investigației pot fi antrenați, după caz, și experți din anumite domenii, împuterniciți de CNPDCP;

(9) Pe parcursul efectuării investigației, inspectorii de protecție a datelor sunt obligați:

a) să informeze persoana supusă investigării despre drepturile și obligațiile acesteia;

b) să prezinte delegația de investigație în cazul ieșirii la fața locului sau informațiile prevăzute la art. 74 alin. (5) lit. b) – i).

c) să efectueze investigația în conformitate cu împuternicirile atribuite de prezenta lege, ținând cont de obiectul și scopul acestuia.

(10) Pe parcursul efectuării investigației, persoana verificată are următoarele drepturi:

a) să fie informată și să obțină o copie a delegației privind efectuarea investigației la fața locului sau informațiile prevăzute la art. 74 alin. (5) lit. b) – i);

b) să prezinte probe în cadrul efectuării investigației;

c) să prezinte explicații înregistrate sub orice formă referitoare la obiectul și scopul investigației;

d) să obțină lista mijloacelor, sistemelor de evidență și documentelor ridicate pe parcursul investigației, semnată de inspectorul de protecție a datelor; e) să fie asistată de avocați, de alți reprezentanți împuterniciți conform legislației.

(11) Dacă persoana supusă investigației cu ieșirea la fața locului solicită prezența avocatului, efectuarea investigației se suspendă până la prezentarea avocatului, dar nu mai mult de 2 ore.

(12) Toate persoanele juridice de drept public sau drept privat și persoanele fizice sunt obligate să se supună investigației efectuate de CNPDCP, inclusiv prin asigurarea condițiilor pentru buna desfășurare a investigației.

(13) Investigația cu ieșirea la fața locului se desfășoară în orele de program ale persoanei juridice.

(14) Rezultatul investigației este consemnat în proiectul de decizie asupra investigației, care se pune la dispoziție persoanei vizate și operatorului sau persoanei împuternicite care au făcut obiectul investigației prin mijloacele disponibile, cu acordarea unui termen de 14 zile pentru înaintarea unor eventuale obiecții. Dacă au fost consumate căile rezonabile de aducere la cunoștință a proiectului de decizie sau se constată eschivarea părților vizate de investigație, CNPDCP emite decizia, în termen de până la 30 de zile.

(15) În cadrul efectuării investigației, inspectorul de protecție a datelor se supune prevederilor legale și efectuează acțiunile de investigare necesare. Orice imixtiune în activitatea de investigare este interzisă și se pedepsește conform legii.

(16) Termenul de efectuare a investigației este de până la 3 luni, cu posibilitatea prelungirii justificate a acestuia cu 30 de zile, dar nu mai mult de 6 luni.

(17) Dacă plângerea nu întrunește cerințele prevăzute de art. 73, aceasta se examinează conform prevederilor Codului administrativ.

Articolul 75. Confidențialitatea investigației

(1) Persoanele care, în virtutea drepturilor și atribuțiilor ce le revin în temeiul prezentei legi, au luat cunoștință de informațiile investigației, inclusiv alte persoane care le-au devenit cunoscute astfel de informații, au obligația să asigure confidențialitatea acestora, în condițiile legislației.

(2) Materialele dosarului acumulate în cadrul investigației, nu pot fi ridicate, interceptate, obținute și/sau utilizate în oricare alte scopuri ulterioare, dacă ar putea înrăutăți situația persoanei vizate, cu excepția cazurilor necesare înfăptuirii justiției.

(3) Inspectorul de protecție a datelor, persoana vizată sau alte persoane, care în virtutea drepturilor și atribuțiilor ce le revin în temeiul prezentei legi, au luat cunoștință sau le-au devenit cunoscute informațiile din cadrul investigației nu pot fi audiați sau interogați de către alte organe sau

organizații în ceea ce privește esența informațiilor din cadrul investigației, cu excepția instanței de judecată.

(4) CNPDCP publică deciziile anonimizate pe pagina oficială web.

Articolul 76. Accesul și păstrarea materialelor investigației

(1) Persoanele vizate și persoanele supuse investigației, au dreptul de a obține acces la materialele și informațiile acumulate în cadrul investigațiilor.

(2) Până la emiterea deciziei conform art. 77, accesul la materialele acumulate poate fi oferit în condițiile alin. (1) doar dacă inspectorul de protecție a datelor consideră posibil, să nu fie afectate interesele altor persoane, de a evita obstrucționarea și/sau prejudicierea investigației sau cerințele legale cu privire la informația cu accesibilitate limitată.

(3) Materialele investigației se păstrează pe o perioadă de 10 ani.

Articolul 77. Emiterea și comunicarea deciziilor

(1) La finalizarea investigației, dacă probele acumulate sunt suficiente, CNPDCP emite decizia motivată privind constatarea sau lipsa încălcării cu emiterea măsurilor prevăzute de art. 56 alin.

(2). În cazul consumării tuturor mijloacelor rezonabile de acumulare a probelor, CNPDCP dispune încetarea investigației din motivul imposibilității acumulării probelor.

(2) Decizia se emite de către director sau directorii adjuncți ai CNPDCP și inspectorii de protecție a datelor în conformitate cu competențele atribuite prin ordinul directorului.

Articolul 78. Executarea deciziilor Centrului

(1) Deciziile devin executorii și urmează a fi îndeplinite în termenul menționat în ele, cu obligația de a informa în scris CNPDCP despre măsurile întreprinse. CNPDCP poate stabili termenul de executare a deciziei de până la 6 luni. În cazuri complexe, atunci când decizia CNPDCP prevede implementarea unor măsuri corective complexe la solicitarea întemeiată a operatorului CNPDCP poate extinde termenul de executare a deciziei peste termenul de 6 luni.

(2) Deciziile CNPDCP sunt investite cu formulă executorie care conferă dreptul la executarea silită în sensul Codului de executare.

Articolul 79. Citarea

(1) CNPDCP poate cita părțile vizate de investigație.

(2) Citația este individuală și trebuie să cuprindă:

a) numele, prenumele sau denumirea persoanei citate, cu indicarea obiectului cauzei și scopului citării;

b) adresa persoanei citate, care trebuie să cuprindă: localitatea, strada, numărul casei, apartamentului, precum și orice alte date necesare pentru a preciza adresa celui citat;

c) ora, ziua, luna, anul și locul de prezentare a persoanei citate, menționându-se consecințele legale în caz de neprezentare;

d) mențiunea că persoana citată are dreptul să fie asistată de un avocat cu care să se prezinte la termenul fixat.

(3) Citarea se poate face la adresa de domiciliu sau adresa juridică, sau prin notă telefonică sau telegrafică, prin telefax, poștă electronică ori prin orice alt sistem de mesagerie electronică în cazul în care sunt disponibile mijloace necesare pentru a dovedi că citația a fost primită.

(4) În cazul în care citarea nu poate fi realizată în condițiile prezentului articol pe motiv că persoana citată nu a putut fi găsită sau din alte motive care pot fi invocate persoanei citate sau altor persoane, CNPDCP poate publica un anunț într-un ziar de nivel național sau local, în care se va menționa citarea persoanei. Publicarea citației în ziar se face cu cel puțin 15 zile înainte de data pentru care persoana citată urmează să se prezinte la CNPDCP. În cazuri de urgență CNPDCP poate reduce acest termen la 5 zile. Publicarea în presă a anunțului privind citarea persoanei se consideră citare legală.

CAPITOLUL X PERSONALUL CNPDCP

Articolul 80. Personalul CNPDCP

(1) Personalul CNPDCP este format din directorul și 2 directorii adjuncți supuși reglementărilor Legii nr. 199/2010 cu privire la statutul persoanelor cu funcții de demnitate publică, funcționari publici cu statut special-inspectorii de protecție a datelor (în continuare - inspector de protecție a datelor) și funcționari publici supuși reglementărilor Legii nr. 158/2008 cu privire la funcția publică și statutul funcționarului public, precum și personal contractual, supus reglementărilor legislației muncii.

(2) Conducerea Centrului, inspectorii de protecție a datelor și funcționarii publici ai CNPDCP dispun de legitimație, al căror modele sunt aprobate de director.

Articolul 81. Atribuțiile și drepturile conducerii CNPDCP

(1) Directorul exercită următoarele atribuții:

a) aprobă și semnează acte administrative cu caracter individual și normativ;

b) aprobă instrucțiuni și /ghiduri în domeniul protecției datelor cu caracter personal;

c) organizează și implementează sistemul de management financiar și control intern și poartă răspundere managerială pentru administrarea alocațiilor bugetare și a patrimoniului public aflat în gestiune;

d) aprobă regulamente interne ale CNPDCP;

e) numește în funcție, modifică, suspendă și încetează, în condițiile legii, raporturile de serviciu ale funcționarilor de demnitate publică, funcționarilor publici și ale funcționarilor publici cu statut special, angajează personalul contractual, modifică, suspendă și încetează raporturile de muncă al acestuia;

f) aprobă și modifică statul de personal și schema de încadrare ale CNPDCP, în conformitate cu prevederile legislației;

g) soluționează aspectele ce țin de stimularea sau stabilirea sporurilor la salariu și de acordare a

primelor în condițiile legii;

h) aplică sancțiuni disciplinare personalului CNPDCP;

i) asigură cooperarea cu autoritățile publice centrale și locale, cu mijloacele de informare în masă, cu asociațiile obștești, precum și cu instituțiile similare din străinătate;

j) acordă grade de calificare personalului Centrului;

k) delegă directorilor adjuncți și angajaților subdiviziunilor interne ale CNPDCP împuternicirile și atribuțiile necesare;

l) îndeplinește alte atribuții în conformitate cu legislația.

(2) Conducerea CNPDCP este în drept să solicite, conform art. 8 alin. (1) lit. a) din Legea nr. 245/2008 cu privire la secretul de stat, desecretizarea informațiilor privind faptele de încălcare a drepturilor omului la prelucrarea datelor cu caracter personal.

Articolul 82. Restricții

(1) Personalului CNPDCP îi este interzis:

a) să fie reprezentantul unui terț în cadrul CNPDCP;

b) să utilizeze în alte scopuri decât cele de serviciu mijloacele financiare, tehnico- materiale, informaționale și alte bunuri ale statului, precum și informația de serviciu;

c) să facă uz de serviciu în interesul personal, a oricăror persoane fizice, entități, partide, alte organizații politice, asociații obștești, inclusiv sindicale și comunități religioase;

d) să desfășoare alte activități incompatibile cu funcția de demnitate publică și funcția publică în conformitate cu prevederile legale, cu excepția activității didactice, științifice, sportive, de creație sau de participare în calitate de expert la nivel european sau internațional.

(2) Suplimentar restricțiilor prevăzute la alin. (1), directorul și directorii adjuncți ai CNPDCP pe perioada mandatului nu pot fi membri ai unui partid politic.

(3) Personalul CNPDCP în termen de o lună de la data numirii sau angajării sale este obligat să înceteze orice activitate incompatibilă cu statutul său.

Articolul 83. Obligațiile personalului CNPDCP

(1) Personalul CNPDCP este obligat:

a) să nu divulge datele cu caracter personal și alte informații oficiale cu accesibilitate limitată care i-a devenit cunoscută în exercițiul funcției, inclusiv după încetarea serviciului în cadrul CNPDCP, dacă legea nu prevede altfel;

b) să nu se lase influențat în luarea deciziilor de către persoane sau structuri din interiorul sau din afara instituției, iar comportamentul său să fie legal, rezervat și respectuos;

c) să asigure securitatea, integritatea și să preîntâmpine accesul persoanelor neautorizate asupra

documentelor și materialelor primite și gestionate în exercițiul funcției.

d) să execute ordinele și dispozițiile legale ale conducerii CNPDCP și/sau a conducătorului superior. În caz de primire din partea superiorului șefului său sau a altor persoane cu funcție de răspundere a unor ordine sau indicații ce vin în contradicție vădită cu legea, angajatul este obligat să asigure respectarea legii;

e) să comunice imediat conducătorului superior despre încercările terților de a-l influența în exercitarea atribuțiilor de serviciu.

Articolul 84. Protecția juridică

(1) Personalul CNPDCP nu poate fi atras la răspunderea penală, contravențională sau civilă pentru actele sau faptele îndeplinite în exercițiul funcției și într-o situație de risc profesional justificat. Riscul se consideră profesional justificat dacă acțiunile decurg în mod obiectiv din informația, faptele și circumstanțele cunoscute, iar scopul legii nu putea fi atins prin acțiuni ce nu ar fi implicat riscul, luându-se toate măsurile posibile pentru a preîntâmpina consecințele negative.

(2) Personalul CNPDCP nu poate fi audiat sau interogat referitor la esența informațiilor ce vizează viața intimă, familială și privată a persoanei vizate, de care a făcut cunoștință în cadrul exercitării atribuțiilor de serviciu cu excepția situației când acesta este audiat în cadrul unei ședințe de judecată. Acțiunile sau procedeele întreprinse cu încălcarea prevederilor prezentului alineat sunt lipsite de forță juridică.

Articolul 85. Statutul funcției de inspector de protecție

(1) Funcția de inspector de protecție a datelor este o funcție publică cu statut special, conferit datorită naturii atribuțiilor de serviciu, fiind exercitată în modul stabilit de prezenta lege și Legea nr. 158/2008 cu privire la funcția publică și statutul funcționarului public în măsura în care prezenta lege nu prevede altfel.

(2) Șefii subdiviziunilor Centrului în care activează inspectorii de protecție sunt funcționari publici cu statut special și au statut de inspectori de protecție a datelor.

Articolul 86. Garanțiile sociale

(1) Dacă, în exercitarea funcției, personalul CNPDCP i se cauzează vătămări a integrității corporale care îl fac incapabil să-și exercite atribuțiile de serviciu sau reduc semnificativ capacitatea de muncă stabilită în modul prevăzut de lege, acesta beneficiază de un ajutor unic echivalent cu mijloacele bănești de întreținere pentru 5 ani în ultima lui funcție din cadrul CNPDCP, precum și de dreptul de a i se achita timp de 10 ani diferența dintre ultimul salariul mediu lunar, din ultima lui funcție și cuantumul pensiei.

(2) Dacă, în procesul investigației, conducerii CNPDCP sau inspectorului de protecție i se cauzează o vătămare a integrității corporale care are urmări mai ușoare decât cele prevăzute la alin. (1), acestuia i se acordă un ajutor unic echivalent cu 5 salarii medii lunare.

(3) Prejudiciul cauzat bunurilor personalului CNPDCP sau bunurilor rudelor acestuia până la gradul I în legătură cu exercitarea atribuțiilor sale de serviciu se repară integral de la bugetul de stat, cu drept de regres împotriva persoanelor culpabile. Cuantumul mijloacelor financiare respective se stabilește și se acordă în temeiul hotărârii irevocabile a instanței de judecată.

CAPITOLUL XI

DISPOZIȚII FINALE ȘI TRANZITORII

Articolul 87. Dispoziții finale și tranzitorii

(1) Prezenta lege intră în vigoare în termen de 6 luni de la data publicării cu excepția alin. (2), (5) – (7) care intră în vigoare din momentul publicării prezentei legi.

(2) Structura și efectivul limită ale CNPDCP sunt stabilite prin Hotărârea Parlamentului la propunerea directorului autorității în termen de 6 luni din momentul publicării prezentei legi.

(3) Directorul și directorul adjunct al CNPDCP aflat în funcție la data intrării în vigoare a prezentei legi, își continuă mandatul pe perioada pentru care au fost numiți.

(4) Personalul CNPDCP, aflat în funcție la momentul intrării în vigoare a prezentei legi, se încadrează în funcțiile noi, cu acordul lui, la propunerea conducerii CNPDCP, fiindu-i păstrat cel puțin nivelul funcției deținute.

(5) În termen de 9 luni de la data publicării prezentei legi, CNPDCP:

a) va prezenta Parlamentului actele normative necesare punerii în aplicare a prezentei legi;

b) va aduce actele sale normative în concordanță cu prevederile prezentei legi.

(6) Guvernul va prezenta propuneri de modificare a legislației în vigoare, în scopul asigurării compatibilității cu prezenta lege.

(7) Ministerul Finanțelor va prevedea și aloca resursele necesare pentru implementarea prevederilor prezentei legi.

(8) Guvernul va asigura CNPDCP cu infrastructura necesară (spațiu de serviciu) pentru buna funcționare a acestuia.

(9) La data intrării în vigoare a prezentei legi se abrogă:

a) Legea nr. 182/2008 cu privire la aprobarea Regulamentului Centrului Național pentru Protecția Datelor cu Caracter Personal, structurii, efectivului-limită și a modului de finanțare a Centrului Național pentru Protecția Datelor cu Caracter Personal;

b) Legea nr. 133/2011 privind protecția datelor cu caracter personal.

(10) Din momentul intrării în vigoare a prezentei legi, din quantumul final al sancțiunii pecuniare stabilite de autoritatea de supraveghere, se va aplica:

a) în primul an – 10 procente din quantumul sancțiunii pecuniare stabilite;

b) în al doilea an - 40 procente din quantumul sancțiunii pecuniare stabilite;

c) în al treilea an – 100 procente din quantumul sancțiunii pecuniare stabilite.

(11) Plângerile și cauzele ale căror proceduri de examinare de către CNPDCP nu s-au încheiat până la data intrării în vigoare a prezentei legi, se examinează conform normelor de procedură prevăzute de prezenta lege. În cazul în care prezenta lege prevede o sancțiune mai gravă, încălcarea săvârșită anterior datei intrării în vigoare a prezentei legi va fi sancționată conform dispozițiilor actelor normative în vigoare la data săvârșirii acesteia. În situațiile în care, potrivit prezentei legi, fapta nu mai este considerată încălcare, aceasta nu se mai sancționează, chiar dacă a fost săvârșită înainte de data intrării în vigoare.

(12) Litigiile care la data intrării în vigoare a prezentei legi se află în proces de examinare se soluționează în conformitate cu normele legii în vigoare la data apariției litigiului.

PREȘEDINTELE PARLAMENTULUI