



CANCELARIA DE STAT A REPUBLICII MOLDOVA

Nr. 31/03-76-5075

Chișinău

8 mai 2024

**Biroul Permanent
al Parlamentului**

În temeiul articolului 73 din Constituția Republicii Moldova, se prezintă spre examinare proiectul de lege privind protecția datelor cu caracter personal, aprobat prin Hotărârea Guvernului nr. 328/2024.

Responsabil de prezentare în Parlament a proiectului de lege este Ministerul Justiției.

Anexe (933 file):

1. Hotărârea Guvernului cu privire la aprobarea proiectului de lege (în limba română și în limba rusă - 2 file);
2. Proiectul de lege (în limba română și în limba rusă - 139 file);
3. Nota informativă la proiectul de lege (46 file);
4. Sinteza obiecțiilor și propunerilor (284 file);
5. Declarațiile de compatibilitate (12 file);
6. Expertiza Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător (8 file);
7. Analiza de impact (16 file);
8. Raportul de expertiză al Centrului Național Anticorupție (7 file);
9. Alte avize (244 file);
10. Tabelul de concordanță (175 file).

Secretar general adjunct al Guvernului

Roman CAZAN

Ex.: Cătălina Șarpe
022 250 135

SECRETARIATUL PARLAMENTULUI REPUBLICII MOLDOVA		
D.D.P. Nr. <u>139</u>		
"08"	<u>05</u>	20 <u>24</u>
Ora _____		

Casa Guvernului,
MD-2012, Chișinău,
Republica Moldova

Telefon:
+ 373 22 250 104

E-mail:
cancelaria@gov.md



UE

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. 328

din 8 mai 2024

Chișinău

**Pentru aprobarea proiectului de lege
privind protecția datelor cu caracter personal**

Guvernul HOTĂRĂȘTE:

Se aprobă și se prezintă Parlamentului spre examinare proiectul de lege privind protecția datelor cu caracter personal.

Prim-ministru



DORIN RECEAN

Contrasemnează:

Ministrul justiției

Veronica Mihailov-Moraru

PARLAMENTUL REPUBLICII MOLDOVA**LEGE**
privind protecția datelor cu caracter personal

Parlamentul adoptă prezenta lege organică.

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), publicat în Jurnalul Oficial al Uniunii Europene L 119/1 din 4 mai 2016.

Capitolul I
DISPOZIȚII GENERALE**Articolul 1. Obiectul și scopul legii**

(1) Prezenta lege stabilește cadrul juridic cu privire la:

- a) protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal;
- b) organizarea și funcționarea Centrului Național pentru Protecția Datelor cu Caracter Personal (denumit în continuare și *Centru*);
- c) supravegherea implementării legislației privind protecția datelor cu caracter personal.
- d) răspunderea juridică și sancțiunile aplicate pentru încălcările legislației privind protecția datelor cu caracter personal.

(2) Prezenta lege are drept scop asigurarea protecției drepturilor și libertăților fundamentale ale persoanelor fizice și în special a dreptului la viața intimă, familială și privată, în legătură cu 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) atribuite la secret de stat, care se efectuează în conformitate cu Legea nr. 245/2008 cu privire la secretul de stat;

b) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice;

c) 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 securității publice și al prevenirii acestora;

d) referitoare la persoanele decedate, cu excepția cazului prevăzut la art. 52.

(3) Prezenta lege nu aduce atingere prevederilor Legii nr. 284/2004 privind serviciile societății informaționale, în special normelor privind răspunderea furnizorilor de servicii și a intermediarilor prevăzute la art. 14-17.

Articolul 3. Domeniul de aplicare teritorial

(1) Prezenta lege se aplică prelucrării datelor cu caracter personal în contextul 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 are sediu 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; sau

b) monitorizarea comportamentului lor dacă acesta se manifestă în cadrul Republicii Moldova.

(3) Prezenta lege se aplică prelucrării datelor cu caracter personal de către misiunile diplomatice și oficiile consulare ale Republicii Moldova, precum și de către alți operatori sau persoane împuternicite de operator care nu au sediu în Republica Moldova, dacă legislația Republicii Moldova se aplică în temeiul dreptului internațional public.

Articolul 4. Noțiuni

În sensul prezentei legi, următoarele noțiuni semnifică:

date cu caracter personal – orice informații privind o persoană fizică identificată sau identificabilă (în continuare – persoană vizată). Persoana 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;

prelucrare – 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;

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

creare de profiluri – 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;

pseudonimizare – 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;

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

operator – 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. În cazul în care scopurile și mijloacele prelucrării sunt stabilite de actele normative, operatorul sau criteriile specifice pentru desemnarea acestuia sunt prevăzute de actele normative respective;

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

sediu – exercitarea efectivă și reală a unei activități în cadrul unor aranjamente stabile.

destinatar – persoana fizică sau juridică, autoritatea publică, agenția sau alt organism căruia îi sunt divulgate datele cu caracter personal, indiferent dacă este sau nu o parte terță. Nu sunt considerate destinatari autoritățile publice cărora li se pot comunica date cu caracter personal în cadrul unei anumite anchete în conformitate cu actele normative; prelucrarea acestor date de către autoritățile publice respective respectă normele aplicabile în materie de protecție a datelor, în conformitate cu scopurile prelucrării;

parte terță – 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;

consimțământ – 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;

încălcarea securității datelor cu caracter personal – 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;

date genetice – 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 analizei unei mostre de material biologic recoltate de la persoana în cauză;

date biometrice – 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;

date privind sănătatea – 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;

număr de identificare național – numărul prin care se identifică o persoană fizică în anumite sisteme de evidență și care are aplicabilitate generală, cum ar fi: numărul de identificare de stat, seria și numărul buletinului de identitate, numărul pașaportului, al permisului de conducere;

reprezentant – persoană fizică sau juridică cu sediu în Republica Moldova, 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 care le revin în temeiul prezentei legi;

întreprindere – 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;

grup de întreprinderi – întreprindere care exercită controlul și întreprinderile controlate de aceasta;

reguli corporatiste obligatorii – politicile în materie de protecție a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator cu sediu 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 unul sau mai multe state în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

cifră totală de afaceri – cifră astfel cum este definită la art. 4 din Legea concurenței nr. 183/2012;

serviciile societății informaționale – serviciile astfel cum sunt definite la art. 4 din Legea nr. 284/2004 privind serviciile societății informaționale;

marketing direct – comunicarea, prin telefon, poștă sau orice alt mijloc de comunicare directă, a unor mesaje publicitare sau de marketing (de promovare a unor bunuri sau servicii) direcționate unor persoane particulare;

organizație internațională – 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 state sau în temeiul unui astfel de acord.

Capitolul II

PRINCIPII

Articolul 5. Principiile prelucrării datelor cu caracter personal

(1) Datele cu caracter personal sunt:

a) prelucrate în mod legal, echitabil și transparent față de persoana vizată (principiul legalității, echității și transparenței);

b) 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. 54 alin. (1) (principiul limitării legate de scop);

c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate (principiul reducerii la minimum a datelor);

d) 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 (principiul exactității);

e) 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. 54 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 (principiul limitării legate de stocare);

f) 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

măsurile tehnice sau organizatorice corespunzătoare (principiul integrității și confidențialității).

(2) Operatorul este responsabil de respectarea alin. (1) și trebuie să poată demonstra această respectare (principiul responsabilității).

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 luarea unor măsuri 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 efectuate în interes public sau în exercitarea unei autorități oficiale 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.

(2) Datele cu caracter personal pot fi prelucrate în temeiul alin. (1) lit. e) în cazul în care prelucrarea este necesară pentru:

a) îndeplinirea unei sarcini de interes public care reiese din actele normative; sau

b) exercitarea de către operator a funcțiilor sau atribuțiilor prevăzute de actele normative.

(3) Temeiurile pentru prelucrarea menționată la alin. (1) lit. c) și e) și alin. (2) trebuie să fie prevăzute în legislația Republicii Moldova.

(4) Alin. (1) lit. f) nu se aplică în cazul prelucrării efectuate de autoritățile publice în îndeplinirea atribuțiilor lor.

(5) 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 poată demonstra 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 despre acest fapt. 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 cont în special de faptul dacă, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract.

Articolul 8. 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. În cazul copilului cu vârsta sub 14 ani, respectiva prelucrare este legală numai dacă și în măsura în care consimțământul respectiv este acordat sau autorizat de reprezentantul legal al copilului.

(2) Operatorul depune toate eforturile rezonabile pentru a verifica dacă reprezentantul legal a acordat sau a autorizat consimțământul, ținând cont 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 categoriilor speciale de date cu caracter personal

(1) Se interzice prelucrarea datelor cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice ori apartenența la sindicate, precum și prelucrarea datelor genetice, datelor biometrice pentru identificarea unică a unei persoane fizice, datelor privind sănătatea sau datelor 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 că interdicția prevăzută la alin. (1) nu poate fi înlăturată 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 a-și da consimțământul;

d) prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către un partid politic, sindicat, cult religios sau orice alt organism fără scop lucrativ cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismelor respective sau la persoane cu care acestea au contacte permanente în legătură cu scopurile sale, precum 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 stabilirea, exercitarea sau apărarea unui drept într-o procedură administrativă, judiciară sau extrajudiciară, ori când instanțele judecătorești acționează în exercițiul funcției lor judiciare;

g) prelucrarea este necesară din motive de interes public major, în temeiul 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 prestare a asistenței medicale sau sociale ori a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate ori de

asistență socială, în temeiul actelor normative sau în temeiul unui contract încheiat cu un prestator de servicii de sănătate și sub rezerva respectării condițiilor și garanțiilor prevăzute la alin. (3);

i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, precum 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; sau

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. 54 alin. (1).

(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 sau sub responsabilitatea unui profesionist supus obligației de păstrare a secretului profesional, în temeiul actelor normative, sau de o altă persoană supusă unei obligații de confidențialitate în temeiul actelor normative.

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

(1) Prelucrarea datelor 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 publice, sau atunci când prelucrarea este autorizată de actele normative care prevăd garanții adecvate pentru drepturile și libertățile persoanelor vizate.

(2) Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități publice.

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), operatorul poate demonstra că nu este în măsură să identifice persoana vizată, operatorul informează persoana vizată în mod corespunzător, dacă 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 acestor articole, oferă informații suplimentare care permit identificarea sa.

Capitolul III

DREPTURILE PERSOANEI VIZATE

Secțiunea 1

Transparență și modalitățile de exercitare a drepturilor persoanei vizate

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, dar în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținând cont 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 la Centru și de a depune o cerere de chemare în judecată.

(5) Informațiile furnizate în temeiul art. 13 și 14, precum 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) să perceapă o taxă rezonabilă ținând cont de costurile administrative pentru furnizarea informațiilor sau a comunicării ori pentru luarea măsurilor solicitate; sau

b) 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 asupra prelucrării avute în vedere. În cazul în care pictogramele sunt prezentate în format electronic, acestea trebuie să poată fi citite automat.

(8) Centrul poate aproba acte în vederea determinării informațiilor care urmează să fie prezentate de pictograme și procedurile pentru furnizarea de pictograme standardizate.

Secțiunea a 2-a

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 un alt stat sau către o organizație internațională și existența sau absența unei decizii a Centrului privind caracterul adecvat sau, în cazul transferurilor menționate la art. 46, 47 sau 49 alin. (2), 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), 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 ori 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 la Centru;

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, inclusiv 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 alt stat sau către o organizație internațională și existența sau absența unei decizii a Centrului privind caracterul adecvat sau, în cazul transferurilor menționate la art. 46, 47 sau 49 alin. (2), 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 ori 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 la Centru;

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, inclusiv 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, ținând cont 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; sau

c) dacă se intenționează divulgarea datelor cu caracter personal către un alt destinatar, cel târziu la data la care acestea sunt divulgate pentru prima oară.

(4) În cazul în care operatorul intenționează să prelucreze 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. 54 alin. (1), sau în măsura în care obligația menționată la alin. (1) este susceptibilă 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 care prevăd măsuri adecvate pentru a proteja interesele legitime ale persoanei vizate; sau

d) în cazul în care datele cu caracter personal trebuie să rămână confidențiale în temeiul unei obligații legale de secret profesional, reglementate de actele normative, inclusiv al unei obligații 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 cu privire la faptul dacă se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, să obțină 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 alte state sau organizații internaționale;

d) dacă 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 la Centru;

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, inclusiv 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 un alt stat sau către 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 a 3-a

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. Ținând cont 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 (dreptul de a fi uitat)

(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 unul din următoarele cazuri:

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 prelucrare;

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;

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 cont de tehnologia disponibilă și de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal despre faptul 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 ori pentru îndeplinirea unei sarcini efectuate în interes public sau în exercitarea 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 art. 9 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. 54 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 stabilirea, exercitarea sau apărarea unui drept într-o procedură administrativă, judiciară sau extrajudiciară.

Articolul 18. Dreptul la restricționarea prelucrării

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

a) persoana vizată contestă exactitatea datelor cu caracter personal, 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 stabilirea, exercitarea sau apărarea unui drept într-o procedură administrativă, judiciară sau extrajudiciară;

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 stabilirea, exercitarea sau apărarea unui drept într-o procedură administrativă, judiciară sau extrajudiciară, ori pentru protecția drepturilor unei alte persoane fizice sau juridice ori din motive de interes public important.

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

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

Operatorul este obligat să comunice 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 art. 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 art. 9 alin. (2) lit. a) ori a unui contract în temeiul art. 6 alin. (1) lit. b); și

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 la portabilitatea datelor 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 la portabilitatea datelor nu aduce atingere drepturilor și libertăților altora.

Secțiunea a 4-a

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) 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 convingătoare care justifică prelucrarea și care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau că scopul este stabilirea, exercitarea sau apărarea unui drept într-o procedură administrativă, judiciară sau extrajudiciară.

(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 contextul utilizării serviciilor societății informaționale, prin derogare de la prevederile Legii nr. 284/2004 privind serviciile societății informaționale, persoana vizată își poate exercita dreptul la opoziție 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. 54 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 fi supusă unei decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce efecte juridice pentru 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;

b) este autorizată prin actele normative care prevăd, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate; sau

c) are la bază consimțământul explicit al persoanei vizate.

(3) În cazurile menționate la alin. (2) lit. a) și c), operatorul 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 pot avea 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 au fost instituite măsuri corespunzătoare pentru protejarea drepturilor, libertăților și intereselor legitime ale persoanei vizate.

Secțiunea a 5-a **Restricții**

Articolul 23. Restricții

(1) Drepturile și obligațiile prevăzute la art. 12-22 și 34, precum și prevederile art. 5 în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la art. 12-22, pot fi restricționate prin lege 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) Orice lege menționată la alin. (1) trebuie să conțină 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 libertățile 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 cont 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. Respectivă măsură se revizuiască 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 în conformitate cu art. 40, sau la un mecanism de certificare aprobat în conformitate cu art. 42, poate fi utilizată ca un 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 un 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. Acordul poate să desemneze un punct de contact pentru persoanele vizate.

(2) Acordul menționat la alin. (1) trebuie să reflecte 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 persoanei împuternicite de operator care nu au sediu 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 cu sediu în 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 prevăzute 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; sau

b) unei autorități sau instituții publice.

(3) Reprezentantul primește din partea operatorului sau a persoanei împuternicite de operator un mandat prin care Centrul 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.

(4) Desemnarea unui reprezentant de către operator sau persoana împuternicită de operator nu aduce atingere dreptului de a depune o plângere la Centru, sau de a depune o cerere de chemare în judecată, împotriva operatorului sau persoanei împuternicite de operator.

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 legislației Republicii Moldova care are 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, precum 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 în 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 persoana împuternicită este obligată să prelucreze datele în temeiul actelor normative. În acest caz, persoana împuternicită informează operatorul despre această obligație legală înainte de prelucrare, cu excepția cazului în care actele normative interzic o astfel de informare din motive importante de interes public;

b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație legală 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 cont 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 cont 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 activităților 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 legislației Republicii Moldova, 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 inițial 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 în conformitate cu art. 40, sau la un mecanism de certificare aprobat în conformitate cu art. 42, poate fi utilizată ca un 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 alt act juridic menționat la alin. (3) și (4) se poate baza, integral sau parțial, pe clauze contractuale standard menționate la alin. (7), inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul art. 42 și 43.

(7) Centrul aprobă clauzele contractuale standard pentru aspectele menționate la alin. (3) și (4).

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

(9) Fără a aduce atingere prevederilor art. 76 și 86-88, 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 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 prelucrează decât în baza instrucțiunilor operatorului, cu excepția cazului în care actele normative obligă prelucrarea datelor.

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, care 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 alte state sau organizații internaționale;

e) dacă este cazul, transferurile de date cu caracter personal către un alt stat sau către o organizație internațională, inclusiv identificarea acestui stat sau a organizației internaționale respective și, în cazul transferurilor menționate la art. 49 alin. (2), 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 persoană împuternicită de operator și, după caz, reprezentantul persoanei împuternicite 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 aceste persoane, precum și, după caz, ale reprezentantului operatorului sau ale reprezentantului persoanei împuternicite de operator;

b) categoriile activităților de prelucrare desfășurate în numele fiecărui operator;

c) dacă este cazul, transferurile de date cu caracter personal către un alt stat sau către o organizație internațională, inclusiv identificarea acestui stat sau a organizației internaționale respective și, în cazul transferurilor prevăzute la art. 49 alin. (2), 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) Evidențele menționate la alin. (1) și (2) sunt ținute 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 Centrului, la cererea acestuia.

(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 prevăzute la art. 9 alin. (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni prevăzute la art. 10.

Articolul 31. Cooperarea cu Centrul

Operatorul și persoana împuternicită de operator, precum și, după caz, reprezentantul acestora, cooperează, la cerere, cu Centru în îndeplinirea sarcinilor sale.

Secțiunea a 2-a 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, inclusiv, printre altele, după caz:

- a) pseudonimizarea și criptarea datelor cu caracter personal;
- b) capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și reziliența 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 periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

(2) La evaluarea nivelului adecvat de securitate, se ține cont în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate într-un alt mod.

(3) Aderarea la un cod de conduită aprobat în conformitate cu art. 40, sau la un mecanism de certificare aprobat în conformitate cu art. 42, poate fi utilizată ca un element prin care să se demonstreze îndeplinirea cerințelor prevăzute la alin. (1).

(4) Operatorul și persoana împuternicită de operator iau măsuri pentru a asigura faptul că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite de operator și care are acces la date cu caracter personal nu le prelucrează decât în baza instrucțiunilor operatorului, cu excepția cazului în care actele normative obligă prelucrarea datelor.

Articolul 33. Notificarea Centrului 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 Centrului, 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 încălcarea este puțin probabil 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 a întârzierii.

(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 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 trebuie să permită Centrului să verifice respectarea prezentului 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 prevăzute la art. 33 alin. (3) lit. b), c) și d).

(3) Informarea persoanei vizate, prevăzută la alin. (1), nu este necesară în cazul în care una din 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 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 încălcarea securității datelor cu caracter personal către persoana vizată, Centrul, după ce a luat în considerare probabilitatea ca încălcarea securității datelor cu caracter personal să genereze un

risc ridicat, poate să îi solicite operatorului informarea persoanei vizate sau poate decide că una dintre condițiile menționate la alin. (3) sunt îndeplinite.

Secțiunea a 3-a

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 preconizate 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 în special 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 prevăzute la art. 9 alin. (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni prevăzute la art. 10; sau

c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

(4) Centrul aprobă lista 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) Centrul poate aproba o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor.

(6) Listele aprobate în temeiul alin. (4) și (5) sunt publicate în Monitorul Oficial al Republicii Moldova și pe pagina web oficială a Centrului.

(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); și

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 operatori sau de persoanele împuternicite de operatori, se are în vedere în mod corespunzător respectarea de către operatori sau persoanele împuternicite a codurilor de conduită, dacă au fost aprobate în conformitate cu art. 40, în special în vederea unei evaluări a impactului asupra protecției datelor.

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

(10) În cazul prelucrării în temeiul art. 6 alin. (1) lit. c) sau e), prevederile de la alin. (1)-(7) nu se aplică dacă deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări generale a impactului în contextul adoptării actelor normative care prevăd temeiurile juridice de prelucrare, cu excepția cazului în care actele normative prevăd că este necesară efectuarea evaluării impactului asupra protecției datelor 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 Centrul înainte de prelucrare 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) În cazul în care consideră că prelucrarea preconizată, 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, Centrul 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 prevăzute la art. 60. Această perioadă poate fi prelungită cu șase săptămâni, ținând cont de complexitatea prelucrării preconizate. Centrul 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 la data la care Centrul a obținut informațiile pe care le-a solicitat în scopul consultării.

(3) Atunci când consultă Centrul în conformitate cu alin. (1), operatorul îi furnizează acestuia:

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; și

f) orice alte informații solicitate de Centru.

(4) Proiectele de acte normative care conțin prevederi referitoare la prelucrarea datelor cu caracter personal sunt transmise Centrului, pentru avizare, în condițiile Legii nr. 100/2017 cu privire la actele normative.

Secțiunea a 4-a **Responsabilul cu protecția datelor**

Articolul 37. Desemnarea responsabilului cu protecția datelor

(1) Operatorul și persoana împuternicită de operator desemnează un responsabil cu protecția datelor în cazul în care:

a) prelucrarea este efectuată de o autoritate sau instituție publică, cu excepția instanțelor judecătorești în activitatea de îndeplinire a justiției;

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 în temeiul art. 9, sau a unor date cu caracter personal referitoare la condamnări penale și infracțiuni, menționată la art. 10.

(2) Un grup de întreprinderi poate desemna un singur responsabil cu protecția datelor, cu condiția ca acesta să fie ușor accesibil din fiecare sediu al întreprinderilor respective.

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

(4) În alte cazuri decât cele prevăzute 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 obligă acest lucru, desemnează un responsabil

cu protecția datelor. Responsabilul cu protecția datelor poate să acționeze pentru astfel de asociații și alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

(5) Responsabilul cu protecția datelor este desemnat în baza calităților profesionale și, în special, în baza cunoștințelor de specialitate ale legislației și ale practicilor în domeniul protecției datelor cu caracter personal, precum și în baza capacității de a îndeplini sarcinile prevăzute la art. 39.

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

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

Articolul 38. Poziția responsabilului cu protecția datelor

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

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

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

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

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

Articolul 39. Sarcinile responsabilului cu protecția datelor

(1) Responsabilul cu 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 prevederi ale actelor normative referitoare la protecția datelor;

b) monitorizarea respectării prezentei legi și a altor prevederi ale actelor normative referitoare la protecția datelor, precum 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 Centrul;

e) asumarea rolului de punct de contact pentru Centru cu privire la aspectele legate de prelucrare, inclusiv consultarea prealabilă prevăzută la art. 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

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

Secțiunea a 5-a

Coduri de conduită și certificare

Articolul 40. Coduri de conduită

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

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

- 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, precum și modalitatea în care trebuie obținut consimțământul reprezentanților legali ai copiilor;
- h) măsurile și procedurile prevăzute la art. 24 și 25, precum și măsurile de asigurare a securității prelucrării prevăzute la art. 32;
- i) notificarea Centrului 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 alte state sau către organizații internaționale; sau

k) procedurile 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 prevăzute la art. 72 și art. 74.

(3) Pe lângă operatorii și persoanele împuternicite de operatori care cad sub incidența prezentei legi, la codurile de conduită aprobate în temeiul alin. (5) pot adera și operatorii sau persoanele împuternicite de operatori care nu cad sub incidența prezentei legi în conformitate cu art. 3, în scopul de a oferi garanții adecvate în cadrul transferurilor de date cu caracter personal către alte state sau către organizații internaționale în condițiile prevăzute la art. 46 alin. (2) lit. d). Acești operatori sau persoane împuternicite de operatori își asumă angajamente cu caracter obligatoriu și executoriu, prin intermediul unor instrumente contractuale sau al altor acte juridice obligatorii, să aplice garanțiile 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 Centrului.

(5) Asociațiile și alte organisme menționate la alin. (2), care intenționează să elaboreze un cod de conduită sau să modifice un cod existent, transmit proiectul de cod sau de modificare Centrului. Centrul emite un aviz cu privire la faptul dacă proiectul de cod sau de modificare este în conformitate cu prezenta lege și îl aprobă în cazul în care constată că acesta oferă garanții adecvate suficiente.

(6) În cazul în care proiectul de cod sau de modificare este aprobat în conformitate cu alin. (5), Centrul înregistrează și publică codul pe pagina sa web oficială.

(7) Centrul ține evidența codurilor de conduită și a modificărilor aprobate într-un registru, precum și asigură publicarea pe pagina sa web oficială a textelor actualizate și consolidate a codurilor de conduită, în urma aprobării modificărilor la acestea.

Articolul 41. Monitorizarea codurilor de conduită aprobate

(1) Fără a aduce atingere sarcinilor și competențelor Centrului prevăzute la art. 59 și 60, monitorizarea respectării unui cod de conduită aprobat în temeiul art. 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 Centru.

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

a) a demonstrat Centrului, 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 examinarea și soluționarea 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 Centrului, într-un mod satisfăcător, că sarcinile și atribuțiile sale nu creează conflicte de interese.

(3) Centrul aprobă cerințele pentru acreditarea unui organism menționat la alin. (1).

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

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

(6) Prezentul articol nu se aplică prelucrării efectuate de autoritățile și instituțiile publice.

Articolul 42. Certificare

(1) Centrul încurajează instituirea de mecanisme de certificare în domeniul protecției datelor cu caracter personal, 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 întreprinderilor micro, mici și mijlocii.

(2) Mecanismele de certificare din domeniul protecției datelor cu caracter personal, 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 cad sub incidența prezentei legi, ci și pentru a demonstra existența unor garanții adecvate oferite de operatorii sau de persoanele împuternicite de operatori care nu cad sub incidența prezentei legi în conformitate cu art. 3, în cadrul transferurilor de date cu caracter personal către alte state sau către 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 acte juridice obligatorii, 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 Centrului.

(5) Organismele de certificare menționate la art. 43 sau Centrul emit o certificare în temeiul prezentului articol, în baza criteriilor de certificare aprobate de către Centru.

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

(7) 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 criteriile relevante să fie îndeplinite în continuare. Certificarea este retrasă, după caz, de către organismele de certificare sau de către Centru, în cazul în care nu mai sunt îndeplinite criteriile pentru certificare.

(8) Centrul regroupează toate mecanismele de certificare și sigiliile și mărcile de protecție a datelor cu caracter personal într-un registru și le publică pe pagina sa web oficială.

Articolul 43. Organisme de certificare

(1) Fără a aduce atingere sarcinilor și competențelor Centrului prevăzute la art. 59 și 60, organismele de certificare care dispun de un nivel adecvat de competență în domeniul protecției datelor cu caracter personal, după ce informează Centrul pentru a-i permite să își exercite competențele în temeiul art. 60 alin. (2) lit. h), emit și reînnoiesc certificarea.

(2) Un organism de certificare este acreditat de către Centrul Național de Acreditare în cazul în care:

a) a demonstrat Centrului Național pentru Protecția Datelor cu Caracter Personal, într-un mod satisfăcător, independența și expertiza sa în legătură cu obiectul certificării;

b) s-a angajat să respecte criteriile aprobate în temeiul art. 42 alin. (5);

c) a instituit proceduri pentru emiterea, revizuirea periodică și retragerea certificării, a sigiliilor și mărcilor din domeniul protecției datelor cu caracter personal;

d) a instituit proceduri și structuri pentru examinarea și soluționarea 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; și

e) a demonstrat Centrului Național pentru Protecția Datelor cu Caracter Personal, într-un mod satisfăcător, că sarcinile și atribuțiile sale nu creează conflicte de interese.

(3) Acreditarea organismelor de certificare menționate la alin. (1) și (2) se realizează în baza cerințelor de acreditare aprobate de Centru. Aceste cerințe completează cele prevăzute de Legea nr. 235/2011 privind activitățile de acreditare și de evaluare a conformității, precum și normele tehnice care descriu metodele și procedurile organismelor de certificare.

(4) Organismele de certificare menționate la alin. (1) sunt responsabile de 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.

(5) Organismele de certificare menționate la alin. (1) transmit Centrului Național pentru Protecția Datelor cu Caracter Personal motivele acordării sau retragerii certificării solicitate.

(6) Cerințele menționate la alin. (3) și criteriile menționate la art. 42 alin. (5) se publică de către Centrul Național pentru Protecția Datelor cu Caracter Personal pe pagina sa web oficială.

(7) Centrul Național de Acreditare, inclusiv la solicitarea Centrului Național pentru Protecția Datelor cu Caracter Personal, 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 dacă măsurile luate de organismul de acreditare încalcă prezenta lege.

(8) Centrul Național pentru Protecția Datelor cu Caracter Personal poate aproba standardele tehnice pentru mecanismele de certificare și pentru sigiliile și mărcile din domeniul protecției datelor cu caracter personal, precum și mecanisme de promovare și recunoaștere a acelor mecanisme de certificare, sigilii și mărci.

Capitolul V

TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ALTE STATE SAU CĂTRE 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-un alt stat sau către o organizație internațională pot fi transferate doar dacă, sub rezerva celorlalte prevederi 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 statul străin

sau de la organizația internațională către un alt stat sau către o altă organizație internațională. Toate prevederile din prezentul capitol se aplică pentru asigurarea faptului că nivelul de protecție a persoanelor fizice garantat prin prezenta lege nu este subminat.

(2) Prezentul capitol nu se aplică transferurilor de date cu caracter personal către statele membre ale Spațiului Economic European. În cazul acestor transferuri nu sunt necesare autorizări speciale.

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

(1) Transferul de date cu caracter personal către un alt stat sau către o organizație internațională se poate realiza atunci când Centrul a decis că statul, un teritoriu sau unul ori mai multe sectoare specificate din acel stat 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, Centrul ține cont, 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 un alt stat sau către o organizație internațională, care sunt respectate în statul respectiv sau în organizația internațională respectivă, jurisprudența, precum și existența unor drepturi efective și opozabile ale persoanelor vizate și a unor remedii 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 statul străin sau sub jurisdicția cărora intră o organizație internațională, cu responsabilitate pentru asigurarea și impunerea respectării normelor de protecție a datelor cu caracter personal, inclusiv 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 Centrul;

c) angajamentele internaționale la care a aderat statul sau organizația internațională în cauză ori alte obligații care decurg din tratatele internaționale, precum și din participarea acesteia la sisteme multilaterale sau regionale, mai ales în domeniul protecției datelor cu caracter personal; și

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

(3) Centrul, după ce evaluează caracterul adecvat al nivelului de protecție, poate decide că un alt stat, un teritoriu sau unul sau mai multe sectoare specificate dintr-un stat sau o organizație internațională asigură un nivel de

protecție adecvat în sensul alin. (2). Decizia prevede un mecanism de revizuire periodică, cel puțin o dată la patru ani, care ia în considerare toate evoluțiile relevante din statul străin sau organizația internațională. Decizia prevede aplicarea geografică și sectorială, și, după caz, identifică autoritatea sau autoritățile de supraveghere menționate la alin. (2) lit. b).

(4) Centrul monitorizează continuu evoluțiile din alte state și de la nivelul organizațiilor internaționale care ar putea afecta funcționarea deciziilor emise în temeiul alin. (3) și a deciziilor emise înainte de intrarea în vigoare a prezentei legi.

(5) În cazul în care informațiile disponibile dezvăluie, în special în urma revizuirii menționate la alin. (3), că un alt stat, un teritoriu sau un sector specificat dintr-un alt stat sau o organizație internațională nu mai asigură un nivel de protecție adecvat în sensul alin. (2), Centrul, dacă este necesar, abrogă sau modifică decizia menționată la alin. (3), fără efect retroactiv.

(6) Centrul poate, în comun cu autoritățile competente din Republica Moldova, iniția consultări cu statul sau organizația internațională în vederea remedierii situației care a stat la baza deciziei emise în conformitate cu alin. (5).

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

(8) Centrul publică în Monitorul Oficial al Republicii Moldova și pe pagina sa web oficială lista statelor, a teritoriilor și sectoarelor specificate dintr-un stat și a organizațiilor internaționale în privința cărora a decis că nivelul de protecție adecvat este asigurat sau nu mai este asigurat.

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 un alt stat sau către 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 Centrului, prin:

a) un act juridic obligatoriu și executoriu între autoritățile sau instituțiile publice;

b) reguli corporatiste obligatorii în conformitate cu art. 47;

c) clauze standard de protecție a datelor aprobate de Centru sau adoptate de Comisia Europeană;

d) 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 dintr-un alt stat de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate; sau

e) 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 dintr-un alt stat de a aplica garanții adecvate, inclusiv cu privire la drepturile persoanelor vizate.

(3) Cu autorizarea din partea Centrului, 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 alt stat sau organizația internațională; sau

b) dispoziții care urmează să fie incluse în acordurile administrative dintre autoritățile sau instituțiile publice, care includ drepturi opozabile și efective pentru persoanele vizate.

Articolul 47. Reguli corporatiste obligatorii

(1) Centrul 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) prevăd cel puțin:

a) structura și datele de contact ale grupului de întreprinderi sau ale grupului de întreprinderi implicate într-o activitate economică comună, precum 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 statului sau a statelor 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 fi supuse unor decizii bazate exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, în conformitate cu art. 22, dreptul de a depune o plângere la Centru și o cerere de chemare în judecată în conformitate cu art. 74, precum și dreptul de a obține remedieri și, după caz, despăgubiri pentru încălcarea regulilor corporatiste obligatorii;

f) acceptarea de către operator sau de persoana împuternicită de operator, care are sediu pe teritoriul Republicii Moldova, a răspunderii pentru orice încălcare a regulilor corporatiste obligatorii de către orice membru în cauză care nu are sediu în Republica Moldova. Operatorul sau persoana împuternicită de operator sunt exonerati de această răspundere, integral sau parțial, numai dacă dovedesc 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 de protecția datelor desemnat în conformitate cu art. 37 sau ale oricărei alte persoane sau entități împuternicite 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 examinării 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 lit. h) și consiliului 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 Centrului, la cerere;

k) mecanismele de raportare și înregistrare a modificărilor aduse regulilor și de raportare a acestor modificări către Centru;

l) mecanismul de cooperare cu Centrul 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 Centrului a rezultatelor verificărilor cu privire la măsurile menționate la punctul j);

m) mecanismele de raportare către Centru a oricăror cerințe legale impuse într-un alt stat unui membru al grupului de întreprinderi sau al grupului de întreprinderi implicate într-o activitate economică comună care pot avea un efect advers considerabil asupra garanțiilor furnizate prin regulile corporatiste obligatorii; și

n) formarea corespunzătoare în domeniul protecției datelor a personalului care are un acces permanent sau periodic la date cu caracter personal.

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

Orice hotărâre a unei instanțe judecătorești și orice decizie a unei autorități publice a unui alt stat, 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 tratat internațional, cum ar fi un tratat de asistență juridică reciprocă în vigoare între statul solicitant 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 un alt stat sau către o organizație internațională poate avea loc numai în una din următoarele condiții:

a) persoana vizată și-a exprimat în mod explicit consimțământul 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 implementarea unor măsuri precontractuale luate 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 într-o procedură administrativă, judiciară sau extrajudiciară;

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 consimțământul;

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.

(2) 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 alin. (1), un transfer către un alt stat sau către 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 Centrul cu privire la transfer. Operatorul, pe lângă furnizarea informațiilor menționate la art. 13 și 14, informează persoana vizată cu privire la transfer și la interesele legitime majore pe care le urmărește.

(3) 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.

(4) Alin. (1) lit. a), b) și c) și alin. (2) nu se aplică în cazul activităților desfășurate de autoritățile publice în exercitarea competențelor lor publice.

(5) Interesul public menționat la alin. (1) lit. d) trebuie să fie prevăzut în actele normative.

(6) În absența unei decizii privind caracterul adecvat al nivelului de protecție, actele normative pot, din considerente importante de interes public, să stabilească în mod expres limite asupra transferului unor categorii specifice de date cu caracter personal către un alt stat sau către o organizație internațională.

(7) Operatorul sau persoana împuternicită de operator consemnează evaluarea, precum și garanțiile adecvate prevăzute la alin. (2), în evidențele menționate la art. 30.

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

În ceea ce privește alte state și organizații internaționale, Centrul ia măsurile corespunzătoare pentru:

a) elaborarea mecanismelor de cooperare internațională pentru a facilita asigurarea aplicării efective a legislației privind protecția datelor cu caracter personal;

b) acordarea asistenței internaționale reciproce 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 alte state.

Capitolul VI

CAZURILE SPECIFICE DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

Articolul 51. Prelucrarea și libertatea de exprimare

(1) Pentru prelucrarea efectuată în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare, prezenta lege nu se aplică în cazul în care sunt întrunite următoarele condiții cumulative:

- a) operatorul prelucrează date cu caracter personal cu intenția de a publica un material jurnalistic, academic, artistic sau literar;
- b) publicarea materialului ar fi de interes public;
- c) aplicarea prevederilor din prezenta lege este incompatibilă cu realizarea scopurilor jurnalistice sau a scopului de exprimare academică, artistică sau literară.

(2) Centrul nu este competent să supravegheze operațiunile de prelucrare efectuate în temeiul alin. (1).

(3) Persoana vizată are dreptul de a depune o cerere de chemare în judecată conform art. 74, precum și de a solicita despăgubiri conform art. 76, în cazul în care consideră că datele sale cu caracter personal au fost prelucrate cu încălcarea alin. (1).

Articolul 52. Prelucrarea și accesul la informațiile de interes public

Datele cu caracter personal deținute de furnizorii de informații pot fi dezvăluite în condițiile Legii nr. 148/2023 privind accesul la informațiile de interes public, cu excepția categoriilor speciale de date cu caracter personal prevăzute la art. 9 alin. (1).

Articolul 53. Prelucrarea unui număr de identificare național

(1) Prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conțin, se poate efectua în situațiile prevăzute la art. 6 alin. (1).

(2) Prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conțin, în scopul prevăzut la art. 6 alin. (1) lit. f), respectiv al realizării intereselor legitime urmărite de operator sau de o parte terță, se efectuează cu instituirea de către operator a următoarelor garanții:

a) punerea în aplicare a măsurilor tehnice și organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum și pentru asigurarea securității și confidențialității prelucrărilor de date cu caracter personal, în conformitate cu art. 32;

b) stabilirea termenelor de stocare în funcție de natura datelor și scopul prelucrării, precum și a termenelor specifice în care datele cu caracter personal trebuie șterse sau revizuite în vederea ștergerii;

c) instruirea periodică cu privire la obligațiile ce le revin persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.

Articolul 54. 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. Respectivul garanții asigură faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivul măsuri pot include pseudonimizarea, cu condiția ca respectivul scopuri să fie îndeplinite în acest mod. Atunci când respectivul 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) Art. 15, 16, 18 și 21 nu se aplică în cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva condițiilor și a garanțiilor prevăzute la alin. (1), în măsura în care drepturile prevăzute la aceste articole 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) Art. 15, 16 și 18-21 nu se aplică în cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public, sub rezerva condițiilor și a garanțiilor prevăzute la alin. (1), în măsura în care drepturile prevăzute la aceste articole 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.

Capitolul VII

CENTRUL NAȚIONAL PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL

Secțiunea 1

Dispoziții generale

Articolul 55. Statutul Centrului

(1) Centrul Național pentru Protecția Datelor cu Caracter Personal este o autoritate publică ce funcționează la nivel național ca structură unică, independentă față de alte autorități publice, față de alte persoane juridice și față de persoanele fizice.

(2) Centrul este persoană juridică de drept public și dispune de ștampilă cu imaginea Stemei de Stat a Republicii Moldova.

(3) Sediul Centrului se află în municipiul Chișinău.

Articolul 56. Finanțarea activității Centrului

(1) Centrul este finanțat de la bugetul de stat.

(2) Centrul elaborează, aprobă și administrează bugetul conform principiilor, regulilor și procedurilor prevăzute de Legea finanțelor publice și responsabilității bugetar-fiscale nr. 181/2014.

(3) Activitatea economico-financiară a Centrului este supusă auditului Curții de Conturi.

Articolul 57. Efectivul-limită și structura Centrului

(1) Efectivul-limită al Centrului se stabilește prin hotărâre a Parlamentului, la propunerea directorului Centrului.

(2) Structura Centrului se aprobă de directorul Centrului.

Secțiunea a 2-a**Misiunea, sarcinile și competențele Centrului****Articolul 58. Misiunea Centrului**

(1) Centrul asigură supravegherea și monitorizarea aplicării prezentei legi și a altor acte normative privind prelucrarea datelor cu caracter personal, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în legătură cu prelucrarea datelor cu caracter personal.

(2) Centrul nu este competent să supravegheze operațiunile de prelucrare efectuate de instanțele judecătorești în activitatea de îndeplinire a justiției.

Articolul 59. Sarcinile Centrului

(1) În vederea realizării misiunii sale, Centrul:

a) monitorizează și asigură aplicarea prezentei legi;

b) promovează acțiuni de sensibilizare și de înțelegere în rândul publicului a riscurilor, normelor, garanțiilor și drepturilor în materie de prelucrare, în special în privința activităților care se adresează în mod specific copiilor;

c) oferă consiliere Parlamentului, Guvernului și altor autorități publice 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 operatori cu privire la obligațiile care le revin în temeiul prezentei legi;

e) furnizează, la cerere, 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) examinează plângerile depuse de o persoană vizată sau un organism, o organizație sau o asociație în conformitate cu art. 72, investighează într-o măsură adecvată obiectul plângerii și informează autorul plângerii 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 autoritate de supraveghere dintr-un alt stat;

g) cooperează, inclusiv prin schimb de informații, cu autoritățile de supraveghere din alte state și oferă asistență reciprocă pentru a asigura coerența aplicării și respectării prezentei legi;

h) desfășoară investigații privind aplicarea prezentei legi, inclusiv în baza unor informații primite de la o autoritate de supraveghere dintr-un alt stat 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, precum și a practicilor comerciale;

j) aprobă clauze contractuale standard menționate la art. 28 alin. (7) și la art. 46 alin. (2) lit. c);

k) aprobă 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) aprobă cerințele de acreditare a organismelor de monitorizare a codurilor de conduită în conformitate cu art. 41 și a organismelor de certificare în conformitate cu art. 43;

q) coordonează procedura de acreditare a organismelor de monitorizare a codurilor de conduită în conformitate cu art. 41 și a organismelor 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) menține la zi evidențe interne privind încălcările prezentei legi și măsurile luate, în special avertismentele emise și sancțiunile impuse în conformitate cu art. 60 alin. (2);

u) îndeplinește orice alte sarcini legate de protecția datelor cu caracter personal.

(2) Îndeplinirea sarcinilor Centrului este gratuită pentru persoana vizată și, după caz, pentru responsabilul cu protecția datelor.

(3) În cazul în care cererile sunt în mod vădit nefondate sau excesive, în special din cauza caracterului lor repetitiv, Centrul poate percepe o taxă rezonabilă, bazată pe costurile administrative, sau poate refuza să le examineze.

Sarcina de a demonstra caracterul evident nefondat sau excesiv al cererii revine Centrului.

Articolul 60. Competențele Centrului

(1) Centrul 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 Centrul le solicită în vederea îndeplinirii sarcinilor sale;

b) de a efectua investigații sub formă de audituri privind protecția datelor;

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) Centrul are 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 preconizate să încalce dispozițiile prezentei legi;

b) de a emite avertismente 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, în modul prevăzut de lege;

f) de a impune o limitare temporară sau definitivă, inclusiv o interdicție asupra prelucrării, în modul prevăzut de lege;

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 criteriile de certificare nu sunt sau nu mai sunt îndeplinite;

i) de a aplica amenzi în conformitate cu art. 86-88, 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-un alt stat sau către o organizație internațională;

(3) Centrul are următoarele competențe de autorizare și de consiliere:

a) de a oferi consiliere operatorului în conformitate cu procedura de consultare prealabilă prevăzută la art. 36;

b) de a emite avize, din proprie inițiativă sau la cerere, Parlamentului, Guvernului, altor autorități publice, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal;

c) de a emite avize și de a aproba proiectele de coduri de conduită, în conformitate cu art. 40 alin. (5);

d) de a acredita organismele de certificare în conformitate cu art. 43;

e) de a emite certificări și de a aproba criteriile de certificare în conformitate cu art. 42 alin. (5);

f) de a aproba clauzele standard în materie de protecție a datelor menționate la art. 28 alin. (7) și la art. 46 alin. (2) lit. c);

g) de a autoriza clauzele contractuale menționate la art. 46 alin. (3) lit. a);

h) de a autoriza acordurile administrative menționate la art. 46 alin. (3) lit. b);

i) de a aproba reguli corporatiste obligatorii în conformitate cu art. 47.

(4) Competențele Centrului sunt exercitate, conform legislației, de către directorul sau directorii adjuncți ai Centrului, de inspectorii de protecție a datelor și de alt personal al Centrului.

Articolul 61. Raportul de activitate

(1) Anual, până la data de 31 martie, Centrul transmite Parlamentului și Guvernului raportul de activitate pentru anul precedent cu privire la activitățile sale, care include, cel puțin, informații cu privire la tipurile de încălcări notificate și tipurile de măsuri luate în conformitate cu art. 60 alin. (2).

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

Secțiunea a 3-a Organizarea Centrului

Articolul 62. Conducerea Centrului

(1) Centrul este condus de un director, asistat de doi directori adjuncți.

(2) Funcțiile de director și directori adjuncți ai Centrului sunt funcții de demnitate publică și sunt incompatibile cu orice altă funcție sau activitate remunerată, cu excepția activităților didactice, științifice și de creație.

(3) Directorul și directorii adjuncți ai Centrului, în cadrul îndeplinirii atribuțiilor lor, sunt independenți de orice influență directă sau indirectă și nu solicită sau acceptă instrucțiuni de la o parte externă.

(4) Directorul și directorii adjuncți ai Centrului sunt obligați să respecte pe parcursul mandatelor, cât și după încetarea acestora, secretul profesional în ceea ce privește informațiile confidențiale de care au luat cunoștință în cadrul îndeplinirii sarcinilor sau al exercitării competențelor lor, în special în privința raportării de către persoanele fizice a încălcărilor prezentei legi.

Articolul 63. Numirea directorului Centrului

(1) Directorul Centrului se numește în funcție de Parlament prin concurs, pentru un mandat de 7 ani. O persoană nu poate fi numită în funcția de director al Centrului pentru două mandate consecutive.

(2) Poate candida la funcția de director al Centrului persoana care îndeplinește următoarele condiții:

- a) deține cetățenia Republicii Moldova;
- b) nu este supusă unei măsuri de ocrotire judiciare sub forma tutelei;
- c) are studii superioare de licență în domeniul dreptului;
- d) are o vechime în muncă de cel puțin 5 ani în domeniul dreptului;
- e) are o reputație ireproșabilă;
- f) nu este membru a unui partid politic;
- g) este aptă din punct de vedere medical pentru exercitarea funcției, conform certificatului medical de sănătate eliberat în condițiile legii;
- h) cunoaște limba română.

(3) Se consideră că nu are o reputație ireproșabilă, în sensul alin. (1) lit. e), persoana:

- a) care are antecedente penale;
- b) care a fost privată de dreptul de a ocupa anumite funcții sau a exercita anumite activități, ca pedeapsă principală sau complementară, printr-o hotărâre judecătorească definitivă;
- c) în privința căreia s-a constatat, printr-un act definitiv, încălcarea regimului juridic al conflictelor de interese, al incompatibilităților, restricțiilor și limitărilor;
- d) în privința căreia există o hotărâre irevocabilă a instanței de judecată prin care s-a dispus confiscarea averii nejustificate;
- e) care are, în ultimii 5 ani, în cazierul privind integritatea profesională, înscrieri cu privire la rezultatul negativ al testului de integritate profesională pentru încălcarea obligației prevăzute la art. 7 alin. (2) lit. a) din Legea nr. 325/2013 privind evaluarea integrității instituționale.
- f) care are interdicția de a ocupa o funcție publică sau de demnitate publică, ce derivă dintr-un act de constatare al Autorității Naționale de Integritate.

(4) Concursul pentru selectarea directorului Centrului se organizează de Comisia juridică, numiri și imunități cu cel puțin trei luni înainte de expirarea mandatului directorului în exercițiu.

(5) Concursul se desfășoară în mod public. Informația despre organizarea și desfășurarea concursului, despre cerințele față de candidați și despre actele care urmează a fi prezentate se plasează pe pagina web oficială a Parlamentului și se publică în mijloacele de informare în masă cu cel puțin 30 de zile înainte de data desfășurării concursului.

(6) Concursul se consideră valabil dacă la el participă cel puțin doi candidați. În cazul în care nu au fost depuse suficiente dosare de participare la concurs sau candidații nu întrunesc cerințele stabilite de prezenta lege, se anunță un concurs repetat, care se organizează în termen de 30 de zile.

(7) CV-urile candidaților se plasează pe pagina web oficială a Parlamentului pentru consultarea publicului.

(8) Evaluarea candidaților se efectuează de Comisia juridică, numiri și imunități.

(9) După evaluare, comisia propune Parlamentului candidatul pentru a fi numit în funcția de director al Centrului.

(10) Candidatul propus se numește în funcția de director al Centrului cu votul majorității deputaților aleși. În cazul în care nu s-a întrunit numărul necesar de voturi pentru numirea directorului, Comisia juridică, numiri și imunități, în termen de 15 zile, anunță un nou concurs care va fi organizat și desfășurat în conformitate cu prezentul articol.

(11) La data numirii în funcție, directorul Centrului depune în fața Parlamentului, următorul jurământ:

„Jur să-mi exercit obligațiile funcționale cu credință și integritate, în serviciul Republicii Moldova, să respect Constituția și legile Republicii Moldova, să protejez drepturile și libertățile fundamentale ale omului, democrația și bunăstarea poporului.”.

(12) Refuzul persoanei de a depune jurământul atrage nulitatea numirii sale în funcție.

Articolul 64. Numirea directorilor adjuncți ai Centrului

(1) Directorii adjuncți ai Centrului se numesc în funcție de Parlament la propunerea directorului Centrului, pentru un mandat de 7 ani.

(2) Poate fi numită în funcția de director adjunct al Centrului persoana care îndeplinește condițiile prevăzute la art. 63 alin. (2) și (3).

(3) Persoana propusă de directorul Centrului se numește în funcția de director adjunct cu votul majorității deputaților aleși.

Articolul 65. Atribuțiile directorului și directorilor adjuncți ai Centrului

(1) Directorul Centrului exercită următoarele atribuții:

- a) conduce, organizează și controlează activitatea Centrului;
- b) reprezintă Centrul pe plan național și internațional;

- c) asigură monitorizarea aplicării prezentei legi și a altor acte normative privind prelucrarea datelor cu caracter personal;
- d) în temeiul și în scopul executării legii, emite ordine, decizii și dispoziții;
- e) aprobă îndrumări metodologice în vederea asigurării unei interpretări și aplicări adecvate a prezentei legi și a altor acte normative privind prelucrarea datelor cu caracter personal;
- f) aprobă sau modifică statul de personal al Centrului, în conformitate cu structura și efectivul-limită stabilit;
- g) aprobă regulamentele subdiviziunilor Centrului;
- h) numește în funcții inspectorii de protecție a datelor, modifică, suspendă și dispune încetarea raporturilor de serviciu ale acestora, în condițiile legii;
- i) numește în funcții funcționarii publici și personalul contractual din aparatul Centrului, modifică, suspendă și dispune încetarea raporturilor de serviciu sau de muncă ale acestora, în condițiile legii;
- j) soluționează, conform legislației, aspectele ce țin de stabilirea sporurilor la salariu și de acordare a primelor;
- k) organizează și implementează sistemul de control intern managerial și poartă răspundere managerială pentru administrarea bugetului Centrului și a patrimoniului public aflat în gestiune;
- l) gestionează finanțe publice și administrează patrimoniul public al Centrului, în conformitate cu principiile bunei guvernări;
- m) poate delega o parte din atribuțiile sale directorilor adjuncți ai Centrului sau funcționarilor publici din cadrul Centrului;
- n) alte atribuții prevăzute de legislație.

(2) Directorii adjuncți ai Centrului asistă directorul în conducerea Centrului și exercită atribuțiile delegate de către director. În cazul absenței directorului Centrului sau al vacanței funcției acestuia, toate atribuțiile lui sunt exercitate de către directorul adjunct desemnat prin ordinul directorului Centrului.

Articolul 66. Încetarea mandatului directorului și al directorilor adjuncți ai Centrului

(1) Mandatul directorului sau al directorilor adjuncți ai Centrului încetează în cazul:

- a) demisiei;
- b) revocării;
- c) expirării mandatului;
- d) atingerii vârstei de pensionare;
- e) decesului.

(2) Revocarea directorului sau a unui director adjunct al Centrului se face în cazul în care:

- a) a săvârșit o încălcare gravă a obligațiilor funcționale prevăzute de lege;
- b) nu și-a depus declarația de avere și interese personale ori a refuzat să o depună;

- c) a obținut calitatea de membru al unui partid politic;
- d) a rămas definitivă o sentință de condamnare a acestuia;
- e) survin circumstanțe care fac ca acesta să nu mai corespundă condițiilor stabilite la art. 63;
- f) din motive de sănătate, este în imposibilitate de a-și exercita atribuțiile pe o perioadă mai mare de 3 luni consecutiv;
- g) este declarat dispărut fără veste, conform legii.

(3) Temeiurile prevăzute la alin. (1)-(2) se constată în cadrul ședinței plenare a Parlamentului, în baza raportului Comisiei juridice, numiri și imunități, prin adoptarea unei hotărâri a Parlamentului prin care se ia act de apariția situației ce determină încetarea mandatului. Încetarea mandatului a directorului sau a directorilor adjuncți ai Centrului se adoptă de către Parlament cu votul majorității deputaților aleși.

(4) În cazul expirării mandatului directorului Centrului, acesta continuă să-și exercite atribuțiile până la numirea unui nou director al Centrului.

(5) Mandatul directorilor adjuncți ai Centrului se încheie odată cu mandatul directorului Centrului, însă aceștia continuă să-și exercite atribuțiile până la numirea unor noi directori adjuncți.

Articolul 67. Personalul Centrului

(1) Personalul Centrului este compus din persoane cu funcții de demnitate publică, funcționari publici și personal contractual.

(2) Atribuțiile și sarcinile personalului Centrului se stabilesc prin regulamentul intern aprobat prin ordinul directorului Centrului.

Articolul 68. Inspectorul de protecție a datelor

(1) Inspectorul de protecție a datelor este responsabil de examinarea plângerilor cu privire la presupusele încălcări ale prezentei legi, de efectuarea investigațiilor legalității prelucrării datelor cu caracter personal, precum și de alte sarcini prevăzute de legislație.

(2) Funcția de inspector de protecție a datelor este o funcție publică, exercitată în modul stabilit de prezenta lege și Legea nr. 158/2008 cu privire la funcția publică și statutul funcționarului public.

(3) Inspectorul de protecție a datelor primește legitimație de serviciu în modul stabilit de Centru.

Articolul 69. Numirea în funcția de inspector de protecție a datelor

(1) Poate candida la funcția de inspector de protecție a datelor persoana care îndeplinește cumulativ următoarele condiții:

- a) deține cetățenia Republicii Moldova;
- b) are domiciliul pe teritoriul Republicii Moldova;
- c) nu este supusă unei măsuri de ocrotire judiciare sub forma tutelei;
- d) are studii superioare în domeniul dreptului;
- e) are o reputație ireproșabilă;

f) nu are, în ultimii 5 ani, în cazierul privind integritatea profesională, înscrieri referitoare la rezultatul negativ al testului de integritate profesională pentru încălcarea obligației prevăzute la art. 7 alin. (2) lit. a) din Legea nr. 325/2013 privind evaluarea integrității instituționale;

g) cunoaște limba română.

(2) Se consideră că nu are o reputație ireproșabilă, în sensul alin. (1) lit. e), persoana:

a) care are antecedente penale;

b) care a fost privată de dreptul de a ocupa anumite funcții sau a exercita anumite activități, ca pedeapsă principală sau complementară, printr-o hotărâre judecătorească definitivă;

c) în privința căreia s-a constatat, printr-un act definitiv, încălcarea regimului juridic al conflictelor de interese, al incompatibilităților, restricțiilor și limitărilor;

d) în privința căreia există o hotărâre irevocabilă a instanței de judecată prin care s-a dispus confiscarea averii nejustificate;

e) care are, în ultimii 5 ani, în cazierul privind integritatea profesională, înscrieri cu privire la rezultatul negativ al testului de integritate profesională pentru încălcarea obligației prevăzute la art. 7 alin. (2) lit. a) din Legea nr. 325/2013 privind evaluarea integrității instituționale.

f) care are interdicția de a ocupa o funcție publică sau de demnitate publică, ce derivă dintr-un act de constatare al Autorității Naționale de Integritate.

Articolul 70. Răspunderea inspectorilor de protecție a datelor

(1) Inspectorul de protecție a datelor este responsabil de legalitatea acțiunilor realizate în cadrul procedurilor de investigare, precum și de calitatea investigației efectuate.

(2) Inspectorul de protecție a datelor poartă răspundere disciplinară, contravențională, civilă sau penală în conformitate cu legislația.

Articolul 71. Statutul personalului Centrului

Activitatea personalului Centrului este supusă reglementărilor din prezenta lege și, după caz, din Legea nr. 199/2010 cu privire la statutul persoanelor cu funcții de demnitate publică, Legea nr. 158/2008 cu privire la funcția publică și statutul funcționarului public, legislația muncii.

Capitolul VIII REMEDIILE LEGALE, RĂSPUNDEREA ȘI SANCTIUNILE

Secțiunea 1 Dispoziții generale

Articolul 72. Dreptul de a depune o plângere la Centru

(1) Fără a aduce atingere art. 74, orice persoană vizată are dreptul de a depune o plângere la Centru, în cazul în care consideră că prelucrarea datelor cu caracter personal care o vizează încalcă prezenta lege.

(2) Termenul de prescripție pentru depunerea plângerii este de un an de la data la care persoana putea să ia cunoștință de săvârșirea presupusei încălcări, însă nu mai târziu de 3 ani de la data săvârșirii acesteia.

(3) În cazul unei presupuse încălcări continue sau prelungite, termenul de prescripție începe să curgă de la data săvârșirii ultimei acțiuni sau inacțiuni.

(4) În cazul în care plângerea este depusă după expirarea termenului de prescripție prevăzut la alin. (2) și (3), Centrul respinge plângerea.

(5) Centrul informează autorul plângerii cu privire la evoluția și rezultatul plângerii, inclusiv posibilitatea de a contesta actele Centrului în conformitate cu art. 73.

(6) Prevederile Codului administrativ al Republicii Moldova nr. 116/2018 se aplică numai în măsura în care nu contravin prevederilor prezentei legi.

Articolul 73. Dreptul de a contesta acțiunile sau inacțiunile Centrului

(1) Acțiunile sau inacțiunile Centrului pot fi contestate direct în instanța de judecată, conform Codului administrativ al Republicii Moldova nr. 116/2018, fără respectarea procedurii prealabile.

(2) În cazul în care Centrul nu examinează o plângere sau nu informează persoana vizată în termen de trei luni cu privire la progresele sau la soluționarea plângerii depuse conform art. 72, persoana afectată poate contesta inacțiunile Centrului direct în instanța de judecată, conform Codului administrativ al Republicii Moldova nr. 116/2018, fără respectarea procedurii prealabile.

Articolul 74. Dreptul de a depune o cerere de chemare în judecată împotriva unui operator sau unei persoane împuternicite de operator

Fără a aduce atingere art. 72 și 73, precum și fără a aduce atingere modalităților alternative de soluționare a litigiilor, orice persoană vizată are dreptul de a depune o cerere de chemare în judecată la instanța judecătorească competentă, 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 75. Reprezentarea persoanelor vizate

Persoana vizată are dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ, care au fost constituite în mod corespunzător în conformitate cu legislația, 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. 72-74, precum și să exercite dreptul de a primi despăgubiri menționat la art. 76 în numele persoanei vizate, dacă acest lucru este prevăzut în actele normative.

Articolul 76. Dreptul la despăgubiri și răspunderea

(1) Orice persoană care a suferit un prejudiciu material sau moral ca urmare a unei încălcări a prezentei legi are dreptul să obțină despăgubiri de la operator sau de la persoana împuternicită de operator pentru prejudiciul suferit.

(2) Orice operator implicat în operațiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operațiunile sale de prelucrare care încalcă prezenta lege. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care nu a respectat obligațiile din prezenta lege care revin în mod specific persoanelor împuternicite de operator sau a acționat în afara sau în contradicție cu instrucțiunile legale ale operatorului.

(3) Operatorul sau persoana împuternicită de operator sunt exonerati de răspundere în temeiul alin. (2) dacă dovedesc că nu sunt răspunzători în niciun fel pentru evenimentul care a cauzat prejudiciul.

(4) În cazul în care mai mulți operatori sau mai multe persoane împuternicite de operator, sau un operator și o persoană împuternicită de operator sunt implicați în aceeași operațiune de prelucrare și răspund, în temeiul alin. (2) și (3), pentru orice prejudiciu cauzat de prelucrare, fiecare operator sau persoană împuternicită de operator sunt răspunzători pentru întregul prejudiciu pentru a asigura despăgubirea efectivă a persoanei vizate.

(5) În cazul în care un operator sau o persoană împuternicită de operator a plătit, în conformitate cu alin. (4), în totalitate despăgubirile pentru prejudiciul cauzat, respectivul operator sau respectiva persoană împuternicită de operator are dreptul să solicite de la ceilalți operatori sau celelalte persoane împuternicite de operator implicate în aceeași operațiune de prelucrare recuperarea acelei părți din despăgubiri care corespunde părții lor de răspundere pentru prejudiciu, în conformitate cu condițiile stabilite la alin. (2).

(6) Acțiunile în exercitarea dreptului de recuperare a despăgubirilor se depun la instanțele judecătorești competente, în conformitate cu legea.

Secțiunea a 2-a**Examinarea preliminară, investigarea și luarea deciziilor****Articolul 77. Inițierea procedurii de examinare**

(1) Centrul inițiază procedura de examinare a presupuselor cazuri de încălcare a prezentei legi sau a altor acte normative privind prelucrarea datelor cu caracter personal:

- a) la plângerea unei persoane vizate; sau
- b) din oficiu.

(2) Centrul poate iniția examinarea din oficiu în baza informațiilor de care dispune referitoare la presupusa încălcare a legislației, în conformitate cu art. 81.

Articolul 78. Etapele procedurii de examinare

(1) Procedura de examinare a presupuselor cazuri de încălcare a legislației privind prelucrarea datelor cu caracter personal cuprinde:

- a) examinarea preliminară; și/sau
- b) investigarea.

(2) Investigarea pe marginea cazului se dispune în condițiile art. 81. În celelalte cazuri etapa investigării este omisă.

Articolul 79. Depunerea plângerii

(1) Plângerea depusă la Centru în conformitate cu art. 72 conține următoarele elemente:

- a) numele și prenumele persoanei vizate;
- b) domiciliul persoanei vizate, precum și adresa de poștă electronică dacă se solicită răspuns pe această cale;
- c) specificarea tuturor circumstanțelor de fapt și de drept privind pretinsa încălcare a legislației privind prelucrarea datelor cu caracter personal în privința persoanei vizate;
- d) informații care permit identificarea operatorului sau a persoanei împuternicite de operator, în măsura în care este posibil;
- e) informații privind depunerea plângerii în termenul de prescripție prevăzut la art. 72 alin. (2) și (3).
- f) măsurile solicitate de a fi întreprinse de Centru;
- g) după caz, informațiile privind adresările înaintate operatorului sau persoanei împuternicite de operator, precum și rezultatul acestor adresări;
- h) după caz, alte informații relevante, în special dacă obiectul plângerii a fost sau se examinează de o instanță de judecată sau dacă autorul plângerii a întreprins alte măsuri, inclusiv, după caz, rezultatul lor;
- i) semnătura persoanei vizate sau a reprezentantului său legal ori împuternicit, iar în cazul plângerilor transmise în formă electronică – semnătura electronică.

(2) Plângerea este însoțită, după caz, de:

- a) documentul confirmativ al reprezentantului legal, procura sau împuternicirea în baza semnăturii electronice a reprezentantului împuternicit;
- b) mandatul acordat în temeiul art. 75;
- c) documente și probe care sunt considerate utile de către autor pentru susținerea plângerii sale.

(3) Centrul facilitează depunerea plângerilor prin punerea la dispoziția publicului a formularului plângerii, inclusiv în format electronic, fără a exclude alte mijloace de comunicare.

Articolul 80. Examinarea preliminară a plângerii

(1) Examinarea preliminară a plângerii privind presupusa încălcare a legislației privind prelucrarea datelor cu caracter personal se efectuează în termen de 30 de zile de la data înregistrării plângerii.

(2) În cadrul examinării preliminare a plângerii, Centrul determină dacă există temeuri rezonabile pentru a suspecta încălcarea legislației privind prelucrarea datelor cu caracter personal.

(3) Plângerile anonime sau cele depuse fără indicarea adresei poștale sau electronice a persoanei vizate nu se examinează.

(4) Dacă plângerea nu corespunde cerințelor prevăzute la art. 79 alin. (1) lit. c)-f), i) sau art. 79 alin. (2) lit. a) sau b), persoanei vizate i se indică asupra neajunsurilor și i se acordă un termen rezonabil pentru înlăturarea lor. În cazul în care nu înlătură neajunsurile în termenul acordat, plângerea nu se examinează, fapt despre care este informată persoana vizată.

(5) Dacă consideră că, în baza informațiilor prezentate de autorul plângerii și a altor informații relevante, nu există temeuri rezonabile pentru a suspecta încălcarea legislației privind prelucrarea datelor cu caracter personal, Centrul respinge motivat plângerea și informează persoana vizată despre acest fapt.

(6) Pentru a respinge o plângere pe motiv că comportamentul sesizat nu contravine legislației privind prelucrarea datelor cu caracter personal sau nu intră în domeniul de aplicare a acesteia, Centrul nu este obligat să țină cont de circumstanțele care nu i-au fost aduse la cunoștință de către autorul plângerii.

(7) Dacă, în procesul examinării preliminare a plângerii sau a investigării în conformitate cu art. 81, există bănuieli rezonabile privind săvârșirea unei infracțiuni, Centrul sesizează organul de urmărire penală. În acest caz, examinarea preliminară sau investigarea continuă. Organul de urmărire penală este obligat să informeze Centrul cu privire la decizia luată.

Articolul 81. Investigația

(1) Investigația reprezintă activitatea de colectare și administrare a informațiilor privind legalitatea prelucrării datelor cu caracter personal, acumulate în condițiile prevăzute de prezenta lege.

(2) Dacă după examinarea preliminară a plângerii se consideră că, în baza informațiilor prezentate de persoana vizată și a celor acumulate pe parcursul examinării preliminare, există temeuri rezonabile pentru a suspecta încălcarea legislației privind protecția datelor cu caracter personal, Centrul emite o dispoziție de inițiere a investigației.

(3) Investigațiile din oficiu se pot efectua:

a) ca urmare a transmiterii notificărilor de încălcare a securității datelor cu caracter personal;

b) pentru verificarea unor date și informații cu privire la presupuse încălcări ale legislației privind prelucrarea datelor cu caracter personal, obținute de Centru din alte surse decât cele care fac obiectul plângerii sau notificării de încălcare a securității datelor cu caracter personal, cum ar fi sesizările sau informațiile primite de la o altă autoritate de supraveghere sau de la o altă autoritate publică, corespondența primită de Centru, mass-media, accesarea rețelei de internet, documentele de constatare întocmite în urma efectuării altor investigații sau orice alte informații. Asemenea surse pot constitui temeii pentru

inițierea unei investigații din oficiu doar dacă circumstanțele sau informațiile pe care acestea le conțin indică în mod rezonabil asupra unei posibile încălcări a legislației privind prelucrarea datelor cu caracter personal;

c) în vederea cooperării internaționale în domeniul protecției datelor cu caracter personal, în cadrul operațiunilor comune și al acordării de asistență reciprocă.

(4) Dispoziția pentru inițierea investigației din oficiu trebuie să conțină analiza și argumentarea necesară privind îndeplinirea condițiilor stabilite la alin. (3).

(5) Investigația din oficiu poate fi inițiată doar în termenele de prescripție prevăzute la art. 72 alin. (2) și (3).

(6) Dispoziția de inițiere a investigației nu stabilește comiterea unei încălcări a legislației privind prelucrarea datelor cu caracter personal. Încălcarea legislației privind prelucrarea datelor cu caracter personal se constată prin decizie a Centrului.

(7) La efectuarea investigației, Centrul are în vedere prioritar posibilitatea efectuării acesteia prin solicitare directă de la persoana investigată și alte persoane atrase în cadrul investigației a documentației și a altor informații sau prin alte metode care fac posibilă obținerea unor astfel de date. Doar în cazul insuficienței documentației și a informației deținute pentru a stabili respectarea legislației de către persoana supusă investigației sau pornind de la tipul investigației și a analizei riscurilor, Centrul realizează investigația cu ieșirea la fața locului, prin emiterea unei delegații de efectuare a investigației cu ieșirea la fața locului. Investigația la fața locului poate fi efectuată numai dacă există indici că pot fi găsite documente sau pot fi obținute informații considerate necesare pentru investigația presupusului caz de încălcare a legislației privind protecția datelor cu caracter personal, inițiată prin dispoziție, fapt care nu necesită a fi demonstrat subiectului supus investigației. În cazul solicitărilor directe de informații fără ieșirea la fața locului, în demersurile adresate, Centrul specifică datele indicate la alin. (8) cu excepția celor indicate la lit. a).

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

- a) numărul și data emiterii;
- b) datele de identificare ale Centrului;
- c) trimitere la prevederile legale, în baza cărora este realizată investigația;
- d) tipul investigației și temeiul inițierii acesteia;
- e) datele despre inspectorii de protecție a datelor care realizează investigația cu ieșirea la fața locului (numele, prenumele și funcția);
- f) datele despre persoana fizică sau juridică supusă investigației (după caz, denumirea/numele persoanei; codul fiscal; sediul/adresa subdiviziunii controlate și codul acesteia, după caz, alte date de contact);
- g) obiectul investigației;
- h) scopul și aspectele ce urmează a fi investigate;
- i) data începerii investigației și durata preconizată a acesteia.

(9) Delegația privind efectuarea investigației cu ieșirea la fața locului se aduce la cunoștință sub semnătură persoanei supuse investigației ori reprezentantului legal sau împuternicit. În cazul refuzului primirii și semnării delegației se întocmește un act, în prezența a doi martori. Prezența martorilor nu este necesară în cazul înregistrării refuzului prin mijloace video și audio.

(10) Inspectorii de protecție a datelor, în limita împuternicirilor ce rezultă din alin. (7) și (8), au următoarele drepturi:

a) să obțină acces la toate datele cu caracter personal și la toate informațiile necesare pentru efectuarea investigației, indiferent de suportul pe care sunt stocate, inclusiv la orice documente, sisteme de evidență, produse de program, echipamente și mijloace de prelucrare a datelor;

b) să aibă acces în orice spații și încăperi legate de obiectul și scopul investigației, aflate în proprietatea sau folosința persoanelor supuse investigației;

c) să solicite și să primească informațiile, documentele și explicațiile solicitate în termenul stabilit, care trebuie să fie unul rezonabil, ținând cont de volumul și complexitatea informațiilor, documentelor și a explicațiilor solicitate. Termenul poate fi prelungit la solicitarea motivată a persoanei supuse investigării;

d) să audieze persoana supusă investigației sau reprezentantul legal sau împuternicit al acesteia asupra faptelor relevante obiectului investigației și, după caz, să înregistreze răspunsurile acestora, inclusiv prin mijloace audio și/sau video, cu informarea prealabilă a persoanei audiate. La cerere, o copie a înregistrării este transmisă 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 examinarea lor;

f) să solicite sprijinul subdiviziunilor abilitate ale Ministerului Afacerilor Interne, care sunt obligate să acorde asistența necesară inspectorilor de protecție a datelor pentru efectuarea investigației. La efectuarea investigației pot fi antrenați, după caz, și experți din anumite domenii, împuterniciți de Centru, care sunt obligați să asigure confidențialitatea informațiilor de care au făcut cunoștință în cadrul investigației.

(11) 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 alin. (8) lit. b)-i);

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

(12) Pe parcursul efectuării investigației, persoana investigată are următoarele drepturi:

a) să obțină o copie a delegației privind efectuarea investigației la fața locului sau informațiile prevăzute la alin. (8) 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 fie asistată de avocați, de alți reprezentanți împuterniciți conform legislației.

(13) Persoana supusă investigației cu ieșirea la fața locului poate fi asistată de avocat. Absența avocatului nu împiedică desfășurarea acțiunilor de investigare.

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

(15) Investigația la fața locului se desfășoară în orele de program ale persoanei supuse investigației sau, în lipsa acestora, între orele 09:00 și 17:00 și se efectuează în prezența persoanei supuse investigației sau a reprezentantului acestuia. Investigația poate continua și după orele de program sau după ora 17:00, după caz, numai cu acordul persoanei supuse investigației sau al reprezentantului acestuia.

(16) Accesul inspectorilor de protecție a datelor în domiciliul sau reședința persoanei fizice, în lipsa consimțământului acesteia, se permite numai în baza mandatului judecătoresc emis în condițiile alin. (17)-(20) și prezentat persoanei fizice respective.

(17) În situația în care inspectorii sunt împiedicați în orice mod în exercitarea atribuțiilor, precum și în cazul în care există o suspiciune întemeiată că informațiile, documentele, echipamentele, mijloacele sau suporturile relevante obiectului investigației care ar putea fi pertinente pentru a dovedi o încălcare gravă a prezentei legi sunt păstrate în încăperi, terenuri sau mijloace de transport ocupate de persoane fizice, Centrul poate solicita un mandat judecătoresc, în condițiile prezentei legi, printr-o cerere adresată instanței judecătorești în a cărei rază teritorială își are sediul Centrul. Cererea de autorizare trebuie să cuprindă toate informațiile de natură să justifice investigația, iar judecătorul sesizat este ținut să verifice dacă cererea este întemeiată.

(18) Mandatul judecătoresc poate fi eliberat numai dacă:

a) există o suspiciune întemeiată că în încăperile ce urmează a fi supuse investigației sunt păstrate informații, documente, echipamente, mijloace sau suporturi relevante obiectului investigației a căror prezentare a fost solicitată de Centru în conformitate cu prezenta lege, dar care nu au fost prezentate în termenul stabilit;

b) există o suspiciune întemeiată că în încăperile ce urmează a fi supuse investigației sunt păstrate informații, documente, echipamente, mijloace sau suporturi relevante obiectului investigației a căror prezentare poate fi solicitată de Centru în conformitate cu prezenta lege și care, dacă ar fi fost cerute, nu ar fi fost prezentate, dar ar fi fost ascunse, înlăturate, modificate sau distruse; sau

c) inspectorilor de protecție a datelor le-a fost restricționat accesul în încăperile, terenurile sau mijloacele de transport ce urmează a fi supuse

investigației, fiind create impedimente de către persoanele fizice sau juridice supuse investigației, precum și există o suspiciune întemeiată că în încăperile, terenurile sau mijloacele de transport respective sunt păstrate informații, documente, echipamente, mijloace sau suporturi relevante obiectului investigației a căror prezentare a fost solicitată de Centru în conformitate cu prezenta lege.

(19) Mandatul judecătoresc trebuie să conțină scopul și obiectul investigației, autorizarea emisă, precum și dreptul de a ataca mandatul cu recurs. Mandatul este valabil o lună de la data emiterii.

(20) În cazul solicitării unui mandat, instanța de judecată este obligată să verifice dacă dispoziția privind efectuarea investigației este autentică și dacă măsurile coercitive preconizate nu sunt arbitrare sau excesive, având în vedere obiectul investigației. Atunci când verifică proporționalitatea măsurilor coercitive, instanța de judecată poate solicita Centrului explicații detaliate, în special privind temeiurile care determină Centru să suspecteze încălcarea prezentei legi, precum și gravitatea încălcării suspectate, importanța probelor căutate, natura implicării persoanei supuse investigării în cauză și probabilitatea rezonabilă că informațiile, documentele, echipamentele, mijloacele sau suporturile relevante obiectului investigației se păstrează în locul pentru care se solicită mandatul.

(21) Mandatul judecătoresc emis în conformitate cu alin. (17)-(20) poate fi atacat cu recurs la Curtea de Apel Centru, care nu este suspensiv de executare, dacă instanța de recurs nu dispune altfel.

(22) Alin. (17)-(21) se aplică în mod corespunzător și în cazul solicitării de la furnizorii rețelei și/sau serviciilor de comunicații electronice a datelor de trafic și/sau a datelor de localizare aferente serviciilor de comunicații electronice furnizate sau a accesului la datele respective.

(23) Rezultatul investigației este consemnat în proiectul de decizie asupra investigației, care prevede constatarea sau lipsa încălcării, precum și măsurile corective și sancțiunile aplicate. Proiectul de decizie se expediază persoanei vizate și a operatorului sau a persoanei împuternicite care au fost supuși investigației, cu acordarea unui termen de 30 de zile pentru înaintarea unor eventuale obiecții, care curge de la data expedierii. Termenul prevăzut la alin. (25) se suspendă la data expedierii proiectului deciziei către părți, până la data prezentării eventualelor obiecții asupra proiectului deciziei sau, în cazul în care observațiile nu sunt prezentate în termenul stabilit, până la data expirării termenului stabilit pentru prezentarea observațiilor.

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

(25) Termenul de efectuare a investigației este de până la 6 luni de la data inițierii investigației, cu posibilitatea prelungirii justificate a acestuia cu câte o lună, dar nu mai mult de 12 luni de la data inițierii acesteia, în funcție de

complexitatea cauzei, volumul de informații ce urmează a fi obținute și examinate, comportamentul participanților la procedura de investigație și alte aspecte relevante. Centrul informează persoana vizată cu privire la prelungirea termenului de efectuare a investigației, precum și motivele acestei prelungiri.

Articolul 82. Solicitarea informațiilor

(1) În scopul exercitării atribuțiilor sale, Centrul are dreptul să solicite și să obțină gratuit, asigurând confidențialitatea informației, de la persoanele fizice și persoanele juridice de drept public și de drept privat orice documente și informații necesare, inclusiv în format digital, care sunt accesibile și pot fi relevante pentru aplicarea legii, fără să poată fi invocată confidențialitatea urmării penale, a secretului bancar, a secretului comercial, a secretului fiscal, a secretului medical, a secretului profesional (cu excepția secretului profesional prevăzut la art. 55 din Legea nr. 1260/2002 cu privire la avocatură), a datelor cu caracter personal și a altor informații cu accesibilitate limitată.

(2) Centrul solicită în scris informațiile necesare, indică temeiul juridic și scopul solicitării informațiilor și stabilește un termen rezonabil în care acestea trebuie furnizate, care este de cel puțin 5 zile lucrătoare, precum și specifică sancțiunile prevăzute de lege.

(3) Solicitățile de informații trebuie să fie proporționale și să nu oblige persoana supusă investigației să recunoască faptul că a comis o încălcare, aceasta fiind obligată să răspundă la întrebări factuale și să furnizeze documente chiar dacă acestea pot fi folosite pentru a stabili împotriva sa sau a altei persoane existența unei încălcări.

(4) În cadrul efectuării investigărilor, comunicările dintre persoana supusă investigației și avocatul acesteia, realizate în cadrul și în scopul exclusiv al exercitării dreptului la apărare al persoanei supuse investigației, care are legătură cu obiectul investigației, nu pot fi folosite ca probă pentru constatarea unei încălcări a legislației privind protecția datelor cu caracter personal. Dacă persoana supusă investigației nu dovedește caracterul protejat al comunicării, aceasta se sigilează și se ridică în două exemplare.

Articolul 83. Confidențialitatea

(1) Persoanele care, în virtutea drepturilor și atribuțiilor ce le revin în temeiul prezentei legi, au luat cunoștință de informațiile investigației, precum și 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 îndeplinirii 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.

Articolul 84. Emiterea și comunicarea deciziilor

(1) La finalizarea investigației Centrul emite decizia motivată privind constatarea sau lipsa încălcării legislației privind prelucrarea datelor cu caracter personal și aplicarea măsurilor prevăzute în secțiunea a 3-a, după caz.

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

(3) Decizia se emite de către directorul Centrului, de către directorul adjunct sau personalul abilitat cu funcții de control ai Centrului, în conformitate cu competențele atribuite prin ordinul directorului Centrului. Decizia se comunică persoanei vizate și persoanei supuse investigației în termen de 10 zile lucrătoare de la data emiterii.

(4) Centrul publică rezumatul deciziilor emise în care reflectă natura încălcărilor depistate, motivarea deciziei, măsurile dispuse, precum și sancțiunile aplicate.

Articolul 85. Executarea deciziilor Centrului

(1) Deciziile Centrului se execută în termenul menționat în ele, cu obligația de a informa în scris Centrul despre măsurile întreprinse. Centrul poate stabili termenul de executare a deciziei de până la 6 luni, ținând cont de complexitatea acțiunilor ce urmează a fi efectuate, de gradul de pericol al încălcărilor care necesită a fi înlăturate, de posibilitățile persoanei supuse investigației de a îndeplini acțiunile prescrise, precum și de prescripțiile anterioare, emise în cazuri similare. În cazuri complexe, atunci când decizia Centrului prevede implementarea unor măsuri corective complexe, la solicitarea întemeiată a operatorului sau a persoanei împuternicite de operator, Centrul poate extinde termenul de executare a deciziei peste termenul de 6 luni.

(2) Termenul de executare benevolă a amenzii este de cel puțin 2 luni de la data comunicării deciziei.

(3) Deciziile Centrului se execută silit în conformitate cu Codul de executare al Republicii Moldova nr. 443/2004.

(4) În partea încasării amenzilor aplicate, deciziile Centrului se execută în conformitate cu procedura de executare a creanțelor bănești bazată pe dispoziții de drept public, aprobate de Guvern.

Secțiunea a 3-a Sancțiunile pecuniare

Articolul 86. Amenda

(1) Amenda reprezintă sancțiunea pecuniară aplicată operatorului de către Centru, în cazul constatării încălcărilor prezentei legi.

(2) Amenda aplicată de Centru se varsă la bugetul de stat.

Articolul 87. Condiții generale pentru aplicarea amenzilor

(1) Centrul asigură faptul că impunerea amenzilor în conformitate cu prezenta secțiune, pentru încălcările prezentei legi prevăzute la art. 88, este, în fiecare caz, eficace, proporțională și disuasivă.

(2) În funcție de circumstanțele fiecărui caz în parte, amenzile sunt aplicate în completarea sau în locul măsurilor menționate la art. 60 alin. (2) lit. a)-h) și j). În cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi aplicată ar constitui o sarcină disproporționată pentru o persoană fizică, poate fi emis un avertisment în locul unei amenzi. În vederea aplicării unei amenzi, precum și în vederea determinării quantumului amenzii, se ține cont, în fiecare caz particular, de următoarele circumstanțe:

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 Centru 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 Centrului, 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. 60 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; și

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) Amenzile pot fi aplicate numai dacă se stabilește că operatorul a săvârșit intenționat sau din neglijență o încălcare prevăzută la art. 88.

(4) 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 nu poate depăși suma prevăzută pentru cea mai gravă încălcare.

Articolul 88. Încălcările pasibile de amendă

(1) În conformitate cu art. 87, se aplică amenzi de până la 1 000 000 lei sau, în cazul unei întreprinderi, de până la 1% din cifra totală de afaceri realizată în anul anterior sancționării, luându-se în calcul cea mai mare valoare, pentru încălcarea următoarelor dispoziții:

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).

(2) În conformitate cu art. 87, se aplică amenzi de până la 2 000 000 lei sau, în cazul unei întreprinderi, de până la 2% din cifra totală de afaceri realizată în anul anterior sancționării, luându-se în calcul cea mai mare valoare, pentru încălcarea următoarelor dispoziții:

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-un alt stat sau către o organizație internațională, în conformitate cu art. 44-49;

d) obligațiile prevăzute la capitolul VI;

e) nerespectarea unei măsuri corective sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emise de Centru în limitele prevăzute de lege, în temeiul art. 60 alin. (2), sau neacordarea accesului, încălcând art. 60 alin. (1);

(3) Pentru încălcarea unei măsuri corective emise de Centru în conformitate cu art. 60 alin. (2) se aplică, în conformitate cu art. 87, amenzi de până la 2 000 000 lei sau, în cazul unei întreprinderi, de până la 2% din cifra totală de afaceri realizată în anul anterior sancționării, luându-se în calcul cea mai mare valoare.

(4) Fără a aduce atingere competențelor corective ale Centrului menționate la art. 60 alin. (2), sancțiunile prevăzute de prezentul articol se aplică și autorităților și instituțiilor publice, conform prezentei legi.

(5) În cazul în care cifra totală de afaceri realizată în anul anterior sancționării nu este înregistrată, se ia în considerare ultimul an anterior sancționării în care întreprinderea a realizat o cifră de afaceri.

Capitolul IX DISPOZIȚII FINALE ȘI TRANZITORII

Articolul 89. Dispozițiile finale

(1) Prezenta lege intră în vigoare la expirarea a 24 de luni de la data publicării în Monitorul Oficial al Republicii Moldova.

(2) Guvernul, până la intrarea în vigoare a prezentei legi:

a) va prezenta Parlamentului propuneri pentru modificarea legislației în conformitate cu prezenta lege;

b) va modifica actele sale normative în conformitate cu prezenta lege;

(3) Centrul, până la intrarea în vigoare a prezentei legi:

a) va propune Parlamentului efectivul-limită a Centrului;

b) va aproba actele normative necesare pentru executarea prezentei legi.

Articolul 90. Dispozițiile tranzitorii

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

(2) Personalul Centrului, aflat în funcție la momentul intrării în vigoare a prezentei legi, se încadrează în funcțiile noi conform schemei de încadrare a personalului, respectându-se prevederile Legii nr. 158/2008 cu privire la funcția publică și statutul funcționarului public și ale legislației muncii.

(3) 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;

c) art. 741-743 și art. 4234 din Codul contravențional al Republicii Moldova nr. 218/2008.

(4) Din momentul intrării în vigoare a prezentei legi, din cuantumul final al sancțiunii pecuniare stabilite de Centru, se va aplica:

a) din primul an – 10 procente din cuantumul amenzii stabilite;

b) din al doilea an – 40 procente din cuantumul amenzii stabilite;

c) din al treilea an – 100 procente din cuantumul amenzii stabilite.

(5) Actele emise de Centru în temeiul art. 32 alin. (3) și alin (5) lit. i) din Legea nr. 133/2011 privind protecția datelor cu caracter personal rămân în vigoare și după intrarea în vigoare a prezentei legi.

(6) Plângerile depuse la Centru până la data intrării în vigoare a prezentei legi se examinează și se soluționează conform legislației în vigoare la data depunerii plângerii.

Președintele Parlamentului

NOTĂ INFORMATIVĂ
la proiectul de lege privind protecția datelor cu caracter personal

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului

Proiectul de lege privind protecția datelor cu caracter personal a fost elaborat de Ministerul Justiției, cu suportul grupului de lucru interinstituțional format din reprezentanți ai Parlamentului, Centrului de Armonizare a Legislației, Consiliului Economic pe lângă Prim-ministrul, Centrului Național pentru Protecția Datelor cu Caracter Personal, Ministerului Economiei, Ministerului Afacerilor Interne, Procuraturii Generale, Centrului Național Anticorupție, Camerei de Comerț Americane din Moldova, Asociației Businessului European, Asociației Naționale a Companiilor din Domeniul TIC, precum și ai Asociației Investitorilor Străini.

2. Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile urmărite

Prezentul proiect de lege transpune *Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (denumit în continuare și **RGPD**)* și are drept scop, în principal, executarea art. 13 alin. (1) din *Acordul de Asociere*, conform căruia Republica Moldova s-a angajat să asigure un nivel înalt de protecție a datelor cu caracter personal în conformitate cu instrumentele internaționale ale Uniunii Europene și ale Consiliului Europei.

Acest angajament a fost reiterat și în *Recomandarea nr. 1/2022 a Consiliului de asociere UE-Republica Moldova din 22 august 2022 privind Programul de asociere UE-Republica Moldova [2022/1997]*, care a stabilit drept o prioritate pe termen scurt și lung a programului de asociere continuarea armonizării cadrului juridic național în domeniul protecției datelor cu caracter personal cu legislația UE, cu un accent special pe *RGPD* și pe Directiva (UE) 2016/680 a Parlamentului European și a Consiliului.

În pofida faptului că un șir de reglementări ale *acquis*-ului comunitar în domeniul protecției datelor cu caracter personal au fost introduse în cadrul normativ național al Republicii Moldova prin intermediul *Legii nr. 175/2021 pentru modificarea unor acte normative*, se constată faptul că aceste modificări reprezintă o preluare selectivă și fragmentară a prevederilor din *RGPD*, care nu

asigură o transpunere corespunzătoare a regimului juridic instituit la nivelul Uniunii Europene și care nu oferă un nivel înalt de protecție a datelor cu caracter personal.

RGPD este un instrument utilizat în scopul unificării normelor juridice în domeniul protecției datelor cu caracter personal la nivelul Uniunii Europene, avînd aplicabilitate generală și fiind obligatoriu în toate elementele sale. Prin urmare, în vederea prevenirii adoptării unor acte naționale contradictorii sau fragmentate, statele nu sunt în drept să aplice un regulament parțial sau să selecteze numai o parte din dispozițiile obligatorii ale acestuia pentru aplicare.

Astfel, cadrul juridic național în domeniul protecției datelor cu caracter personal va asigura garanții suficiente pentru protejarea drepturilor subiecților de date, doar în rezultatul alinierii legislației naționale și a transunerii în totalitate a prevederilor din *RGPD*.

Nu în ultimul rînd, prezentul proiect de lege urmărește realizarea acțiunii nr. 27 (capitolul 23) din *Planul național de acțiuni pentru aderarea Republicii Moldova la Uniunea Europeană pe anii 2024-2027*, aprobat prin *Hotărîrea Guvernului nr. 829/2023*.

3. Descrierea gradului de compatibilitate, pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

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

Pentru analiza comparativă a gradului de transpunere a fost elaborat tabelul de concordanță, care este anexat la prezentul proiect.

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

Din punct de vedere structural, proiectul de lege este împărțit în 9 capitole:

- I. Dispoziții generale;
- II. Principii;
- III. Drepturile persoanei vizate;
- IV. Operatorul și persoana împuternicită de operator;
- V. Transferurile de date cu caracter personal către alte state sau către organizații internaționale;
- VI. Cazurile specifice de prelucrare a datelor cu caracter personal;
- VII. Centrul Național pentru Protecția Datelor cu Caracter Personal;
- VIII. Remediile legale, răspunderea și sancțiunile;
- IX. Dispoziții finale și tranzitorii.

În conformitate cu art. 71 alin. (4) din *Legea nr. 100/2017 cu privire la actele normative*, la interpretarea actului normativ se ține cont de nota informativă care a însoțit proiectul actului normativ, precum și de alte documente care permit identificarea voinței autorității publice care a adoptat, a aprobat sau a emis actul normativ. Astfel, în continuare vor fi elucidate principalele prevederi ale prezentului proiect de lege.

Adițional, pornind de la faptul că acest proiect de lege reprezintă o transpunere deplină a RGPD, la interpretarea acestei legi se va ține cont de:

- a) jurisprudența Curții de Justiție a Uniunii Europene; și
- b) orientările metodologice ale Comitetului European pentru Protecția Datelor și a altor instituții europene din acest domeniu.

CAPITOLUL I – DISPOZIȚII GENERALE

Primul capitol reglementează obiectul, scopul și domeniul de aplicare al prezentei legi, precum și definește principalele noțiuni utilizate în cuprinsul legii.

Protecția conferită de prezenta lege vizează persoanele fizice, indiferent de cetățenia sau de locul lor de reședință, în ceea ce privește prelucrarea datelor cu caracter personal ale acestora. Prezenta lege nu se aplică prelucrării datelor cu caracter personal care privesc persoane juridice și, în special, întreprinderi cu personalitate juridică, inclusiv numele și tipul de persoană juridică și datele de contact ale persoanei juridice.

Pentru a preveni apariția unui risc major de eludare, protecția persoanelor fizice trebuie să fie neutră din punct de vedere tehnologic și să nu depindă de tehnologiile utilizate. Protecția persoanelor fizice se aplică prelucrării datelor cu caracter personal prin mijloace automatizate, precum și prelucrării manuale, în cazul în care datele cu caracter personal sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidență. Dosarele sau seturile de dosare, precum și copertele acestora, care nu sunt structurate în conformitate cu criteriile specifice nu ar trebui să intre în domeniul de aplicare al prezentei legi.

Prezenta lege nu se aplică prelucrării datelor cu caracter personal atribuite la secret de stat, care se efectuează în conformitate cu *Legea nr. 245/2008 cu privire la secretul de stat*. Or, art. 2 alin. (2) lit. a) din *RGPD*, în coroborare cu recitalul 16 din acest act normativ, prevede expres că *RGPD* nu se aplică activităților ce vizează securitatea națională.

Prezenta lege nu se aplică prelucrării datelor cu caracter personal de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice și care, prin urmare, nu are legătură cu o activitate profesională sau comercială. Activitățile personale sau domestice ar putea include corespondența și repertoriul de adrese sau activitățile din cadrul rețelelor sociale și activitățile online

desfășurate în contextul respectivelor activități. Cu toate acestea, prezenta lege se aplică operatorilor sau persoanelor împuternicite de operatori care furnizează mijloacele de prelucrare a datelor cu caracter personal pentru astfel de activități personale sau domestice.

Protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora, precum și libera circulație a acestor date, va face obiectul unui act legislativ separat, care va transpune *Directiva (UE) 2016/680*. Prin urmare, prezenta lege nu se aplică activităților de prelucrare în aceste scopuri.

Orice prelucrare a datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau al unei persoane împuternicite de operator din Republica Moldova trebuie efectuată în conformitate cu prezenta lege, indiferent dacă procesul de prelucrare în sine are loc sau nu în cadrul Republicii Moldova. Este importantă accentuarea faptului că, în sensul prezentei legi, noțiunea de „sediul” semnifică exercitarea efectivă și reală a unei activități în cadrul unor înțelegeri/aranjamente stabile. Astfel, forma juridică a unor astfel de înțelegeri, prin intermediul unei sucursale sau al unei filiale cu personalitate juridică, nu este factorul determinant în această privință.

Pentru asigurarea faptului că persoanele fizice nu sunt lipsite de protecția la care au dreptul în temeiul prezentei legi, prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Republicii Moldova de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Republica Moldova face obiectul prezentei legi în cazul în care activitățile de prelucrare au legătură cu oferirea de bunuri sau servicii unor astfel de persoane vizate, indiferent dacă acestea sunt sau nu legate de o plată. Pentru a determina dacă un astfel de operator sau o astfel de persoană împuternicită de operator oferă bunuri sau servicii unor persoane vizate care se află pe teritoriul Republicii Moldova, trebuie să se stabilească dacă reiese că operatorul sau persoana împuternicită de operator intenționează să furnizeze servicii persoanelor vizate din Republica Moldova. Întrucât simplul fapt că există acces la un site al operatorului, al persoanei împuternicite de operator sau al unui intermediar în Republica Moldova, că este disponibilă o adresă de e-mail și alte date de contact sau că este utilizată o limbă folosită în general într-un alt stat în care operatorul își are sediul este insuficient pentru a confirma o astfel de intenție, factori precum utilizarea limbii române sau a monedei naționale a Republicii Moldova cu posibilitatea de a comanda bunuri și servicii în respectiva limbă sau menționarea

unor clienți sau utilizatori care se află pe teritoriul Republicii Moldova pot conduce la concluzia că operatorul intenționează să ofere bunuri sau servicii unor persoane vizate în Republica Moldova.

Prelucrarea datelor cu caracter personal ale persoanelor vizate care se află pe teritoriul Republicii Moldova de către un operator sau o persoană împuternicită de acesta care nu își are sediul în Republica Moldova face, de asemenea, obiectul prezentei legi, în cazul în care este legată de monitorizarea comportamentului unor astfel de persoane vizate, în măsura în care acest comportament se manifestă pe teritoriul Republicii Moldova. Pentru a se determina dacă o activitate de prelucrare poate fi considerată ca „*monitorizare a comportamentului*” a persoanelor vizate, urmează să se stabilească dacă persoanele fizice sunt urmărite pe internet, inclusiv posibila utilizare ulterioară a unor tehnici de prelucrare a datelor cu caracter personal care constau în crearea unui profil al unei persoane fizice, în special în scopul de a lua decizii cu privire la aceasta sau de a analiza sau de a face previziuni referitoare la preferințele personale, comportamentele și atitudinile acesteia.

Prezenta lege se aplică, de asemenea, prelucrării datelor cu caracter personal de către misiunile diplomatice și oficiile consulare ale Republicii Moldova, precum și de către alți operatori sau persoane împuternicite de operator care nu au sediu în Republica Moldova, însă legislația Republicii Moldova se aplică în temeiul dreptului internațional public.

Principiile protecției datelor se aplică oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Datele cu caracter personal care au fost supuse pseudonimizării, care ar putea fi atribuite unei persoane fizice prin utilizarea de informații suplimentare, sunt considerate informații referitoare la o persoană fizică identificabilă. Pentru a se determina dacă o persoană fizică este identificabilă, trebuie să se ia în considerare toate mijloacele, cum ar fi individualizarea, pe care este probabil, în mod rezonabil, să le utilizeze fie operatorul, fie o altă persoană, în scopul identificării, în mod direct sau indirect, a persoanei fizice respective. Pentru a se determina dacă este probabil, în mod rezonabil, să fie utilizate mijloace pentru identificarea persoanei fizice, trebuie luate în considerare toți factorii obiectivi, precum costurile și intervalul de timp necesare pentru identificare, ținându-se seama atât de tehnologia disponibilă la momentul prelucrării, cât și de dezvoltarea tehnologică. Principiile protecției datelor, prin urmare, nu se aplică informațiilor anonime, adică informațiilor care nu sunt legate de o persoană fizică identificată sau identificabilă sau datelor cu caracter personal care sunt anonimizate astfel încât persoana vizată nu este sau nu mai este identificabilă. Astfel, prezenta lege nu se aplică prelucrării unor astfel

de informații anonime, inclusiv în cazul în care acestea sunt utilizate în scopuri statistice sau de cercetare.

Prezenta lege nu se aplică datelor cu caracter personal referitoare la persoane decedate, cu excepția cazului prevăzut la art. 52 din lege (accesul la informațiile de interes public). Astfel, în cazul unei cereri de comunicare a informațiilor de interes public, înaintate în temeiul *Legii nr. 148/2023 privind accesul la informațiile de interes public*, persoanele decedate beneficiază de protecția juridică conferită de legea privind protecția datelor cu caracter personal. Prin urmare, o eventuală dezvăluire sau diseminare proactivă a unor informații privind o persoană decedată trebuie să fie conformă cu prezenta lege și *Legea nr. 148/2023 privind accesul la informațiile de interes public*, în mod identic ca și în cazul persoanelor care sunt în viață.

Aplicarea pseudonimizării datelor cu caracter personal poate reduce riscurile pentru persoanele vizate și poate ajuta operatorii și persoanele împuternicite de aceștia să își îndeplinească obligațiile de protecție a datelor. Introducerea explicită a conceptului de „pseudonimizare” în prezenta lege nu este destinată să împiedice alte eventuale măsuri de protecție a datelor.

Pentru a încuraja aplicarea pseudonimizării atunci când sunt prelucrate date cu caracter personal, trebuie să fie posibile măsuri de pseudonimizare, permițând în același timp analiza generală, în cadrul aceleiași operator atunci când operatorul a luat măsurile tehnice și organizatorice necesare pentru a se asigura că prezenta lege este pusă în aplicare în ceea ce privește respectiva prelucrare a datelor și că informațiile suplimentare pentru atribuirea datelor cu caracter personal unei anumite persoane vizate sunt păstrate separat. Operatorul care prelucrează datele cu caracter personal trebuie să indice persoanele autorizate din cadrul aceleiași operator.

Persoanele fizice pot fi asociate cu identificadorii online furnizați de dispozitivele, aplicațiile, instrumentele și protocoalele lor, cum ar fi adresele IP, identificadorii cookie sau alți identifikatori precum etichetele de identificare prin frecvențe radio. Aceștia pot lăsa urme care, în special atunci când sunt combinate cu identifikatori unici și alte informații primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice și pentru identificarea lor.

Autoritățile publice cărora le sunt divulgate date cu caracter personal în conformitate cu o obligație legală în vederea exercitării funcției lor oficiale, cum ar fi autoritățile fiscale și vamale, unitățile de investigare financiară, autoritățile administrative independente sau autoritățile piețelor financiare responsabile de reglementarea și supravegherea piețelor titlurilor de valoare, nu sunt considerate destinatari în cazul în care primesc date cu caracter personal care sunt necesare pentru efectuarea unei anumite anchete de interes general, în conformitate cu

legislația Republicii Moldova. Cererile de divulgare trimise de autoritățile publice urmează să fie întotdeauna prezentate în scris, motivate și ocazionale și nu trebuie să se refere la un sistem de evidență în totalitate sau să conducă la interconectarea sistemelor de evidență. Prelucrarea datelor cu caracter personal de către autoritățile publice respective trebuie să respecte normele aplicabile în materie de protecție a datelor în conformitate cu scopurile prelucrării.

Consimțământul urmează a fi acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal, ca de exemplu o declarație făcută în scris, inclusiv în format electronic, sau verbal. Acesta ar putea include bifarea unei căsuțe atunci când persoana vizitează un site, alegerea parametrilor tehnici pentru serviciile societății informaționale sau orice altă declarație sau acțiune care indică în mod clar în acest context acceptarea de către persoana vizată a prelucrării propuse a datelor sale cu caracter personal. Prin urmare, absența unui răspuns, căsuțele bifate în prealabil sau absența unei acțiuni nu constituie un consimțământ. Consimțământul trebuie să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul trebuie acordat pentru toate scopurile prelucrării. În cazul în care consimțământul persoanei vizate urmează a fi oferit în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul.

Uneori, nu este posibil, în momentul colectării datelor cu caracter personal, să se identifice pe deplin scopul prelucrării datelor în scopuri de cercetare științifică. Din acest motiv, persoanelor vizate trebuie să li se permită să își exprime consimțământul pentru anumite domenii ale cercetării științifice atunci când sunt respectate standardele etice recunoscute pentru cercetarea științifică. Persoanele vizate trebuie să aibă posibilitatea de a-și exprima consimțământul doar pentru anumite domenii de cercetare sau părți ale proiectelor de cercetare în măsura permisă de scopul preconizat.

Datele genetice sunt definite drept date cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care rezultă în urma unei analize a unei mostre de material biologic al persoanei fizice în cauză, în special a unei analize cromozomiale, a unei analize a acidului dezoxiribonucleic (ADN) sau a acidului ribonucleic (ARN) sau a unei analize a oricărui alt element ce permite obținerea unor informații echivalente.

Datele cu caracter personal privind sănătatea includ toate datele având legătură cu starea de sănătate a persoanei vizate care dezvăluie informații despre starea de sănătate fizică sau mentală trecută, prezentă sau viitoare a persoanei

vizate. Acestea includ informații despre persoana fizică colectate în cadrul înscrierii acesteia la serviciile de asistență medicală sau în cadrul acordării serviciilor respective persoanei fizice în cauză; un număr, un simbol sau un semn distinctiv atribuit unei persoane fizice pentru identificarea singulară a acesteia în scopuri medicale; informații rezultate din testarea sau examinarea unei părți a corpului sau a unei substanțe corporale, inclusiv din date genetice și eșantioane de material biologic; precum și orice informații privind, de exemplu, o boală, un handicap, un risc de îmbolnăvire, istoricul medical, tratamentul clinic sau starea fiziologică sau biomedicală a persoanei vizate, indiferent de sursa acestora, ca de exemplu, un medic sau un alt cadru medical, un spital, un dispozitiv medical sau un test de diagnostic in vitro.

Un grup de întreprinderi cuprinde o întreprindere care exercită controlul și întreprinderile controlate de aceasta, în cadrul căruia întreprinderea care exercită controlul ar trebui să fie întreprinderea care poate exercita o influență dominantă asupra celorlalte întreprinderi, de exemplu în temeiul proprietății, al participării financiare sau al regulilor care o reglementează sau al competenței de a pune în aplicare norme în materie de protecție a datelor cu caracter personal. O întreprindere care controlează prelucrarea datelor cu caracter personal în întreprinderile sale afiliate este considerată, împreună cu acestea din urmă, drept „grup de întreprinderi”.

Copiii au nevoie de o protecție specifică a datelor lor cu caracter personal, întrucât pot fi mai puțin conștienți de riscurile, consecințele, garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal. Această protecție specifică se aplică în special utilizării datelor cu caracter personal ale copiilor în scopuri de marketing sau pentru crearea de profiluri de personalitate sau de utilizator și la colectarea datelor cu caracter personal în momentul utilizării serviciilor oferite direct copiilor. Consimțământul titularului răspunderii părintești nu ar trebui să fie necesar în contextul serviciilor de prevenire sau consiliere oferite direct copiilor.

CAPITOLUL II – PRINCIPII

Orice prelucrare de date cu caracter personal trebuie să fie legală și echitabilă. Trebuie să fie transparent pentru persoanele fizice că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc și în ce măsură datele cu caracter personal sunt sau vor fi prelucrate. Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal sunt ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar. Acest principiu se referă în

special la informarea persoanelor vizate privind identitatea operatorului și scopurile prelucrării, precum și la oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care le privesc care sunt prelucrate. Persoanele fizice trebuie informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor cu caracter personal și cu privire la modul în care să își exercite drepturile în legătură cu prelucrarea. În special, scopurile specifice în care datele cu caracter personal sunt prelucrate trebuie să fie explicite și legitime și să fie determinate la momentul colectării datelor respective. Datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar pentru scopurile în care sunt prelucrate. Aceasta necesită, în special, asigurarea faptului că perioada pentru care datele cu caracter personal sunt stocate este limitată strict la minimum. Datele cu caracter personal pot fi prelucrate doar dacă scopul prelucrării nu poate fi îndeplinit în mod rezonabil prin alte mijloace. În vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, urmează să se stabilească de către operator termene pentru ștergere sau revizuirea periodică. Trebuie să fie luate toate măsurile rezonabile pentru a se asigura că datele cu caracter personal care sunt inexacte sunt rectificate sau șterse. Datele cu caracter personal urmează a fi prelucrate într-un mod care să asigure în mod adecvat securitatea și confidențialitatea acestora, inclusiv în scopul prevenirii accesului neautorizat la acestea sau utilizarea neautorizată a datelor cu caracter personal și a echipamentului utilizat pentru prelucrare.

Pentru ca prelucrarea datelor cu caracter personal să fie legală, aceasta trebuie efectuată pe baza consimțământului persoanei vizate sau în temeiul unui alt motiv legitim, prevăzut de legislație, fie în prezenta lege, fie în alt act normativ, inclusiv necesitatea respectării obligațiilor legale la care este supus operatorul sau necesitatea de a executa un contract la care persoana vizată este parte sau pentru a parcurge etapele premergătoare încheierii unui contract, la solicitarea persoanei vizate.

În cazul în care prelucrarea se bazează pe consimțământul persoanei vizate, operatorul trebuie să fie în măsură să demonstreze faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare. În special, în contextul unei declarații scrise cu privire la un alt aspect, garanțiile trebuie să asigure că persoana vizată este conștientă de faptul că și-a dat consimțământul și în ce măsură a făcut acest lucru. În conformitate cu prevederile privind clauzele abuzive în contractele încheiate cu consumatorii, urmează a fi furnizată o declarație de consimțământ formulată în prealabil de către operator, într-o formă inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu, iar această

declarație nu trebuie să conțină clauze abuzive. Pentru ca acordarea consimțământului să fie în cunoștință de cauză, persoana vizată trebuie să fie la curent cel puțin cu identitatea operatorului și cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimțământul nu poate fi considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată.

Pentru a garanta faptul că a fost acordat în mod liber, consimțământul nu poate să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată și operator, în special în cazul în care operatorul este o autoritate publică, iar acest lucru face improbabilă acordarea consimțământului în mod liber în toate circumstanțele aferente respectivei situații particulare. Consimțământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimțământul separat pentru diferitele operațiuni de prelucrare a datelor cu caracter personal, deși acest lucru este adecvat în cazul particular, sau dacă executarea unui contract, inclusiv furnizarea unui serviciu, este condiționată de consimțământ, în ciuda faptului că consimțământul în cauză nu este necesar pentru executarea contractului.

Prelucrarea este considerată legală în cazul în care este necesară în cadrul unui contract sau în vederea încheierii unui contract.

În cazul în care prelucrarea este efectuată în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini efectuate în interes public sau în exercitarea unei autorități oficiale cu care este investit operatorul, prelucrarea trebuie să aibă un temei în legislație.

Prelucrarea datelor cu caracter personal este, de asemenea, considerată legală în cazul în care este necesară în scopul asigurării protecției unui interes esențial pentru viața persoanei vizate sau pentru viața unei alte persoane fizice. Prelucrarea datelor cu caracter personal care are drept temei interesele vitale ale unei alte persoane fizice trebuie efectuată numai în cazul în care prelucrarea nu se poate baza în mod evident pe un alt temei juridic. Unele tipuri de prelucrare pot servi atât unor motive importante de interes public, cât și intereselor vitale ale persoanei vizate, de exemplu în cazul în care prelucrarea este necesară în scopuri umanitare, inclusiv în vederea monitorizării unei epidemii și a răspândirii acesteia sau în situații de urgențe umanitare, în special în situații de dezastre naturale sau provocate de om.

Interesele legitime ale unui operator, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terțe părți, pot constitui

un temei juridic pentru prelucrare, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate, luând în considerare așteptările rezonabile ale persoanelor vizate bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. În orice caz, existența unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul și în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele și drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanțe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară. Întrucât legiuitorul trebuie să furnizeze temeiul juridic pentru prelucrarea datelor cu caracter personal de către autoritățile publice, temeiul juridic respectiv nu se aplică prelucrării de către autoritățile publice în îndeplinirea sarcinilor care le revin. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză. Prelucrarea de date cu caracter personal care are drept scop marketingul direct poate fi considerată ca fiind desfășurată pentru un interes legitim.

Operatorii care fac parte dintr-un grup de întreprinderi sau instituții afiliate unui organism central pot avea un interes legitim de a transmite date cu caracter personal în cadrul grupului de întreprinderi în scopuri administrative interne, inclusiv în scopul prelucrării datelor cu caracter personal ale clienților sau angajaților. Principiile generale ale transferului de date cu caracter personal, în cadrul unui grup de întreprinderi, către o întreprindere situată într-o țară terță rămân neschimbate.

Prelucrarea datelor cu caracter personal în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor, și anume capacitatea unei rețele sau a unui sistem de informații de a face față, la un anumit nivel de încredere, evenimentelor accidentale sau acțiunilor ilegale sau rău intenționate care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor cu caracter personal stocate sau transmise, precum și securitatea serviciilor conexe oferite de aceste rețele și sisteme, sau accesibile prin intermediul acestora, de către autoritățile publice, echipele de intervenție în caz de urgență informatică, echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de rețele și servicii de comunicații electronice, precum și de către furnizorii de servicii și tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză. Acesta ar

putea include, de exemplu, prevenirea accesului neautorizat la rețelele de comunicații electronice și a difuzării de coduri dăunătoare și oprirea atacurilor de „blocare a serviciului”, precum și prevenirea daunelor aduse calculatoarelor și sistemelor de comunicații electronice.

Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele cu caracter personal au fost inițial colectate sunt permise doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele cu caracter personal au fost inițial colectate. În acest caz nu este necesar un temei juridic separat de cel pe baza căruia a fost permisă colectarea datelor cu caracter personal. În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, actele normative pot stabili și specifica sarcinile și scopurile pentru care prelucrarea ulterioară poate fi considerată compatibilă și legală. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice urmează a fi considerate ca reprezentând operațiuni de prelucrare legale compatibile. Temeiul juridic prevăzut în actele normative pentru prelucrarea datelor cu caracter personal poate constitui, de asemenea, un temei juridic pentru prelucrarea ulterioară. Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate inițial datele cu caracter personal, operatorul, după ce a îndeplinit toate cerințele privind legalitatea prelucrării inițiale, trebuie să țină seama, printre altele, de orice legătură între respectivele scopuri și scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de așteptările rezonabile ale persoanelor vizate, bazate pe relația lor cu operatorul, în ceea ce privește utilizarea ulterioară a datelor, de natura datelor cu caracter personal, de consecințele prelucrării ulterioare preconizate asupra persoanelor vizate, precum și de existența garanțiilor corespunzătoare atât în cadrul operațiunilor de prelucrare inițiale, cât și în cadrul operațiunilor de prelucrare ulterioare preconizate.

În cazul în care persoana vizată și-a dat consimțământul sau prelucrarea se bazează pe actele normative, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja, în special, obiective importante de interes public general, operatorul are posibilitatea de a prelucra în continuare datele cu caracter personal, indiferent de compatibilitatea scopurilor. În orice caz, aplicarea principiilor stabilite de prezenta lege și, în special, informarea persoanei vizate cu privire la aceste alte scopuri și la drepturile sale, inclusiv dreptul la opoziție, trebuie să fie garantate. Indicarea unor posibile infracțiuni sau amenințări la adresa siguranței publice de către operator și transmiterea către o

autoritate competentă a datelor cu caracter personal relevante în cazuri individuale sau în mai multe cazuri legate de aceeași infracțiune sau de aceleași amenințări la adresa siguranței publice este considerată ca fiind în interesul legitim urmărit de operator. Cu toate acestea, o astfel de transmitere în interesul legitim al operatorului sau prelucrarea ulterioară a datelor cu caracter personal este interzisă în cazul în care prelucrarea nu este compatibilă cu o obligație legală, profesională sau cu o altă obligație de păstrare a confidențialității.

Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale necesită o protecție specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor și libertăților fundamentale. Aceste date cu caracter personal includ datele cu caracter personal care dezvăluie originea rasială sau etnică. Prelucrarea fotografiilor nu este considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidența definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice. Asemenea date cu caracter personal nu pot fi prelucrate, cu excepția cazului în care prelucrarea este permisă în cazuri specifice prevăzute de prezenta lege, ținând seama de faptul că actele normative pot prevedea dispoziții specifice cu privire la protecția datelor în scopul adaptării aplicării normelor din prezenta lege în vederea respectării unei obligații legale sau a îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul. Pe lângă cerințele specifice pentru o astfel de prelucrare, se aplică principiile generale și alte norme prevăzute de prezenta lege, în special în ceea ce privește condițiile pentru prelucrarea legală. Sunt permise derogări de la interdicția generală de prelucrare a acestor categorii speciale de date cu caracter personal, printre altele atunci când persoana vizată își dă consimțământul explicit sau în ceea ce privește nevoile specifice în special atunci când prelucrarea este efectuată în cadrul unor activități legitime de către anumite asociații sau fundații al căror scop este de a permite exercitarea libertăților fundamentale.

Derogarea de la interdicția privind prelucrarea categoriilor speciale de date cu caracter personal este permisă, de asemenea, în cazul în care actele normative prevăd acest lucru și fac obiectul unor garanții adecvate, astfel încât să fie protejate datele cu caracter personal și alte drepturi fundamentale, atunci când acest lucru se justifică din motive de interes public, în special în cazul prelucrării datelor cu caracter personal în domeniul legislației privind ocuparea forței de muncă, protecția socială, inclusiv pensiile, precum și în scopuri de securitate, supraveghere și alertă în materie de sănătate, pentru prevenirea sau controlul

bolilor transmisibile și a altor amenințări grave la adresa sănătății. Această derogare poate fi incidentă în scopuri medicale, inclusiv sănătatea publică și gestionarea serviciilor de asistență medicală, în special în vederea asigurării calității și eficienței din punctul de vedere al costurilor ale procedurilor utilizate pentru soluționarea cererilor de prestații și servicii în cadrul sistemului de asigurări de sănătate, sau în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. De asemenea, prelucrarea unor asemenea date cu caracter personal este permisă, printr-o derogare, atunci când este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiție, indiferent dacă are loc în cadrul unei proceduri în fața unei instanțe sau în cadrul unei proceduri administrative sau a unei proceduri extrajudiciare.

Categoriile speciale de date cu caracter personal care necesită un nivel mai ridicat de protecție pot fi prelucrate doar în scopuri legate de sănătate atunci când este necesar pentru realizarea acestor scopuri în beneficiul persoanelor fizice și al societății în general, în special în contextul gestionării serviciilor și sistemelor de sănătate sau de asistență socială, inclusiv prelucrarea acestor date de către autoritățile de management și de către autoritățile centrale naționale din domeniul sănătății în scopul controlului calității, furnizării de informații de gestiune și al supravegherii generale a sistemului de sănătate sau de asistență socială la nivel național și local, precum și în contextul asigurării continuității asistenței medicale sau sociale și a asistenței medicale transfrontaliere ori în scopuri de securitate, supraveghere și alertă în materie de sănătate ori în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice în temeiul actelor normative, care trebuie să urmărească un obiectiv de interes public, precum și în cazul studiilor realizate în interes public în domeniul sănătății publice.

Prelucrarea categoriilor speciale de date cu caracter personal poate fi necesară din motive de interes public în domeniile sănătății publice, fără consimțământul persoanei vizate. O astfel de prelucrare este condiționată de măsuri adecvate și specifice destinate să protejeze drepturile și libertățile persoanelor fizice. În acest context, conceptul de „sănătate publică” urmează a fi interpretat astfel cum este definit în *Regulamentul (CE) nr. 1338/2008 al Parlamentului European și al Consiliului*, și anume toate elementele referitoare la sănătate, precum starea de sănătate, inclusiv morbiditatea sau handicapul, factorii determinanți care au efect asupra stării de sănătate, necesitățile în domeniul asistenței medicale, resursele alocate asistenței medicale, furnizarea asistenței medicale și asigurarea accesului universal la aceasta, precum și cheltuielile și sursele de finanțare în domeniul sănătății și cauzele mortalității. Prelucrarea datelor privind sănătatea din motive de interes public nu trebuie să

ducă la prelucrarea acestor date în alte scopuri de către părți terțe, cum ar fi angajatorii sau societățile de asigurări și băncile.

În plus, prelucrarea datelor cu caracter personal de către autoritățile publice în vederea realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public, ale asociațiilor religioase recunoscute oficial se efectuează din motive de interes public.

În cazul în care, în cadrul activităților electorale, funcționarea sistemului democratic necesită ca partidele politice să colecteze date cu caracter personal privind opiniile politice ale persoanelor, prelucrarea unor astfel de date poate fi permisă din motive de interes public, cu condiția să se prevadă garanțiile corespunzătoare.

Dacă datele cu caracter personal prelucrate de un operator nu îi permit acestuia să identifice o persoană fizică, operatorul de date nu are obligația de a obține informații suplimentare în vederea identificării persoanei vizate, cu unicul scop de a respecta oricare dintre dispozițiile prezentei legi. Cu toate acestea, operatorul nu poate să refuze să preia informațiile suplimentare furnizate de persoana vizată cu scopul de a sprijini exercitarea drepturilor acesteia. Identificarea include identificarea digitală a unei persoane vizate, de exemplu prin mecanisme de autentificare precum aceleași acreditări utilizate de către persoana vizată pentru a accesa serviciile online oferite de operatorul de date.

CAPITOLUL III – DREPTURILE PERSOANEI VIZATE

Principiul transparenței prevede că orice informații care se adresează publicului sau persoanei vizate să fie concise, ușor accesibile și ușor de înțeles și să se utilizeze un limbaj simplu și clar, precum și vizualizare acolo unde este cazul. Aceste informații ar putea fi furnizate în format electronic, de exemplu atunci când sunt adresate publicului, prin intermediul unei pagini web. Acest lucru este important în special în situații în care datorită multitudinii subiecților și a complexității, din punct de vedere tehnologic, a practicii, este dificil ca persoana vizată să știe și să înțeleagă dacă datele cu caracter personal care o privesc sunt colectate, de către cine și în ce scop, cum este cazul publicității online. Întrucât copiii necesită o protecție specifică, orice informații și orice comunicare, în cazul în care prelucrarea vizează un copil, trebuie să fie exprimată într-un limbaj simplu și clar, astfel încât copilul să îl poată înțelege cu ușurință.

Urmează a fi instituite modalități de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite prin prezenta lege, inclusiv mecanismele prin care aceasta poate solicita și, dacă este cazul, obține, în mod gratuit, în special, acces la datele cu caracter personal, precum și rectificarea sau

ștergerea acestora, și exercitarea dreptului la opoziție. Operatorul ar trebui să ofere, de asemenea, modalități de introducere a cererilor pe cale electronică, mai ales în cazul în care datele cu caracter personal sunt prelucrate prin mijloace electronice. Operatorul este obligat să răspundă cererilor persoanelor vizate fără întârzieri nejustificate și cel târziu în termen de o lună și, în cazul în care nu intenționează să se conformeze respectivele cereri, să motiveze acest refuz.

Conform principiilor prelucrării echitabile și transparente, persoana vizată este informată cu privire la existența unei operațiuni de prelucrare și la scopurile acesteia. Operatorul trebuie să furnizeze persoanei vizate orice informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă, ținând seama de circumstanțele specifice și de contextul în care sunt prelucrate datele cu caracter personal. În plus, persoana vizată trebuie informată cu privire la crearea de profiluri, precum și la consecințele acesteia. Atunci când datele cu caracter personal sunt colectate de la persoana vizată, aceasta trebuie informată, de asemenea, dacă are obligația de a furniza datele cu caracter personal și care sunt consecințele în cazul unui refuz. Aceste informații 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 ar trebui să poată fi citite automat.

Informațiile în legătură cu prelucrarea datelor cu caracter personal referitoare la persoana vizată urmează a fi furnizate acesteia la momentul colectării de la persoana vizată sau, în cazul în care datele cu caracter personal sunt obținute din altă sursă, într-o perioadă rezonabilă, în funcție de circumstanțele cazului. În cazul în care datele cu caracter personal pot fi divulgate în mod legitim unui alt destinatar, persoana vizată trebuie informată atunci când datele cu caracter personal sunt divulgate pentru prima dată destinatarului. În cazul în care operatorul intenționează să prelucreze datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul trebuie să furnizeze persoanei vizate, înainte de această prelucrare ulterioară, informații privind scopul secundar respectiv și alte informații necesare. În cazul în care originea datelor cu caracter personal nu a putut fi comunicată persoanei vizate din cauză că au fost utilizate surse diverse, informațiile generale urmează a fi furnizate.

Cu toate acestea, nu este necesară impunerea obligației de a furniza informații în cazul în care persoana vizată deține deja informațiile, în cazul în care înregistrarea sau divulgarea datelor cu caracter personal este prevăzută în mod expres de lege sau în cazul în care informarea persoanei vizate se dovedește imposibilă sau ar implica eforturi disproporționate. Acesta din urmă ar putea fi

cazul în special atunci când prelucrarea se efectuează în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. În această privință, urmează a fi luate în considerare numărul persoanelor vizate, vechimea datelor și orice garanții adecvate adoptate.

O persoană vizată are dreptul de acces la datele cu caracter personal colectate care o privesc și trebuie să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia. Acest lucru include dreptul persoanelor vizate de a avea acces la datele lor privind sănătatea, de exemplu datele din registrele lor medicale conținând informații precum diagnostice, rezultate ale examinărilor, evaluări ale medicilor curanți și orice tratament sau intervenție efectuată. Prin urmare, orice persoană vizată are dreptul de a cunoaște și de a i se comunica în special scopurile în care sunt prelucrate datele, dacă este posibil perioada pentru care se prelucrează datele cu caracter personal, destinatarii datelor cu caracter personal, logica de prelucrare automată a datelor cu caracter personal și, cel puțin în cazul în care se bazează pe crearea de profiluri, consecințele unei astfel de prelucrări. Dacă acest lucru este posibil, operatorul de date ar trebui să poată furniza acces de la distanță la un sistem sigur, care să ofere persoanei vizate acces direct la datele sale cu caracter personal. Acest drept nu trebuie să aducă atingere drepturilor sau libertăților altora, inclusiv secretului comercial sau proprietății intelectuale și, în special, drepturilor de autor care asigură protecția programelor software. Cu toate acestea, considerațiile de mai sus nu pot să aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate. Atunci când operatorul prelucrează un volum mare de informații privind persoana vizată, operatorul poate solicita ca, înainte de a îi fi furnizate informațiile, persoana vizată să precizeze informațiile sau activitățile de prelucrare la care se referă cererea sa.

Operatorul trebuie să ia toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online și al identificărilor online. Un operator nu poate să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale.

O persoană vizată are dreptul la rectificarea datelor cu caracter personal care o privesc și „dreptul de a fi uitată”, în cazul în care păstrarea acestor date încalcă prezenta lege sau alte acte normative. În special, persoanele vizate au dreptul ca datele lor cu caracter personal să fie șterse și să nu mai fie prelucrate, în cazul în care acestea nu mai sunt necesare pentru scopurile în care sunt colectate sau prelucrate, în cazul în care persoanele vizate și-au retras consimțământul pentru prelucrare sau în cazul în care acestea se opun prelucrării

datelor cu caracter personal care le privesc sau în cazul în care prelucrarea datelor cu caracter personal ale acestora nu este conformă cu prezenta lege. Acest drept este relevant în special în cazul în care persoana vizată și-a dat consimțământul când era copil și nu cunoștea pe deplin riscurile pe care le implică prelucrarea, iar ulterior dorește să elimine astfel de date cu caracter personal, în special de pe internet. Persoana vizată are posibilitatea de a-și exercita acest drept în pofida faptului că nu mai este copil. Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală în cazul în care este necesară pentru exercitarea dreptului la libertatea de exprimare și de informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul, din motive de interes public în domeniul sănătății publice, în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice sau pentru constatarea, exercitarea sau apărarea unui drept în instanță.

Pentru a se consolida „*dreptul de a fi uitat*” în mediul online, dreptul de ștergere se extinde astfel încât un operator care a făcut publice date cu caracter personal are obligația de a informa operatorii care prelucrează respectivele date să șteargă orice linkuri către acestea sau orice copii sau reproduceri ale acestora. În acest scop, operatorul în cauză trebuie să ia măsuri rezonabile, ținând seama de tehnologia disponibilă și de mijloacele aflate la dispoziția lui, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal în ceea ce privește cererea persoanei vizate.

Metodele de restricționare a prelucrării de date cu caracter personal ar putea include, printre altele, transferarea temporară a datelor cu caracter personal selectate într-un alt sistem de prelucrare, sau anularea accesului utilizatorilor la datele selectate sau înlăturarea temporară a datelor publicate de pe o pagină web. În ceea ce privește sistemele automatizate de evidență a datelor, restricționarea prelucrării trebuie, în principiu, asigurată prin mijloace tehnice în așa fel încât datele cu caracter personal să nu facă obiectul unor operațiuni de prelucrare ulterioară și să nu mai poată fi schimbate. Faptul că prelucrarea datelor cu caracter personal este restricționată trebuie indicat în mod clar în sistem.

Pentru a spori suplimentar controlul asupra propriilor date, persoana vizată, în cazul în care datele cu caracter personal sunt prelucrate prin mijloace automate, poate primi datele care o privesc și pe care le-a furnizat unui operator, într-un format structurat, utilizat în mod curent, prelucrabil automat și interoperabil și să le poată transmite unui alt operator. Operatorii urmează a fi încurajați să dezvolte formate interoperabile care să permită portabilitatea datelor. Acest drept se aplică în cazul în care persoana vizată a furnizat datele cu caracter personal pe baza

propriului consimțământ sau în cazul în care prelucrarea datelor este necesară pentru executarea unui contract. Acest drept nu se aplică în cazul în care prelucrarea se bazează pe un alt temei juridic decât consimțământul sau contractul. Prin însăși natura sa, acest drept nu poate fi exercitat împotriva operatorilor care prelucrează date cu caracter personal în cadrul exercitării funcțiilor lor publice. Acesta nu se aplică în special în cazul în care prelucrarea de date cu caracter personal este necesară în vederea respectării unei obligații legale căreia îi este supus operatorul sau în cazul îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea unei autorități publice cu care este investit operatorul. Dreptul persoanei vizate de a transmite sau de a primi date cu caracter personal care o privesc nu creează pentru operatori obligația de a adopta sau de a menține sisteme de prelucrare care să fie compatibile din punct de vedere tehnic. În cazul în care, într-un anumit set de date cu caracter personal, sunt implicate mai multe persoane vizate, dreptul de a primi datele cu caracter personal nu aduce atingere drepturilor și libertăților altor persoane vizate, în conformitate cu prezenta lege. De asemenea, acest drept nu aduce atingere dreptului persoanei vizate de a obține ștergerea datelor cu caracter personal și limitărilor dreptului respectiv, astfel cum sunt prevăzute în prezenta lege, și, în special, nu implică ștergerea acelor date cu caracter personal referitoare la persoana vizată care au fost furnizate de către aceasta în vederea executării unui contract, în măsura în care și atât timp cât datele respective sunt necesare pentru executarea contractului. Persoana vizată are dreptul ca datele cu caracter personal să fie transmise direct de la un operator la altul, dacă acest lucru este fezabil din punct de vedere tehnic.

În cazurile în care datele cu caracter personal ar putea fi prelucrate în mod legal deoarece prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este investit operatorul sau pe baza intereselor legitime ale unui operator sau ale unei părți terțe, o persoană vizată are dreptul de a se opune prelucrării oricăror date cu caracter personal care se referă la situația sa particulară. Revine operatorului sarcina de a demonstra că interesele sale legitime și imperioase prevalează asupra intereselor sau a drepturilor și libertăților fundamentale ale persoanei vizate.

În cazul în care datele cu caracter personal sunt prelucrate în scopuri de marketing direct, persoana vizată are dreptul de a se opune unei astfel de prelucrări, inclusiv creării de profiluri în măsura în care aceasta are legătură cu marketingul direct, indiferent dacă prelucrarea în cauză este cea inițială sau una ulterioară, în orice moment și în mod gratuit. Acest drept trebuie adus în mod

explicit în atenția persoanei vizate și prezentat în mod clar și separat de orice alte informații.

Persoana vizată are dreptul de a nu face obiectul unei decizii, care poate include o măsură, care evaluează aspecte personale referitoare la persoana vizată, care se bazează exclusiv pe prelucrarea automată și care produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă, cum ar fi refuzul automat al unei cereri de credit online sau practicile de recrutare pe cale electronică, fără intervenție umană. O astfel de prelucrare include „*crearea de profiluri*”, care constă în orice formă de prelucrare automată a datelor cu caracter personal prin evaluarea aspectelor personale referitoare la o persoană fizică, în special în vederea analizării sau preconizării anumitor aspecte privind randamentul la locul de muncă al persoanei vizate, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, atunci când aceasta produce efecte juridice care privesc persoana vizată sau o afectează în mod similar într-o măsură semnificativă. Cu toate acestea, luarea de decizii pe baza unei astfel de prelucrări, inclusiv crearea de profiluri, ar trebui permisă în cazul în care este autorizată în mod expres de actele normative, inclusiv în scopul monitorizării și prevenirii fraudei și a evaziunii fiscale, desfășurate în conformitate cu reglementările, standardele și recomandările relevante, și în scopul asigurării securității și fiabilității unui serviciu oferit de operator sau în cazul în care este necesară pentru încheierea sau executarea unui contract între persoana vizată și un operator sau în cazul în care persoana vizată și-a dat în mod explicit consimțământul. În orice caz, o astfel de prelucrare trebuie să facă obiectul unor garanții corespunzătoare, care trebuie să includă o informare specifică a persoanei vizate și dreptul acesteia de a obține intervenție umană, de a-și exprima punctul de vedere, de a primi o explicație privind decizia luată în urma unei astfel de evaluări, precum și dreptul de a contesta decizia. O astfel de măsură nu se referă la un copil.

Pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoana vizată, având în vedere circumstanțele specifice și contextul în care sunt prelucrate datele cu caracter personal, operatorul trebuie să utilizeze proceduri matematice sau statistice adecvate pentru crearea de profiluri, să implementeze măsuri tehnice și organizatorice adecvate pentru a asigura în special faptul că factorii care duc la inexactități ale datelor cu caracter personal sunt corecți și că riscul de erori este redus la minimum, precum și să securizeze datele cu caracter personal într-un mod care să țină seama de pericolele potențiale la adresa intereselor și drepturilor persoanei vizate și care să prevină, printre altele, efectele discriminatorii împotriva persoanelor pe motiv de rasă sau origine etnică, opinii

politice, religie sau convingeri, apartenență sindicală, caracteristici genetice, stare de sănătate sau orientare sexuală sau care să ducă la măsuri care să aibă astfel de efecte. Procesul decizional automatizat și crearea de profiluri pe baza unor categorii speciale de date cu caracter personal este permis numai în condiții specifice.

Crearea de profiluri este supusă normelor prezentei legi care reglementează prelucrarea datelor cu caracter personal, precum temeiurile juridice ale prelucrării sau principiile de protecție a datelor.

Actele legislative pot impune restricții în privința unor principii specifice, în privința dreptului de informare, a dreptului de acces la datele cu caracter personal și de rectificare sau ștergere a acestora, în privința dreptului la portabilitatea datelor, a dreptului la opoziție, a deciziilor bazate pe crearea de profiluri, precum și în privința comunicării unei încălcări a securității datelor cu caracter personal persoanei vizate și a anumitor obligații conexe ale operatorilor, în măsura în care acest lucru este necesar și proporțional într-o societate democratică pentru a se garanta siguranța publică, inclusiv protecția vieții oamenilor, în special ca răspuns la dezastre naturale sau provocate de om, prevenirea, investigarea și urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa siguranței publice sau împotriva încălcării eticii în cazul profesiilor reglementate și prevenirea acestora, alte obiective importante de interes public general ale Republicii Moldova, în special un interes economic sau financiar important al Republicii Moldova, menținerea de registre publice din motive de interes public general, prelucrarea ulterioară a datelor cu caracter personal arhivate pentru a transmite informații specifice legate de comportamentul politic în perioada regimurilor fostelor state totalitare, protecția persoanei vizate sau a drepturilor și libertăților unor terți, inclusiv protecția socială, sănătatea publică și scopurile umanitare. Aceste restricții ar trebui să fie conforme cu cerințele prevăzute de *Constituția Republicii Moldova* și de *Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale*.

CAPITOLUL IV – OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Se stabilește responsabilitatea și răspunderea operatorului pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul este obligat să implementeze măsuri adecvate și eficace și să fie în măsură să demonstreze conformitatea activităților de prelucrare cu prezenta lege, inclusiv eficacitatea măsurilor. Aceste măsuri trebuie să țină seama

de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul pentru drepturile și libertățile persoanelor fizice.

Riscul pentru drepturile și libertățile persoanelor fizice, prezentând grade diferite de probabilitate de materializare și de gravitate, poate fi rezultatul unei prelucrări a datelor cu caracter personal care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care: prelucrarea poate conduce la discriminare, furt sau fraudă a identității, pierdere financiară, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt dezavantaj semnificativ de natură economică sau socială; persoanele vizate ar putea fi private de drepturile și libertățile lor sau împiedicate să-și exercite controlul asupra datelor lor cu caracter personal; datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, apartenența sindicală; sunt prelucrate date genetice, date privind sănătatea sau date privind viața sexuală sau privind condamnările penale și infracțiunile sau măsurile de securitate conexe; sunt evaluate aspecte de natură personală, în special analizarea sau previzionarea unor aspecte privind randamentul la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, locația sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale; sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale unor copii; sau prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate.

Probabilitatea de a se materializa și gravitatea riscului pentru drepturile și libertățile persoanei vizate sunt determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal. Riscul urmează a fi apreciat pe baza unei evaluări obiective prin care se stabilește dacă operațiunile de prelucrare a datelor prezintă un risc sau un risc ridicat.

Orientări pentru implementarea unor măsuri adecvate și pentru demonstrarea conformității de către operator sau persoana împuternicită de operator, mai ales în ceea ce privește identificarea riscului legat de prelucrare, evaluarea acestuia din punctul de vedere al originii, naturii, probabilității de a se materializa și al gravității, precum și identificarea bunelor practici pentru atenuarea riscului ar putea fi oferite în special prin coduri de conduită aprobate, certificări aprobate, orientări ale Centrului sau prin indicații furnizate de un responsabil cu protecția datelor. Centrul poate, de asemenea, să emită orientări cu privire la operațiunile de prelucrare care sunt considerate puțin susceptibile de a genera un risc ridicat pentru drepturile și libertățile persoanelor fizice și să

indice măsurile care se pot dovedi suficiente în asemenea cazuri pentru a aborda un astfel de risc.

Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezenta lege. Pentru a fi în măsură să demonstreze conformitatea cu prezenta lege, operatorul trebuie să adopte politici interne și să pună în aplicare măsuri care să respecte în special principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor. Astfel de măsuri ar putea consta, printre altele, în reducerea la minimum a prelucrării datelor cu caracter personal, pseudonimizarea acestor date cât mai curând posibil, transparența în ceea ce privește funcțiile și prelucrarea datelor cu caracter personal, abilitarea persoanei vizate să monitorizeze prelucrarea datelor, abilitarea operatorului să creeze elemente de siguranță și să le îmbunătățească. Atunci când elaborează, proiectează, selectează și utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal pentru a-și îndeplini rolul, producătorii acestor produse și furnizorii acestor servicii și aplicații ar trebui să fie încurajați să aibă în vedere dreptul la protecția datelor la momentul elaborării și proiectării unor astfel de produse, servicii și aplicații și, ținând cont de stadiul actual al dezvoltării, să se asigure că operatorii și persoanele împuternicite de operatori sunt în măsură să își îndeplinească obligațiile referitoare la protecția datelor. Principiul protecției datelor începând cu momentul conceperii și cel al protecției implicite a datelor trebuie să fie luate în considerare și în contextul licitațiilor publice.

Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de operator, inclusiv în ceea ce privește monitorizarea de către Centru și măsurile adoptate de acesta, necesită o atribuire clară a responsabilităților în temeiul prezentei legi, inclusiv în cazul în care un operator stabilește scopurile și mijloacele prelucrării împreună cu alți operatori sau în cazul în care o operațiune de prelucrare este efectuată în numele unui operator.

Atunci când un operator sau o persoană împuternicită de operator care nu este stabilită în Republica Moldova prelucrează date cu caracter personal ale unor persoane vizate care se află pe teritoriul Republicii Moldova, iar activitățile sale de prelucrare au legătură cu 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, sau cu monitorizarea comportamentului unor persoane vizate dacă acesta se manifestă în cadrul Republicii Moldova, operatorul sau persoana împuternicită de operator trebuie să desemneze un reprezentant, cu

excepția cazului în care prelucrarea are caracter ocazional, nu include prelucrarea pe scară largă a unor categorii speciale de date cu caracter personal și nici prelucrarea de date referitoare la condamnări penale și la infracțiuni, și este puțin susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice, având în vedere natura, contextul, domeniul de aplicare și scopurile prelucrării, precum și a cazului în care operatorul este o autoritate publică sau un organism public. Reprezentantul acționează în numele operatorului sau al persoanei împuternicite de operator, putând fi contactat de Centru. Reprezentantul trebuie desemnat în mod explicit, printr-un mandat scris al operatorului sau al persoanei împuternicite de operator, să acționeze în numele acestuia în ceea ce privește obligațiile lor în temeiul prezentei legi. Desemnarea unui astfel de reprezentant nu aduce atingere responsabilității sau răspunderii operatorului sau a persoanei împuternicite de operator în temeiul prezentei legi. Un astfel de reprezentant își îndeplinește sarcinile în conformitate cu mandatul primit de la operator sau de la persoana împuternicită de operator, inclusiv cooperează cu Centrul în ceea ce privește orice acțiune întreprinsă pentru a asigura respectarea prezentei legi. Reprezentantul desemnat trebuie să fie supus unor proceduri de asigurare a respectării legii în cazul încălcării prezentei legi, de către operator sau de către persoana împuternicită de operator.

Pentru a asigura respectarea cerințelor impuse de prezenta lege în ceea ce privește prelucrarea care trebuie efectuată în numele operatorului de către persoana împuternicită de operator, atunci când atribuie activități de prelucrare unei persoane împuternicite de operator, acesta din urmă trebuie să utilizeze numai persoane împuternicite care oferă garanții suficiente, în special în ceea ce privește cunoștințele de specialitate, fiabilitatea și resursele, pentru a implementa măsuri tehnice și organizatorice care îndeplinesc cerințele impuse de prezenta lege, inclusiv pentru securitatea prelucrării. Aderarea de către persoana împuternicită de operator la un cod de conduită aprobat sau la un mecanism de certificare aprobat poate fi utilizată drept element care să demonstreze respectarea obligațiilor de către operator. Efectuarea prelucrării de către o persoană împuternicită de un operator urmează să fie reglementată printr-un contract sau un alt tip de act juridic care creează obligații pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopurile prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate, și trebuie să țină seama de sarcinile și responsabilitățile specifice ale persoanei împuternicite de operator în contextul prelucrării care trebuie efectuată, precum și de riscul pentru drepturile și libertățile persoanei vizate. Operatorul și persoana împuternicită de operator pot alege să utilizeze un contract individual sau clauze contractuale standard care sunt aprobate de Centru. După

finalizarea prelucrării în numele operatorului, persoana împuternicită de operator urmează să returneze sau să șteargă, în funcție de opțiunea operatorului, datele cu caracter personal, cu excepția cazului în care există o cerință de stocare a datelor cu caracter personal în temeiul actelor normative care instituie obligații pentru persoana împuternicită de operator.

În vederea demonstrării conformității cu prezenta lege, operatorul sau persoana împuternicită de operator trebuie să păstreze evidențe ale activităților de prelucrare aflate în responsabilitatea sa. Fiecare operator și fiecare persoană împuternicită de operator are obligația de a coopera cu Centrul și de a pune la dispoziția acestuia, la cerere, aceste evidențe, pentru a putea fi utilizate în scopul monitorizării operațiunilor de prelucrare respective.

În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezenta lege, operatorul sau persoana împuternicită de operator urmează să evalueze riscurile inerente prelucrării și să implementeze măsuri pentru atenuarea acestor riscuri, cum ar fi criptarea. Măsurile respective trebuie să asigure un nivel corespunzător de securitate, inclusiv confidențialitatea, luând în considerare stadiul actual al dezvoltării și costurile implementării în raport cu riscurile și cu natura datelor cu caracter personal a căror protecție trebuie asigurată. La evaluarea riscului pentru securitatea datelor cu caracter personal, se acordă atenție riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, în mod accidental sau ilegal, care pot duce în special la prejudicii fizice, materiale sau morale.

Pentru asigurarea respectării dispozițiilor prezentei legi în cazurile în care operațiunile de prelucrare sunt susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul este responsabil de efectuarea unei evaluări a impactului asupra protecției datelor, care să estimeze, în special, originea, natura, specificitatea și gravitatea acestui risc. Rezultatul evaluării este luat în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă prezenta lege. În cazul în care o evaluare a impactului asupra protecției datelor arată că operațiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile și al costurilor implementării, trebuie să aibă loc o consultare a Centrului înainte de prelucrare.

Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a

pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză. Prin urmare, de îndată ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul trebuie să notifice această încălcare Centrului, fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore după ce a luat la cunoștință de existența acesteia, cu excepția cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta ar trebui să cuprindă motivele întârzierii, iar informațiile pot fi furnizate treptat, fără altă întârziere.

Operatorul ar trebui să comunice persoanei vizate o încălcare a securității datelor cu caracter personal, fără întârzieri nejustificate, atunci când încălcarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanei fizice, pentru a-i permite să ia măsurile de precauție necesare. Comunicarea trebuie să descrie natura încălcării securității datelor cu caracter personal și să cuprindă recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Comunicările către persoanele vizate urmează a fi efectuate în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu Centrul, respectându-se orientările furnizate de acesta sau de alte autorități competente, cum ar fi autoritățile de aplicare a legii. De exemplu, necesitatea de a atenua un risc imediat de producere a unui prejudiciu ar presupune comunicarea cu promptitudine către persoanele vizate, în timp ce necesitatea de a implementa măsuri corespunzătoare împotriva încălcării în continuare a securității datelor cu caracter personal sau împotriva unor încălcări similare ale securității datelor cu caracter personal ar putea justifica un termen mai îndelungat pentru comunicare.

Urmează să se stabilească dacă au fost implementate toate măsurile tehnologice de protecție și organizatorice corespunzătoare în scopul de a se stabili imediat dacă s-a produs o încălcare a securității datelor cu caracter personal și de a se informa cu promptitudine Centrul și persoana vizată. Faptul că notificarea a fost efectuată fără întârziere nejustificată urmează a fi stabilit luându-se în considerare, în special, natura și gravitatea încălcării securității datelor cu caracter personal, precum și consecințele și efectele negative ale acesteia asupra persoanei vizate. Această notificare poate conduce la o intervenție a Centrului, în conformitate cu sarcinile și competențele specificate în prezenta lege.

La stabilirea de norme detaliate privind formatul și procedurile aplicabile notificării referitoare la încălcările securității datelor cu caracter personal, urmează să se acorde atenția cuvenită circumstanțelor în care a avut loc încălcarea, stabilindu-se inclusiv dacă protecția datelor cu caracter personal a fost sau nu a fost asigurată prin măsuri tehnice de protecție corespunzătoare, care să limiteze efectiv probabilitatea fraudării identității sau a altor forme de utilizare abuzivă. În plus, astfel de norme și proceduri trebuie să țină cont de interesele legitime ale autorităților de aplicare a legii în cazurile în care divulgarea timpurie ar putea îngreuna în mod inutil investigarea circumstanțelor în care a avut loc o încălcare a datelor cu caracter personal.

Trebuie instituite proceduri și mecanisme eficace care să pună accentul pe notificarea despre tipurile de operațiuni de prelucrare susceptibile să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice prin însăși natura lor, prin domeniul lor de aplicare, prin contextul și prin scopurile lor. Astfel de tipuri de operațiuni de prelucrare pot fi cele care presupun, în special, utilizarea unor noi tehnologii sau care reprezintă un nou tip de operațiuni, pentru care nicio evaluare a impactului asupra protecției datelor nu a fost efectuată anterior de către operator ori care devin necesare dată fiind perioada de timp care s-a scurs de la prelucrarea inițială.

În astfel de cazuri, operatorul trebuie să efectueze, înainte de prelucrare, o evaluare a impactului asupra protecției datelor, în scopul evaluării gradului specific de probabilitate a materializării riscului ridicat și gravitatea acestuia, având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și sursele riscului. Respectiva evaluare a impactului urmează să includă, în special, măsurile, garanțiile și mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecției datelor cu caracter personal și pentru demonstrarea conformității cu prezenta lege.

Aceasta urmează să se aplice, în special, operațiunilor de prelucrare la scară largă, care au drept obiectiv prelucrarea unui volum considerabil de date cu caracter personal la nivel regional, național sau supranațional, care ar putea afecta un număr mare de persoane vizate și care sunt susceptibile de a genera un risc ridicat, de exemplu, din cauza sensibilității lor, în cazul în care, în conformitate cu nivelul atins al cunoștințelor tehnologice, se folosește la scară largă o tehnologie nouă, precum și altor operațiuni de prelucrare care generează un risc ridicat pentru drepturile și libertățile persoanelor vizate, în special în cazul în care operațiunile respective limitează capacitatea persoanelor vizate de a-și exercita drepturile. Urmează a fi efectuată o evaluare a impactului asupra protecției datelor și în situațiile în care datele cu caracter personal sunt prelucrate în scopul luării de decizii care vizează anumite persoane fizice în urma unei evaluări

sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, pe baza creării de profiluri pentru datele respective, sau în urma prelucrării unor categorii speciale de date cu caracter personal, a unor date biometrice sau a unor date privind condamnările penale și infracțiunile sau măsurile de securitate conexe. Este la fel de necesară o evaluare a impactului asupra protecției datelor pentru monitorizarea la scară largă a zonelor accesibile publicului, mai ales în cazul utilizării dispozitivelor optoelectronice sau pentru orice alte operațiuni în cazul în care Centrul consideră că prelucrarea este susceptibilă de a genera un risc ridicat pentru drepturile și libertățile persoanelor vizate, în special deoarece acestea împiedică persoanele vizate să exercite un drept sau să utilizeze un serviciu ori un contract, sau deoarece acestea sunt efectuate în mod sistematic la scară largă. Prelucrarea datelor cu caracter personal nu este considerată a fi la scară largă în cazul în care prelucrarea se referă la date cu caracter personal de la pacienți sau clienți de către un anumit medic, un alt profesionist în domeniul sănătății sau un avocat. În aceste cazuri, o evaluare a impactului asupra protecției datelor nu este obligatorie.

În unele circumstanțe ar putea fi rezonabil și util din punct de vedere economic ca o evaluare a impactului asupra protecției datelor să aibă o perspectivă mai extinsă decât cea a unui singur proiect, de exemplu în cazul în care autorități sau organisme publice intenționează să instituie o aplicație sau o platformă de prelucrare comună sau în cazul în care mai mulți operatori preconizează să introducă o aplicație comună sau un mediu de prelucrare comun în cadrul unui sector sau segment industrial sau pentru o activitate orizontală utilizată la scară largă.

În cazul în care o evaluare a impactului asupra protecției datelor arată că prelucrarea ar genera, în absența garanțiilor, măsurilor de securitate și mecanismelor de atenuare a riscului, un risc ridicat pentru drepturile și libertățile persoanelor fizice, iar operatorul consideră că riscul nu poate fi atenuat prin mijloace rezonabile sub aspectul tehnologiilor disponibile și al costurilor implementării, Centrul trebuie să fie consultat înainte de începerea activităților de prelucrare. Un astfel de risc ridicat este susceptibil să fie generat de anumite tipuri de prelucrare, precum și de amploarea și frecvența prelucrării, care pot duce și la producerea unor prejudicii sau pot atinge drepturile și libertățile persoanelor fizice. Centrul urmează să răspundă cererii de consultare într-un anumit termen. Cu toate acestea, lipsa unei reacții din partea Centrului în termenul respectiv nu aduce atingere niciunei intervenții a Centrului în conformitate cu sarcinile și competențele sale prevăzute în prezenta lege, inclusiv competența de a interzice operațiuni de prelucrare. Ca parte a acestui proces de consultare, rezultatul unei evaluări a impactului asupra protecției datelor efectuate cu privire la prelucrarea

în cauză poate fi transmis Centrului, în special măsurile avute în vedere pentru a atenua riscul pentru drepturile și libertățile persoanelor fizice.

Persoana împuternicită de operator trebuie să acorde asistență operatorului, dacă este necesar și la cerere, la asigurarea respectării obligațiilor care decurg din realizarea de evaluări ale impactului asupra protecției datelor și din consultarea prealabilă a Centrului.

În timpul elaborării unei măsuri legislative sau de reglementare care prevede prelucrarea unor date cu caracter personal trebuie, de asemenea, să aibă loc o consultare a Centrului, pentru a garanta conformitatea prelucrării avute în vedere cu prezenta lege și, în special, pentru a atenua riscul la care este expusă persoana vizată.

În cazul în care prelucrarea este efectuată de o autoritate publică, cu excepția instanțelor judecătorești atunci când acționează în calitate lor judiciară, în cazul în care, în sectorul privat, prelucrarea este efectuată de un operator a cărui activitate principală constă în operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate pe scară largă, sau în cazul în care activitatea principală a operatorului sau a persoanei împuternicite de operator constă în prelucrarea pe scară largă de categorii speciale de date cu caracter personal și de date privind condamnările penale și infracțiunile, o persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor trebuie să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității, la nivel intern, cu prezenta lege. În sectorul privat, activitățile principale ale unui operator se referă la activitățile sale de bază, și nu la prelucrarea datelor cu caracter personal drept activități auxiliare. Nivelul necesar al cunoștințelor de specialitate urmează să fie stabilit în special în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Acești responsabili cu protecția datelor, indiferent dacă sunt sau nu angajați ai operatorului, trebuie să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent.

Asociațiile sau alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori urmează a fi încurajate să elaboreze coduri de conduită, în limitele prezentei legi, astfel încât să se faciliteze aplicarea efectivă a prezentei legi, luându-se în considerare caracteristicile specifice ale prelucrării efectuate în anumite sectoare și necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii. În special, astfel de coduri de conduită ar putea să ajusteze obligațiile operatorilor și ale persoanelor împuternicite de operatori, ținând seama de riscul aferent prelucrării care este susceptibil de a fi generat pentru drepturile și libertățile persoanelor fizice.

Atunci când elaborează un cod de conduită sau când modifică sau extind un astfel de cod, asociațiile și alte organisme care reprezintă categorii de operatori sau persoane împuternicite de operatori trebuie să consulte părțile implicate relevante, inclusiv persoanele vizate, dacă este fezabil, și să ia în considerare contribuțiile transmise și opiniile exprimate în cadrul unor astfel de consultări.

Pentru a se îmbunătăți transparența și conformitatea cu prezenta lege, se încurajeze instituirea de mecanisme de certificare, precum și de sigilii și mărci în materie de protecție a datelor, care să permită persoanelor vizate să evalueze rapid nivelul de protecție a datelor aferent produselor și serviciilor relevante.

CAPITOLUL V – TRANSFERURILE DE DATE CU CARACTER PERSONAL CĂTRE ALTE STATE SAU CĂTRE ORGANIZAȚII INTERNAȚIONALE

Fluxurile de date cu caracter personal către și dinspre alte state și organizații internaționale sunt necesare pentru dezvoltarea comerțului internațional și a cooperării internaționale. Creșterea acestor fluxuri a generat noi provocări și preocupări cu privire la protecția datelor cu caracter personal. Cu toate acestea, în cazul în care se transferă date cu caracter personal din Republica Moldova către operatori, persoane împuternicite de operatori sau alți destinatari din alte state sau organizații internaționale, nivelul de protecție a persoanelor fizice asigurat în Republica Moldova prin prezenta lege nu poate fi diminuat, inclusiv în cazurile de transferuri ulterioare de date cu caracter personal dinspre alt stat sau organizație internațională către operatori, persoane împuternicite de operatori din aceeași sau dintr-un alt stat sau organizație internațională. În orice caz, transferurile către alte state și organizații internaționale pot fi desfășurate numai în conformitate deplină cu prezenta lege. Un transfer ar putea avea loc numai dacă, sub rezerva respectării celorlalte dispoziții ale prezentei legi, operatorul sau persoana împuternicită de operator îndeplinește condițiile prevăzute de dispozițiile prezentei legi privind transferul de date cu caracter personal către alte state sau către organizații internaționale.

Cu toate acestea, se va reține faptul că condițiile instituite de Capitolul V nu se aplică transferurilor de date cu caracter personal către statele membre ale Spațiului Economic European. În cazul acestor transferuri nu sunt necesare întrunirea unor condiții sau autorizări speciale. Or, la nivelul acestor state este aplicabil direct *RGPD*-ul, fapt ce, *a priori*, asigură un nivel ridicat de protecție a datelor cu caracter personal.

Prezenta lege nu aduce atingere acordurilor internaționale încheiate între Republica Moldova și alte state în vederea reglementării transferului de date cu

caracter personal, inclusiv garanții adecvate pentru persoanele vizate. Republica Moldova poate încheia acorduri internaționale care implică transferul de date cu caracter personal către alte state sau către organizații internaționale, în măsura în care astfel de acorduri nu afectează prezenta lege sau alte acte normative și includ un nivel corespunzător de protecție a drepturilor fundamentale ale persoanelor vizate.

Centrul poate decide că un stat, un teritoriu sau un anumit sector dintr-un alt stat sau o organizație internațională oferă un nivel adecvat de protecție a datelor, asigurând astfel securitate juridică și uniformitate în ceea ce privește statul sau organizația internațională care este considerată a furniza un astfel de nivel de protecție. În aceste cazuri, transferurile de date cu caracter personal către statul sau organizația internațională respectivă pot avea loc fără a fi necesar să se obțină autorizări suplimentare. De asemenea, Centrul poate să decidă, după trimiterea unei notificări și a unei justificări complete statului sau organizației internaționale, să anuleze o astfel de decizie.

În conformitate cu valorile fundamentale pe care se întemeiază Republica Moldova, în special protecția drepturilor omului, Centrul, în evaluarea sa referitoare la statul sau la un teritoriu sau la un sector specificat dintr-un stat, trebuie să ia în considerare modul în care aceasta respectă statul de drept, accesul la justiție, precum și normele și standardele internaționale în materie de drepturi ale omului și legislația sa generală și sectorială, inclusiv legislația privind securitatea publică, apărarea și securitatea națională, precum și ordinea publică și dreptul penal. Adoptarea unei decizii privind caracterul adecvat al nivelului de protecție pentru un teritoriu sau un sector specificat dintr-un alt stat urmează să țină seama de criterii clare și obiective, cum ar fi activitățile specifice de prelucrare și domeniul de aplicare al standardelor legale aplicabile și legislația în vigoare în statul respectiv. Statul trebuie să ofere garanții care să asigure un nivel adecvat de protecție, echivalent în esență cu cel asigurat în cadrul Republicii Moldova, în special atunci când datele cu caracter personal sunt prelucrate în unul sau mai multe sectoare specifice. În special, statul trebuie să asigure o supraveghere efectivă independentă în materie de protecție a datelor și să prevadă mecanisme de cooperare cu Centrul, iar persoanele vizate trebuie să beneficieze de drepturi efective și opozabile și de reparații efective pe cale administrativă și judiciară.

Pe lângă angajamentele internaționale asumate de alt stat sau de organizația internațională, Centrul trebuie să țină seama de obligațiile care decurg din participarea statului sau a organizației internaționale la sistemele multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal, precum și de punerea în aplicare a unor astfel de obligații. În special, urmează să

fie luată în considerare aderarea statului la *Convenția Consiliului European din 28 ianuarie 1981 pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal și protocolul adițional la aceasta.*

Centrul trebuie să monitorizeze funcționarea deciziilor privind nivelul de protecție dintr-un alt stat sau un teritoriu sau un anumit sector dintr-un alt stat sau dintr-o organizație internațională și să monitorizeze funcționarea deciziilor adoptate. În deciziile sale privind caracterul adecvat al nivelului de protecție, Centrul trebuie să prevadă un mecanism de revizuire periodică a modului lor de funcționare. Această revizuire periodică urmează să fie efectuată în consultare cu statul sau organizația internațională în cauză și ar trebui să ia în considerare toate evoluțiile relevante din statul sau organizația internațională.

Centrul poate să recunoască faptul că un stat, un teritoriu sau un sector specificat dintr-un stat sau o organizație internațională nu mai asigură un nivel adecvat de protecție a datelor. În consecință, transferul de date cu caracter personal către statul sau organizația internațională respectivă este interzisă, cu excepția cazului în care sunt îndeplinite cerințele prevăzute în prezenta lege privind transferurile în baza unor garanții adecvate, inclusiv regulile corporatiste obligatorii și derogările de la situațiile specifice. Centrul trebuie, în timp util, să informeze statul sau organizația internațională cu privire la motivele acestei decizii și să inițieze consultări cu aceasta pentru remedierea situației.

În absența unei decizii privind caracterul adecvat al nivelului de protecție, operatorul sau persoana împuternicită de operator urmează să adopte măsuri pentru a compensa lipsa protecției datelor dintr-un stat prin intermediul unor garanții adecvate pentru persoana vizată. Astfel de garanții adecvate pot consta în utilizarea regulilor corporatiste obligatorii, a clauzelor standard de protecție a datelor aprobate de Comisia Europeană sau Centru, ori a clauzelor contractuale autorizate Centru. Respectivul garanții trebuie să asigure respectarea cerințelor în materie de protecție a datelor și drepturi ale persoanelor vizate corespunzătoare prelucrării în Republica Moldova, inclusiv disponibilitatea unor drepturi opozabile ale persoanelor vizate și a unor căi de atac eficiente, printre care dreptul de acces la reparații efective pe cale administrativă sau judiciară și dreptul de a solicita despăgubiri, în Republica Moldova sau într-un alt stat. Acestea ar trebui să se refere în special la respectarea principiilor generale privind prelucrarea datelor cu caracter personal: principiul protecției datelor începând cu momentul conceperii și principiul protecției implicite a datelor. Transferurile pot fi efectuate și de către autoritățile sau organismele publice cu autorități sau organisme publice din alte state sau cu organizații internaționale cu atribuții și funcții corespunzătoare, inclusiv pe baza dispozițiilor care prevăd drepturi opozabile și efective pentru persoanele vizate, care trebuie introduse în acordurile

administrative, cum ar fi un memorandum de înțelegere. Autorizația din partea Centrului ar trebui obținută atunci când garanțiile sunt oferite în cadrul unor acorduri administrative fără caracter juridic obligatoriu.

Posibilitatea ca operatorul sau persoana împuternicită de operator să utilizeze clauze standard în materie de protecție a datelor, aprobate de Comisia Europeană sau de Centru, nu ar trebui să împiedice operatorii sau persoanele împuternicite de aceștia să includă clauzele standard în materie de protecție a datelor într-un contract mai amplu, precum un contract între persoana împuternicită de operator și o altă persoană împuternicită de operator, și nici să adauge alte clauze sau garanții suplimentare, atât timp cât acestea nu contravin, direct sau indirect, clauzelor contractuale standard aprobate de Comisia Europeană sau de Centru sau nu prejudiciază drepturile sau libertățile fundamentale ale persoanelor vizate. Operatorii și persoanele împuternicite de operatori sunt încurajați să ofere garanții suplimentare prin intermediul unor angajamente contractuale care să completeze clauzele standard în materie de protecție.

Un grup de întreprinderi sau un grup de întreprinderi implicat într-o activitate economică comună pot utiliza regulile corporatiste obligatorii aprobate pentru transferurile sale internaționale dinspre Republica Moldova către organizații din cadrul aceluiași grup de întreprinderi sau grup de întreprinderi implicate într-o activitate economică comună, cu condiția ca astfel de reguli corporatiste să includă toate principiile esențiale și drepturile opozabile în scopul asigurării unor garanții adecvate pentru transferurile sau categoriile de transferuri de date cu caracter personal.

Există posibilitatea de a se efectua transferuri în anumite circumstanțe în care persoana vizată și-a dat consimțământul explicit, în care transferul este ocazional și necesar în legătură cu un contract sau cu o acțiune în justiție, indiferent dacă este în contextul unei proceduri judiciare sau în contextul unei proceduri administrative sau extrajudiciare, inclusiv în cadrul procedurilor înaintate organismelor de reglementare. De asemenea, există posibilitatea de a se efectua transferuri în cazul în care motive importante de interes public stabilite în actele normative impun acest lucru sau în cazul în care transferul se efectuează dintr-un registru instituit prin lege și destinat să fie consultat de către public sau de către persoane care au un interes legitim. În acest ultim caz, un astfel de transfer nu trebuie să implice totalitatea datelor cu caracter personal sau ansamblul categoriilor de date conținute în registru, iar atunci când registrul este destinat să fie consultat de persoane care au un interes legitim, transferul poate fi efectuat doar la cererea persoanelor respective sau dacă acestea sunt destinatarii,

luând pe deplin în considerare interesele și drepturile fundamentale ale persoanei vizate.

Aceste derogări se aplică, în special, transferurilor de date solicitate și necesare din considerente importante de interes public, de exemplu în cazul schimbului internațional de date între autoritățile din domeniul concurenței, administrațiile fiscale sau vamale, între autoritățile de supraveghere financiară, între serviciile competente în materie de securitate socială sau de sănătate publică, de exemplu în cazul depistării punctelor de contact pentru bolile contagioase sau pentru reducerea și/sau eliminarea dopajului în sport. Un transfer de date cu caracter personal este, de asemenea, considerat legal în cazul în care este necesar în scopul protejării unui interes care este esențial în interesele vitale ale persoanei vizate sau ale unei alte persoane, inclusiv pentru integritatea fizică sau pentru viața acesteia, în cazul în care persona vizată nu are capacitatea să își dea consimțământul. În absența unei decizii privind caracterul adecvat al nivelului de protecție, actele normative pot, din considerente importante de interes public, stabili în mod expres limite asupra transferului unor categorii specifice de date către un alt stat sau către o organizație internațională. Orice transfer către o organizație umanitară internațională al datelor cu caracter personal ale unei persoane vizate care se află în incapacitate fizică sau juridică de a își da consimțământul, în vederea îndeplinirii unei sarcini care decurge din Convențiile de la Geneva sau în vederea conformării cu dreptul internațional umanitar aplicabil în conflictele armate, ar putea fi considerat necesar pentru un motiv important de interes public sau pentru că este în interesul vital al persoanei vizate.

Transferurile care pot fi considerate ca nefiind repetitive și care se referă doar la un număr limitat de persoane vizate, ar putea, de asemenea, să fie efectuate în scopul realizării intereselor legitime urmărite de operator, atunci când asupra respectivelor interese nu prevalează interesele sau drepturile și libertățile persoanei vizate și atunci când operatorul a evaluat toate circumstanțele aferente transferului de date. Operatorul trebuie să acorde o atenție deosebită naturii datelor cu caracter personal, scopului și duratei operațiunii sau operațiunilor propuse de prelucrare, precum și situației din țara de origine, din țara terță și din țara de destinație finală și trebuie să ofere garanții adecvate pentru protecția drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal. Astfel de transferuri sunt posibile numai în cazurile reziduale în care nu se poate aplica niciunul dintre celelalte motive de transfer. În ceea ce privește scopurile de cercetare științifică sau istorică sau scopurile statistice, urmează să se ia în considerare așteptările legitime ale societății cu privire la creșterea nivelului de cunoștințe. Operatorul trebuie să informeze Centrul și persoana vizată cu privire la transfer.

În orice caz, atunci când Centrul nu a luat o decizie cu privire la nivelul adecvat de protecție a datelor dintr-un alt stat, operatorul sau persoana împuternicită de operator trebuie să utilizeze soluții care să ofere persoanelor vizate drepturi opozabile și efective în ceea ce privește prelucrarea datelor lor în Republica Moldova odată ce aceste date au fost transferate, astfel încât persoanele vizate să beneficieze în continuare de drepturi fundamentale și garanții.

Unele state au adoptat legi, reglementări și alte acte juridice care au drept obiectiv să reglementeze în mod direct activitățile de prelucrare a datelor ale persoanelor fizice și juridice aflate sub jurisdicția Republicii Moldova. Aceasta poate include hotărâri ale instanțelor judecătorești sau decizii ale autorităților administrative din alte state care solicită unui operator sau unei persoane împuternicite de operator să transfere sau să divulge date cu caracter personal și care nu se bazează pe un acord internațional, cum ar fi un tratat de asistență juridică reciprocă, în vigoare între statul solicitant și Republica Moldova. Aplicarea extraterritorială a acestor legi, reglementări și alte acte juridice poate încălca dreptul internațional și poate împiedica asigurarea protecției persoanelor fizice asigurată în Republica Moldova prin prezenta lege. Transferurile sunt permise numai în cazul îndeplinirii condițiilor prevăzute de prezenta lege pentru un transfer către alte state. Acesta ar putea fi cazul, *inter alia*, atunci când divulgarea este necesară dintr-un motiv important de interes public recunoscut în actele normative.

Fluxul transfrontalier de date cu caracter personal în afara Republicii Moldova poate expune unui risc sporit capacitatea persoanelor fizice de a-și exercita drepturile în materie de protecție a datelor, în special pentru a-și asigura protecția împotriva utilizării sau a divulgării ilegale a acestor informații. În același timp, Centrul poate constata că se află în imposibilitatea de a examina plângeri sau de a efectua investigații referitoare la activitățile desfășurate în afara frontierelor Republicii Moldova. Eforturile acestuia de a conlucra în context transfrontalier pot fi, de asemenea, îngreunate de insuficiența competențelor de prevenire sau remediere, de caracterul eterogen al regimurilor juridice și de existența unor obstacole de ordin practic, cum ar fi constrângerile în materie de resurse. Prin urmare, este necesar să se promoveze o cooperare mai strânsă între autoritățile de supraveghere a protecției datelor pentru a putea face schimb de informații și a desfășura investigații împreună cu omologii internaționali. În scopul elaborării de mecanisme de cooperare internațională pentru a facilita și a oferi asistență internațională reciprocă în asigurarea aplicării legislației din domeniul protecției datelor cu caracter personal, Centrul urmează să facă schimb de informații și să coopereze în cadrul activităților legate de exercitarea

competențelor sale cu autoritățile competente din alte state, pe bază de reciprocitate și în conformitate cu prezenta lege.

CAPITOLUL VI – CAZURILE SPECIFICE DE PRELUCRARE A DATELOR CU CARACTER PERSONAL

Capitolul VI conține reglementări specifice pentru anumite cazuri de prelucrare a datelor cu caracter personal, pornind de la particularitățile deosebite ale anumitor relații sociale.

Astfel, acest capitol conține norme juridice speciale cu privire la următoarele situații de prelucrare a datelor cu caracter personal:

- 1) libertatea de exprimare;
- 2) accesul la informațiile de interes public;
- 3) prelucrarea unui număr de identificare național;
- 4) prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice.

1) Prelucrarea și libertatea de exprimare

În conformitate cu art. 51 alin. (1), pentru prelucrarea efectuată în scopuri jurnalistice sau în scopul exprimării academice, artistice sau literare, prezenta lege nu se aplică în cazul în care sunt întrunite următoarele condiții cumulative:

- a) operatorul prelucrează date cu caracter personal cu intenția de a publica un material jurnalistic, academic, artistic sau literar;
- b) publicarea materialului ar fi de interes public;
- c) aplicarea prevederilor din prezenta lege este incompatibilă cu realizarea scopurilor jurnalistice sau a scopului de exprimare academică, artistică sau literară.

Această prevedere are drept scop reconcilierea a două drepturi fundamentale: dreptul la protecția datelor cu caracter personal, pe de o parte, și dreptul la libertatea de exprimare, pe de altă parte. Or, obligația respectării prevederilor prezentei legi ar putea constitui un impediment nejustificat pentru diseminarea unor informații, opinii sau idei de interes public.

Astfel, art. 51 alin. (1) prevede inaplicabilitatea prezentei legi, și exonerarea de la obligația respectării prevederilor acesteia, pentru prelucrarea realizată în scopuri jurnalistice (sau în scopul exprimării academice, artistice sau literare), însă numai în cazul în care sunt întrunite trei condiții cumulative, prevăzute la lit. a)-c). Aceste condiții derivă nemijlocit din jurisprudența Curții

de Justiție a Uniunii Europene, precum și din legislația statelor membre ale Uniunii Europene care au transpus în legile de implementare a *RGPD*-ului raționamentele expuse în jurisprudența Curții (în special Regatul Unit).

Se va reține faptul că, precum reiese din jurisprudența constantă a Curții de Justiție a Uniunii Europene, noțiunea de „*scopuri jurnalistice*” se referă la activitățile care au ca scop aducerea la cunoștința publicului a unor informații, opinii sau idei, indiferent de mijlocul de transmitere a acestora.¹

Astfel, această noțiune urmează a fi interpretată în sens larg și nu se limitează doar la jurnaliști sau organizațiile mass-media. Această noțiune este aplicabilă oricărei persoane care prelucrează date cu caracter personal cu scopul de a aduce la cunoștința publicului a unor informații, opinii sau idei.

Cu titlu de exemplu, Curtea de Justiție a Uniunii Europene a reținut că înregistrarea video a unor agenți de poliție, de către o persoană, în incinta unei secții de poliție, în timpul unei audieri, și publicarea materialului video astfel înregistrat pe un site internet de materiale video pe care utilizatorii le pot trimite, viziona și distribui (în speță, platforma YouTube), pot constitui o prelucrare de date cu caracter personal „*în scopuri jurnalistice*”, atât timp cât reiese din acest material video că înregistrarea și publicarea menționate au ca unic scop aducerea la cunoștința publicului a unor informații, opinii sau idei.²

Cu toate acestea, precum reiese din conținutul art. 51 alin. (1), pentru ca prezenta lege să nu fie aplicabilă unei prelucrări de date cu caracter personal în scopuri jurnalistice (sau în scopul exprimării academice, artistice sau literare), este imperativă întrunirea a trei condiții cumulative:

a) operatorul prelucrează date cu caracter personal cu intenția de a publica un material jurnalistic, academic, artistic sau literar;

Pentru ca această condiție să fie întrunită, nu este relevant dacă materialul jurnalistic (*i.e.*, materialul care are drept scop aducerea la cunoștința publicului a unor informații, opinii sau idei), sau materialul academic, artistic sau literar, a fost finalmente publicat sau diseminat public. Or, acest aspect ține de discreția editorială a operatorului. Însă, este imperativ să existe intenția operatorului de a publica (*i.e.*, de a aduce la cunoștința publicului) un astfel de material. În caz contrar, prelucrarea datelor nu va fi considerată realizată „*în scopuri jurnalistice*” sau „*în scopul exprimării academice, artistice sau literare*”.

¹ Hotărârea Curții de Justiție a Uniunii Europene din 14 februarie 2019, Cauza C-345/17, *Buivids*, § 53;

² *Ibidem*, § 69.

b) publicarea materialului ar fi de interes public;

Această condiție este esențială pentru aprecierea faptului dacă prevederile prezentei legi nu sunt aplicabile în cazul unei anumite prelucrări de date cu caracter personal realizată în scopurile expuse *supra*. Această condiție derivă, atât din jurisprudența Curții de Justiție a Uniunii Europene, cât și, în special, din jurisprudența constantă a Curții Europene a Drepturilor Omului.

Astfel, publicarea, sau eventuala publicare, a unui material jurnalistic (sau a unui material academic, artistic ori literar) trebuie să fie de „*interes public*”.

În vederea stabilirii faptului dacă publicarea materialului ar fi de „*interes public*” se va ține cont de raționamentele expuse detaliat în Hotărârea Curții Europene a Drepturilor Omului din 12 iunie 2014 în cauza *Couderc și Hachette Filipacchi Associés împotriva Franței (40454/07)*, paragrafele 97-103.

În această hotărâre, Curtea a subliniat că definirea a ceea ce poate constitui un subiect de interes public va depinde de circumstanțele fiecărui caz. Interesul public se referă la chestiuni care afectează publicul într-o asemenea măsură, încât acesta să manifeste un interes în mod legitim, care îi atrage atenția sau care îl privește într-o măsură semnificativă, în special pentru că afectează bunăstarea cetățenilor sau viața comunității. Acesta este și cazul chestiunilor apte să dea naștere unor controverse considerabile, care privesc o problemă socială importantă sau care implică o problemă cu privire la care publicul ar avea un interes să fie informat. Interesul public nu poate fi redus la setea publicului de informații despre viața privată a altora sau la dorința atingerii unei audiențe bazate pe senzații tari sau chiar pe indecență. Pentru a se stabili dacă publicarea se referă la un subiect de o importanță generală, este necesar să se evalueze publicarea ca întreg, având în vedere contextul în care apare.

c) aplicarea prevederilor din prezenta lege este incompatibilă cu realizarea scopurilor jurnalistice sau a scopului de exprimare academică, artistică sau literară.

Pentru aprecierea existenței unei incompatibilități dintre aplicarea prevederilor prezentei legi, pe de o parte, și realizarea scopurilor jurnalistice (sau a scopului de exprimare academică, artistică sau literară), pe de altă parte, se va ține cont de prevederile specifice din

prezenta lege, precum și de scopul concret pe care îl urmărește operatorul.

În multe cazuri, aplicabilitatea acestei condiții ar fi evidentă, deoarece ar fi imposibil de respectat deplin prevederile prezentei și, în același timp, de a atinge un scop jurnalistic.

Cu titlu de exemplu, nu ar fi posibilă respectarea principiului prelucrării datelor cu caracter personal în mod transparent și efectuarea, în același timp, a unor activități de supraveghere sau investigații journalistice.

În calitate de regulă generală, această condiție este incidentă odată ce respectarea prevederilor prezentei ar prejudicia disproporțional realizarea unui scop jurnalistic sau a scopului de exprimare academică, artistică sau literară.

În fine, este imperativ să accentuăm că art. 51 nu este incident în contextul accesului la informațiile de interes public (*i.e.* accesul persoanelor la informațiile deținute de autoritățile publice). Or, autoritățile publice, sau alți furnizori de informații în sensul *Legii nr. 148/2023 privind accesul la informațiile de interes public*, nu prelucrează date cu caracter personal în scopuri journalistice sau în vederea publicării unui material jurnalistic (precum este prevăzut la art. 51 alin. (1) lit. a)). Prin urmare, aceste entități nu pot aplica prevederile art. 51.

Mai important, se va reține că aspectele legate de accesul la informațiile de interes public sunt reglementate exclusiv prin prisma art. 52 din prezenta lege.

2) Prelucrarea și accesul la informațiile de interes public

În conformitate cu art. 52, datele cu caracter personal deținute de furnizorii de informații pot fi dezvăluite în condițiile *Legii nr. 148/2023 privind accesul la informațiile de interes public*, cu excepția categoriilor speciale de date cu caracter personal.

Astfel, această prevedere asigură compatibilitatea prezentei legi cu prevederile *Legii nr. 148/2023 privind accesul la informațiile de interes public*, în special, în contextul aplicării criteriului proporționalității limitării reglementat la art. 9 din această lege.

Este important de precizat că art. 52 și, implicit, prevederile *Legii nr. 148/2023 privind accesul la informațiile de interes public*, se aplică în mod egal tuturor solicitanților de informații, fără nicio diferențiere după careva criterii. Or, reglementările internaționale interzic instituirea unor regimuri juridice preferențiale de acces la informație, *i.e.* care să fie aplicabile doar în raport cu anumite categorii de subiecți (cum ar fi jurnaliștii sau instituțiile mass-media).

În acest sens, *Raportul explicativ al Convenției Consiliului Europei privind accesul la documentele oficiale*, prevede următoarele:

„Convenția oferă „oricărei persoane” dreptul de a avea acces la documentele oficiale, indiferent de motivele și intențiile lor. Deși prevederile Convenției sunt de o deosebită importanță pentru jurnaliști, deoarece le oferă instrumentele necesare pentru a-și exercita rolul de „câine de pază” în privința bunei funcționări a instituțiilor publice – un rol crucial într-o societate democratică, care a fost recunoscut deplin de către jurisprudența Curții Europene a Drepturilor Omului – Convenția nu face nicio distincție între aceștia și alți indivizi.”.

[...]

Paragraful 3 prevede că solicitările accesului la documente oficiale trebuie să fie tratate în mod egal. În calitate de regulă, solicitările trebuie soluționate în ordinea primirii. Nici o distincție în această privință nu trebuie făcută pe baza naturii solicitării sau a statutului solicitantului.”³

3) Prelucrarea unui număr de identificare național

Se va reține că definiția noțiunii de „*număr de identificare național*” este oferită la art. 4 din prezenta lege. Astfel, prin număr de identificare național se înțelege numărul prin care se identifică o persoană fizică în anumite sisteme de evidență și care are aplicabilitate generală, cum ar fi: numărul de identificare de stat, seria și numărul buletinului de identitate, numărul pașaportului, al permisului de conducere.

Prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conțin, se poate efectua în situațiile prevăzute la art. 6 alin. (1).

Cu toate acestea, prelucrarea unui număr de identificare național, inclusiv prin colectarea sau dezvăluirea documentelor ce îl conțin, în scopul prevăzut la art. 6 alin. (1) lit. f) (realizarea intereselor legitime urmărite de operator sau de o parte terță), se efectuează cu instituirea de către operator a următoarelor garanții:

- a) punerea în aplicare a măsurilor tehnice și organizatorice adecvate pentru respectarea, în special, a principiului reducerii la minimum a datelor, precum și pentru asigurarea securității și confidențialității prelucrărilor de date cu caracter personal, în conformitate cu art. 32;
- b) stabilirea termenelor de stocare în funcție de natura datelor și scopul prelucrării, precum și a termenelor specifice în care datele cu caracter personal trebuie șterse sau revizuite în vederea ștergerii;

³ *Raportul explicativ al Convenției Consiliului Europei privind accesul la documentele oficiale*, §§ 17 și 48; <https://rm.coe.int/16800d3836>

- c) instruirea periodică cu privire la obligațiile ce le revin persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, prelucrează date cu caracter personal.

4) Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice

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. Respectivul garanții asigură faptul că au fost instituite măsuri tehnice și organizatorice necesare pentru a se asigura, în special, respectarea principiului reducerii la minimum a datelor. Respectivul măsuri pot include pseudonimizarea, cu condiția ca respectivul scopuri să fie îndeplinite în acest mod. Atunci când respectivul 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.

Art. 15, 16, 18 și 21 nu se aplică în cazul în care datele cu caracter personal sunt prelucrate în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva condițiilor și a garanțiilor expuse *supra*, în măsura în care drepturile prevăzute la aceste articole sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

Art. 15, 16 și 18-21 nu se aplică în cazul în care datele cu caracter personal sunt prelucrate în scopuri de arhivare în interes public, sub rezerva condițiilor și a garanțiilor expuse *supra*, în măsura în care drepturile prevăzute la aceste articole sunt de natură să facă imposibilă sau să afecteze în mod grav realizarea scopurilor specifice, iar derogările respective sunt necesare pentru îndeplinirea acestor scopuri.

CAPITOLUL VII – CENTRUL NAȚIONAL PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL

Capitolul VII conține prevederile instituționale ale noii legi, care reglementează instituirea, organizarea și funcționarea autorității naționale de supraveghere a Republicii Moldova – Centrul Național pentru Protecția Datelor cu Caracter Personal.

Acest capitol reglementează structurat următoarele aspecte instituționale:

- a) statutul și structura Centrului;
- b) misiunea, sarcinile și competențele Centrului;
- c) statutul și atribuțiile conducerii Centrului;

d) componența și atribuțiile persoanelor din aparatul Centrului;

Centrul asigură supravegherea și monitorizarea aplicării prezentei legi și a altor acte normative privind prelucrarea datelor cu caracter personal, în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în legătură cu prelucrarea datelor cu caracter personal.

Cu toate acestea, Centrul nu este competent să supravegheze operațiunile de prelucrare efectuate de instanțele judecătorești în activitatea de înlăptuire a justiției.

Se va reține faptul că, în conformitate cu art. 57 alin. (2) din proiectul de lege, structura și efectivul-limită ale Centrului urmează a fi stabilite prin hotărâre a Parlamentului, la propunerea Centrului.

CAPITOLUL VIII – REMEDIILE LEGALE, RĂSPUNDEREA ȘI SANCTIUNILE

Capitolul VIII conține normele juridice procedurale ale noii legi, care reglementează, în special:

- a) modalitatea depunerii plângerilor la Centru;
- b) procedura de examinare a plângerilor de către Centru (inclusiv examinarea preliminară și investigarea);
- c) aplicarea sancțiunilor pecuniare sub formă de amendă pentru încălcările prezentei legi.

Orice persoană vizată are dreptul de a depune o plângere la Centru, în cazul în care aceasta consideră că drepturile sale în temeiul prezentei legi sunt încălcate.

Adițional, persoana vizată are dreptul de a mandata un organism, o organizație sau o asociație fără scop lucrativ, ale cărei obiective statutare sunt în interesul public și care își desfășoară activitatea în domeniul asigurării protecției datelor cu caracter personal, să depună o plângere în numele său la Centru, să exercite dreptul la o cale de atac în numele persoanelor vizate sau, în cazul în care este prevăzut în actele normative, să exercite dreptul de a primi despăgubiri în numele persoanelor vizate.

Operatorul sau persoana împuternicită de operator urmează să plătească despăgubiri pentru orice prejudiciu pe care o persoană îl poate suferi ca urmare a unei prelucrări care încalcă prezenta lege. Operatorul sau persoana împuternicită de operator trebuie să fie exonerată de răspundere dacă dovedesc că nu sunt în niciun fel răspunzători pentru prejudiciu. Conceptul de prejudiciu urmează a fi interpretat în sens larg, din perspectiva jurisprudenței Curții Europene a

Drepturilor Omului, într-un mod care să reflecte pe deplin obiectivele prezentei legi. Această dispoziție nu aduce atingere niciunei cereri de despăgubire care rezultă din încălcarea altor acte normative. O prelucrare care încalcă prezenta lege include și prelucrarea care încalcă actele delegate și de punere în aplicare adoptate în conformitate cu prezenta lege. Persoanele vizate trebuie să primească despăgubiri integrale și eficiente pentru prejudiciul pe care le-au suferit. În cazul în care operatorii sau persoanele împuternicite de operatori sunt implicate în aceeași prelucrare, fiecare operator sau fiecare persoană împuternicită de operator este considerată răspunzătoare pentru întregul prejudiciu. Cu toate acestea, atunci când procedurile juridice care le vizează sunt conexate, în conformitate cu actele normative, despăgubirile pot fi împărțite în funcție de răspunderea fiecărui operator sau a fiecărei persoane împuternicite de operator, cu condiția să se asigure despăgubirea integrală și efectivă a persoanei vizate care a suferit prejudiciul. Orice operator sau persoană împuternicită de operator care a plătit despăgubiri integrale poate formula ulterior o acțiune în regres împotriva altor operatori sau persoane împuternicite de operatori implicate în aceeași prelucrare.

Pentru a consolida respectarea aplicării normelor prevăzute în prezenta lege, art. 86-88 instituite sancțiuni pecuniare aplicate de Centru pentru încălcările săvârșite de către operatori.

Se va reține că în cazul unei încălcări minore sau în cazul în care amenda susceptibilă de a fi impusă ar constitui o sarcină disproporționată pentru o persoană fizică, poate fi emis un avertisment în locul unei amenzi. Cu toate acestea, urmează să se ia în considerare în mod corespunzător natura, gravitatea și durata încălcării, caracterul deliberat al încălcării, acțiunile întreprinse pentru a reduce prejudiciul cauzat, gradul de răspundere sau orice încălcări anterioare relevante, modul în care încălcarea a fost adusă la cunoștința Centrului, conformitatea cu măsurile adoptate împotriva operatorului sau a persoanei împuternicite de operator, aderarea la un cod de conduită și orice alt factor agravant sau atenuant.

În cazul în care se impun amenzi unor persoane care nu sunt întreprinderi, Centrul trebuie să țină seama de nivelul general al veniturilor din Republica Moldova, precum și de situația economică a persoanei atunci când estimează cuantumul adecvat al amenzii.

CAPITOLUL IX – DISPOZIȚII FINALE ȘI TRANZITORII

Prezenta lege urmează să intre în vigoare la expirarea a 24 de luni de la data publicării legii în Monitorul Oficial al Republicii Moldova.

Până la intrarea în vigoare a prezentei legi, Guvernul și Centrul urmează să elaboreze și înainteze proiectele de acte normative care sunt necesare pentru implementarea efectivă a legii.

Adițional, art. 90 reglementează aspectele tranzitorii, care cuprind măsurile ce se instituie cu privire la continuarea raporturilor juridice născute în temeiul vechilor reglementări ce urmează a fi abrogate.

5. Fundamentarea economico-financiară

Implementarea prezentului proiect de lege nu necesită cheltuieli financiare suplimentare din bugetul de stat.

6. Modul de încorporare a actului în cadrul normativ în vigoare

Guvernul, până la intrarea în vigoare a prezentei legi, va prezenta Parlamentului propuneri pentru aducerea legislației în concordanță cu prezenta lege, precum și va aduce actele sale normative în concordanță cu prezenta lege.

În aceeași perioadă, Centrul va propune Parlamentului structura și efectivul său limită, precum și va aproba actele normative necesare implementării prezentei legi.

7. Avizarea și consultarea publică a proiectului

În conformitate cu prevederile *Legii nr. 239/2008 privind transparența în procesul decizional*, proiectul de lege a fost plasat pentru consultări publice pe pagina web oficială a Ministerului Justiției (www.justice.gov.md), în compartimentul *Transparență decizională*, directoriul *Registrul proiectelor de acte normative*. Adițional, proiectul a fost plasat și pe platforma www.particip.gov.md.

În privința proiectului au fost organizate două runde de avizare și consultare publică cu subiecții interesați.

În cadrul primei avizări și consultări publice au prezentat avize următorii participanți: Centrul Național pentru Protecția Datelor cu Caracter Personal, Centrul de Armonizare a Legislației, Ministerul Afacerilor Interne, Ministerul Finanțelor, Ministerul Afacerilor Externe și Integrării Europene, Agenția de Guvernare Electronică, Agenția Servicii Publice, Banca Națională a Moldovei, Comisia Națională a Pieței Financiare, Consiliul Concurenței, Serviciul Prevenirea și Combaterea Spălării Banilor, Serviciul de Informații și Securitate, Procuratura Generală, Autoritatea Națională de Integritate, Consiliul Superior al Magistraturii, Agenția de Administrare a Instanțelor Judecătorești, Curtea Supremă de Justiție, Curtea de Apel Chișinău, Curtea de Apel Bălți, Curtea de

Apel Cahul, Curtea de Apel Comrat, Asociația Patronală „Camera de Comerț Americană din Moldova”, Asociația Națională a Companiilor din Domeniul TIC, Asociația Investitorilor Străini, Asociația Băncilor din Moldova.

În cadrul avizării și consultării publice repetate au prezentat avize/expertize următorii participanți: Centrul de Armonizare a Legislației, Consiliul Superior al Magistraturii, Consiliul Concurenței, Comisia Națională a Pieței Financiare, Serviciul Prevenirea și Combaterea Spălării Banilor, Autoritatea Națională de Integritate, Curtea de Apel Chișinău, Centrul Național pentru Protecția Datelor cu Caracter Personal, Serviciul de Informații și Securitate, Asociația Patronală „Camera de Comerț Americană din Moldova”, Asociația Națională a Companiilor din Domeniul TIC, Asociația Investitorilor Străini, Ministerul Dezvoltării Economice și Digitalizării, Ministerul Afacerilor Interne, Ministerul Finanțelor, Agenția Servicii Publice, Agenția de Guvernare Electronică, Procuratura Generală, Banca Națională a Moldovei, Centrul Național Anticorupție, Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător.

Toate obiecțiile, propunerile și recomandările înaintate au fost incluse în tabelele de sinteză, anexate la prezentul proiect.

8. Constatările expertizei anticorupție

În privința proiectului a fost realizată expertiza anticorupție nr. ELO24/9366 din 3 ianuarie 2024.

În expertiză s-a constatat faptul că proiectul corespunde interesului public general, deoarece va contribui la realizarea angajamentelor asumate de către Republica Moldova în raport cu Uniunea Europeană, prin prisma asigurării unui nivel adecvat de protecție a datelor cu caracter personal.

Adițional, în expertiză au fost formulate câteva obiecții și recomandări, care au fost examinate și incluse în tabelul de sinteză, anexat la prezentul proiect.

9. Constatările expertizei de compatibilitate cu legislația Uniunii Europene

În Declarația de compatibilitate a Centrului de Armonizare a Legislației nr. 31/02-69-12574 din 30 noiembrie 2023 s-a constatat transpunerea totală a prevederilor obligatorii ale *Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE.*

10. Constatările altor expertize

În privința prezentului proiect de lege a fost realizată expertiza grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător, care a susținut proiectul cu condiția luării în considerare a obiecțiilor și recomandărilor.

Obiecțiile și recomandările din expertiză au fost examinate și incluse în tabelul de sinteză, anexat la prezentul proiect.

Ministru

Veronica MIHAILOV-MORARU

Digitally signed by Mihailov-Moraru Veronica
Date: 2024.05.08 09:08:30 EEST
Reason: MoldSign Signature
Location: Moldova

