Parlamentul
Republicii Moldova

SS nr. 86
21.11.2018

Deputat în Parlamentul
Republicii Moldova

Biroul Permanent al Parlamentului

În conformitate cu prevederile art. 73 din Constituţia Republicii Moldova şi ale art. 47 din Regulamentul Parlamentului, se înaintează, cu titlu de iniţiativă legislativă, proiectul de lege privind protecţia datelor cu caracter personal.

Anexe:

1. Proiectul de lege
2. Nota informativă
3. Avize ale autorităţilor

22 11 422 18

Deputat în Parlament:

Republica Moldova, MD-2073, Chişinău
Bd. Ştefan cel Mare şi Sfînt 105

info@parlament.md
www.parlament.md

„UE"
Proiect

L E G E
privind protecţia datelor cu caracter personal

Parlamentul adoptă prezenta lege organică.

În scopul asigurării respectării dreptului fundamental al omului la inviolabilitatea vieţii intime, familiale şi private, consacrat la art. 28 din Constituţia Republicii Moldova;

Conştientizând obligaţiile asumate de Republica Moldova prin aderarea la Convenţia nr. 108 pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal şi Protocolul adiţional la Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, cu privire la autorităţile de supraveghere şi fluxul transfrontalier al datelor;

Prezenta Lege transpune Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor) şi Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, publicate în Jurnalul Oficial al UE nr. L 119 din 4 mai 2016.

Capitolul I
DISPOZIŢII GENERALE

Articolul 1. Scopul legii

Scopul prezentei legi este asigurarea dreptului la protecţia datelor cu caracter personal, ce derivă, inclusiv din dreptul constituţional la inviolabilitatea vieţii intime, familiale şi private.

Articolul 2. Domeniul material de aplicare

(1) Prezenta lege se aplică prelucrării datelor cu caracter personal, efectuată total sau parţial prin mijloace automatizate, precum şi prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidenţă a datelor sau care sunt destinate să facă parte dintr-un sistem de evidenţă a datelor.

(2) Domeniul de acţiune al prezentei legi se extinde asupra:

a) prelucrării datelor cu caracter personal efectuate pe teritoriul Republicii Moldova, inclusiv informaţiilor care consemnează date cu caracter personal atribuite la secret de stat, secret profesional, secret bancar, secret medical, secret comercial, secret fiscal şi altor informaţii cu accesibilitate limitată sau operaţiunilor administrative desfăşurate în legătură cu gestionarea dosarului civil, contravenţional sau penal, precum şi mijloacelor utilizate în acest sens;

b) prelucrării datelor cu caracter personal efectuate în cadrul misiunilor diplomatice şi oficiilor consulare ale Republicii Moldova, precum şi de către alţi operatori aflaţi în afara teritoriului ţării, dar pe teritorii în care se aplică dreptul intern al Republicii Moldova, în temeiul dreptului internaţional public;

c) prelucrării datelor cu caracter personal efectuate asupra subiecţilor de date personale aflaţi în Republica Moldova de către operatorii stabiliţi în afara teritoriului Republicii Moldova, atunci când activităţile de prelucrare sunt legate de oferirea de bunuri sau servicii unor astfel de subiecţi de date personale în Republica Moldova, indiferent dacă se solicită sau nu efectuarea unei plăţi de către subiectul de date personale sau sunt legate de monitorizarea comportamentului lor dacă acest comportament se manifestă în cadrul Republicii Moldova.

Cerinţele acestor dispoziţii nu se aplică cazului în care prelucrarea este efectuată în scopul tranzitului pe teritoriul Republicii Moldova a datelor cu caracter personal;

d) prelucrării datelor cu caracter personal de către operatori - organe de ocrotire a legii, care au competenţe stabilite prin lege în scopul prevenirii, investigării, depistării şi/sau urmăririi penale a infracţiunilor sau executării pedepselor penale, detenţia preventivă, inclusiv protejarea şi prevenirea ameninţărilor la adresa ordinii publice, securităţii naţionale şi a statului şi în cadrul dosarului penal sau acţiunilor speciale de investigaţie;

e) prelucrării datelor cu caracter personal ce vizează persoanele decedate, cu excepţia prelucrării categoriilor de date precum: nume, prenume, data luna şi anul naşterii sau decesului, precum şi în cazul realizării drepturilor succesorale.

(3) Domeniul de acţiune al prezentei legi nu se extinde asupra:

a) prelucrării datelor cu caracter personal efectuate de către persoane fizice exclusiv pentru nevoi personale, familiale sau domestice. Nevoile personale, familiale sau domestice nu sunt activităţi profesionale sau comerciale;

b) prelucrării datelor cu caracter personal în cadrul activităţii informative (spionaj) şi contrainformative (contraspionaj), agentura şi sursa de informaţii, în condiţiile legii;

c) datelor cu caracter personal care sunt anonimizate;

d) operaţiunilor de prelucrare şi transmitere transfrontalieră a datelor cu caracter personal ce se referă la făptuitorii sau victimele crimelor de genocid, ale crimelor de război şi ale crimelor împotriva umanităţii.

Articolul 3. Noţiuni principale

Termenii şi expresiile utilizate în prezenta lege au următoarele semnificaţii:

date cu caracter personal (în continuare *date personale*) - înseamnă orice informaţie ce identifică sau duce la identificarea subiectului de date cu caracter personal. Datele personale pot fi de două categorii: obişnuite şi speciale.

categoria obişnuită de date personale - înseamnă, dar nu se limitează la: nume, prenume, patronimic, numărul de identificare de stat, adresa, numărul de telefon, numărul de înmatriculare a automobilului, date de localizare, vocea, un identificator online sau la unul sau mai mulţi factori specifici identităţii fizice, fiziologice, economice, culturale sau sociale ale persoanei fizice;

categoria specială de date personale - reprezintă datele care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenenţa la un sindicat şi prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viaţa sexuală sau orientarea sexuală ale unei persoane fizice, precum şi cele referitoare la condamnările penale şi infracţiuni, măsurile procesuale de constrângere sau sancţiunile contravenţionale;

date genetice - reprezintă datele personale referitoare la caracteristicile genetice moştenite sau dobândite ale unei persoane fizice, care oferă informaţii unice privind fiziologia sau sănătatea persoanei respective şi care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;

date biometrice - reprezintă datele personale 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 - reprezintă datele personale legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistenţă medicală, care dezvăluie informaţii despre starea de sănătate a acesteia;

subiect de date personale (în continuare *subiect de date*) - înseamnă persoana fizică identificată sau identificabilă. Persoana decedată nu poate fi subiect de date;

prelucrarea datelor personale – înseamnă orice operaţiune sau set de operaţiuni 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 dispoziţie în orice alt mod, alinierea sau combinarea, restricţionarea, ştergerea sau distrugerea;

prelucrarea transfrontalieră a datelor personale - înseamnă prelucrarea datelor personale cu element de extraneitate la care participă o persoană fizică sau juridică de drept public sau privat aflată în alt stat;

creare de profiluri - înseamnă orice formă de prelucrare automatizată a datelor personale care constă în utilizarea datelor personale 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;

operator – înseamnă persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție, organizație sau persoane autorizate, care singur sau împreună cu altele stabilesc scopurile și/sau mijloacele de prelucrare a datelor personale, prelucrează sau intenționează să prelucreze aceste date;

operator asociat - înseamnă doi sau mai mulți operatori care stabilesc în comun scopurile și/sau mijloacele de prelucrare a datelor personale;

persoana împuternicită de operator - înseamnă persoana fizică sau juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție, organizație sau persoană autorizată, care prelucrează datele personale în numele operatorului. De regulă, persoana împuternicită este o persoană juridică sau fizică, alta decât operatorul;

sistem de evidență - înseamnă orice serie structurată de date personale automatizată, manuală sub formă de cartotecă sau mixtă și accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice. În calitate de sistem de evidență a datelor personale se constituie inclusiv, dar nu se limitează la registrele, dosarele, bazele de date, sistemele informaționale și informatice în care sunt stocate și prelucrate automatizat sau manual sub formă de cartotecă sau mixtă date personale prelucrate pentru un anumit scop;

destinatar – înseamnă persoana fizică sau persoană juridică, autoritatea publică, orice altă instituție, organizație sau persoane autorizate sau alt organism căreia (căruia) îi sunt divulgate, datele personale, indiferent dacă este sau nu terț. În cadrul operațiunilor de prelucrare a acestor date, destinatarul respectă prevederile legislației privind protecția datelor personale ce țin de limitarea scopului și asigurarea regimului de confidențialitate și securitate. Autoritățile publice cărora li se pot comunica, date personale în cadrul unei anumite investigații în conformitate cu prevederile legislației, inclusiv instanțele de judecată la înfăptuirea justiției și organele de ocrotire a legii în scopurile stabilite la art. 2 alin. (2) lit. d) nu sunt considerate destinatari; prelucrarea acelor date de către acele autorități publice se va face în baza normelor aplicabile privind protecția datelor personale, conform scopului prelucrării;

terț - înseamnă o persoană fizică sau juridică, de drept public sau privat, autoritate publică, instituție, agenție, alta decât subiectul de date, operatorul,

persoana împuternicită de operator şi persoanele care, sub directa autoritate a operatorului sau a persoanei împuternicite de operator, sunt autorizate să prelucreze date personale;

consimţământul subiectului de date personale – înseamnă orice manifestare de voinţă liberă, specifică, informată şi lipsită de ambiguitate a subiectului de date personale prin care acesta acceptă, printr-o declaraţie sau printr-o acţiune fără echivoc, ca datele personale care îl privesc să fie prelucrate;

încălcarea securităţii datelor personale - înseamnă o încălcare a securităţii care duce, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor personale transmise, stocate sau prelucrate într-un alt mod, sau la accesul neautorizat la acestea;

marketing direct sau prospectare comercială – înseamnă metode de cercetare a pieţii, de distribuţie a produselor şi serviciilor în care sunt utilizate concepte, tehnici şi instrumente de marketing, inclusiv prin intermediul poştei, serviciilor de comunicaţii electronice sau al altor servicii de expediere, concretizate într-un demers orientat direct către subiectul de date personale, urmărind generarea unei reacţii cuantificabile a acestuia;

pseudonimizare - înseamnă prelucrarea datelor personale într-un asemenea mod încât acestea să nu mai poată fi atribuite unui subiect de date fără a se utiliza informaţii suplimentare, cu condiţia ca aceste informaţii suplimentare să fie stocate separat şi să facă obiectul unor măsuri de natură tehnică şi organizatorică care să asigure neatribuirea respectivelor date personale unei persoane fizice identificate sau identificabile;

anonimizarea – înseamnă modificarea datelor personale în aşa fel încât să nu poată fi identificată sau să ducă la identificarea subiectului de date, astfel încât detaliile privind circumstanţele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile. Datele anonimizate nu reprezintă date personale;

organ de ocrotire a legii – înseamnă în sensul prezentei legi:

- autoritate publică sau o subdiviziune a unei astfel de autorităţi, competentă pentru prevenirea, investigarea, depistarea infracţiunilor, în scopul punerii în aplicare a procedurilor penale, urmăririi penale a infracţiunilor sau executării pedepselor penale, inclusiv protejarea şi prevenirea ameninţărilor la adresa ordinii publice, cum ar fi, dar nu se limitează la: poliţia, organele procuraturii, organele vamale, instituţiile penitenciare, organele pentru prevenirea şi combaterea corupţiei, spălării banilor, finanţării terorismului, recuperării bunurilor infracţionale, organele de probaţiune, organele securităţii statului;

- autoritate publică sau o subdiviziune a unei astfel de autorităţi care acţionează în domeniul securităţii naţionale sau securităţii de stat, care efectuează măsuri speciale de investigaţii;

persoanele juridice de drept public - înseamnă în sensul prezentei legi, dar nu se limitează la: Parlamentul Republicii Moldova, Aparatul Preşedintelui Republicii Moldova, Guvernul Republicii Moldova, ministerele, celelalte

organe de specialitate ale administraţiei publice centrale şi locale de nivelul I şi II, autorităţile şi instituţiile publice autonome, autorităţile administraţiei publice şi instituţiile publice din subordinea acestora, întreprinderile de stat şi alte instituţii similare, instituţii de învăţământ, instituţiile din domeniul sănătăţii, culturii etc;

persoanele juridice de drept privat - înseamnă în sensul prezentei legi persoanele juridice care sunt constituite în scop lucrativ (comercial) şi scop nelucrativ (necomercial);

reprezentant - înseamnă persoană fizică sau juridică stabilită în Republica Moldova, sau într-un stat membru al Uniunii Europene care va fi responsabil pentru Republica Moldova, desemnată în scris de către operator sau persoana împuternicită de operator în conformitate cu art. 32, care reprezintă operatorul sau persoana împuternicită de operator, în ceea ce priveşte obligaţiile care le revin în temeiul prezentei legi;

organizaţie internaţională - înseamnă o organizaţie şi organismele sale subordonate reglementate de dreptul internaţional public sau orice alt organism care este instituit printr-un acord încheiat între două sau mai multe ţări sau în temeiul unui astfel de acord;

întreprindere - înseamnă o persoană fizică sau juridică ce desfăşoară o activitate economică, indiferent de forma juridică a acesteia, inclusiv parteneriate sau asociaţii care desfăşoară în mod regulat o activitate economică;

grup de întreprinderi - înseamnă o întreprindere care exercită controlul şi întreprinderile controlate de aceasta;

reguli corporatiste obligatorii - înseamnă politicile în materie de protecţie a datelor personale care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită în Republica Moldova, în ceea ce priveşte transferurile sau seturile de transferuri de date personale către un operator sau o persoană împuternicită de operator în una sau mai multe ţări în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună;

servicii ale societăţii informaţionale - înseamnă orice serviciu prestat la distanţă, prin mijloace electronice şi la solicitarea individuală a beneficiarului serviciului.

Capitolul II
CONDIŢIILE DE BAZĂ PENTRU PRELUCRAREA DATELOR PERSONALE

Articolul 4. Principiile aferente prelucrării datelor personale

(1) Datele personale se prelucrează cu respectarea următoarelor principii:

a) legalităţii, echităţii şi transparenţei - datele personale urmează a fi prelucrate în mod legal, echitabil şi transparent faţă de subiectul de date.

Cerința de transparență nu se aplică prelucrării efectuate de autoritățile de ocrotire a legii în contextul activităților prevăzute la art. 2 alin. (2) lit. (d);

b) limitării legate de scop - datele personale urmează a fi 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. 14, 15, 16 ale prezentei legi;

c) minimizării datelor - datele personale urmează a fi adecvate, relevante și limitate la ceea ce este necesar în legătură cu realizarea obiectivelor pentru care sunt prelucrate;

d) exactității - datele personale urmează a fi exacte și, dacă este necesar, actualizate. Trebuie să se ia toate măsurile necesare pentru a se asigura că datele personale care sunt inexacte, urmează a fi șterse, distruse sau rectificate fără întârziere având în vedere scopurile pentru care sunt prelucrate;

e) limitării legate de stocare - datele personale urmează a fi păstrate într-o formă care permite identificarea subiectului de date pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele. Datele personale 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 art. 14, 15, 16 ale prezentei legi, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în prezenta lege în vederea garantării drepturilor și libertăților subiectului datelor;

f) integrității și confidențialității - datele personale urmează a fi prelucrate într-un mod care asigură securitatea adecvată a acestora, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale sau ilicite, prin luarea de măsuri tehnice sau organizatorice corespunzătoare;

(2) Datele personale urmează a fi marcate atunci când sunt transmise către alți operatori, terți sau destinatari. Modalitatea și forma de marcare se aprobă de Centru.

(3) Operatorul este responsabil de asigurarea conformării cu alin. (1) și poate demonstra această respectare. Datele personale urmează a fi prelucrate sub răspunderea operatorului, care asigură și demonstrează conformitatea fiecărei operațiuni de prelucrare cu dispozițiile prezentei legi.

Articolul 5. Legalitatea prelucrării

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

a) subiectul de date și-a dat consimțământul pentru prelucrarea datelor sale personale pentru unul sau mai multe scopuri specifice;

b) prelucrarea este necesară pentru executarea unui contract la care subiectul de date este parte sau pentru a face demersuri la cererea subiectului de date înainte de încheierea unui contract.

c) prelucrarea este necesară în vederea îndeplinirii unei obligaţii legale care îi revine operatorului;

d) prelucrarea este necesară pentru protejarea vieţii, integrităţii fizice sau a sănătăţii persoanei vizate sau ale altei persoane fizice;

e) prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea competenţelor autorităţii publice cu care este învestit operatorul;

f) prelucrarea este necesară în scopul realizării intereselor legitime urmărite de operator sau de o parte terţă, cu excepţia cazului în care prevalează interesele sau drepturile şi libertăţile fundamentale ale subiectului de date, care necesită protejarea datelor personale, în special atunci cînd subiectul de date este un copil. Lit. f) nu se aplică în cazul prelucrării efectuate de autorităţi publice în îndeplinirea atribuţiilor lor.

(2) În cazul în care prelucrarea în alt scop decât cel pentru care datele personale au fost colectate nu se bazează pe consimţământul subiectului de date sau pe un temei legal, care constituie o măsură necesară şi proporţională într-o societate democratică pentru a proteja obiectivele menţionate la articolul 28 alineatul (1), operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele personale au fost colectate iniţial, trebuie sa ţină cont de următoarele:

a) orice legătură dintre scopurile în care datele personale au fost colectate şi scopurile prelucrării ulterioare preconizate;

b) contextul în care datele personale au fost colectate, în special în ceea ce priveşte relaţia dintre subiectul de date şi operator;

c) natura datelor personale, în special în cazul prelucrării unor categorii speciale de date personale;

d) posibilele consecinţe pentru subiecţii de date în urma prelucrării ulterioare preconizate;

e) existenţa unor garanţii adecvate, care pot include criptarea sau pseudonimizarea.

(3) Cerinţele statuate de prezentul articol sunt obligatorii atât pentru cel ce deţine datele personale cât şi pentru cel care intenţionează să intre în posesia acestor date, fiind necesar a fi justificat scopul, temeiul legal şi legătura de cauzalitate dintre categoriile de date personale şi cauza/sesizarea/cererea/adresarea, interesul legitim.

(4) Prelucrarea datelor personale se efectuează în conformitate cu prevederile prezentei legi. Pentru refuzul de a efectua prelucrarea ilegală a datelor personale nu poate surveni răspundere disciplinară, civilă, contravenţională sau penală.

Articolul 6. Autoritatea de supraveghere

(1) Centrul Naţional pentru Protecţia Datelor cu Caracter Personal (în continuare - Centrul) este autoritatea publică de asigurare a dreptului la protecţia datelor personale, inclusiv ce derivă din dreptul constituţional la inviolabilitatea vieţii intime, familiale şi private şi este autoritatea învestită cu

dreptul inalienabil de a efectua supravegherea, prevenirea cazurilor de încălcare a prezentei legi (prin informare, instruire, reglementare şi alte acţiuni ce nu vin în contradicţie cu legea), de a efectua investigaţia respectării principiilor de protecţie a datelor personale prevăzute de legislaţia în vigoare etc.

(2) Activitatea Centrului este reglementată de Legea privind Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, prezenta lege şi alte acte normative care vin să pună în aplicare legile date.

(3) Centrul în activitatea sa, se poate baza pe documentele emise de instituţiile Uniunii Europene în domeniul protecţiei datelor personale şi sferei de securitate a datelor personale în cazul în care este necesar pentru îndeplinirea sarcinilor sale.

(4) Centrul nu este în drept să investigheze activităţile instanţelor de judecată atunci când acţionează în calitatea lor judiciară. Instanţele de judecată trebuie să fie considerate acţionând în calitatea lor judiciară numai de către judecător în cadrul desfăşurării procedurilor judiciare cu condiţia existenţei scopului şi temeiului legal al prelucrării, cu excepţia situaţiei în care datele personale sunt colectate, dezvăluite sau prelucrate în oricare alt fel de către sau la solicitarea judecătorului în afara procedurilor judiciare necesare. Activităţile organizatorice şi administrative de primire, repartizare, gestionare şi stocare a datelor personale nu se consideră a fi acţiuni în calitatea lor judiciară.

Articolul 7. Conţinutul solicitării de informaţii ce conţin date personale

În cazul în care operatorul, operatorul asociat, persoana împuternicită de operator, destinatarul, precum şi alte entităţi care nu sunt considerate a fi destinatari, terţul, indiferent de tipul proprietăţii şi domeniul de activitate, forma juridică de organizare, solicită informaţii ce conţin date personale, cererea trebuie să fie motivată, să includă scopul solicitării, temeiul legal, categoriile de date personale solicitate şi să demonstreze legătura de cauzalitate dintre categoriile de date personale solicitate şi interesul legitim urmărit.

Articolul 8. Prelucrarea datelor personale şi condiţiile privind consimţământul

(1) În cazul în care prelucrarea se bazează pe consimţământ, operatorul trebuie să fie în măsură să demonstreze că subiectul de date şi-a dat consimţământul pentru prelucrarea datelor sale personale.

(2) În cazul în care consimţământul subiectului datelor este dat în contextul unei declaraţii scrise care se referă şi la alte aspecte, cererea privind consimţământul trebuie să fie prezentată într-o formă care o diferenţiază în mod clar de celelalte aspecte, într-o formă inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. Nici o parte a respectivei declaraţii nu este obligatorie dacă aceasta constituie o încălcare a prezentei legi.

(3) În cazul subiectului de date minor sau al subiectului de date major în privinţa căruia a fost instituită o măsură de ocrotire judiciară,

consimţământul privind prelucrarea datelor personale se acordă în formă scrisă sau electronică conform cerinţelor faţă de semnătura electronică şi documentul electronic,de către reprezentantul lui legal, sau, după caz, dacă situaţia specifică necesită, comsitamintul poate fi obţinut inclusiv prin bifarea unei căsuţe sau altă modalitate care poate demonstra autenticitatea acesteia. Operatorul depune toate eforturile rezonabile pentru a verifica în astfel de cazuri că reprezentantul legal a acordat sau a autorizat consimţământul, ţinând seama de tehnologiile disponibile.

(4) În cazul în care se aplică art. 5 alin. (1) lit. a), în ceea ce priveşte oferirea de servicii ale societăţii informaţionale în mod direct unui copil, prelucrarea datelor personale ale unui copil este legală dacă acesta are cel puţin vârsta de 16 ani. Dacă copilul are sub vârsta de 16 ani, respectiva prelucrare este legală numai dacă şi în măsura în care consimţământul respectiv este acordat sau autorizat de titularul răspunderii părinteşti asupra copilului.

(5) Consimţământul acordat ulterior prelucrării datelor personale, nu are efect retroactiv.

(6) Subiectul de date are dreptul să îşi retragă în orice moment consimţământul. Retragerea consimţământului nu afectează legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia. Înainte de acordarea consimţământului, subiectul de date este informat cu privire la acest lucru. Retragerea consimţământului se face la fel de simplu ca şi acordarea acestuia.

(7) La evaluarea caracterului necondiţionat al acordării consimţământului se va ţine seama de necesitatea, pertinenţa şi volumul categoriilor de date personale prelucrate în raport cu scopul declarat.

(8) Forma consimţământului trebuie să corespundă mijloacelor prin care se colectează datele personale.

(9) Existenţa consimţământului nu exclude obligaţiile operatorului de a respecta condiţiile prevăzute în art. 4 din prezenta lege.

(10) Chiar dacă subiectul de date şi-a dat consimţământul, în cazul în care se constată o încălcare a prezentei legi, în special în cazurile de încălcare a art. 4, Centrul poate decide cu privire la o prelucrare de date personale pentru a restabili conformitatea acesteia cu prevederile prezentei legi.

Articolul 9. Prelucrarea categoriei speciale de date personale

(1) Este interzisă prelucrarea categoriei speciale de date personale.

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

a) subiectul de date şi-a dat consimţământul explicit pentru unul sau mai multe scopuri specifice, cu excepţia cazului când legea prevede că interdicţia menţionată în alin. (1), nu poate fi ridicată prin consimţământul subiectului de date;

b) prelucrarea este necesară în scopul îndeplinirii obligaţiilor şi al exercitării unor drepturi specifice ale operatorului sau ale subiectului datelor în domeniul ocupării forţei de muncă, al protecţiei muncii şi protecţiei sociale, în măsura în care acest lucru este prevăzut de lege ori de un acord colectiv de

muncă încheiat în temeiul legii, care prevede garanţii adecvate pentru drepturile fundamentale şi interesele subiectului datelor;

c) prelucrarea este necesară pentru protejarea intereselor vitale ale subiectului datelor sau ale unei alte persoane fizice, atunci când subiectul de date se află în incapacitate fizică sau juridică de a-şi da consimţământul;

d) prelucrarea este efectuată în cadrul activităţilor lor legitime şi cu garanţii adecvate de către o fundaţie, o asociaţie sau orice alt organism fără scop lucrativ şi cu specific politic, filozofic, religios sau sindical, cu condiţia ca prelucrarea să se refere numai la membrii sau la foştii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale şi ca datele personale să nu fie comunicate terţilor fără consimţământul subiecţilor de date;

e) prelucrarea se referă la date personale care sunt făcute publice în mod voluntar şi manifest de către subiectul de date;

f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanţă sau ori de câte ori instanţele acţionează în exerciţiul funcţiei lor judiciare;

g) prelucrarea este efectuată de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor, cu condiţia ca aceasta să se efectueze cu respectarea drepturilor subiectului de date şi a celorlalte cerinţe şi garanţii prevăzute de prezenta lege. Orice sistem de evidenţă care conţine date personale în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor se ţine doar de către o autoritate de stat investită cu acest drept.

h) prelucrarea este necesară în scopuri legate de medicină preventivă sau a muncii, de evaluarea capacităţii de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistenţă medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor şi serviciilor de sănătate sau de asistenţă socială, în temeiul legii sau în temeiul unui contract încheiat cu un cadru medical şi sub rezerva respectării condiţiilor şi garanţiilor prevăzute la alin. (3);

i) prelucrarea este necesară din motive de interes public în domeniul sănătăţii publice, cum ar fi protecţia împotriva ameninţărilor transfrontaliere grave la adresa sănătăţii sau asigurarea de standarde ridicate de calitate şi siguranţă a asistenţei medicale şi a medicamentelor sau a dispozitivelor medicale, în temeiul legii, care prevede măsuri adecvate şi specifice pentru protejarea drepturilor şi libertăţilor subiectului de date, în special a secretului profesional;

j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu art. 14, 15, 16, care trebuie să fie proporţională cu obiectivul urmărit, respectă esenţa dreptului la protecţia datelor personale şi prevede măsuri corespunzătoare şi specifice pentru protejarea drepturilor fundamentale şi a intereselor subiectului de date;

k) prelucrarea este expres prevăzută în lege.

(3) Categoria specială de date personale poate fi prelucrată în scopurile menţionate la alin. (2) lit. (h) în cazul în care datele respective sunt prelucrate de către un profesionist supus obligaţiei de păstrare a secretului profesional sau sub responsabilitatea acestuia sau de o altă persoană supusă, de asemenea, unei obligaţii de confidenţialitate sau în conformitate cu actele normative.

Articolul 10. Prelucrarea care nu necesită identificare

(1) În cazul în care scopurile pentru care un operator prelucrează date personale nu necesită sau nu mai este necesară identificarea unui subiect de date de către operator, operatorul nu are obligaţia de a păstra, obţine sau prelucra informaţii suplimentare pentru a identifica subiectul de date în scopul unic al respectării prezentei legi.

(2) Dacă, în cazurile menţionate la alin. (1), operatorul poate demonstra că nu este în măsură să identifice subiectul de date, operatorul informează subiectul de date în mod corespunzător, în cazul în care este posibil. În astfel de cazuri, art. 20-25 nu se aplică, cu excepţia cazului în care subiectul de date, în scopul exercitării drepturilor sale în temeiul respectivelor articole, oferă informaţii suplimentare care permit identificarea sa.

Articolul 11. Minimizarea datelor personale prelucrate în scopul identificării subiectului de date

(1) Datele personale pot fi colectate pentru a identifica subiectul de date numai dacă scopul pentru care sunt obţinute aceste date este indispensabil în legătură cu serviciul furnizat sau cu un anumit caz.

(2) Operatorul şi/sau persoana împuternicită de operator trebuie să justifice, la cererea subiectului de date, necesitatea de a colecta fiecare categorie de date personale.

(3) În cazul în care operatorul deţine date personale care identifică subiectul, datele acestui subiect se actualizează şi se identifică prin prezentarea unui document de identitate original care confirmă aceste date, fără a-l ridica sau obţine copii de pe acesta.

(4) Ridicarea sau reţinerea sub orice formă a documentelor oficiale de identitate sau identificare a persoanei este interzisă, cu excepţia cazurilor prevăzute de lege.

(5) În cazul în care operatorul are îndoieli întemeiate cu privire la identitatea subiectului de date acesta poate solicita furnizarea de informaţii suplimentare necesare pentru a confirma identitatea subiectului de date.

Articolul 12. Prelucrarea datelor personale şi libertatea de exprimare şi de acces la informaţie

(1) Regimul juridic prevăzut de prezenta lege, asigură şi recunoaşte dreptul la libertatea de exprimare şi de acces la informaţie oricărei persoane.

(2) Orice persoană are dreptul de a prelucra date personale în scopurile exprimării academice, artistice sau literare, precum şi în cazul jurnaliştilor

pentru prelucrarea datelor personale în scopuri jurnalistice, dacă aceasta se face în scopul publicării informaţiilor care vizează interesul public.

(3) Normele prezentei legi, cu excepţia competenţelor Centrului şi prevederilor statuate la art. 1-4, 13, 36 şi Capitolului VIII şi IX, nu se aplică prelucrării datelor personale în scopuri academice, artistice, jurnalistice sau literare, dacă acestea sunt necesare pentru a concilia (proporţionalitatea şi echilibrul) dreptul la protecţia datelor personale cu libertatea de exprimare şi de informare în care, în acelaşi timp:

a) prelucrarea datelor personale se realizează în scopul exercitării dreptului la libertatea de exprimare şi de informare, respectând în acelaşi timp dreptul persoanei la protecţia datelor personale şi nu există interese ale subiectului de date care trebuie protejate, cu condiţia ca garanţiile subiecţilor de date nu sunt afectate, iar securitatea fizică şi psihică a subiecţilor de date nu sunt puse în pericol, care sunt mai importante decât interesul public;

b) prelucrarea datelor personale se efectuează în vederea publicării informaţiilor de interes public;

c) dispoziţiile prezentei legi sunt incompatibile şi/sau împiedică exercitarea dreptului la libertatea de exprimare şi de informare.

(4) Libertatea de exprimare şi informare pot fi supuse restricţiilor prevăzute de lege şi care sunt necesare într-o societate democratică, în interesul securităţii naţionale, integrităţii teritoriale sau siguranţei publice, pentru prevenirea dezordinii sau infracţionalităţii, pentru protecţia sănătăţii sau a moralei, pentru protejarea reputaţiei sau a drepturilor altora, pentru prevenirea divulgării informaţiilor primite cu titlu confidenţial sau pentru menţinerea autorităţii şi imparţialităţii sistemului judiciar.

(5) Realizarea drepturilor subiecţilor de date în raport cu prelucrarea datelor personale efectuată în condiţiile prezentului articol, poate avea loc prin raportarea situaţiei de facto la proporţionalitatea asigurării echilibrului dreptului la protecţia datelor personale cu dreptul de acces la informaţie şi dreptul la libertatea de exprimare.

(6) Prelucrarea datelor personale efectuată cu respectarea prevederilor alin. (1) - (5), exclude răspunderea contravenţională, penală sau civilă.

Articolul 13. Stocarea şi utilizarea datelor personale

(1) Condiţiile şi termenele de stocare şi utilizare a datelor personale se stabilesc de legislaţie ţinându-se cont de prevederile art. 4 şi 5.

(2) În cazul în care legislaţia nu prevede în mod expres condiţiile şi termenele pentru stocarea şi utilizarea datelor personale, ele sunt stabilite de către operator. Operatorii autorităţi şi instituţii publice consultă Centrul privind termenele pentru stocarea şi utilizarea datelor personale.

(3) La atingerea scopurilor pentru care datele personale au fost prelucrate acestea vor fi:

a) şterse sau distruse ireversibil;

b) transformate în documente de arhivă de interes public şi stocate în conformitate cu prevederile legislaţiei în domeniul arhivelor, accesul la ele fiind limitat pentru întreaga perioada de stocare;

c) în cazurile prevăzute expres de lege, transferate unui alt operator;

d) anonimizate sau pseudonimizate.

(4) Sistemele informaţionale automatizate de stat, inclusiv registrele de stat în care sunt prelucrate date personale pot fi stocate fizic doar în Republica Moldova.

Articolul 14. Prelucrarea în scop de arhivare în interes public

(1) În cazul în care datele personale au fost arhivate în interes public, ele pot fi ulterior prelucrate numai în următoarele cazuri:

a) subiectul de date, reprezentantul legal al acestuia sau succesorii săi şi-au exprimat consimţământul;

b) în scopuri de cercetare statistică, istorică sau ştiinţifică;

c) în scopuri de înfăptuire a justiţiei.

(2) În cazurile prevăzute la alin. (1), prelucrarea ulterioară a acestor date se efectuează în conformitate cu prezenta lege.

(3) În cazul în care datele personale sunt prelucrate în scopuri de arhivare în interes publice, drepturile de acces, de rectificare, de limitare a prelucrării, de opoziţie, şi de portabilitate a datelor nu sunt aplicabile subiecţilor de date, în măsura în care aceste drepturi pot face imposibilă sau să aducă atingere gravă scopurilor specifice, iar astfel de derogări sunt necesare pentru îndeplinirea acestui scop.

(4) În cazul în care prelucrarea menţionată la alin. (3) serveşte în acelaşi timp şi altui scop, derogările se aplică numai prelucrării în scopurile menţionate.

(5) Prelucrarea în scopuri de arhivare în interes public se efectuează cu respectarea garanţiilor corespunzătoare, în conformitate cu prezenta lege, pentru a asigura drepturile şi libertăţile subiecţilor de date. Aceste măsuri de siguranţă garantează faptul că au fost stabilite măsuri tehnice şi organizatorice necesare pentru a asigura, în special, respectarea principiului minimizării datelor. Aceste măsuri pot include pseudonimizarea, cu condiţia ca aceste scopuri să fie realizate în acest mod. Atunci când aceste scopuri pot fi obţinute prin prelucrare ulterioară care nu mai permite (în continuare) identificarea subiecţilor de date, scopurile respective vor fi realizate în acest mod.

Articolul 15. Prelucrarea datelor în scopuri statistice

(1) Prelucrarea datelor personale în scopuri statistice înseamnă orice operaţiune de colectare şi prelucrare de date personale necesară pentru anchetele statistice sau pentru producerea de rezultate statistice. Scopurile statistice presupun că rezultatul prelucrării în scopuri statistice nu reprezintă date personale, ci date agregate şi că acest rezultat sau datele nu sunt utilizate în sprijinul unor măsuri sau decizii privind o anumită persoană fizică.

(2) Prelucrarea datelor personale în scopuri statistice se efectuează cu respectarea deplină a dreptului la protecţia datelor personale în conformitate cu prezenta lege, precum şi alte acte normative care nu contravin principiilor de protecţie a datelor personale.

(3) În cazul în care datele personale sunt prelucrate în scopuri statistice, dreptul de acces, de restricţionare, rectificare şi de opoziţie nu se aplică în măsura în care aceste drepturi sunt susceptibile de a face imposibilă sau de a aduce atingere gravă realizării scopurilor specifice, iar astfel de derogări sunt necesare pentru îndeplinirea acestor scopuri.

(4) În cazul în care prelucrarea menţionată la alin. (3) serveşte în acelaşi timp şi altui scop, derogările se aplică numai prelucrării în scopurile menţionate.

(5) Prelucrarea în scopuri statistice se efectuează cu respectarea garanţiilor corespunzătoare, în conformitate cu prezenta lege, pentru a asigura drepturile şi libertăţile subiecţilor de date. Aceste măsuri de siguranţă garantează faptul că au fost stabilite măsuri tehnice şi organizatorice necesare pentru a asigura, în special, respectarea principiului minimizării datelor. Aceste măsuri pot include pseudonimizarea, cu condiţia ca aceste scopuri să fie realizate în acest mod. Atunci când aceste scopuri pot fi obţinute prin prelucrare ulterioară care nu mai permite (în continuare) identificarea subiecţilor de date, scopurile respective vor fi realizate în acest mod

Articolul 16. Prelucrarea datelor în scopuri de cercetare ştiinţifică sau istorică

(1) Prelucrarea dator personale în scopuri de cercetare ştiinţifică trebuie înţeleasă în sens larg, incluzând dezvoltarea tehnologică şi activităţile demonstrative, cercetarea fundamentală, cercetarea aplicată şi cercetarea finanţată din surse private.

(2) Prelucrarea datelor personale în scopuri de cercetare istorică se înţelege prelucrarea ce se referă la cercetarea istorică şi genealogică.

(3) Prelucrarea datelor personale în scopuri de cercetare ştiinţifică sau istorică se efectuează cu respectarea deplină a dreptului la viaţa privată, intimă şi familială - protecţia datelor personale în conformitate cu prezenta lege, precum şi alte acte normative care nu contravin principiilor de protecţie a datelor personale.

(4) În cazul în care datele personale sunt prelucrate în scopuri de cercetare ştiinţifică sau istorică dreptul de acces, de restricţionarea, rectificare şi de opoziţie nu se aplică în măsura în care aceste drepturi sunt susceptibile de a face imposibilă sau de a aduce atingere gravă realizării scopurilor specifice, iar astfel de derogări sunt necesare pentru îndeplinirea acestor scopuri.

(5) În cazul în care prelucrarea menţionată la alin. (4) serveşte în acelaşi timp şi altui scop, derogările se aplică numai prelucrării în scopurile menţionate.

(6) Prelucrarea în scopuri de cercetare ştiinţifică sau istorică se efectuează cu respectarea garanţiilor corespunzătoare, în conformitate cu

prezenta lege, pentru a asigura drepturile şi libertăţile subiecţilor. Aceste măsuri de siguranţă garantează faptul că au fost stabilite măsuri tehnice şi organizatorice necesare pentru a asigura, în special, respectarea principiului minimizării datelor. Aceste măsuri pot include pseudonimizarea, cu condiţia ca aceste scopuri să fie realizate în acest mod. Atunci când aceste scopuri pot fi obţinute prin prelucrare ulterioară care nu mai permite (în continuare) identificarea subiecţilor de date, scopurile respective vor fi realizate în acest mod.

Capitolul III
DREPTURILE SUBIECŢITLOR DE DATE PERSONALE

Articolul 17. Transparenţa informaţiilor, a comunicărilor şi a modalităţilor de exercitare a drepturilor subiectului de date

(1) Operatorul furnizează subiectului de date orice informaţii menţionate la art. 18 şi 19 şi orice comunicare în temeiul art. 20-27 şi 38 referitoare la prelucrare, într-o formă concisă, transparentă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu, în special ce ţine de informaţii adresate nemijlocit unui copil. Informaţiile se furnizează în scris sau prin alte modalităţi, inclusiv, atunci când este oportun, în format electronic. La solicitarea subiectului de date, informaţiile pot fi furnizate verbal, cu condiţia ca identitatea subiectului de date a fost verificată şi dovedită prin alte mijloace.

(2) Operatorul facilitează exercitarea drepturilor subiectului de date în temeiul art. 20-27. În cazurile menţionate la art. 10 alin. (2), operatorul dă curs cererii subiectului de date, cu excepţia cazului în care operatorul demonstrează că nu este în măsură să identifice subiectul de date.

(3) Operatorul furnizează subiectului de date informaţii privind acţiunile întreprinse în urma unei cereri în temeiul art. 20-27, în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu cel mult două luni, atunci cînd este necesar, ţinîndu-se seama de complexitatea şi numărul cererilor, operatorul informînd despre acest fapt subiectul de date cu invocarea motivelor prelungirii. În cazul în care subiectul de date introduce o cerere în format electronic cu semnătură electronică, informaţiile sunt furnizate în format electronic acolo unde este posibil, cu excepţia cazului în care subiectul de date solicită un alt format.

(4) Dacă nu se iau măsuri cu privire la cererea subiectului de date, operatorul informează subiectul de date, fără întârziere şi în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu s-au luat măsuri şi la posibilitatea de a depune o cerere la Centru şi/sau de a se adresa în instanţa de judecată.

(5) Informaţiile furnizate în temeiul art. 18 şi 19 şi orice comunicare în temeiul art. 20-27 şi 38 sunt oferite gratuit. În cazul în care cererile din partea unui subiect de date sunt în mod vădit nefondate, excesive sau repetate, operatorul motivat poate, după caz:

a) să perceapă o taxă rezonabilă ţinând cont de costurile administrative pentru furnizarea informaţiilor sau a comunicării, sau pentru luarea măsurilor solicitate;

b) să refuze de a da curs cererii.

(6) Fără a aduce atingere art. 10, în cazul în care operatorul are îndoieli întemeiate cu privire la identitatea persoanei care înaintează cererea în temeiul art. 20-26, operatorul poate solicita furnizarea de informaţii suplimentare necesare pentru a confirma identitatea subiectului de date.

(7) Informaţiile care urmează să fie furnizate subiecţilor de date în temeiul art. 18 şi 19 pot fi furnizate în combinaţie cu imagini standardizate pentru a oferi într-un mod uşor vizibil, inteligibil şi clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere. În cazul în care imaginile sunt prezentate în format electronic, acestea trebuie să poată fi citite automat.

Articolul 18. Informarea subiectului de date

(1) În cazul în care datele personale sunt colectate direct de la subiectul de date, operatorul sau persoana împuternicită de către operator are obligaţia să-i furnizeze gratuit următoarele informaţii:

a) identitatea şi datele de contact ale operatorului/operatorilor asociaţi, persoana împuternicită de operator sau, după caz, a reprezentantului operatorului;

b) datele de contact ale responsabilului de protecţia datelor personale, după caz;

c) scopurile în care sunt prelucrate datele personale, categoriile de date personale, temeiul juridic al prelucrării;

d) interesele legitime urmărite de operator sau de terţ, în cazul în care prelucrarea se face în temeiul art. 5 alin. (1) lit. f);

e) destinatarii sau categoriile de destinatari ai datelor personale;

f) faptul că operatorul intenţionează să transfere datele personale în altă ţară sau organizaţie internaţională şi existenţa sau absenţa nivelului adecvat de protecţie.

(2) În momentul obţinerii datelor personale operatorul va furniza subiectului de date următoarele informaţii suplimentare necesare pentru a asigura o prelucrare echitabilă şi transparentă:

a) perioada de stocare a datelor personale sau dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă, inclusiv şi acţiunile întreprinse asupra acestora la atingerea scopurilor pentru care au fost prelucrate;

b) existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea, ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;

c) atunci când prelucrarea are la bază consimţământul subiectului de date sau art. 9 alin. (2) lit. a) existenţa dreptului de a retrage consimţământul

în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;

d) dacă furnizarea de date personale reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă subiectul de date este obligat să furnizeze aceste date personale şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;

e) existenţa unui proces decizional automatizat cu crearea de profiluri, menţionat la art. 27 alin. (1) şi (4) precum şi cel puţin în cazurile respective informaţii pertinente privind logica utilizată, importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru subiectul de date;

f) dreptul de a depune o cerere către Centru.

(3) Informarea subiectului de date de regulă se face în formă scrisă, electronică sau în orice alt format cu condiţia că operatorul poate demonstra că subiectul de date a fost informat.

(4) În cazul în care operatorul intenţionează să prelucreze ulterior datele personale în alt scop decât cel pentru care au fost obţinute datele personale, operatorul furnizează subiectului de date înainte de această prelucrare ulterioară, informaţii cu privire la acest alt scop şi cu orice alte informaţii relevante, prevăzute în alin. (2).

(5) Prevederile alin. (1), (2) şi (4) nu se aplică în cazul în care subiectul de date deţine informaţiile respective.

Articolul 19. Informaţii care se furnizează în cazul în care datele personale nu au fost obţinute de la subiectul de date

(1) În cazul în care datele personale nu au fost obţinute de la subiectul de date, operatorul furnizează subiectului datelor următoarele informaţii:

a) identitatea şi datele de contact ale operatorului/operatorilor asociaţi, persoana împuternicită de operator sau, după caz, a reprezentantului operatorului;

b) datele de contact ale responsabilului cu protecţia datelor personale, după caz;

c) scopul prelucrării datele personale, precum şi temeiul juridic al prelucrării;

d) categoriile de date personale vizate;

e) destinatarii sau categoriile de destinatari ai datelor personale, după caz;

f) dacă este cazul, intenţia operatorului de a transfera date personale unui destinatar din altă ţară sau organizaţie internaţională şi existenţa sau absenţa unei decizii a Centrului privind asigurarea unui nivel adecvat de protecţie a datelor personale sau în cazul efectuării transferurilor în baza art. 50, 51 şi 53 alin. (2).

(2) Pe lângă informaţiile menţionate la alin. (1), operatorul furnizează subiectului de date următoarele informaţii necesare pentru a asigura prelucrarea corectă şi transparentă faţă de subiectul de date:

a) perioada pentru care datele personale vor fi stocate sau, dacă acest lucru nu este posibil, criteriile utilizate pentru stabilirea acestei perioade;

b) interesele legitime urmărite de operator sau de o terţă parte, în cazul în care prelucrarea se bazează pe art. 5 alin. (1) lit. f);

c) existenţa dreptului de a solicita operatorului, în ceea ce priveşte datele personale referitoare la subiectul de date, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării şi a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;

d) existenţa dreptului de retragere a consimţământului în orice moment, fără a afecta legalitatea prelucrării, înainte de retragerea sa, dacă prelucrarea se bazează pe art. 5 alin. (1) lit. a) sau la art. 9 alin. (2) lit. a);

e) dreptul de a depune o cerere la Centru;

f) proveniența datelor personale și, dacă este cazul, proveniența surselor accesibile public;

g) existenţa unui proces automatizat de luare a deciziilor, inclusiv a creării de profiluri, menţionat la art. 27, alin. (1) şi (4) şi cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări asupra subiectului de date.

(3) Operatorul furnizează informaţiile menţionate la alin. (1) şi (2):

a) într-o perioadă rezonabilă de timp după obţinerea datelor personale, dar nu mai târziu de o lună, ţinând cont de circumstanţele specifice în care sunt prelucrate datele personale;

b) dacă datele personale vor fi utilizate pentru comunicarea cu subiectul de date, cel târziu în momentul primei comunicări către subiectul de date; sau

c) dacă se prevede o divulgare către un alt destinatar, cel mai târziu când datele personale sunt dezvăluite pentru prima dată.

(4) În cazul în care operatorul intenţionează să prelucreze în continuare datele personale în alt scop decât cel pentru care au fost obţinute datele personale, operatorul furnizează subiectului de date înainte de această prelucrare ulterioară informaţii cu privire la acest alt scop şi cu orice alte informaţii relevante menţionate la alin. (2).

(5) Alin. (1) - (4) nu se aplică atunci când şi în măsura în care:

a) subiectul de date deţine deja informaţiile;

b) furnizarea de astfel de informaţii se dovedeşte imposibilă sau ar presupune un efort disproporţionat, în special în ceea ce priveşte prelucrarea în scopuri de arhivare în interesul public, cercetări ştiinţifice sau istorice sau scopuri statistice, sub rezerva condiţiilor şi garanţiilor menţionate în art. 14, 15, 16 sau în măsura în care obligaţia menţionată la alin. (1) este de natură să facă imposibilă sau să afecteze grav atingerea obiectivelor acestei prelucrări. În astfel de cazuri, operatorul ia măsurile necesare pentru a proteja drepturile şi libertăţile subiectului de date şi interesele legitime, inclusiv punerea la dispoziţia publicului a informaţiilor;

c) obţinerea sau divulgarea este prevăzută în mod expres de legea la care este supus operatorul şi care prevede măsurile adecvate pentru a proteja interesele legitime ale subiectului de date;

d) în cazul în care datele personale trebuie să rămână confidenţiale, sub rezerva respectării unei obligaţii privind secretul profesional reglementat de lege, inclusiv obligaţia legală de păstrare a secretului.

Articolul 20. Dreptul de acces al subiectului de date personale

(1) Subiectul de date are dreptul de a obţine din partea operatorului o confirmare că se prelucrează sau nu date personale care-l privesc şi, în caz afirmativ, are acces la datele respective şi la următoarele informaţii:

a) scopurile prelucrării;

b) categoriile de date personale vizate;

c) destinatarii sau categoriile de destinatari cărora datele personale le-au fost sau urmează să le fie divulgate, în special destinatari din alte ţări sau organizaţii internaţionale;

d) perioada pentru care se preconizează că vor fi stocate datele personale, sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

e) existenţa dreptului de a solicita operatorului rectificarea sau ştergerea datelor personale ori restricţionarea prelucrării datelor personale referitoare la subiectul de date sau a dreptului de a se opune prelucrării;

f) privind dreptul de a depune o cerere în adresa Centrului;

g) în cazul în care datele personale nu sunt colectate de la subiectul de date, orice informaţii disponibile privind sursa acestora;

h) existenţa unui proces decizional automatizat incluzând crearea de profiluri, menţionat la art. 27, precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru subiectul de date.

(2) În cazul în care datele personale sunt transferate către un alt stat sau o organizaţie internaţională, subiectul de date urmează a fi informat, inclusiv cu privire la existenţa garanţiilor adecvate referitoare la acest transfer conform art. 50.

(3) La cererea subiectului de date care urmează a fi semnată ograf sau să corespundă cerinţelor semnăturii electronice şi documentului electronic, operatorul furnizează o copie a datelor personale care fac obiectul prelucrării. Pentru orice alte copii solicitate de subiectul de date, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative în temeiul unui regulament elaborat de către operator. În cazul în care subiectul de date introduce cererea în format electronic şi cu excepţia cazului în care subiectul de date solicită un alt format, informaţiile sunt furnizate într-un format electronic utilizat în mod curent.

(4) Dreptul de a obţine o copie menţionată la alin. (3) se aplică în aşa fel încât să nu aducă atingere drepturilor şi libertăţilor altor subiecţi de date.

(5) Subiectul de date are dreptul să obţină la cerere, gratuit şi fără întârzieri nejustificate, după caz accesul fizic la datele personale stocate care îl privesc şi care sunt prelucrate în sistemele de evidenţă, cu excepţia în care acest drept ar putea fi susceptibil de a aduce atingere cerinţelor de securitate asigurate sau din punct de vedere tehnic nu este posibil a fi realizat sau pot fi aduse atingeri drepurilor şi libertăţilor altor subiecţi de date.

Articolul 21. Dreptul la rectificare

Subiectul de date are dreptul de a obţine de la operator, la cerere şi fără întârziere nejustificată:

a) rectificarea datelor inexacte sau neveridice care-l vizează;

b) completarea datelor incomplete care-l vizează;

c) actualizarea datelor care-l vizează.

Articolul 22. Dreptul la ştergerea datelor (dreptul de a fi uitat)

(1) Subiectul de date are dreptul de a obţine de la operator ştergerea datelor personale care îl vizează, iar operatorul are obligaţia de a şterge datele personale fără întârzieri nejustificate, în cazul în care se aplică unul dintre următoarele motive:

a) datele personale nu mai sunt necesare pentru îndeplinirea scopurilor pentru care au fost colectate sau prelucrate;

b) subiectul de date îşi retrage consimţământul în baza căruia are loc prelucrarea, în conformitate cu art. 5 alin. (1) lit. a) sau cu art. 9 alin. (2) lit. a), şi nu există niciun alt temei juridic pentru prelucrarea;

c) subiectul de date se opune prelucrării în temeiul art. 26 alin. (1) şi nu există motive legitime care să prevaleze în ceea ce priveşte prelucrarea sau subiectul de date se opune prelucrării în temeiul art. 26 alin. (2);

d) datele personale au fost prelucrate ilegal;

e) datele personale trebuie şterse pentru a asigura respectarea unei cerinţe legale aplicate operatorului în condiţiile legii;

f) datele personale au fost colectate în legătură cu oferirea de servicii ale societăţii informaţionale menţionate la art. 8 alin. (4).

(2) În cazul în care operatorul a făcut publice datele personale şi este obligat, în temeiul alin. (1), să le şteargă, operatorul, ţinând seama de tehnologia disponibilă şi de costul implementării, ia măsuri rezonabile, inclusiv măsuri tehnice, pentru a informa operatorii care prelucrează datele personale că subiectul de date a solicitat ştergerea de către aceşti operatori a oricăror link-uri către datele respective sau a oricăror copii sau reproduceri ale acestor date personale.

(3) În cazul în care dreptul la ştergerea datelor personale a fost satisfăcut, operatorii, persoanele împuternicite de operator, terţii, destinatarii şi entităţile care nu sunt destinatare care prelucrează aceste date sunt obligaţi să-şi ajusteze operaţiunile de prelucrare, imediat sau cel mult în termen de o lună din momentul informării. Acest termen poate fi extins cu 15 zile lucrătoare, după caz, în funcţie de complexitate. Operatorul informează

subiectul de date cu privire la o astfel de extindere în termen de 15 zile lucrătoare de la primirea cererii, împreună cu motivele întârzierii. În cazul în care subiectul de date depune cererea prin mijloace electronice, informaţiile sunt furnizate pe cale electronică, în măsura posibilităţilor, cu excepţia cazului în care subiectul de date solicită altfel.

(4) Alineatele (1) - (3) nu se aplică în măsura în care prelucrarea este justificată şi necesară:

a) pentru respectarea unei obligaţii legale sau pentru îndeplinirea unei sarcini îndeplinite în interes public sau în cadrul exercitării unei autorităţi oficiale cu care este învestit operatorul;

b) din motive de interes public în domeniul sănătăţii publice, în conformitate cu art. 9 alin. (2) lit. h) şi i) şi art. 9 alin. (3);

c) pentru constatarea, exercitarea sau apărarea unui drept în instanţa judecătorească;

d) în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică sau în scopuri statistice, în conformitate cu art. 14 - 16 în măsura în care dreptul menţionat la alin. (1) este de natură să facă imposibilă sau să afecteze grav realizarea obiectivelor de prelucrare.

Articolul 23. Dreptul la restricţionarea prelucrării

(1) Subiectul de date are dreptul de a obţine din partea operatorului restricţionarea prelucrării în cazul în care se aplică unul din următoarele cazuri:

a) subiectul de date contestă exactitatea datelor personale, pentru o perioadă care îi permite operatorului să verifice exactitatea acestora;

b) subiectul de date consideră prelucrarea ca fiind ilegală şi se opune ştergerii datelor personale, solicitând în schimb restricţionarea utilizării lor;

c) operatorul nu mai are nevoie de datele personale în scopul prelucrării, dar subiectul date i le solicită pentru constatarea, exercitarea sau apărarea unui drept în instanţă; sau

d) subiectul de date s-a opus prelucrării în conformitate cu art. 26 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 restricţionată în temeiul alin. (1), astfel de date personale pot, cu excepţia stocării, să fie prelucrate numai cu consimţământul subiectului de date sau pentru constatarea, exercitarea sau apărarea unui drept în instanţă, pentru protecţia drepturilor unei alte persoane fizice sau juridice sau din motive de interes public.

(3) Subiectul de date, care a obţinut restricţionarea prelucrării în temeiul alin. (1) este informat de către operator înainte de ridicarea restricţiei de prelucrare.

Articolul 24. Obligaţia de notificarea privind rectificarea, ştergerea datelor personale sau restricţionarea prelucrării

Operatorul comunică fiecărui destinatar căruia i-au fost divulgate datele personale orice rectificare sau ştergere a datelor personale sau restricţionare a prelucrării efectuate în conformitate cu art. 21, 22, alin. (1) şi art. 23, cu excepţia cazului în care acest lucru se dovedeşte imposibil sau presupune eforturi disproporţionate. Operatorul informează subiectul de date cu privire la respectivii destinatari, dacă subiectul de date solicită acest lucru.

Articolul 25. Dreptul la portabilitatea datelor personale

(1) Subiectul de date are dreptul de a primi datele personale care îl privesc, pe care acesta le-a furnizat operatorului într-un format structurat, utilizat în mod curent şi care poate fi citit automatizat şi are dreptul de a transmite aceste date altui operator, fără obstacole din partea operatorului căruia i-au fost furnizate datele personale, în cazul în care prelucrarea este efectuată prin mijloace automatizate şi prelucrarea se bazează pe consimţământ în temeiul art. 5 alin. (1) lit. a) sau al art. 9 alin. (2) lit. a), sau pe un contract în temeiul art. 5 alin. (1) lit. b)

(2) Întru exercitarea dreptului său la portabilitatea datelor în temeiul alin. (1), subiectul de date are dreptul ca datele personale să fie transmise direct de la un operator la altul acolo unde acest lucru este fezabil din punct de vedere tehnic.

(3) Exercitarea dreptului menţionat la alin. (1) nu aduce atingere art. 22. Respectivul drept nu se aplică prelucrării necesare pentru îndeplinirea unei sarcini executate în interes public sau în cadrul exercitării unei autorităţi oficiale cu care este învestit operatorul.

(4) Dreptul menţionat la alin. (1) nu aduce atingere drepturilor şi libertăţilor altor subiecţi de date.

Articolul 26. Dreptul la opoziţie

(1) Subiectul de date are dreptul de a se opune, în orice moment, din motive legate de situaţia particulară, în care se află, prelucrării în temeiul art. 5 alin. (1) lit. e) sau f) a datelor personale care îl privesc, inclusiv creării de profiluri pe baza respectivelor dispoziţii. Operatorul nu mai prelucrează datele personale, cu excepţia cazului în care operatorul demonstrează că are motive legitime şi imperioase care justifică prelucrarea şi care prevalează asupra intereselor, drepturilor şi libertăţilor subiectului de date sau că scopul este constatarea, exercitarea sau apărarea unui drept în instanţa de judecată.

(2) Atunci când prelucrarea datelor personale are drept scop marketingul direct, subiectul de date are dreptul de a se opune în orice moment prelucrării în acest scop a datelor personale care îl privesc, inclusiv creării de profiluri, în măsura în care este legată de marketingul direct respectiv.

(3) În cazul în care subiectul de date se opune prelucrării în scopul marketingului direct, datele personale nu mai sunt prelucrate în acest scop.

(4) Cel tîrziu în momentul primei comunicări cu subiectul de date, dreptul menţionat la alin. (1) şi (2) este adus în mod explicit în atenţia

subiectului de date şi este prezentat în mod clar şi separat de orice alte informaţii.

(5) În contextul utilizării serviciilor societăţii informaţionale, subiectul de date îşi poate exercita dreptul de a se opune prin mijloace automatizate care utilizează specificaţii tehnice.

(6) În cazul în care datele personale sunt prelucrate în scopuri de cercetare ştiinţifică sau istorică sau în scopuri statistice, în conformitate cu art. 14-16, subiectul de date, din motive legate de situaţia sa particulară, are dreptul de a se opune prelucrării datelor personale care îl privesc, cu excepţia cazului în care prelucrarea este necesară pentru îndeplinirea unei sarcini din motive de interes public.

Articolul 27. Procesul decizional individual automatizat, inclusiv crearea de profiluri

(1) Subiectul de date are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrare automatizată, inclusiv crearea de profiluri, care produce efecte juridice care privesc subiectul de date sau îl afectează în mod similar într-o măsură semnificativă.

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

a) este necesară pentru încheierea sau executarea unui contract între subiectul de date şi un operator de date;

b) este autorizată prin act normativ, care se aplică operatorului şi care prevede, de asemenea, măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale subiectului de date;

c) are la bază consimţământul explicit al subiectului de date.

(3) În cazurile menţionate la alin. (2) lit. a) şi c), operatorul de date pune în aplicare măsuri corespunzătoare pentru protejarea drepturilor, libertăţilor şi intereselor legitime ale subiectului de date, cel puţin dreptul de a beneficia de intervenţie umană din partea operatorului, de a-şi exprima punctul de vedere şi de a contesta decizia.

(4) Deciziile menţionate la alin. (2) nu au la bază categoriile speciale de date personale, cu excepţia cazului în care se aplică art. 9 alin. (2) lit. a) sau g) şi în care au fost instituite măsuri adecvate de protejare a drepturilor, libertăţilor şi intereselor legitime ale subiectului de date.

Articolul 28. Restricţii

(1) Drepturile şi obligaţiile prevăzute la art. 17-27 şi la art. 38, precum şi la art. 4, în măsura în care prevederile acestuia corespund drepturilor şi obligaţiilor prevăzute la art. 17-27, pot fi restricţionate de un act legislativ când o astfel de restricţie respectă esenţa drepturilor şi libertăţilor fundamentale şi constituie o măsură necesară şi proporţională într-o societate democratică pentru:

a) protecţia securităţii naţionale şi a statului;

b) protecţia ordinii publice;

c) prevenirea, investigarea, descoperirea sau urmărirea penală a infracţiunilor sau executarea sancţiunilor penale, inclusiv protejarea împotriva ameninţărilor la adresa ordinii publice;

d) alte obiective importante ale statului de interes general, în special un interes economic sau financiar important, inclusiv în domeniile monetar, bugetar şi fiscal şi în domeniul sănătăţii publice şi al securităţii sociale;

e) protecţia independenţei justiţiei şi a procedurilor judiciare;

f) prevenirea, investigarea, depistarea şi urmărirea penală a încălcărilor deontologice în cazul profesiilor reglementate;

g) funcţia de monitorizare, inspectare sau reglementare legată, chiar şi ocazional, de exercitarea autorităţii publice în cazurile menţionate la lit. a) - f);

h) protecţia subiectului de date sau a drepturilor şi libertăţilor altor subiecţi de date;

i) punerea în aplicare a pretenţiilor de drept civil.

(2) Orice măsură legislativă menţionată la alin. (1) conţine dispoziţii specifice cel puţin, în corespundere cu prezenta lege, în ceea ce priveşte:

a) scopurile prelucrării sau ale categoriilor de prelucrare;

b) categoriile de date personale;

c) domeniul de aplicare al restricţiilor introduse;

d) garanţiile pentru a preveni abuzurile sau accesul sau transferul ilegal;

e) menţionarea operatorului sau a categoriilor de operatori;

f) perioadele de stocare şi garanţiile aplicabile, ţinând seama de natura, domeniul de aplicare şi scopurile prelucrării sau categoriilor de date prelucrate;

g) riscurile pentru drepturile şi libertăţile subiecţilor de date; şi

h) dreptul subiecţilor de date de a fi informaţi cu privire la restricţie, cu excepţia cazului în care acesta poate aduce atingere scopului restricţiei.

Capitolul IV
OPERATORUL ŞI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Articolul 29. Responsabilitatea operatorului

(1) Ţinând seama de natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi de riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul pune în aplicare măsuri tehnice şi organizatorice adecvate pentru a garanta şi a fi în măsură să demonstreze că prelucrarea se efectuează în conformitate cu cerinţele prezentei legi şi/sau alte acte regulatorii în domeniul protecţiei datelor personale. Operatorul este obligat să verifice sistematic respectarea cerinţelor de conformitate şi securitate prevăzute de prezenta lege şi să le actualizeze.

(2) Atunci când sunt proporţionale în raport cu operaţiunile de prelucrare, măsurile menţionate la alin. (1) includ implementarea de către operator a unor politici adecvate de protecţie a datelor.

(3) Operatorul va prelucra datele în conformitate cu prezenta lege şi va asigura conformitatea activităţilor de prelucrare a datelor cu prevederile prezentei legi. Operatorul este responsabil de prelucrarea datelor, cu excepţia situaţiilor în care operatorul poate dovedi că persoana împuternicită de operator nu respectă cerinţele contractului sau a altui act juridic sau au fost încălcate prevederile legale.

(4) În cazul în care legislaţia nu prevede în mod expres condiţiile şi termenele de stocare şi utilizare a datelor personale, operatorul le va defini în condiţiile art. 13.

(5) Datele personale prelucrate de către operator, pot fi transmise către un alt operator sau operator asociat pentru prelucrare-în scopuri similare sau altele decât cele pentru care au fost colectate, doar în baza temeiului legal menţionat în art. 5 alin. (1) şi în conformitate cu principiile de protecţie a datelor personale menţionate în art. 4 alin. (1).

(6) Aderarea la codurile de conduită aprobate aşa cum este menţionat la art. 46 sau la mecanismele de certificare aprobate menţionate la art. 47 pot fi utilizate ca element prin care să se demonstreze respectarea obligaţiilor operatorului.

Articolul 30. Asigurarea protecţiei datelor personale începând cu momentul conceperii şi în mod implicit

(1) Având în vedere stadiul actual al tehnologiei, costurile implementării, natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscurile cu grade diferite de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice pe care le prezintă prelucrarea, operatorul, atît în momentul stabilirii mijloacelor de prelucrare, cît şi în cel al prelucrării în sine, pune în aplicare măsuri tehnice şi organizatorice adecvate (cum ar fi pseudonimizarea, anonimizarea şi altele), care sunt destinate să pună în aplicare în mod eficient principiile de protecţie a datelor personale (precum minimizarea datelor), şi să integreze garanţiile necesare în cadrul prelucrării, pentru a îndeplini cerinţele prezentei legi şi a proteja drepturile subiectului de date.

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

(3) În scopul asigurării implementării cerinţelor de protecţie a datelor personale „confidenţialitate în momentul conceperii şi confidenţialitate implicită", la momentul creării/conceperii sistemelor de evidenţă a datelor personale operatorul urmează să coordoneze cu Centrul crearea sistemelor date, dacă aceste sisteme va prelucra categoria specială de date personale.

(4) Autorităţile şi instituţiile publice coordonează cu Centrul înainte de momentul conceperii şi pe parcurs, crearea oricărui sistem de evidenţă în care sunt prelucrate date personale.

(5) Avizul Centrului în condiţiile prezentului articol relevă conformitatea prelucrării la momentul examinării situaţiei, care se emite în baza evaluării impactului asupra protecţiei datelor personale şi a informaţiilor şi materialelor prezentate de către entitatea solicitantă. Atunci când se cere avizul Centrului, solicitantul prezintă:

a) dacă este cazul, responsabilităţile respective ale operatorului, ale operatorilor asociaţi şi ale persoanelor împuternicite de operator implicate în activităţile de prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

b) scopurile şi mijloacele prelucrării preconizate;

c) măsurile şi garanţiile prevăzute pentru protecţia drepturilor şi libertăţilor subiecţilor de date, în conformitate cu prezenta lege;

d) datele de contact ale responsabilului de protecţia datelor personale, dacă este cazul;

e) evaluarea impactului asupra protecţiei datelor personale; şi

f) orice alte informaţii solicitate de Centru în legătură cu prelucrarea datelor personale.

(6) Emiterea avizului, nu exclude posibilitatea Centrului de a interveni la orice etapă, în cazul în care au apărut noi circumstanţe şi/sau au fost identificate anumite riscuri pentru asigurarea drepturilor şi libertăţilor subiecţilor de date.

(7) Un mecanism de certificare aprobat în conformitate cu art. 47 poate fi utilizat drept element care să demonstreze îndeplinirea cerinţelor prevăzute la alin. (1) şi (2). Prezentul alineat nu se aplică în raport cu prelucrarea datelor personale efectuată în condiţiile art. 2 alin. (2) lit. d).

Articolul 31. Operatori asociaţi

(1) Operatorii asociaţi stabilesc într-un mod transparent responsabilităţile fiecăruia în ceea ce priveşte îndeplinirea obligaţiilor care le revin în temeiul prezentei legi, în special în ceea ce priveşte exercitarea drepturilor subiecţilor de date şi îndatoririle fiecăruia de furnizare a informaţiilor prevăzute la art. 18 şi 19, printr-un acord sau alt act juridic cu excepţia cazurilor şi în măsura în care responsabilităţile respective ale operatorilor sunt determinate prin lege la care sunt supuşi aceştia. Acordul sau actul juridic poate să conţină clauze referitoare la desemnarea punctului de contact pentru subiecţii de date.

(2) Acordul menţionat la alin. (1) reflectă în mod adecvat rolurile şi raporturile respective ale operatorilor asociaţi faţă de subiecţii de date. Acordul este adus la cunoştinţa subiectului de date în limita informaţiilor ce nu prezintă risc pentru măsurile de securitate aplicate de operator, în caz contrar se va aduce la cunoştinţa acestuia doar esenţa acordului.

(3) Indiferent de clauzele acordului menţionat la alin. (1) subiectul de date îşi poate exercita drepturile conform acestei legi în raport cu fiecare dintre operatori.

Articolul 32. Reprezentanţii operatorilor sau ai persoanelor care nu au sediul stabilit în Republica Moldova

(1) În cazul aplicării art. 2 alin. (2) lit. c), operatorii sau persoanele împuternicite de operatori care nu au sediul stabilit în Republica Moldova desemnează în scris un reprezentant în Republica Moldova sau într-un stat membru al Uniunii Europene care va fi responsabil pentru Republica Moldova.

(2) Obligaţia 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 şi care este puţin susceptibilă de a genera un risc pentru drepturile şi libertăţile subiecţilor de date, ţinând cont de natura, contextul, domeniul de aplicare şi scopurile prelucrării;

b) unei autorităţi sau unei entităţi publice.

(3) Reprezentantul primeşte de la operator sau de la persoană împuternicită de operator o împuternicire prin care Centrul şi subiectul de date se pot adresa reprezentantului faţă de operator sau persoana împuternicită de operator, cu privire la toate aspectele legate de prelucrare pentru a asigura respectarea prezentei legi.

(4) Desemnarea unui reprezentant de către operator sau de către persoana împuternicită de operator nu aduce atingere acţiunilor legale care ar putea fi iniţiate împotriva operatorului sau a persoanei împuternicite de operator.

Articolul 33. 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 garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încît prelucrarea să respecte cerinţele prevăzute în prezenta lege şi să asigure protecţia drepturilor subiectului de date.

(2) Persoana împuternicită de operator nu poate contracta o altă persoană împuternicită de operator fără a primi în prealabil o autorizaţie specifică sau generală, oferită în formă scrisă din partea operatorului. În cazul autorizaţiei scrise generale, persoana împuternicită de operator informează operatorul despre modificările intenţionate privind adăugarea sau înlocuirea altor persoane împuternicite, oferind astfel operatorului posibilitatea de a se opune unor astfel de modificări.

(3) Prelucrarea de către o persoană împuternicită de un operator este reglementată printr-un contract sau alt act juridic care are caracter obligatoriu pentru părţi şi care stabileşte obiectul şi durata prelucrării, natura şi scopul prelucrării, tipul de date personale, categoriile subiecţilor de date, obligaţiile şi drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoana împuternicită de operator:

a) prelucrează datele personale numai pe baza unor instrucţiuni documentate din partea operatorului, inclusiv în ceea ce priveşte transferurile de date personale către o altă ţară sau o organizaţie internaţională, cu excepţia cazului în care această obligaţie îi revine persoanei împuternicite. În acest caz, notifică această obligaţie juridică operatorului înainte de prelucrare, cu excepţia cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;

b) se asigură că persoanele autorizate să prelucreze datele personale s-au angajat să respecte confidenţialitatea sau au o obligaţie statutară adecvată de confidenţialitate;

c) adoptă toate măsurile necesare în conformitate cu art. 36;

d) respectă condiţiile menţionate la alin. (2) şi (4) privind contractarea unei altei persoane împuternicite de operator;

e) ţinând seama de natura prelucrării, oferă asistenţă operatorului prin măsuri tehnice şi organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligaţiei operatorului de a răspunde cererilor privind exercitarea de către subiectul de date a drepturilor prevăzute în capitolul III;

f) ajută operatorul să asigure respectarea obligaţiilor prevăzute la art. 36, 37, 38, 40, 41, ţinând seama de caracterul prelucrării şi informaţiile aflate la dispoziţia persoanei împuternicite de operator;

g) la alegerea operatorului, şterge sau returnează operatorului toate datele personale după încetarea furnizării serviciilor legate de prelucrare şi elimină copiile existente, cu excepţia cazului în care legea prevede altfel;

h) pune la dispoziţia operatorului toate informaţiile necesare pentru a demonstra respectarea obligaţiilor prevăzute la prezentul articol, permite desfăşurarea auditului, inclusiv a inspecţiilor, efectuate de operator sau alt auditor mandatat şi contribuie la acestea. Persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucţiune încalcă prezenta lege sau alte acte normative în domeniul protecţiei datelor personale.

(4) În cazul în care o persoană împuternicită de un operator contractează o altă persoană împuternicită pentru efectuarea unor activităţi ce vizează prelucrarea datelor personale efectuată în numele operatorului, persoana împuternicită de operator vizată este obligată să respecte aceleaşi obligaţii privind protecţia datelor prevăzute în contract sau în alt act juridic încheiat între operator şi 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 special furnizarea de garanţii suficiente pentru punerea în aplicare a unor măsuri tehnice şi organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerinţele prezentei legi. În cazul în care această a doua persoană împuternicită nu îşi respectă obligaţiile privind protecţia datelor, persoana împuternicită iniţială rămâne pe deplin răspunzătoare faţă de operator în ceea ce priveşte îndeplinirea obligaţiilor acestei a doua persoane împuternicite.

(5) Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, menţionat la art. 45, sau la un mecanism de certificare aprobat, menţionat la art. 47, poate fi utilizată ca element prin care să se demonstreze existenţa garanţiilor suficiente menţionate la alin. (1) şi (4).

(6) Fără a aduce atingere unui contract individual încheiat între operator şi persoana împuternicită de operator, contractul sau celălalt act juridic menţionat la alin. (3) şi (4) se poate baza, integral sau parţial, pe clauze contractuale standard menţionate la alin. (7) şi (8), inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul art. 47 şi 48.

(7) Centrul poate să prevadă clauze contractuale standard pentru aspectele menţionate la alin. (3) şi (4).

(8) Contractul sau celălalt act juridic menţionat la alin. (3) şi (4) se formulează în scris, inclusiv în format electronic conform cerinţelor semnăturii electronice şi documentului electronic.

(9) Fără a aduce atingere art. 88 şi art. 89 în cazul în care o persoană împuternicită de operator încălcă prezenta lege, prin stabilirea scopurilor şi mijloacelor de prelucrare a datelor personale, persoana împuternicită de operator este considerată a fi un operator în ceea ce priveşte prelucrarea respectivă.

(10) Persoana împuternicită de operator va prelucra datele personale sub răspunderea operatorului dacă o astfel de prelucrare corespunde cu regimul juridic prevăzut de prezenta lege.

Articolul 34. Prelucrarea datelor personale sub autoritatea operatorului sau a persoanei împuternicite de operator

(1) Persoana împuternicită de operator şi orice persoană care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator, care are acces la datele personale, nu le prelucrează decât cu respectarea instrucţiunilor operatorului, cu excepţia cazului în care acest lucru este impus de lege.

(2) Prelucrarea datelor personale de către persoanele care activează în baza unui raport juridic de muncă sub autoritatea operatorului sau a persoanei împuternicite de operator în conformitate cu contractul sau cu alt act juridic, sunt operaţiuni de prelucrare a datelor personale efectuate de către operator.

(3) În cazul în care prelucrarea datelor personale enunţată la alin. (1) este efectuată în alte scopuri decât cele stabilite de către operator, chiar dacă persoana se află sau nu în raporturi juridice de muncă cu operatorul de date, aceasta va avea calitatea de operator de date personale în raport cu prelucrarea.

Articolul 35. Evidenţa activităţilor de prelucrare

(1) Operatorul şi după caz reprezentantul operatorului păstrează/ţin evidenţa activităţilor de prelucrare a datelor personale sub răspunderea lor. Respectiva evidenţă cuprinde următoarele informaţii:

a) denumirea operatorului, numele şi datele persoanei care au prelucrat datele personale, ale operatorului asociat, ale reprezentantului operatorului şi ale responsabilului de protecţia datelor;

b) scopul şi temeiul legal al prelucrării;

c) descrierea categoriilor de subiecţi de date şi a categoriilor de date personale prelucrate;

d) categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele personale, inclusiv destinatarii din alte ţări sau organizaţii internaţionale;

e) dacă este cazul, transferurile de date personale către o altă ţară sau o organizaţie internaţională, inclusiv identificarea ţării sau a organizaţiei internaţionale respective şi, în cazul transferurilor menţionate la art. 53 alin. (2) documentaţia care dovedeşte existenţa unor garanţii adecvate;

f) termenele-limită preconizate pentru ştergerea diferitelor categorii de date, acolo unde este posibil;

g) acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la art. 36 alin. (1).

(2) Fiecare operator şi, după caz, persoana împuternicită de operator păstrează o evidenţă a tuturor categoriilor de activităţi de prelucrare desfăşurate în numele operatorului, care cuprind:

a) numele şi datele de contact ale persoanei sau a persoanelor împuternicite de operator şi ale fiecărui operator în numele căruia acţionează această persoană (aceste persoane), precum şi ale reprezentantului operatorului sau al persoanei împuternicite de operator, după caz;

b) operaţiunile de prelucrare a datelor desfăşurate în numele fiecărui operator, cu indicarea scopului şi temeiului legal al prelucrării;

c) dacă este cazul, transferurile de date personale către o altă ţară sau o organizaţie internaţională, inclusiv identificarea ţării sau a organizaţiei internaţionale respective şi, în cazul transferurilor prevăzute la art. 53 alin. (2) documentaţia care dovedeşte existenţa unor garanţii adecvate;

d) acolo unde este posibil, o descriere generală a măsurilor tehnice şi organizatorice de securitate menţionate la art. 36 alin. (1).

(3) Evidenţa activităţilor de prelucrare a datelor personale se ţin în formă automatizată, mixtă sau manuală pentru o perioadă de 5 ani.

(4) Operatorul sau persoana împuternicită de acesta, după caz, reprezentantul operatorului sau al persoanei împuternicite de operator precum şi entităţile care nu sunt considerate a fi destinatari, terţul, indiferent de tipul proprietăţii şi domeniul de activitate, forma juridică de organizare pun evidenţa activităţilor de prelucrare la dispoziţia Centrului, la cererea acestuia. Atunci când este cazul, Centrul poate solicita informaţii suplimentare privind evidenţa activităţilor de prelucrare a datelor personale.

(5) Prevederile menţionate la alin. (1), (2) şi (3) nu se aplică instituţiilor de drept public sau privat, cu mai puţin de 20 de angajaţi, cu excepţia cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile şi libertăţile persoanelor vizate, prelucrarea nu este

ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la art. 9 alin. (1).

(6) Operatorii - autorităţile publice centrale şi locale de toate nivelurile vor adopta regulamente interne detaliate privind implementarea acestor cerinţe precum şi modalitatea de control intern privind realizarea acestora.

Capitolul V
SECURITATEA PRELUCRĂRII DATELOR PERSONALE

Articolul 36. Securitatea prelucrării

(1) Având în vedere stadiul dezvoltării tehnologice actual prelucrării, costurile implementării şi natura, domeniul de aplicare, contextul şi scopurile prelucrării, precum şi riscul cu diferite grade de probabilitate şi gravitate pentru drepturile şi libertăţile persoanelor fizice, operatorul, operatorul asociat, persoana împuternicită de operator, destinatarul, precum şi entităţile care nu sunt considerate a fi destinatari, terţul, indiferent de tipul proprietăţii şi domeniul de activitate, forma juridică de organizare, implementează măsuri tehnice şi organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele:

a) securitatea spaţiului unde se prelucrează, păstrează datele-personale, inclusiv a mijloacelor de prelucrare şi păstrare a acestor date;

b) identificarea şi autorizarea-persoanelor care au aces la sistemele de evidenţă ce conţin date personale;

c) implimentarea procedurilor de autorizare şi acordare a dreptului de acces la sistemele de evidenţă şi a măsurilor de control (autorizaţie de acces incusiv după nivelul de ierarhie, stabilirea drepturilor, obligaţiilor, restricţiilor, efectuarea controlului privind realizarea măsurilor de securitate şi responsabilizarea angajaţilor, monitorizarea activităţilor în cazuri de urgenţă);

d) instalărea şi/sau modificarea mijloacelor, soluţiilor de software/hardware , stabilirea listei acestora, precum şi a regulilor de gestionare a fişierelor temporare;

e) protecţia suporturilor de păstrare a datelor personale (evidenţa suporturilor de păstrare a datelor personale, controlul utilizării, modalitatea blocării, utilizării neautorizate, ştergerea, pseudonimizarea şi criptarea datelor personale, sau anonimizarea datelor personale stocate);

f) protecţia antivirus (realizarea protecţiei antivirus precum şi actualizarea mijloacelor de asigurare a protecţiei contra programelor dăunătoare şi signaturilor de virus);

g) protecţia contra intruziunilor, inclusiv în cazul utilizării tehnologiilor fără fir;

h) integritatea datelor personale (asigurarea păstrării informaţiei ce conţine date personale cu toate atributele sale iniţiale şi modificarea ei doar de către persoanele autorizate. La transmiterea informaţiilor ce conţin date personale este necesară utilizarea mijloacelor de protecţie criptografică şi semnătura electronică. Datele personale trebuie stocate, prelucrate sau

transmise cu luarea măsurilor corespunzătoare împotriva distrugerii, modificării accidentale ori ilicite, împotriva pierderii sau deteriorării accidentale şi împotriva stocării, prelucrării, accesării ori divulgării ilicite);

i) disponibilitatea datelor personale (asigurarea prin mijloace tehnice a accesului la informaţie pentru o anumită perioadă de timp stabilită, conform specificaţiilor tehnice, efectuarea copiilor de rezervă a informaţiilor ce conţin date personale, asigurarea posibilităţii restabilirii acestora pentru un interval de timp);

j) confidenţialitatea datelor personale (asigurarea, inclusiv, prin mijloace tehnice a accesului la informaţii ce conţin date personale doar a persoanelor autorizate şi doar la datele personale prestabilite pentru acces);

k) marcarea informaţiilor ce conţin date personale;

l) evidenţa activităţilor, evenimentelor şi/sau acţiunilor înregistrate de sistemul de audit a securităţii în sistemele de date personale va fi păstrată pentru o perioadă de 5 ani;

m) gestionarea incidentelor de securitate a datelor personale, în conformitate cu art. 37 şi 38;

n) efectuarea anuală, sau ori de câte ori este necsară a controalelor interne de securitate (identificarea şi analiza vulnerabilităţilor sistemelor de evidenţa gestionate, verificarea respectării măsurilor de securitate implementate şi aprecierea periodică ale eficacităţii măsurilor tehnice şi organizatorice pentru a garanta securitatea datelor personale);

o) asigurarea măsurilor de securitate stabilite în acest capitol urmează să fie efectuată şi în cazul utilizării mediilor virtuale.

(2) La evaluarea nivelului adecvat de securitate, se va ţine seama în special de riscurile de distrugere, pierdere, modificare, divulgare sau acces neautorizat accidental sau intenţionat la datele personale transmise, stocate sau prelucrate, de alte criterii care pot inluenţa securitatea datelor personale.

(3) Operatorul şi persoana împuternicită de operator iau măsuri pentru a asigura faptul că orice persoană care acţionează sub autoritatea operatorului sau a persoanei împuternicite de operator şi care are acces la date personale nu le prelucrează decât la cererea operatorului, cu excepţia cazului în care această obligaţie îi revine în temeiul legislaţiei.

(4) Descrierea detaliată a măsurilor de securitate a prelucrării datelor personale, la necesitate se stabilesc prin hotărîre de Parlament.

(5) Operatorul, operatorul asociat, persoana împuternicită de operator, destinatarul, precum şi entităţile care nu sunt considerate a fi destinatari, terţul, indiferent de tipul proprietăţii şi domeniul de activitate, forma juridică de organizare, trebuie să pună la dispoziţia Centrului, la cerere, informaţii detaliate despre măsurile de securitate întreprinse. Centru asigură confidenţialitatea acestor informaţii şi nedivulgrea lor.

Articolul 37. Notificarea Centrului în cazul încălcării securităţii datelor personale

(1) În cazul în care are loc o încălcare a securităţii datelor personale, operatorul notifică acest lucru Centrului, fără întârzieri nejustificate, imediat dar nu mai mult de 72 de ore de la data la care a luat cunoştinţă de aceasta, cu excepţia cazului în care nu este susceptibilă să genereze un risc pentru drepturile şi libertăţile subiecţilor de date. În cazul în care Centrul nu a fost notificat în termenul stabilit, notificarea trebuie să fie însoţită de o explicaţie motivată.

(2) Persoana împuternicită de operator înştiinţează operatorul fără întârzieri nejustificate după ce ia cunoştinţă despre o încălcare a securităţii datelor personale.

(3) Notificarea trebuie să conţină:

a) descrierea caracterului încălcării securităţii datelor personale, acolo unde este posibil, categoriile şi numărul aproximativ al subiecţilor de date în cauză, precum şi categoriile şi numărul aproximativ al înregistrărilor de date personale în cauză;

b) numele şi datele de contact ale responsabilului cu protecţia datelor sau ale altui punct de contact de unde se pot obţine mai multe informaţii;

c) descrierea eventualelor consecinţe ale încălcării securităţii datelor personale;

d)măsurile luate sau propuse spre a fi luate de operator pentru a remedia problema încălcării securităţii datelor personale, inclusiv, după caz, măsuri pentru a atenua eventualele efecte adverse ale acesteia;

c) altă informaţie relevantă

(4) Atunci când nu este posibil să se furnizeze informaţiile în acelaşi timp, acestea pot fi furnizate în mai multe etape, fără întârzieri nejustificate.

(5) Operatorul păstrează documente referitoare la toate cazurile de încălcare a securităţii datelor personale, care cuprind o descriere a situaţiei de fapt în care a avut loc încălcarea securităţii datelor personale, a efectelor acesteia şi a măsurilor de remediere întreprinse. Această documentaţie trebuie să permită Centrului să verifice respectarea prezentului articol.

(6) Ţinând cont de prevederile acestui articol, Centrul aprobă prin ordin modul şi termenele de raportare a incidentelor de securitate, precum şi anexele relevante.

Articolul 38. Informarea subiecţilor de date privind încălcarea securităţii protecţiei datelor personale

(1) În cazul în care încălcarea securităţii datelor personale este susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile subiecţilor de date, operatorul informează subiectul de date fără întârzieri nejustificate cu privire la această încălcare.

(2) În informarea transmisă subiecţilor de date prevăzută la alin. (1) se include o descriere într-un limbaj clar şi simplu a caracterului încălcării securităţii datelor personale, precum şi cel puţin informaţiile specificate la art. 37 alin. (3) lit. (b), (c) şi (d).

(3) Informarea subiecţilor menţionată la alin. (1) nu este necesară în cazul în care oricare dintre următoarele condiţii este îndeplinită:

a) operatorul a implementat măsuri de protecţie tehnice şi organizatorice adecvate şi aceste măsuri au fost aplicate datelor personale afectate de încălcarea securităţii datelor personale, în special măsuri prin care se asigură că datele personale devin neinteligibile oricărei persoane care nu este autorizată să le acceseze, cum ar fi criptarea;

b) operatorul a luat măsuri ulterioare care să asigure că riscul ridicat pentru drepturile şi libertăţile subiecţilor de date menţionate la alin. (1) nu mai este susceptibil să se materializeze;

c) ar necesita un efort disproporţionat. În această situaţie, se efectuează în loc o informare publică sau o măsură similară prin care subiecţii datelor să fie informaţi în mod echivalent de eficient.

(4) În cazul în care operatorul nu a comunicat deja încălcarea securităţii datelor personale subiectului de date, Centrul, luând în considerare probabilitatea încălcării datelor personale să genereze un risc ridicat, poate să îi solicite acestuia să facă acest lucru sau poate decide că oricare dintre condiţiile menţionate la alin. (3) sunt îndeplinite.

Articolul 39. Cerinţele pentru accesarea şi publicarea datelor personale

(1) Persoanele care au acces la datele personale sunt obligate să prelucreze datele personale în conformitate cu art. 4 şi 5.

(2) Persoana are dreptul să acceseze informaţii, inclusiv datele personale, în următoarele cazuri:

a) prelucrarea se referă la date făcute publice în mod voluntar şi manifest de către subiectul de date;

b) datele personale au fost anonimizate;

c) datele personale au fost pseudonimizate cu condiţia reducerii riscului de încălcare a protecţiei datelor personale;

d) existenţa unui temei legal.

(3) Prelucrarea datelor personale din surse publice, publicarea sau oferirea spre acces nerestricţionat, nu exclude aceste informaţii de sub obligativitatea asigurării regimului juridic al prelucrării datelor personale prevăzut de prezenta lege.

(4) Autorităţile publice nu au dreptul să transmită informaţii care conţin date personale pentru reutilizare către persoane juridice de drept public sau drept privat, persoane fizice, cu excepţia cazului când există un temei legal în conformitate cu art. 5.

Articolul 40. Evaluarea impactului asupra protecţiei datelor personale

(1) Având în vedere natura, domeniul de aplicare, contextul şi 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

şi libertăţile subiecţilor de date, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operaţiunilor de prelucrare prevăzute asupra protecţiei datelor personale. O evaluare unică poate aborda un set de operaţiuni de prelucrare similare care prezintă riscuri ridicate similare.

(2) La realizarea unei evaluări a impactului asupra protecţiei datelor, operatorul solicită avizul responsabilului de protecţia datelor, dacă acesta a fost desemnat.

(3) Evaluarea impactului asupra protecţiei datelor menţionată la alin. (1) se impune, în special, în cazul:

a) unei evaluări sistematice şi cuprinzătoare a aspectelor personale referitoare la subiecţii de date care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, şi care stă la baza unor decizii care produc efecte juridice privind subiectul de date sau care îl afectează în mod similar într-o măsură semnificativă;

b) prelucrării pe scară largă a unor categorii speciale de date, menţionată la art. 9 alin. (1);

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

(4) Centru stabileşte şi publică pe pagina web oficială lista tipurilor de operaţiuni de prelucrare care fac obiectul cerinţei de efectuare a unei evaluări a impactului asupra protecţiei datelor personale.

(5) Centrul poate stabili şi publica pe pagina web oficială lista tipurilor de operaţiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecţiei datelor personale.

(6) Evaluarea conţine:

a) o descriere sistematică a operaţiunilor de prelucrare preconizate şi a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

b) o evaluare a necesităţii şi proporţionalităţii operaţiunilor de prelucrare în legătură cu aceste scopuri;

c) o evaluare a riscurilor pentru drepturile şi libertăţile subiecţilor de date menţionată în alin. (1);

d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanţiile, măsurile de securitate şi mecanismele menite să asigure protecţia datelor personale şi să demonstreze conformitatea cu dispoziţiile legislaţiei, luând în considerare drepturile şi interesele legitime ale subiecţilor de date şi ale altor persoane interesate;

e) impactul operaţiunii de prelucrare;

f) şi alte informaţii relevante.

(7) Operatorul solicită, acolo unde este cazul, avizul subiecţilor de date sau a reprezentanţilor acestora privind această prelucrare, fără a aduce atingere protecţiei intereselor comerciale sau publice ori securităţii operaţiunilor de prelucrare.

(8) Atunci cînd prelucrarea în temeiul art. 5 alin. (1) lit. c) şi e) are un temei juridic care reglementează operaţiunea de prelucrare specifică sau setul de operaţiuni specifice în cauză şi doar cu condiţia că s-a efectuat o evaluare a

impactului asupra protecţiei datelor ca parte a unei evaluări a impactului general în contextul adoptării respectivului temei juridic, alineatele (1) - (7) nu se aplică.

(9) Operatorul, acolo unde este necesar, efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecţiei datelor, cel puţin atunci când are loc o modificare a riscului reprezentat de operaţiunile de prelucrare.

Articolul 41. Consultarea prealabilă

(1) Operatorul consultă Centrul înainte de prelucrare atunci când evaluarea impactului asupra protecţiei datelor prevăzută la art. 40 indică faptul că prelucrarea ar genera un risc ridicat în absenţa unor măsuri luate de operator pentru atenuarea riscului.

(2) Atunci când consideră că prelucrarea prevăzută 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 consultare în scris operatorului şi, după caz, persoanei împuternicite de operator, în cel mult 2 luni de la primirea cererii de consultare, şi îşi poate utiliza oricare dintre competenţele menţionate de prezenta lege şi Legea Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova. Această perioadă poate fi prelungită cu cel mult 2 luni, ţinându-se seama de complexitatea prelucrării prevăzute. Centrul informează operatorul şi, după caz, persoana împuternicită de operator, în termen de o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când Centrul va obţinut informaţiile pe care le-a solicitat în scopul consultării.

(3) Pentru consultarea prealabilă a Centrului, operatorul furnizează acestuia:

a) dacă este cazul, responsabilităţile respective ale operatorului, ale operatorilor asociaţi şi ale persoanelor împuternicite de operator implicate în prelucrare, în special pentru prelucrarea în cadrul unui grup de întreprinderi;

b) scopurile şi mijloacele prelucrării intenţionate;

c) măsurile şi garanţiile furnizate pentru a proteja drepturile şi libertăţile subiecţilor de date în temeiul prezentei legi;

d) dacă este cazul, datele de contact ale responsabilului cu protecţia datelor;

e) evaluarea impactului privind protecţia datelor prevăzută la art. 40; şi

f) orice alte informaţii solicitate de Centru.

(4) Autorităţile de drept public remit în mod obligatoriu spre avizare Centrului proiectele de acte normative care vizează sau implică prelucrarea datelor personale, inclusiv în ceea ce priveşte prelucrarea datelor în domeniul ordinii publice, securităţii statului, protecţiei sociale şi sănătăţii publice.

(5) Prin derogare de la alin. (1), operatorul este obligat de a consulta Centrul şi de a obţine în prealabil autorizarea din partea acestuia în legătură cu prelucrarea datelor personale în vederea îndeplinirii unei sarcini exercitate de

acesta în interes public, inclusiv prelucrarea în legătură cu ordinea publică, protecţia socială şi sănătatea publică.

Articolul 42. Desemnarea responsabilului de protecţia datelor personale

(1) Operatorul şi persoana împuternicită de operator desemnează responsabili de protecţia datelor personale ori de cîte ori:

a) prelucrarea este efectuată de o autoritate publică sau o instituţie ce prestează servicii publice, cu excepţia celei de înfăptuire a justiţiei.

b) activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în operaţiuni de prelucrare care, prin natura, domeniul de aplicare şi/sau scopurile lor, necesită o monitorizare periodică şi sistematică a subiecţilor de date, pe scară largă;

c) activităţile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, menţionată la art. 9.

(2) Un grup de întreprinderi, asociaţii, concerne, consorţii numi un responsabil unic de protecţia datelor, cu condiţia ca acesta să fie uşor accesibil pentru fiecare întreprindere.

(3) În cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau o instituţie publică, poate fi desemnat un responsabil unic de protecţia datelor personale pentru mai multe dintre aceste autorităţi sau organe care nu au personalitate juridică distinctă, luînd în considerare structura organizatorică şi dimensiunea acestora.

(4) În alte cazuri decât cele menţionate la alin. (1), operatorul sau persoana împuternicită de operator ori asociaţiile şi alte instituţii care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde actul normativ solicită acest lucru, desemnează un responsabil de protecţia datelor. Responsabilul de protecţia datelor personale poate să acţioneze în favoarea unor astfel de asociaţii şi alte instituţii care reprezintă operatori sau persoane împuternicite de operatori.

(5) Responsabilii de protecţia datelor personale sînt desemnaţi pe baza calităţilor profesionale şi, în special, a cunoştinţelor speciale în domeniul protecţiei datelor sau securităţii informaţionale, precum şi pe baza capacităţii de a îndeplini sarcinile prevăzute la art. 44.

(6) Responsabilii de protecţia datelor personale pot fi membri ai personalului operatorului sau persoanei împuternicite de operator sau pot să îşi îndeplinească sarcinile în baza unui contract civil.

(7) Operatorul sau persoana împuternicită de operator publică pe pagina web oficială şi la sediul său datele de contact ale responsabililor de protecţia datelor.

(8) Operatorul sau persoana împuternicită de operator, organele de ocrotire a legii în dependenţă de numărul de angajaţi, de volumul şi de categoriile de date personale prelucrate şi riscuri, pot crea subdiviziuni structurale responsabile de protecţia datelor.

Articolul 43. Funcţia responsabilului de protecţia datelor personale

(1) Operatorul şi persoana împuternicită de operator se asigură că responsabilul de protecţia datelor personale este implicat în mod corespunzător şi în timp util în toate aspectele legate de protecţia datelor personale.

(2) Operatorul şi persoana împuternicită de operator sprijină responsabilii de protecţia datelor personale în îndeplinirea sarcinilor menţionate la art. 44, asigurîndu-le resursele necesare pentru executarea acestor sarcini în vederea asigurării accesului la datele personale, la operaţiunile de prelucrare, inclusiv la documentele ce reglementează aceste operaţiuni. Deasemenea, este necesară asigurarea resurselor pentru menţinerea şi creşterea cunoştinţelor lor de specialitate.

(3) Operatorul şi persoana împuternicită de operator se asigură că responsabilii de protecţia datelor personale nu primesc nici un fel de indicaţii în ceea ce priveşte îndeplinirea acestor sarcini. Aceştia nu pot fi demişi sau sancţionaţi de către operator sau de persoana împuternicită de operator pentru îndeplinirea legitimă a sarcinilor sale.

(4) Responsabilul cu protecţia datelor personale răspunde direct în faţa persoanei din cel mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

(5) Subiecţii de date pot contacta responsabilul de protecţia datelor personale cu privire la toate chestiunile legate de prelucrarea datelor lor şi la exercitarea drepturilor lor în temeiul prezentei legi.

(6) Responsabilul de protecţia datelor personale în cadrul îndeplinirii atribuţiilor, au obligaţia de a asigura confidenţialitatea informaţiilor la care au acces în modul prevăzut de lege chiar şi după eliberarea din funcţie.

(7) Responsabilul de protecţia datelor personale poate îndeplini şi alte sarcini şi atribuţii. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini şi atribuţii nu generează un conflict de interese sau nu împiedică, obstrucţionează în nici un fel executarea sarcinilor de bază.

Articolul 44. Sarcinile responsabilului de protecţia datelor personale

(1) Responsabilii de protecţia datelor personale are următoarele sarcini:

a) informarea şi consultarea operatorului, sau a persoanei împuternicite de operator, precum şi a angajaţilor care se ocupă de prelucrarea datelor personale cu privire la obligaţiile care le revin în temeiul prezentei legi şi al altor dispoziţii normative referitoare la protecţia datelor personale;

b) monitorizarea respectării prezentei legi, a altor dispoziţii normative referitoare la protecţia datelor personale şi a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce priveşte protecţia datelor personale, inclusiv alocarea responsabilităţilor şi acţiunile de sensibilizare şi de formare a personalului implicat în operaţiunile de prelucrare, precum şi auditurile aferente;

c) consultarea, la cerere, în ceea ce priveşte evaluarea impactului asupra protecţiei datelor personale şi monitorizarea funcţionării acesteia, în conformitate cu art. 40;

d) cooperarea cu Centrul;

e) asumarea rolului de punct de contact cu Centrul privind aspectele legate de prelucrare, inclusiv activităţile menţionate la art. 41, precum şi, dacă este cazul, consultarea cu privire la orice altă chestiune

f) alte sarcini prevăzute de lege.

(2) La îndeplinirea sarcinilor sale, responsabilul de protecţia datelor personale ţine seama în mod corespunzător de riscul operaţiunilor de prelucrare, luînd în considerare natura, domeniul de aplicare, contextul şi scopurile prelucrării.

(3) Responsabilii de protecţia datelor personale sînt obligaţi de a raporta, în scris sau electronic, conducerii operatorului sau a persoanei împuternicite ori de cîte ori vor constata o anumită încălcare a principiilor de protecţie a datelor, inclusiv situaţiile care pot genera riscuri sau pot aduce atingere drepturilor subiecţilor de date, condiţiilor de conformitate şi securitate la prelucrarea datelor personale.

Articolul 45. Codurile de conduită

(1) Asociaţiile şi alte organisme care reprezintă categoriile de operatori sau persoane împuternicite de operatori pot pregăti coduri de conduită pentru a contribui la aplicarea corectă a prezentei legi, ţinând seama de caracteristicile specifice ale diferitelor sectoare de prelucrare sau prin modificarea sau extinderea celor existente pentru a specifica modul de aplicare a prezentei legi, cum ar fi:

a) prelucrarea în mod echitabil şi transparent;

b) interesele legitime urmărite de operatori în contexte specifice;

c) colectarea de date personale;

d) pseudonimizarea datelor personale;

e) informarea publicului şi a subiecţilor de date;

f) exercitarea drepturilor subiecţilor de date;

g) informarea şi protecţia copilului şi modul în care trebuie obţinut consimţământul reprezentantului legal al acestuia;

h) măsurile şi procedurile privind responsabilitatea operatorului de date, în special menţinerea principiilor de protecţie a datelor personale din momentul conceperii şi prin confidenţialitatea prestabilită şi măsurile de securitate pentru prelucrarea datelor personale în conformitate cu art. 29, 30 şi 36;

i) notificarea Centrului privind încălcarea securităţii datelor personale şi informarea subiecţilor de date cu privire la astfel de încălcări;

j) transferul de date personale către alte ţări sau organizaţii internaţionale;

k) procedurile extrajudiciare şi alte proceduri de soluţionare a litigiilor dintre operatori şi subiecţii de date în ceea ce priveşte prelucrarea, fără a aduce

atingere drepturilor subiectului de date de a depune o cerere la Centru sau de a contesta decizia operatorului sau a persoanei împuternicite de operator.

(2) Codul de conduită trebuie să includă mecanisme care să permită unui organism care are un nivel corespunzător de expertiză în legătură cu obiectul codului să efectueze o monitorizare obligatorie a respectării dispoziţiilor sale de către operatori sau persoane împuternicite de operatori care se angajează să îl aplice fără a aduce atingere sarcinilor şi competenţelor Centrului.

(3) La codurile de conduită aprobate în temeiul alin. (4) şi care au valabilitate generală în temeiul alin. (7), pot adera nu numai operatorii sau persoanele împuternicite de operatori care fac obiectul dispoziţiilor prezentei legi, ci şi operatorii sau persoanele împuternicite de operatori care nu fac obiectul reglementării prezentei legi, pentru a oferi garanţii adecvate în cazul transferurilor transfrontaliere în condiţiile menţionate la art. 51, alin. (2), lit. e). Aceşti operatori sau persoane împuternicite de operatori îşi asumă angajamente obligatorii şi executorii prin intermediul instrumentelor contractuale sau al altor instrumente obligatorii din punct de vedere juridic în scopul aplicării garanţiilor adecvate, inclusiv a drepturilor conexe ale subiecţilor de date.

(4) Asociaţiile şi alte organisme care reprezintă categoriile de operatori sau persoane împuternicite de operatori, care intenţionează să elaboreze un cod de conduită, să modifice sau să extindă un cod existent, transmit proiectul de modificare sau de extindere în adresa Centrului, care emite un aviz cu privire la respectarea prezentei legi, modificarea sau extinderea acestuia şi dacă se constată că acesta oferă garanţii adecvate aprobă, înregistrează şi publică codul de conduită.

(5) În cazul în care Centrul, la evaluarea proiectului, constată nerespectarea prezentei legi, remite asociaţiei şi altui organism menţionat la alin. (4) un aviz în care se constată deficienţele ce trebuie înlăturate în proiectul de cod, în termenul specificat în aviz.

(6) În cazul în care asociaţia şi un alt organism menţionat la alin. (4) elimină deficienţele constatate în aviz în termenul stabilit, Centrul aprobă, înregistrează şi publică codul de conduită.

(7) În cazul în care un proiect de cod de conduită, de modificare sau de extindere are legătură cu activităţile de prelucrare din alte ţări, înainte de aprobare, Centrul îl poate transmite, autorităţii de supraveghere din ţările respective spre avizare.

(8) Prezentul articol nu se aplică prelucrării efectuate de autorităţile şi instituţiile publice.

Articolul 46. Monitorizarea codurilor de conduită aprobate

(1) Fără a aduce atingere sarcinilor şi competenţelor Centrului, monitorizarea respectării unui cod de conduită în temeiul art. 45 poate fi realizată de un organism care dispune de un nivel adecvat de expertiză în legătură cu obiectul codului şi care este acreditat de Centru.

(2) Organismul menţionat la alin. (1) poate fi acreditat pentru a monitoriza conformitatea cu un cod de conduită dacă:

a) a demonstrat Centrului într-un mod satisfăcător independenţa şi expertiza sa în legătură cu obiectul Codului de conduită;

b) a stabilit proceduri pentru a evalua eligibilitatea operatorilor şi a persoanelor împuternicite de operatori de a aplica codul, de a monitoriza conformitatea cu codul şi de a revizui periodic funcţionarea acestuia;

c) a instituit proceduri şi structuri pentru a gestiona cererile privind încălcările codului sau modul în care codul a fost sau este implementat de către un operator sau persoana împuternicită de operator şi pentru a asigura transparenţa acestor proceduri şi structuri pentru subiecţii datelor şi pentru public şi a demonstrat Centrului, într-o manieră satisfăcătoare, că sarcinile şi atribuţiile sale nu creează conflicte de interese.

(3) Fără a aduce atingere sarcinilor şi competenţelor Centrului organismul este supus unor garanţii adecvate, ia măsurile corespunzătoare în cazul încălcării de către un operator sau de către persoana împuternicită de operator, inclusiv suspendarea sau excluderea acelui operator sau persoanei împuternicite de operator din cod. Organismul informează Centrul cu privire la aceste măsuri şi motivele care l-au determinat să facă acest lucru.

(4) Centrul revocă acreditarea organismului în cazul în care condiţiile de acreditare nu mai sunt îndeplinite ori măsurile luate de organismul competent în cauză încalcă această lege sau la cererea organismului.

Articolul 47. Certificarea

(1) Fiecare operator sau persoană împuternicită de operator poate obţine certificate sau mărci cu scopul de a demonstra că operaţiunile de prelucrare a datelor personale efectuate de operator sau persoana împuternicită de operator respectă prezenta lege.

(2) Certificarea este voluntară şi disponibilă printr-un proces transparent.

(3) Se instituie mecanisme de certificare a protecţiei datelor personale sau mărci aprobate prin prezenta lege nu numai pentru a fi respectate de operatori sau persoane împuternicite de operatori care fac obiectul prezentei legi, ci şi pentru a demonstra existenţa unor garanţii adecvate furnizate de operatori sau persoane împuternicite de operatori care nu fac obiectul acestei legi în conformitate cu art. 2, în contextul transmiterilor transfrontaliere către alte ţări sau organizaţii internaţionale în condiţiile menţionate la art. 50 alin. (2) lit. f). Aceşti operatori sau persoane împuternicite de operatori îşi asumă angajamente obligatorii şi executorii prin intermediul instrumentelor contractuale sau altor instrumente obligatorii din punct de vedere juridic în scopul aplicării garanţiilor adecvate, inclusiv a drepturilor subiecţilor de date.

(4) Operatorul sau persoana împuternicită de operator care supune activităţile sale de prelucrare mecanismului de certificare oferă organismului de certificare, după caz, Centrului toate informaţiile necesare pentru

desfăşurarea procedurii de certificare, precum şi accesul la activităţile de prelucrare respective.

(5) Organismul de certificare este responsabil de efectuarea unei evaluări adecvate pentru a elibera sau retrage certificatul sau mărcile.

(6) Organismele de certificare transmit Centrului temeiurile pentru eliberarea sau retragerea certificatului sau mărcii necesare.

(7) Certificarea se eliberează unui operator sau persoanei împuternicite de operator pentru o perioadă de trei ani şi poate fi reînnoită în aceleaşi condiţii, în situaţiile în care cerinţele relevante să fie în continuare îndeplinite. Certificarea este retrasă, după caz, de către organismul de certificare sau de către Centru dacă cerinţele de certificare nu mai sunt îndeplinite.

(8) Certificarea în temeiul prezentului articol nu reduce responsabilitatea operatorului sau a persoanei împuternicite de operator de a se conforma prezentei legi şi nu aduce atingere sarcinilor şi competenţelor Centrului.

(9) Modul de eliberare a certificatelor sau mărcilor, precum şi modelul acestora se aprobă de Centru.

Articolul 48. Organismele de certificare

(1) Organismele de certificare sunt acreditate de către Centru. La solicitarea organismului de certificare, Centrul eliberează şi reînnoieşte acreditarea organismului de certificare care are un nivel adecvat de competenţă în domeniul protecţiei datelor personale.

(2) Organismul de certificare este acreditat în conformitate cu alineatul respectiv numai dacă:

a) a demonstrat Centrului, în mod satisfăcător, independenţa şi expertiza sa în legătură cu obiectul de certificare;

b) s-a angajat să respecte criteriile aprobate de Centru;

c) a stabilit proceduri pentru emiterea, revizuirea periodică şi retragerea certificării în domeniul protecţiei datelor personale;

d) a instituit proceduri şi structuri pentru gestionarea cererilor privind încălcările de certificare sau modul în care certificarea a fost sau este aplicată de către operator sau persoana împuternicită de operator şi asigurând că aceste proceduri şi structuri să fie transparente pentru subiecţii datelor şi pentru public;

e) a demonstrat Centrului, în mod satisfăcător, că sarcinile şi atribuţiile sale nu creează conflicte de interese.

(3) Acreditarea organismelor de certificare menţionate la alin. (1) şi (2) se efectuează pe baza criteriilor aprobate de Centru care se publică în Monitorul Oficial.

(4) Acreditarea se eliberează pentru o perioadă de cinci ani şi poate fi reînnoită în aceleaşi condiţii, dacă organismul de certificare îndeplineşte cerinţele prevăzute în prezentul articol şi informaţia se publică în Monitorul Oficial.

(5) Fără a aduce atingere dispoziţiilor Capitolului IX, Centrul retrage acreditarea acordată unui organism de certificare în temeiul alin. (1), în cazul în care condiţiile de acreditare nu sunt sau nu mai sunt îndeplinite ori măsurile luate de organismul de certificare încalcă prezenta lege.

CAPITOLUL VI
TRANSMITEREA TRASNFRONTALIERĂ A DATELOR PERSONALE

Articolul 49. Transmiterea transfrontalieră a datelor personale

(1) Transmiterea transfrontalieră a datelor personale care constituie obiectul prelucrărilor sau care sunt colectate în scopul de a fi supuse prelucrării către un alt stat, se efectuiază pe orice suport sau prin orice mijloc.

(2) Datele personale destinate transmiterii către un alt stat sunt protejate în conformitate cu prezenta lege.

(3) Transferul de date personale către o altă ţară sau o organizaţie internaţională se poate realiza atunci când Centrul a emis o decizie că o ţară, un teritoriu ori unul sau mai multe sectoare specificate din acea ţară sau organizaţia internaţională în cauză asigură un nivel de protecţie adecvat. Transferurile realizate în aceste condiţii nu necesită autorizări speciale. Decizia va prevedea un mecanism de revizuire periodică, cel puţin o dată la patru ani, care ia în considerare toate evoluţiile relevante din această ţară sau organizaţie internaţională.

(4) Decizia privind nivelul adecvat de protecţie se stabileşte de Centru ţinându-se cont de următoarele condiţii:

a) statul de drept, respectarea drepturilor omului şi a libertăţilor fundamentale, legislaţia relevantă, atât generală, cât şi sectorială, inclusiv privind ordinea publică, apărarea, securitatea naţională şi a statului, legislaţia penală şi civilă, precum şi accesul autorităţilor publice la datele personale, punerea în aplicare a acestei legislaţii, normele de protecţie a datelor personale, normele profesionale şi măsurile de securitate, inclusiv normele privind transferul ulterior de date personale către o altă ţară sau organizaţie internaţională, care sunt respectate în ţara respectivă sau în organizaţia internaţională respectivă, jurisprudenţa, precum şi existenţa unor drepturi efective şi opozabile ale subiecţilor de date şi existenţa instrumentelor aplicabile în scopul reparării efective pe cale administrativă şi judiciară pentru subiecţii de date ale căror date personale sunt transferate;

b) existenţa şi funcţionarea eficientă a unei autorităţi de supraveghere independente în această ţară sau sub jurisdicţia cărora intră o organizaţie internaţională, cu responsabilitate pentru asigurarea şi impunerea respectării normelor de protecţie a datelor personale, incluzând competenţe adecvate de asigurare a respectării aplicării, pentru acordarea de asistenţă şi consultarea

subiecţilor de date cu privire la exercitarea drepturilor acestora şi pentru cooperarea cu Centrul; şi

c) angajamentele internaţionale la care a aderat ţara sau organizaţia internaţională în cauză sau alte obligaţii care decurg din convenţii sau instrumente obligatorii din punct de vedere juridic, precum şi din participarea acesteia la sisteme multilaterale sau regionale, mai ales în domeniul protecţiei datelor personale.

(5) La stabilirea nivelului adecvat de protecţie Centrul ia în considerare deciziile Comisiei Uniunii Europene, dacă o ţară terţă, un teritoriu sau unul sau mai multe sectoare specificate în respectiva ţară terţă sau o organizaţie internaţională asigură un nivel adecvat de protecţie.

(6) În cazul în care informaţiile disponibile dezvăluie, în special în urma revizuirii menţionate la alin. (3), că o ţară, un teritoriu sau un sector specificat din acea ţară sau o organizaţie internaţională nu mai asigură un nivel de protecţie adecvat în sensul alin. (4) din prezentul articol, Centrul, dacă este necesar, abrogă, modifică sau suspendă, prin intermediul altui act administrativ, decizia menţionată la alin. (3) fără a avea efect retroactiv.

(7) O decizie luată în temeiul alin. (4) nu aduce atingere transferurilor de date personale către ţară, un teritoriu sau unul sau mai multe sectoare specificate din acea ţară sau către organizaţia internaţională în cauză în conformitate cu art. 50-53.

(8) Centru publică în Monitorul Oficial şi pe pagina web oficială lista ţărilor, a teritoriilor şi sectoarelor specificate dintr-o ţară şi a organizaţiilor internaţionale în cazul cărora a decis că nivelul de protecţie adecvat este asigurat sau nu mai este asigurat.

(9) Transmiterile transfrontaliere de date personale către un stat membru al Spaţiului Economic European nu necesită o autorizaţie din partea Centrului.

(10) Operatorul şi persoana împuternicită de operator sunt obligaţi să prelucreze datele personale gestionate în sisteme de evidenţă aflate în afara teritoriului Republicii Moldova în conformitate cu prevederile prezentei legi şi să întreprindă măsurile ce se impun a fi efectuate în vederea înlăturării încălcărilor admise la prelucrarea acestor date.

(11) Operatorul şi persoana împuternicită de acesta poartă răspundere în conformitate cu prezenta lege, în cazul transferului transfrontalier de date personale.

Articolul 50. Transmiterea transfrontalieră în baza garanţiilor adecvate

(1) În absenţa unui nivel adecvat de protecţie a datelor personale în sensul art. 49 alin. (3), operatorul sau persoana împuternicită de operator poate transfera date personale, într-o ţară care nu este membru al Spaţiului Economic European sau către o organizaţie internaţională, numai dacă operatorul sau persoana împuternicită de operator a oferit garanţii adecvate şi

cu condiţia să existe drepturi opozabile şi căi de atac eficiente pentru subiecţii de date.

(2) În conformitate cu alin. (1), garanţiile adecvate pot fi furnizate fără să fie nevoie de autorizaţie specifică din partea Centrului, prin:

a) un instrument obligatoriu din punct de vedere juridic şi executoriu între autorităţile sau organismele publice;

b) reguli corporatiste obligatorii în conformitate cu art. 51;

c) clauze standard de protecţie a datelor personale adoptate de Centru;

d) clauze standard de protecţie a datelor personale adoptate de către Comisia Europeană sau de către alte autorităţi responsabile din Uniunea Europeană, care, după caz, sunt acceptate de Centru;

e) un cod de conduită aprobat în conformitate cu art. 45, însoţit de un angajament obligatoriu şi executoriu din partea operatorului sau a persoanei împuternicite de operator din altă ţară de a aplica garanţii adecvate, inclusiv cu privire la drepturile persoanelor vizate;

f) un mecanism de certificare aprobat în conformitate cu art. 47, împreună cu angajamentele obligatorii şi executorii ale operatorului sau persoanei împuternicite de operator din ţara de a aplica garanţiile corespunzătoare, inclusiv în ceea ce priveşte drepturile subiecţilor de date.

(3) Sub rezerva autorizaţiei din partea Centrului, garanţiile corespunzătoare menţionate la alin. (1) pot fi prevăzute, în special prin:

a) clauze contractuale între operator sau persoana împuternicită de operator şi operatorul, persoana împuternicită de operator sau destinatarul datelor personale din altă ţară sau organizaţia internaţională;

b) dispoziţiile care trebuie introduse în acordurile administrative între autorităţile sau organismele publice care includ drepturi opozabile şi efective ale subiecţilor de date.

(4) În cazurile specificate la alin. (3), Centrul va ţine cont de mecanismul pentru asigurarea coerenţei existent în Uniunea Europeană.

(5) Operatorul şi persoana împuternicită de acesta poartă răspundere pentru încălcarea prevederilor prezentei legi în cazul transferului transfrontalier de date personale, chiar dacă există garanţii adecvate privind transferul transfrontalier de date personale.

Articolul 51. Reguli corporatiste obligatorii

(1) Centrul aprobă reguli corporatiste obligatorii, cu condiţia că acestea:

a) sunt obligatorii şi se aplică fiecărui membru interesat al grupului de întreprinderi sau grupului de întreprinderi care desfăşoară o activitate economică comună, inclusiv angajaţilor acestora, precum şi sunt puse în aplicare de către membrii în cauză;

b) conferă în mod expres drepturi opozabile subiecţilor datelor în ceea ce priveşte prelucrarea datelor lor personale;

c) să îndeplinească cerinţele prevăzute la alin. (2).

(2) Regulile corporatiste obligatorii cuprind:

a) structura şi datele de contact ale grupului de întreprinderi sau ale grupului de întreprinderi implicate într-o activitate economică comună şi ale fiecărui membru al său;

b) transferurile sau seturile de transferuri de date, inclusiv categoriile de date personale, tipul de prelucrare şi scopurile acesteia, tipul de subiecţi de date vizaţi şi identificarea ţării sau ţărilor în care datele vor fi transferate;

c) caracterul lor obligatoriu din punct de vedere juridic, atât pe plan intern, cât şi pe plan internaţional;

d) aplicarea principiilor generale de protecţie a datelor, în special limitarea scopului, minimizarea datelor, perioadele de stocare limitate, calitatea datelor, protecţia datelor din momentul conceperii şi în faza implicită, temeiul juridic pentru prelucrare, prelucrarea categoriilor speciale de date personale, securitatea datelor şi cerinţele privind transferurile viitoare către organismele care nu fac obiectul normelor corporatiste obligatorii;

e) drepturile subiecţilor de date în ceea ce priveşte prelucrarea şi mijloacele de exercitare a acestor drepturi, inclusiv dreptul de a nu face obiectul deciziilor bazate exclusiv pe prelucrarea automatizată, inclusiv crearea de profiluri în conformitate cu art. 27, dreptul de a depune o cerere la Centru în conformitate cu art. 78, de a solicita despăgubiri în faţa instanţelor competente din Republica Moldova în conformitate cu art. 89 şi, după caz, compensarea pentru încălcarea normelor corporatiste obligatorii în conformitate cu art. 90;

f) acceptarea de către operatorul sau persoana împuternicită de operator stabilită în Republica Moldova a răspunderii pentru orice încălcare a normelor corporatiste obligatorii de către orice membru în cauză care nu îşi are sediul în Republica Moldova. Operatorul sau persoana împuternicită de operator este scutit de această răspundere, integral sau parţial, numai dacă dovedeşte că acel membru nu este responsabil pentru evenimentul care a cauzat prejudiciul;

g) modalitatea în care informaţiile privind regulile corporatiste obligatorii, în special cele specificate la lit. d), e) şi f), sunt furnizate subiecţilor de date, în completarea informaţiilor menţionate la art. 18 şi 19;

h) sarcinile oricărui responsabil de protecţia datelor personale desemnat în conformitate cu art. 42 sau ale oricărei alte persoane sau entităţi însărcinate cu monitorizarea respectării regulilor corporatiste obligatorii din cadrul grupului de întreprinderi sau al grupului de întreprinderi care desfăşoară o activitate economică comună, a activităţilor de formare a personalului şi gestionare a cererilor;

i) procedurile de formulare a cererilor;

j) mecanismele din cadrul grupului de întreprinderi sau al grupului de întreprinderi care desfăşoară o activitate economică comună pentru a asigura verificarea conformităţii cu regulile corporatiste obligatorii. Aceste mecanisme includ audituri privind protecţia datelor şi metode pentru asigurarea unor acţiuni corective pentru a proteja drepturile subiectului datelor. Rezultatele unei astfel de verificări ar trebui să fie comunicate persoanei sau entităţii menţionate la lit. h) şi consiliului de administrare al întreprinderii care exercită

controlul unui grup de întreprinderi sau al unui grup de întreprinderi care desfăşoară o activitate economică comună şi ar trebui să fie puse la dispoziţie la solicitarea Centrului.

k) mecanismele de raportare şi înregistrare a modificărilor aduse regulilor şi de raportare a acestor modificări Centrului;

l) mecanismul de cooperare cu Centrul pentru a asigura respectarea de către orice membru al grupului de întreprinderi sau grupului de întreprinderi care desfăşoară o activitate economică comună, în special prin punerea la dispoziţia Centrului a rezultatelor verificărilor măsurilor menţionate la lit. j);

m) mecanismele de raportare către Centru a cerinţelor legale impuse unui membru al grupului de întreprinderi sau unui grup de întreprinderi care desfăşoară o activitate economică comună într-o ţară din afara Spaţiului Economic European sau o ţară terţă, un teritoriu sau unul sau mai multe sectoare specificate în respectiva ţară terţă sau o organizaţie internaţională asigură un nivel adecvat de protecţie recunoscută de Comisia Europeană, care ar putea avea în fond efecte negative asupra garanţiilor oferite de normele corporatiste obligatorii;

n) formarea corespunzătoare în domeniul protecţiei datelor a personalului care are acces permanent sau periodic la datele personale;

o) alte aspecte relevante.

(3) Centrul poate specifica formatul şi procedurile aplicabile regulilor corporatiste obligatorii în sensul prezentului articol, de asemenea, poate lua în consideraţie orice decizie emisă de Comisia Europeană cu privire la chestiuni similare.

Articolul 52. Transferurile sau divulgările de informaţii neautorizate

(1) Fără a aduce atingere prevederilor art. 49 şi 50, transferul datelor personale poate fi efectuat în condiţiile prevăzute de o lege specială sau de un tratat sau acord internaţional ratificat de Republica Moldova, în special dacă transferul este efectuat în scopul prevenirii sau investigării infracţiunilor. Legea specială, tratatul sau acordul internaţional trebuie să conţină garanţii suficiente pentru protecţia drepturilor persoanelor care fac obiectul datelor personale.

(2) Orice hotărâre a unei instanţe judecătoreşti şi orice hotărâre a unei autorităţi administrative a unei alte ţări care impune operatorului sau persoanei împuternicite de operator stabilită în Republica Moldova să transfere sau să dezvăluie date personale în această ţară pot fi recunoscute sau pot fi executorii doar dacă se bazează pe un acord internaţional, cum ar fi un tratat de asistenţă juridică reciprocă, în baza unor garanţii adecvate stabilite de Centru, în vigoare între ţara solicitantă şi Republica Moldova. Aceasta nu aduce atingere altor temeiuri de transfer în temeiul prezentului capitol.

Articolul 53. Derogări pentru situaţii specifice

(1) În absenţa unei decizii privind caracterul adecvat de protecţie în conformitate cu art. 49 alin. (3) sau a unor garanţii adecvate în conformitate cu

art. 50, inclusiv a normelor corporatiste obligatorii, un transfer sau un set de transferuri de date personale către o altă țară sau o organizație internațională poate să aibă loc numai în una dintre următoarele condiții:

a) subiectul de date și-a exprimat în mod explicit acordul cu privire la transferul propus, după ce a fost informat asupra posibilelor riscuri pe care astfel de transferuri le pot implica pentru subiectul de date 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 subiectul de date și persoana care efectuează controlul sau punerea în aplicare a măsurilor precontractuale luate la cererea subiectului de date;

c) transferul este necesar pentru încheierea sau executarea unui contract încheiat în interesul subiectului datelor între operator și o altă persoană fizică sau juridică;

d) transferul este necesar din motive importante de interes public;

e) transferul este necesar pentru stabilirea, exercitarea sau apărarea unui drept în instanță;

f) transferul este necesar pentru a proteja interesele vitale ale subiectului de date sau ale altor persoane, în cazul în care subiectul de date nu are capacitate fizică sau juridică de a-și exprima consimțământul;

g) transferul se face dintr-un registru care, potrivit unei legi din Republica Moldova, are ca scop informarea publicului și care este deschis spre consultare fie publicului în general, fie unei persoane care poate demonstra un interes legitim, dar numai în măsura în care condițiile prevăzute de lege pentru consultare sunt îndeplinite în cazul particular.

(2) În cazul în care un transfer nu ar putea să se întemeieze pe o dispoziție prevăzută la art. 49, inclusiv dispoziții privind reguli corporatiste obligatorii, și nu este aplicabilă niciuna dintre derogările pentru situații specifice prevăzute la alin. (1), un transfer către o altă țară sau o organizație internațională poate avea loc numai în cazul în care transferul nu este repetitiv, se referă doar la un număr limitat de subiecți de date, este necesar în scopul realizării intereselor legitime majore urmărite de operator asupra căruia nu prevalează interesele sau drepturile și libertățile subiectului de date și operatorul a evaluat toate circumstanțele aferente transferului de date personale și, pe baza acestei evaluări, a prezentat garanții corespunzătoare în ceea ce privește protecția datelor personale. Operatorul informează Centrul cu privire la transfer. Operatorul furnizarea informațiile menționate la art. 18 și 19 și informează subiectul de date 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 personale sau ansamblul categoriilor de date personale 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) şi c) şi alin. (3) nu se aplică activităţilor desfăşurate de autorităţile publice în exercitarea atribuţiilor lor publice, în cazul în care se prelucrează un volum redus de date personale.

(5) Interesul public menţionat la alin. (1) lit. d) se recunoaşte de legislaţia naţională sub incidenţa căruia cade operatorul.

(6) În absenţa unei decizii a Centrului privind caracterul adecvat al nivelului de protecţie, legislaţia din motive de interes public, poate să stabilească în mod expres limitele pentru transferul anumitor categorii de date personale către o ţară din afara Spaţiul Economic European sau o altă ţară terţă, un teritoriu sau unul sau mai multe sectoare specificate în respectiva ţară terţă sau o organizaţie internaţională.

(7) Operatorul sau persoana împuternicită de operator documentează garanţiile corespunzătoare menţionate la alin. (2) în evidenţa menţionată la art. 35.

Articolul 54. Cooperare internaţională în domeniul protecţiei datelor personale

În ceea ce priveşte prelucrarea transfrontalieră a datelor personale, Centrul ia măsurile necesare ca:

a) să elaboreze mecanisme de cooperare internaţională pentru a facilita aplicarea eficientă a legislaţiei privind protecţia datelor personale;

b) să ofere asistenţă reciprocă internaţională în aplicarea legislaţiei privind protecţia datelor personale, inclusiv prin sesizare, notificarea cererilor, asistenţă în materie de investigaţii şi schimb de informaţii, sub rezerva garanţiilor adecvate pentru protecţia datelor personale şi a altor drepturi şi libertăţi fundamentale;

c) să se angajeze cu părţile interesate relevante în cadrul discuţiilor şi activităţilor care vizează promovarea cooperării internaţionale în aplicarea legislaţiei privind protecţia datelor personale;

d) să promoveze schimbul şi documentarea legislaţiei şi a practicilor privind protecţia datelor personale, inclusiv în ceea ce priveşte conflictele jurisdicţionale cu alte ţări.

Capitolul VII
PREVEDERI SPECIALE PRIVIND PRELUCRAREA DATELOR PERSONALE DE CĂTRE ORGANELE DE OCROTIRE A LEGII

Articolul 55. Dispoziţii specifice

(1) În scopurile stabilite la art. 2 alin. (2) lit. d) operatorii - organele de ocrotire a legii vor aplica norme specifice în ceea ce priveşte prelucrarea datelor personale. Prelucrărilor de date personale efectuate de către organele de ocrotire a legii în afara scopurilor stabilite la art. 2 alin. (2) lit. d) se aplică celelalte cerinţe prevăzute de prezenta lege.

(2) Aplicarea normelor specifice nu exclude obligaţia organelor de ocrotire a legii de a respecta celelalte cerinţe ale prezentei legi în situaţia în care nu este prevăzută o reglementare specială.

Articolul 56. Legalitatea prelucrării

(1) Prelucrarea datelor personale de către organele de ocrotire a legii este permisă numai în baza unei legi specifice şi numai în măsura în care această prelucrare este necesară pentru îndeplinirea unei sarcini de către organul de ocrotire a legii în scopurile prevăzute la articolul 2 alin. (2) lit. d).

(2) Prelucrarea datelor personale de către organele de ocrotire a legii în scopurile specifice stabilite la articolul 2 alin. (2) lit. d), poate fi aplicată în alte scopuri decît cele descrise în art. 2 alin. (2) lit. d), în măsura în care operatorul este prevăzut de lege să prelucreze astfel de date şi prelucrarea este necesară şi proporţională cu acest alt scop, în conformitate cu legea.

(3) Actele normative care reglementează domeniului de activitate a organelor de ocrotire a legii trebuie să stipuleze scopul prelucrării datelor personale, categoriile de date personale care urmează să fie prelucrate şi alte detalii referitoare la prelucrarea datelor personale.

(4) Organele de ocrotire a legii vor institui mecanisme interne eficiente de încurajare a denunţării confidenţiale a cazurilor de încălcare a prezentei legi în cadrul acestor organe. În cazul în care cererea de denunţ va fi adresată Centrului, acesta va asigura confidenţialitatea identităţii persoanei care a efectuat denunţul.

Articolul 57. Termenul de stocare şi revizuire

(1) Termenul de stocare a datelor personale se stabileşte corespunzător scopului prelucrării şi se asigură revizuirea periodică a necesităţii de stocare a acestora.

(2) Termenul de stocare trebuie să fie stipulat de o normă specifică prevăzută în legea specială. Dacă legea nu prevede astfel de termen, operatorul va stabili termen corespunzător, după consultarea Centrului.

(3) Operatorul instituie mecanisme procedurale pentru a asigura respectarea termenelor de stocare.

(4) După expirarea termenului de stocare, datele personale se şterg, se distrug sau se transformă în document de arhivă în conformitate cu legislaţia în vigoare.

Articolul 58. Distincţia dintre categorii diferite de subiecţi de date

Operatorul este obligat să facă distincţia clară pe cît posibil, cu argumentarea necesară, la prelucrarea datelor personale ale diferitelor categorii de subiecţi de date, cum ar fi bănuiţii, învinuiţii, martorii, victimele, terţii, persoanele aflate în perioada de probaţiune, condamnaţii, persoanele reţinute, arestate şi altele.

Articolul 59. Distincţia dintre datele personale în baza faptelor şi în bază de evaluări

(1) Organul de ocrotire a legii va face distincţia pe cît posibil, cu argumentarea necesară, între datele personale în baza faptelor şi datele personale în bază de evaluări.

(2) Organul de ocrotire a legii ia toate măsurile necesare pentru a se asigura că datele personale care sunt inexacte, incomplete sau nu mai sunt actuale nu sunt transmise sau puse la dispoziţie. În acest scop, fiecare autoritate competentă verifică, în măsura în care este posibil, calitatea datelor personale înainte ca acestea să fie transmise sau puse la dispoziţie. În măsura în care acest lucru este posibil, în cadrul tuturor transmiterilor de date personale, se adaugă informaţii necesare care permit evaluarea gradului de exactitate, caracterul integral, gradul de fiabilitate şi de actualitate al datelor personale.

(3) În cazul în care se constată transmiterea unor date personale incorecte sau transmiterea unor date personale în mod ilegal, acest lucru se comunică de îndată destinatarului. Într-un astfel de caz, datele personale sunt rectificate sau şterse sau prelucrarea este restricţionată.

Articolul 60. Prelucrarea categoriilor speciale de date personale

Organul de ocrotire a legii prelucrează categorii speciale de date personale numai atunci când este strict necesar, sub rezerva garanţiilor corespunzătoare pentru drepturile şi libertăţile subiectului datelor:

a) dacă este autorizat de o lege specială;

b) întru protejarea vieţii, integrităţii fizice sau a sănătăţii subiectului datelor sau ale altei persoane fizice;

c) atunci când o astfel de prelucrare se referă la datele personale care sunt în mod evident făcute publice de către subiectul de date.

Articolul 61. Procesul decizional individual automatizat inclusiv crearea de profiluri

(1) O decizie întemeiată exclusiv pe prelucrarea automată, inclusiv crearea de profiluri, care produce un efect juridic negativ pentru subiectul de date sau care o afectează în mod semnificativ, este interzisă, cu excepţia cazului în care este autorizată de o lege specială care se aplică organului de ocrotire a legii şi care prevede garanţii adecvate pentru drepturile şi libertăţile subiectului de date, cel puţin dreptul de a obţine intervenţia umană din partea operatorului.

(2) Deciziile menţionate la alin. (1) nu se bazează pe categorii speciale de date personale, cu excepţia datelor personale referitoare la condamnările penale, în cazul în care există măsuri adecvate pentru a proteja drepturile şi libertăţile subiectului de date, precum şi în interesele legitime ale acestuia, cu consultarea Centrului.

(3) Este interzisă crearea de profiluri care conduce la discriminarea subiecţilor de date pe baza unor categorii speciale de date personale.

Articolul 62. Comunicarea şi modalităţile de exercitare a drepturilor subiecţilor de date

(1) Organele de ocrotire a legii transmit gratuit subiectului de date informaţiile în conformitate cu art. 63 şi în legătură cu art. 61, 64 – 67 şi 70 referitoare la prelucrare, într-o formă concisă, inteligibilă şi uşor accesibilă, utilizând un limbaj clar şi simplu. Informaţiile se transmit prin orice mijloace adecvate, inclusiv prin mijloace electronice. Ca regulă generală, operatorul transmite informaţiile în acelaşi format în care a fost primită cererea.

(2) Art. 18-26 nu se aplică prelucrării datelor personale de către organele de ocrotire a legii.

(3) Operatorul realizează drepturile subiectului de date în temeiul art. 61 şi 64-67.

(4) Operatorul informează în scris persoana vizată cu privire la modul în care a dat curs cererii acesteia, fără întârzieri nejustificate.

(5) În cazul în care cererile din partea unui subiect de date sunt în mod vădit nefondate sau excesive, repetate, operatorul motivat poate, după caz:

a) să perceapă o taxă rezonabilă ţinând cont de costurile administrative pentru furnizarea informaţiilor sau a comunicării, sau pentru luarea măsurilor solicitate;

b) să refuze de a da curs cererii.

(6) În cazul în care operatorul are îndoieli întemeiate cu privire la identitatea subiectului de date care înaintează cererea menţionată la art. 64 sau 66, acesta poate solicita furnizarea de informaţii suplimentare necesare pentru a confirma identitatea persoanei vizate.

Articolul 63. Informaţii care trebuie puse la dispoziţia subiectului de date

(1) Operatorul va pune la dispoziţia subiectului de date următoarele informaţii:

a) identitatea şi datele de contact ale operatorului;

b) datele de contact ale responsabilului de protecţia datelor personale, după caz;

c) scopurile în care sunt prelucrate datele personale;

d) dreptul de a depune o cerere la Centrul şi datele de contact ale autorităţii de supraveghere;

e) existenţa dreptului de a solicita operatorului accesul şi rectificarea sau ştergerea datelor personale şi restricţionarea prelucrării datelor personale referitoare la subiectul de date;

f) altă informaţie relevantă.

(2) În afară de informaţiile menţionate la alin. (1), operatorul furnizează subiectului datelor, în anumite cazuri, următoarele informaţii suplimentare care să permită exercitarea drepturilor sale:

a) temeiul juridic al prelucrării;

b) perioada pentru care vor fi stocate datele personale sau, dacă acest lucru nu este posibil, criteriile utilizate pentru stabilirea acestei perioade;

c) dacă este cazul, categoriile de destinatari ai datelor personale, inclusiv în alte ţări sau în organizaţii internaţionale;

d) dacă este necesar, informaţii suplimentare, în special în cazul în care datele personale sunt colectate fără ştirea subiectului datelor.

(3) În cazul în care legislaţia specială prevede acest lucru, operatorul poate amâna, restricţiona sau omite furnizarea de informaţii către subiectul de date în temeiul alin. (2), în condiţiile în care este necesară şi proporţională într-o societate democratică, cu respectarea drepturilor fundamentale şi a intereselor legitime ale persoanei fizice în cauză, pentru:

a) a evita obstrucţionarea investigaţiilor organelor de ocrotirii a legii şi/sau activităţilor procedurale desfăşurate în conformitate cu legea;

b) a nu se prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracţiunilor sau executarea pedepselor penale;

c) protecţia ordinii publice;

d) protecţia securităţii naţionale;

e) protecţia securităţii statului;

f) protecţia drepturilor şi libertăţilor altor persoane fizice.

Articolul 64. Dreptul de acces al subiectului de date

Subiectul de date are dreptul să obţină de la operator o confirmare dacă se prelucrează sau nu datele cu caracter personal care-l privesc şi, în caz afirmativ, are acces la datele respective şi la următoarele informaţii:

a) scopurile şi temeiul legal al prelucrării;

b) categoriile de date personale în cauză;

c) destinatarii sau categoriile de destinatari cărora le-au fost comunicate datele personale, în special destinatarii din alte state sau organizaţii internaţionale;

d) atunci când este posibil, perioada prevăzută pentru care vor fi stocate datele personale sau, dacă nu este posibil, criteriile utilizate pentru stabilirea acestei perioade;

e) existenţa dreptului de a solicita rectificarea sau ştergerea de către operator a datelor personale sau limitarea prelucrării datelor personale referitoare la subiectul de date;

f) dreptul de a depune o cerere şi datele de contact ale Centrului;

g) comunicarea datelor personale care fac obiectul prelucrării şi a oricăror informaţii disponibile cu privire la originea lor.

Articolul 65. Limitarea dreptului de acces

(1) Operatorul poate restrînge total sau parţial exercitarea dreptului de acces al subiectului de date dacă este justificat şi constituie o măsură necesară şi proporţională, cu condiţia că legea specială prevede o astfel de procedură, în scopul:

a) de a evita obstrucţionarea investigaţiilor organele de ocrotire a legii sau acţiunilor procedurale desfăşurate în conformitate cu legea;

b) de a nu se prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracţiunilor sau executarea pedepselor penale;

c) protecţiei ordinii publice;

d) protecţiei securităţii naţionale şi statului;

e) protecţiei drepturilor şi libertăţilor altor persoane.

(2) În cazul restrîngerii totale sau parţiale a exercitării dreptului de acces al subiectului de date operatorul informează în scris subiectul de date, fără întârzieri nejustificate, cu privire la refuz sau limitarea accesului şi la motivele refuzului sau ale limitării. Astfel de informaţii pot fi omise atunci când furnizarea lor ar contraveni unuia dintre scopurile de la alin. (1). O astfel de restricţie privind furnizarea de informaţii subiectului datelor este limitată în timp în conformitate cu prevederile legale.

(3) Operatorul trebuie să informeze subiectul de date cu privire la posibilitatea de a depune o cerere la Centru sau despre dreptul de a se adresa în judecata.

(4) Operatorul trebuie să documenteze motivele de fapt şi de drept pe care se bazează decizia care se consemnează în Registrul automatizat de aplicare a excepţiilor. Aceste informaţii sunt puse la dispoziţia Centrului.

Articolul 66. Dreptul la rectificare sau la ştergere a datelor personale şi restricţionarea prelucrării

(1) Subiectul de date are dreptul să obţină de la operator, fără întârzieri nejustificate, rectificarea datelor personale inexacte care îl privesc. În cazul în care acest lucru este posibil şi ţinând seama de scopurile prelucrării, subiectul de date are dreptul la completarea datelor personale incomplete, inclusiv prin furnizarea unei declaraţii suplimentare.

(2) Subiectul de date are dreptul de a solicita ştergerea datelor personale, iar operatorul trebuie să realizeze această solicitare, dacă prelucrarea încalcă dispoziţiile prevăzute la art. 4, 56 sau 60, sau în cazul în care datele personale trebuie şterse pentru îndeplinirea unei obligaţii legale care îi revine operatorului în conformitate cu art. 57.

(3) În loc de ştergere, operatorul restricţionează prelucrarea atunci când:

a) exactitatea datelor personale este contestată de subiectul de date, iar exactitatea sau inexactitatea acestora nu poate fi stabilită cu certitudine;

b) datele personale trebuie păstrate ca mijloace de probă.

În cazul în care prelucrarea este restricţionată în conformitate cu lit. a), operatorul informează subiectul de date înainte de ridicarea restricţiilor de prelucrare.

(4) Operatorul informează în scris subiectul de date cu privire la orice refuz de rectificare sau ştergere a datelor personale sau de restricţionare a prelucrării şi motivele refuzului. Operatorul poate restricţiona, parţial sau, dacă este justificat, integral, de a furniza astfel de informaţii, dacă acest lucru

este prevăzut expres de legislaţia specială. O astfel de restricţie este permisă în măsura în care este o măsură necesară şi proporţională într-o societate democratică, cu respectarea drepturilor fundamentale şi a intereselor legitime ale persoanei fizice în cauză, pentru:

a) a evita obstrucţionarea investigaţiilor organelor de ocrotire a legii sau acţiunilor procedurale desfăşurate în conformitate cu legea;

b) a nu se prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracţiunilor sau executarea pedepselor penale;

c) protecţia ordinii publice;

d) protecţia securităţii naţionale şi a statului;

e) protecţia drepturilor şi libertăţilor altor persoane.

(5) Dacă temeiul pentru restricţiile din alin. (4) nu mai sunt aplicabile, operatorul va întreprinde acţiunile solicitate de către subiectul de date, cu excepţia cazului în care acest lucru ar prejudicia scopul prevăzut de alin. (4).

(6) Operatorul comunică rectificarea datelor personale inexacte autorităţii competente de la care provin datele personale inexacte.

(7) În cazul în care datele personale au fost rectificate sau şterse sau prelucrarea a fost restricţionată în conformitate cu alin. (1), (2) şi (3) operatorul notifică destinatarii, iar destinatarii rectifică sau şterg datele personale sau restricţionează prelucrarea datelor personale aflate sub responsabilitatea lor.

(8) Operatorul informează subiectul de date cu privire la posibilitatea de a depune o cerere la Centru sau de a se adresa în instanţa de judecată, în cazul în care subiectul de date consideră nejustificat refuzul de a corecta sau a şterge datele personale.

Articolul 67. Notificarea încălcării securităţii datelor personale către Centru de către organul de ocrotire a legii

(1) Organul de ocrotire a legii notifică Centrul despre încălcarea securităţii datelor personale în conformitate cu art. 37.

(2) În cazurile în care încălcarea securităţii datelor personale implică date personale care au fost transmise de un operator dintr-un alt stat sau către un astfel de operator, informaţiile prevăzute la art. 37 alin. (3) se comunică operatorului din respectivul stat fără întârziere nejustificată.

Articolul 68. Comunicarea încălcării securităţii datelor personale către subiectul de date de către organul de ocrotire a legii

(1) Organul de ocrotire a legii comunică subiectului de date despre încălcarea securităţii datelor personale în conformitate cu art. 38.

(2) Prin derogare de la art. 38, comunicarea încălcării securităţii datelor personale subiectului de date poate fi întârziată, restricţionată sau, dacă este justificat, omisă, în cazul în care acest lucru este necesar şi proporţional pentru:

a) a evita obstrucţionarea investigaţiilor organelor de ocrotire a legii sau acţiunilor procedurale desfăşurate în conformitate cu legea;

b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracţiunilor sau executarea pedepselor penale;

c) protecţia ordinii publice;
d) protecţia securităţii naţionale şi a statului;
e) protecţia drepturilor şi libertăţilor altor persoane

(3) În cazul în care motivele de restricţie prevăzute la alin. (2) nu mai sunt aplicabile, operatorul informează subiectul de date cu privire la încălcarea securităţii datelor personale, cu excepţia situaţiei în care acest lucru ar aduce atingere scopului prevăzut la alin. (2) într-un alt caz.

Articolul 69. Evidenţa activităţilor de prelucrare

(1) Organul de ocrotire a legii este obligat să ţină evidenţa operaţiunilor de prelucrare a datelor personale în sistemele automatizate, mixte sau manuale: colectare, culegere, consultare, modificare, dezvăluire, răspândire, imprimare, transfer, combinare şi ştergere.

(2) Evidenţa activităţilor de prelucrare trebuie să permită determinarea scopului şi temeiului legal, a datei şi a timpului, stabilirea persoanei care a accesat sau dezvăluit, precum şi a identităţii destinatarilor datelor personale.

(3) Evidenţa activităţilor de prelucrare pot fi utilizate numai pentru verificarea legalităţii prelucrării datelor, verificărilor interne, asigurării integrităţii şi a securităţii datelor personale şi în cadrul urmăririi penale.

(4) Organul de ocrotire a legii, care acţionează în calitate de operator sau persoană împuternicită de operator, trebuie să pună la dispoziţia Centrului, la cerere, evidenţa activităţilor de prelucrare, cu indicarea inclusiv a scopului accesării subiectului de date, data şi ora acestor operaţiuni, identitatea persoanei care a accesat informaţia, cît şi a destinatarului acestora. Centrul poate solicita informaţii suplimentare privind evidenţa activităţilor de prelucrare, în acest fel, organul de ocrotire a legii furnizează Centrului suplimentar informaţiile necesare.

Articolul 70. Obligaţia organului de ocrotire a legii de în raport cu atribuţiile Centrului

(1) În cazul în care cererea a fost prezentată Centrului în conformitate cu art. 75 privind activităţile de prelucrare, de către organul de ocrotire a legii, inclusiv, fără a se limita la excepţiile prevăzute în art. 65 şi 66, operatorul, persoana împuternicită de operator sau terţul trebuie să se conformeze cererii Centrului de a furniza informaţiile solicitate.

(2) În timp ce furnizează Centrului informaţii în conformitate cu alin. (1), organul de ocrotire a legii acordă informaţiile referitoare la: datele personale prelucrate, scopul, temeiul legal şi legătura de cauzalitate dintre subiectul de date, calitatea acestuia şi operaţiunile efectuate, inclusiv identitatea persoanei care a accesat informaţia, cît şi a destinatarului acestora.

(3) În temeiul interpelării motivate a Centrului, organul de ocrotire a legii pune la dispoziţie informaţii şi documente suplimentare pentru a confirma informaţiile furnizate..

(4) La finalizarea investigaţiei desfăşurate, Centrul informează subiectul de date precum şi organul de ocrotire a legii despre decizia adoptată pe caz.

(5) În cazurile în care, pe baza informaţiei justificate a organului de ocrotire a legii, informarea subiectului datelor prevăzută la alin. (4), ar submina scopul prelucrării, Centrul informează subiectul de date că a investigat şi a efectuat toate verificările necesare. O astfel de excepţie privind furnizarea de informaţii subiectului de date este limitată în timp pe o perioada de 30 de zile, cu posibilitatea prelungirii întemeiate până la 6 luni de către organul de ocrotire a legii. În cazul în care se constată că prelucrarea datelor personale nu este justificată şi nu are legătură de cauzalitate cu scopul declarat, Centrul solicită organului de ocrotire a legii să informeze subiectul de date despre prelucrarea efectuată.

(6) Organul de ocrotire a legii şi/sau subiectul de date poate contesta decizia Centrului prin acţiune în contencios administrativ. Cauza se examinează în şedinţă închisă, în absenţa subiectului de date, cu participarea Centrului şi a organului de ocrotire a legii.

Articolul 71. Aplicarea excepţiilor şi înregistrarea acestora

(1) În scopurile prevăzute la art. 2 alin. (2) lit. d) organul de ocrotire a legii poate aplica excepţii privind furnizarea de informaţii subiectului de date referitoare la prelucrarea datelor personale în orice sistem informaţional.

(2) Organul de ocrotire a legii în cazul aplicării excepţiilor stabilite la alin. (1), este obligat să ţină evidenţa acestora prin consemnarea în Registrul automatizat al aplicării excepţiilor ţinut de Centru, creat şi reglementat prin Hotărâre de Parlament.

(3) Pot fi aplicate excepţiile stabilite la alin. (1) doar dacă legea specială stabileşte cazurile aplicării acestora, termenul limită precum şi periodicitatea prelungirii acestora, modul de verificare şi informare a subiectului de date.

(4) Neaplicarea excepţiilor, omiterea termenului de prelungire a excepţiilor sau depăşirea acestora, exclude posibilitatea aplicării excepţiilor pe aceleaşi temeiuri de drept.

(5) După încetarea situaţiei care justifică aplicarea alin. (1) - (4), organele de ocrotire a legii sunt obligate să informeze în scris sau în format electronic potrivit cerinţelor documentului electronic şi semnăturii electronice, subiecţii de date în modul stabilit la art. 63 şi 64.

(6) În cazurile prevăzute de alin. (4) - (5), la realizarea dreptului de acces la datele personale operatorii sunt în drept să informeze subiectul de date şi nu poartă răspundere pentru o astfel de informare.

(7) Evidenţa activităţilor de prelucrare a datelor personale privind aplicarea excepţiei, se păstrează cel puţin 10 ani din momentul aplicării.

Articolul 72. Transferul transfrontalier de date personale între organele de ocrotire a legii

(1) Orice transfer de date personale de către organele de ocrotire a legii care sunt în curs de prelucrare sau sunt destinate prelucrării în contextul transferului în afara Republicii Moldova în Spaţiul Economic European sau la o organizaţie internaţională, sau la o altă ţară, un teritoriu sau unul sau mai

multe sectoare specificate în respectiva țară sau o organizație internațională care asigură un nivel adecvat de protecție recunoscută de Comisia Europeană inclusiv pentru transferuri ulterioare către o altă țară sau organizație internațională, se permit doar în următoarele condiții:

a) transferul este necesar în scopurile prevăzute la art. 2 alin. (2) lit. d);

b) datele personale sunt transferate unui operator dintr-o țară sau organizație internațională care este o autoritate competentă în scopurile menționate la art. 2 alin. (2) lit. d);

c) transferul este permis numai după ce Centrul a acordat o autorizație în conformitate cu art. 49 alin. (3) sau transferul este permis în conformitate cu art. 52 alin. (1).

(2) Condițiile de la art. 53 alin. (1) nu se aplică atunci când transferul se face în conformitate cu prezentul articol.

Articolul 73. Derogări pentru situații specifice

(1) În circumstanțe excepționale, în cazul în care nu sunt îndeplinite condițiile din art. 72 alin. (1), un transfer sau o categorie de transferuri de date personale către o altă țară sau o organizație internațională poate avea loc numai cu condiția ca transferul să fie necesar:

a) pentru protejarea vieții, integrității fizice sau a sănătății subiectului de date sau ale unei alte persoane;

b) pentru protejarea intereselor legitime ale subiectului de date, dacă aceasta este prevăzută de o lege specială;

c) pentru prevenirea unei amenințări imediate și grave la adresa ordinii publice a Republicii Moldova sau a altei țări;

d) în cazuri individuale, în scopurile prevăzute la art. 2 alin. (2) lit. d);

e) într-un caz individual de stabilire, exercitare sau apărare a revendicărilor legale legate de scopurile prevăzute la art. 2 alin. (2) lit. d).

(2) Datele personale nu se transferă în cazul în care organul de ocrotire a legii care transferă, stabilește că drepturile și libertățile fundamentale ale subiectului datelor în cauză depășesc interesul public pentru transferul prevăzut la alin. (1) lit. d) și e).

(3) În cazul în care un transfer se bazează pe alin. (1), un astfel de transfer este documentat, iar documentația este pusă la dispoziția Centrului, la cerere, inclusiv data și ora transferului, informații despre autoritatea competentă destinatară, justificarea și motivele transferului, datele personale transferate.

Articolul 74. Transferuri de date personale către alți destinatari în afara Republicii Moldova

(1) În cazul în care destinatarul nu este o autoritate desemnată la art. 72 alin. (1) lit. b) și fără a aduce atingere vreunui acord internațional încheiat și ratificat de Republica Moldova cu alte state în domeniul cooperării judiciare în materie penală și al cooperării polițienești, care conține garanții privind protecția drepturilor subiectului de date, organele de ocrotire a legii, în cazuri

individuale şi specifice, vor transfera date personale direct destinatarilor stabiliţi în afara Republicii Moldova numai dacă sunt respectate celelalte prevederi ale prezentei legi şi sunt îndeplinite toate condiţiile următoare:

a) transferul este strict necesar pentru îndeplinirea unei sarcini a organului de ocrotire a legii care realizează transferul şi este prevăzute de o lege specială, în scopul prevăzut în art. 2 alin. (2) lit. d);

b) organul de ocrotire a legii care transferă datele personale stabileşte că niciunul din drepturile şi libertăţile fundamentale ale subiectului datelor în cauză nu depăşesc interesul public care necesită transferul în cauză;

c) organul de ocrotire a legii care transferă datele personale consideră că transferul către o autoritate competentă în scopurile menţionate la art. 2 alin. (2) lit. d) în altă ţara este ineficient sau inadecvat, în special deoarece transferul nu poate fi realizat în timp util;

d) autoritatea competentă în scopurile menţionate la art. 2 alin. (2) lit. d) din o altă ţară este informată fără întârzieri nejustificate, cu excepţia cazului în care aceasta este ineficient sau inadecvat;

e) organul de ocrotire a legii care transferă datele personale informează destinatarul cu privire la scopul specific sau scopurile pentru care datele personale trebuie să fie prelucrate numai de acesta, cu condiţia ca această prelucrare să fie necesară.

(2) Organul de ocrotire a legii informează Centrul, cu privire la transferurile efectuate în temeiul prezentului articol până la efectuarea transferului sau în termen de două zile de la efectuarea transferului, în caz contrar Centrul va constata încălcarea principiilor de protecţie a datelor personale şi prevederile prezentei norme.

(3) În cazul în care un transfer se bazează pe alin. (1), un astfel de transfer trebuie să fie documentat. Documentaţia trebuie să includă data şi ora transferului, informaţii despre autoritatea competentă destinatară, justificarea şi motivele transferului, datele personale transferate şi legătura dintre datele personale transferate şi condiţia prevăzută la alin. (1) lit. a).

Capitolul VIII
CONDIŢII PENTRU DEPUNERE A CERERILOR, PROCEDURA DE EXAMINARE ŞI EFECTUARE A INVESTIGAŢIILOR, PROCESUL DE LUARE A DECIZIILOR, EXECUTATEA DECIZIILOR, CONFIDENŢIALITATEA, ACCESUL ŞI PĂSTRAREA MATERIALELOR INVESTIGAŢIEI

Articolul 75. Dreptul de a depune o cerere

(1) În cazul în care subiectul de date consideră că prelucrarea datelor personale care-l vizează încalcă legea are dreptul de a depune o cerere la Centru, în termen de 3 luni din momentul depistării pretinsei încălcări.

(2) În cazul în care cererea se referă la exercitarea drepturilor subiecţilor de date prevăzute în Capitolul III, această cerere va fi iniţial înaintată operatorilor de date în condiţiile legii. Dacă subiectul de date nu primeşte un

răspuns din partea operatorului în termenii stabiliţi conform Capitolului III sau atunci când răspunsul sau acţiunile întreprinse de opcrator sunt considerate inadecvate sau nu rezolvă cererea, subiectul de date, în termen de 30 zile din momentul cînd a primit răspunsul sau trebuia să primească răspunsul, are dreptul de a depune o cerere la Centru.

(3) Cererile depuse cu încălcarea procedurii şi termenelor de prescripţie prevăzute la alin. (1) şi (2) nu se examinează, fapt despre care, Centrul informează subiectul de date în termen de 10 zile lucrătoare.

(4) Subiectul de date care, din motive temeinice şi justificate, a omis termenul de prescpripţie poate fi repus în termen în condiţiile Codului de procedură civilă.

Articolul 76. Cerinţe pentru depunerea cererii

(1) Cererea poate fi depusă la sediul Centrului, prin trimitere postala sau prin mijloace electronice, în conformitate cu cerinţele semnăturii electronice şi documentului electronic, personal de subiectul de date sau de reprezentantul acestuia, utilizând formularul manual sau electronic, aprobat de Centru. În cazul depunerii cererii de către reprezentant, se prezintă în modul corespunzător împuternicirile conferite de subiectul de date reprezentantului în raport cu Centrul, precum şi volumul datelor personale în privinţa cărora reprezentantul are dreptul de a le prelucra.

(2) Forma şi cuprinsul cererii adresate Centrului trebuie sa cuprindă:

a) numele, prenumele, adresa subiectului de date şi, după caz, numele, prenumele reprezentantului, numărul de telefon, email;

b) descrierea detaliată a circumstanţelor de fapt şi de drept a cauzei;

c) numele, prenumele sau denumirea, adresa, numărul telefonul al operatorului şi/sau a persoanei împuternicite de operator;

d) alte informaţii necesare după caz, inclusiv dacă obiectul cererii este sau a fost examinat de o instanţă de judecată, autoritate publică, în cadrul unui proces de mediere sau arbitraj între aceleaşi părţi;

e) data întocmirii cererii

f) semnătura olografă sau electronică a subiectului de date sau al reprezentatului acestuia.

(3) În toate cazurile, cererile urmează să fie însoţite de probe corespunzătoare ce confirmă pretinsele încălcări. Probele şi alte înscrisuri prezentate în copii la rândul lor urmează a fi autentificate în modul corespunzător prin înscrierea „copia corespunde originalului" şi cu aplicarea datei şi semnăturii olografe, sau cu aplicarea semnăturii electronice, pentru cererile prezentate în format electronic. La cerere urmează a fi anexate doar informaţii şi documente care sînt pertinente şi nu sunt excesive faptei sesizate.

(4) Centrul poate identifica şi audia subiecul de date şi/sau reprezentantul acestuia.

(5) Examinarea cererii care nu corespunde cerinţelor prevăzute de prevederile alin. (1) - (4) se suspendă. În acest caz, Centrul informează subiectul de date în termen de 10 zile lucrătoare despre necesitatea înlăturătii

neconformităţilor admise. În cazul în care subiectul de date nu furnizează informaţiile solicitate de Centru, în termen de 30 zile lucrătoare din data primirii somaţiei, cererea se consideră inadmisibilă şi se lasă fără examinare, fapt despre care se informează subiectul de date. În termen de trei luni de la primirea răspunsului Centrului, subiectul de date are dreptul de a depune o altă cerere în adresa Centrului, care să corespundă tuturor cerinţelor prevăzute de lege.

(6) În cazul în care o cerere depusă la Centru cu acelaşi obiect şi cu aceleaşi părţi este examinată de o instanţă de judecată, autoritate publică, în cadrul unui proces de mediere sau arbitraj Centrul respinge cererea sau suspendă examinarea acesteia până la încheierea examinării şi/sau după caz, pînă la adoptarea unei decizii definitive, cu informarea persoanei care a depus cererea despre motivele care au dus la respingerea cererii sau la suspendarea examinării acesteia în termen de 10 zile lucrătoare de la constatarea faptului dat.

(7) În cazul suspendării cererii persoana care a depus cererea are obligaţia de a informa Centrul despre înlăturarea circumstanţelor stabilite la alin. (6). În cazul respingerii cererii, dacă termenul pentru depunearea acesteia a expirat ca urmare a examinării în cadrul instanţei de judecată, autorităţii publice, în cadrul unui proces de mediere sau arbitraj, subiectul de date poate depune, în mod repetat, în termen de 3 luni de la primirea soluţiei pe caz, o cererea la Centru.

(8) Prin derogare de la alin. (6), în cazul în care pot fi afectate drepturile altor subiecţi de date ori afectate măsurile de securitate, sau dacă Centrul consideră obiectul cererii unul relevant poate dispune efectuarea investigaţiilor necesare.

(9) Cererile adresate repetat, care nu conţin argumente ori informaţii noi sau sunt în mod vădit nefondate nu se examinează, fapt despre care este informat subiectul de date.

(10) Cererile care conţin un limbaj necenzurat sau ofensator, ameninţări la securitatea naţională, la ordinea publică, la viaţa şi sănătatea persoanei oficiale, precum şi a membrilor familiei acesteia, nu se examinează.

Articolul 77. Competenţa de examinare

(1) Centrul are competenţă să investigheze şi să soluţioneze cazurile de încălcare ale dispoziţiilor normative în domeniul protecţiei datelor personale, cu sau fără ieşirea la faţa locului, în următoarele situaţii:

a) la depunerea cererii subiectului de date sau a reprezentantului legal privind neconformitatea prelucrării datelor personale;

b) la sesizarea din oficiu, sau în cazul în care Centrul a fost informat sau dispune de informaţii privind încălcarea în masă, sistemică sau gravă a principiilor de protecţie a datelor cu caracter personal, cazurile de importanţă socială sau în cazurile de supraveghere şi prevenire.

(2) În cazul în care presupusa încălcare a prelucrării datelor personale se află în afara domeniului de aplicare a prezentei legi, Centrul, la cererea subiectului de date, acordă asistenţă privind punerea în practică a Convenţiei pentru protecţia persoanelor cu privire la prelucrarea automatizată a datelor personale.

(3) În cazul în care o cerere se referă la prelucrarea datelor transfrontaliere sau implică un element de extranietate, Centrul aplică, după caz, mecanismele de cooperare stabilite în temeiul art. 54 din prezenta lege şi dupa caz art. 6 alin. 7-10 din Legea privind Centrul Naţional pentru Protecţia Datelor cu Caracter Personal. Această dispoziţie se aplică numai în cazul în care reşedinţa obişnuită sau locul de muncă al subiectului de date sau locul în care este stabilit operatorul sau persoana împuternicită de operator care face obiectul unei cereri, este în Republica Moldova.

Articolul 78. Investigaţia

(1) Investigaţia reprezintă activitatea desfăşurată de către inspectorii de protecţie a datelor, de conducătorii subdiviziunilor specializate din cadrul Centrului în scopul de verificare a respectării cerinţelor prezentei legi şi altor acte normative ce vizează domeniul protecţiei datelor personale de către: operatori, operatori asociaţi, persoane împuternicite de operatori, destinatari, precum şi autorităţi care nu sunt considerate a fi destinatari, terţi, indiferent de tipul proprietăţii şi domeniul de activitate, forma juridică de organizare. Investigaţia unor cauze complicate şi de proporţii poate fi efectuată de un grup de inspectori de protecţie cu indicarea persoanei care va conduce investigaţia.

(2) În cadrul investigaţiei Centrul dispune atât în privinţa conformităţii prelucrării de date, cât şi asupra mijloacelor prin care a avut loc prelucrarea datelor personale.

(3) Centrul solicită de la subiecţii de date şi/sau subiecţii de drept specificaţi la alin. (1), documente, informaţii şi după caz mijloace necesare pentru confirmarea sau infirmarea pretinselor fapte de încălcare a legislaţiei privind protecţia datelor personale, indică temeiul juridic şi scopul solicitării informaţiei, stabileşte termenul în care acestea trebuie furnizate, specifică sancţiunile prevăzute de lege pentru nefurnizarea de informaţii ori pentru furnizarea unei informaţii inexacte, incomplete sau care induce în eroare.

(4) Pentru a colecta probe necesare pentru confirmarea sau infirmarea încălcării legislaţiei privind protecţia datelor personale, Centrul poate dispune prin decizie, în cadrul aceleiaşi investigaţii sau în cadrul unei altei investigaţii, ieşirea la faţa locului.

(5) În cazul investigaţiei cu ieşirea la faţa locului, directorul Centrului, directorul adjunct sau o altă persoana responsabilă, desemnată în acest sens prin ordinul directorului Centului, emite o decizie în care se indică scopul şi obiectul investigaţiei, persoanele delegate privind efectuarea investigaţiei, perioada de timp, precum şi drepturile şi obligaţiile părţilor implicate în investigaţie.

(6) Decizia privind efectuarea investigaţiei cu ieşirea la faţa locului se aduce la cunoştinţă sub semnătură persoanei, entităţii supuse investigaţiei, sau reprezentantului legal. În cazul refuzului primirii şi semnării deciziei se întocmeşte un act, în prezenţa unui martor sau în cazul înregistrării video şi audio prin care se consemnează acest fapt nu este necesară prezenţa martorului.

(7) Inspectorii de protecţie a datelor îşi exercită drepturile în cadrul investigaţiilor la faţa locului în limita împuternicirilor consemnate în decizie în conformitate cu prevederile prezentei legi, Legii privind Centrul Naţional pentru Protecţia Datelor Personale, precum şi altor acte normative interne.

(8) În cadrul investigaţiei, inspectorii de protecţie a datelor au următoarele drepturi:

a) să dispună de acces şi să examineze sistemele de evidenţă a datelor personale, soluţiile software şi suporturile hardware, datele personale şi orice documente legate de obiectul şi scopul investigaţiei, indiferent de echipamentul şi/sau suportul pe care sunt stocate datele;

b) să intre în încăperi, pe terenuri sau în mijloace de transport aflate în proprietatea sau folosinţa subiecţilor de drept menţionaţi la alin. (1);

c) să ridice mijloace prin care se efectuează prelucrarea datelor personale, să colecteze, să obţină copii sau extrase, sub orice formă, din sistemele de evidenţă şi documentele care conţin date personale;

d) să sigileze încăperile şi mijloacele, unde şi prin care se efectuează prelucrarea datelor personale, sistemele de evidenţă şi documentele aferente obiectului şi scopului investigaţiei, pe perioada şi în măsura în care este necesar pentru desfăşurarea investigaţiei. Sigilarea şi desigilarea poate fi efectuată doar de către Centru, cu consemnarea faptului dat într-un proces-verbal semnat de persoanele cointeresate;

e) să audieze şi să solicite persoanei, entităţii supuse investigaţiei sau reprezentantului legal sau altor persoane care pot oferi Centrului informaţiile necesare pentru soluţionarea unei cereri în legătură cu prelucrarea datelor cu caracter personal în cadrul investigaţiei şi de a înregistra, cu informarea prealabilă a persoanei supuse investigaţiei, inclusiv prin mijloace audio, video sau prin alte mijloace, răspunsurile acestora;

f) să solicite şi să primească informaţiile referitoare la obiectul şi scopul investigaţiei, stocate pe calculatoare sau alte dispozitive electronice, într-o formă care să permită ridicarea şi transportarea acestora, precum şi să fie vizibile şi lizibile;

g) să exercite investigaţii de securitate în cadrul oricăror sisteme de evidenţă în care se conţin date personale sau prin care pot fi ptelucrate date personale, inclusiv cu efectuarea unor măsuri tehnice pentru simularea unui model de accesare a sistemelor de evidenţă ce conţin date personale, în scopul verificării nivelului de protecţie a acestora, precum şi în scopul preîntîmpinării unor eventuale cazuri de acces ilicit sau întîmplător asupra acestor sisteme, depistării locurilor slabe în mecanismele de protejare a acestora, după caz în colaborare cu alte autorităţi;

h) să solicite sprijinul subdiviziunilor abilitate ale organelor de ocrotire a legii, care sînt obligate să acorde asistenţa necesară angajaţilor Centrului. La efectuarea investigaţiei pot fi antrenaţi, după caz, şi experţi din anumite domenii, împuterniciţi de Centru;

i) alte drepturi prevăzute de prezenta lege, Legea privind Centrul Naţional pentru Protecţia Datelor cu Caracter Personal şi alte acte normative.

(9) Pe parcursul efectuării investigaţiei, inspectorii de protecţie a datelor şi experţii împuterniciţi de Centru în acest sens sînt obligaţi:

a) să informeze persoana supusă investigării despre drepturile şi obligaţiile acesteia;

b) să efectueze investigaţia în conformitate cu împuternicirile atribuite de prezenta lege, ţinând cont de obiectul şi scopul acestuia.

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

a) să fie informată şi să obţină o copie a deciziei privind efectuarea investigaţiei la faţa locului;

b) să prezinte probe în cadrul efectuării investigaţiei;

c) să prezinte explicaţii înregistrate sub orice formă referitoare la obiectul şi scopul investigaţiei;

d) să identifice datele şi informaţiile ce constituie secret şi alte informaţii confidenţiale furnizate în procesul efectuării investigaţiei, cu efectuarea menţiunilor corespunzătoare;

e) să obţină lista mijloacelor, sistemelor de evidenţă şi documentelor ridicate pe parcursul investigaţiei, semnată de inspectorul de protecţie a datelor;

f) să fie asistată de avocaţi, de alţi reprezentanţi împuterniciţi conform legislaţiei. Dacă persoana supusă investigaţiei solicită prezenţa avocatului, efectuarea investigaţiei se suspendă pînă la prezentarea avocatului, dar nu mai mult de 2 ore.

(11) Toate autorităţile/entităţile şi persoanele fizice sînt obligate să se supună investigaţiei efectuate de Centru, inclusiv prin asigurarea condiţiilor pentru buna desfăşurare a investigaţiei.

(12) Acţiunile de investigare se efectuează în orice perioadă relevantă pentru acumularea informaţiilor necesare soluţionării cazului.

(13) Investigaţia cu ieşirea la faţa locului se desfăşoară în orele de program al autorităţii/entităţii supuse investigaţiei. Investigaţia poate continua şi în afara orelor de program numai cu acordul reprezentantului entităţii supuse controlului.

(14) Rezultatul investigării cu ieşirea la faţa locului este consemnat într-un act, care se întocmeşte în două exemplare, se numerotează şi se semnează pe fiecare pagină de inspectorii de protecţie a datelor. Actul se aduce la cunoştinţă persoanei supuse investigaţiei în termen de 10 zile lucrătoare din momentul finalizării investigaţiei cu ieşirea la faţa locului sub semnătură. Persoana supusă investigaţiei este obligată să confirme prin semnătură, inclusiv prin intermediul persoanelor cu funcţie de răspundere sau altui

reprezentant al său, primirea exemplarului de act, chiar şi în caz de dezacord cu constatările expuse în acesta. În cazul în care reprezentantul persoanei supuse investigaţiei refuză să primească şi să confirme prin semnătură primirea exemplarului de act, în acesta se face menţiunea privind refuzul de a primi exemplarul de act şi/sau de a confirma prin semnătură primirea exemplarului de act, semnat de inspectorii de protecţie a datelor care au efectuat investigaţia, iar actul va fi expediat persoanei supuse investigaţiei prin scrisoare recomandată, cu aviz de primire.

(15) Condiţiile, termenele şi procedura de păstrare a mijloacelor, copiilor sau extraselor, a sistemelor de evidenţă şi documentelor ridicate în temeiul prezentului articol, se stabilesc de Centru, în conformitate cu actele normative.

(16) În cazul în care există o bănuială rezonabilă că purtătorii de informaţie privind activitatea şi obiectul investigaţiei care ar putea fi pertinente pentru a dovedi o încălcare a legislaţiei privind protecţia datelor personale sînt păstrate în alte încăperi, terenuri şi mijloace de transport, inclusiv în locuinţele membrilor organelor de conducere sau ale subiecţilor enunţaţi la alin. (1), decît cele indicate în decizia de efectuare a investigaţiei cu ieşirea la faţa locului, investigaţia poate fi extinsă şi efectuată asupra bunurilor date cu acceptul scris al persoanelor vizate, sau reprezentantului legal al acestora. Situaţia descrisă se referă la orice tip de proprietate, folosinţă, posesie, uzucapiune cum ar fi, dar nu se limitează la arendă, locaţiune, leasing.

(17) Accesul reprezentanţilor Centrului în domiciliu, în sediu sau alte încăperi, terenuri şi mijloace de transport, echipamentele de prelucrare, la programele şi aplicaţiile, precum şi la documentele, înregistrările referitoare la prelucrarea de date personale, ce aparţin, sînt în posesie sau în folosinţa persoanei la care se efectuează investigaţia, în lipsa acceptului scris, se permite numai în baza mandatului judiciar emis în condiţiile prezentului articol şi prezentat persoanei supuse investigaţiei sau reprezentantului său.

(18) Pentru a nu prejudicia investigaţia sub aspect de ascundere, modificare, ştergere, distrugere a sistemelor de evidenţă a datelor personale, echipamentelor de prelucrare, programelor şi aplicaţiilor, precum şi orice document sau înregistrare referitoare la prelucrarea de date personale, Centrul poate solicita direct instanţei de judecată eliberarea mandatului judiciar. Cererea de solictare a mandatului se judecă cu participarea Centrului în termen de cel mult 48 de ore de la data înregistrării acesteia. Încheierea se motivează şi se comunică Centrului imediat, dar nu mai mult de 48 de ore de la pronunţare.

(19) Mandatul judiciar poate fi eliberat dacă:

a) există o bănuială rezonabilă că în domiciliu, în sediu sau alte încăperi, terenuri şi mijloace de transport, sînt amplasate sisteme de evidenţă a datelor personale, mijloace de prelucrare, programe şi aplicaţii, precum şi păstrate documente sau înregistrări referitoare la prelucrarea de date personale sau alte documente care au putut fi ascunse, îndepărtate, înlăturate, modificate sau distruse; sau

b) există o bănuială rezonabilă că în domiciliu, în sediu sau alte încăperi, terenuri şi mijloace de transport, ce urmează a fi supus investigaţiei sînt amplasate sisteme de evidenţă a datelor personale, mijloace de prelucrare, programe şi aplicaţii, precum şi orice document sau înregistrare referitoare la prelucrarea de date personale sau alte documente a căror prezentare a fost solicitată de Centru în conformitate cu prezenta lege, dar care nu au fost prezentate în termenul stabilit.

(20) Mandatul judiciar este valabil 30 de zile de la data emiterii şi poate fi prelungit cu încă 30 de zile. Hotărîrea/decizia privind refuzul eliberarii mandatului judiciar poate fi atacată cu recurs în termen de 10 zile din momentul informării.

(21) În cazul solicitării unui mandat judiciar, instanţa de judecată este obligată să verifice dacă efectuarea investigaţiei şi măsurile care urmează a fi luate nu sînt arbitrare sau excesive, avînd în vedere obiectul investigaţiei.

(22) În caz de necesitate, instanţa de judecată poate solicita suplimentar Centrului explicaţii detaliate, în special privind temeiurile care determină Centrul să bănuiască încălcarea legislaţiei privind protecţia datelor personale, precum şi privind gravitatea încălcării suspectate, importanţa probelor căutate, natura implicării operatorului sau persoanei împuternicite de operator şi probabilitatea rezonabilă că sistemele de evidenţă a datelor personale, mijloacele de prelucrare, programele şi aplicaţiile, precum şi documentele sau înregistrările referitoare la prelucrarea de date personale legate de obiectul investigaţiei se păstrează sau sînt amplasate în locul pentru care se solicită mandatul. În cadrul examinării solicitării mandatului judiciar instanţa de judecată aplică în mod corespunzător prevederile prezentului articol.

(23) În cadrul efectuării investigaţiei, inspectorul de protecţie a datelor se supune prevederilor legale, decide cu privire la orientarea efectuării investigaţiei şi efectuează acţiunile de investigare, cu excepţia cazurilor cînd este necesar încuviinţarea, autorizarea, confirmarea sau verificarea acţiunilor acestuia de către conducătorii ierarhic superiori, după caz, conducerea Centrului sau de către instanţa de judecată. Orice imixtiune în activitatea inspectorului de protecţie este interzisă.

(24) Investigaţia se efectuează în termen rezonabil în funcţie de gravitatea presupusei încălcări, precum şi de alte criterii care ar determina durata de efectuare a acesteia, însă care nu poate depăşi 2 ani.

(25) Controlul general asupra respectării termenului rezonabil de efectuare a investigaţiei este pus în sarcina directorului adjunct şi instanţa de judecată.

(26) Dacă la scurgerea termenului de 2 ani, Centrul nu are acumulate probe suficiente pentru a aprecia cu certitudine existenţa sau lipsa încălcării, efectuarea investigaţiei poate fi suspendată pe termen maxim de 1 un an de zile, cu informarea subiectului de date, care a depus cererea. Reluarea examinării investigaţiei poate avea loc în intervalul acestui termen, cu condiţia apariţiei probelor noi ce sunt pertinente şi concludente pentru soluţionarea cazului.

(27) În cazul în care, la expirarea termenului de suspendare, prevăzut la alin. (26), nu apar circumstanţe relevante pentru reluarea investigaţiei, Centrul emite o decizie privind lipsa faptei încălcării, cu informarea corespunzătoare a subiectului de date, care a depus cererea.

(28) Centrul informează subiectul de date cu privire la progresul şi rezultatele investigaţiei ori de câte ori este necesar la cererea subiectului de date, sau la fiecare trei luni.

(29) Centrul elaborează şi aprobă Regulamentul privind efectuarea investigaţiei în conformitate cu prevederile prezentei legi şi Legii privind Centrul Naţional pentru Protecţia Datelor cu Caracter Personal.

Articolul 79. Probele

(1) Centrul poate să utilizeze orice mijloc de probă şi informaţii care servesc la constatarea existenţei sau lipsei încălcării.

(2) În scopul aplicării prezentei legi, Centrul admite atît probe directe, cît şi probe indirecte:

a) probele directe sînt depoziţiile martorilor sau ale altor persoane, probele materiale, înscrisurile, înregistrările audio şi/sau video, concluziile experţilor şi orice alte dovezi care probează în mod expres existenţa sau lipsa unei încălcări a legii;

b) probele indirecte sînt probele care nu dovedesc în mod direct existenţa sau lipsa unei încălcări a legii, însă pot conduce la anumite concluzii logice cu alte probe directe sau indirecte, precum că o încălcare a legii există sau a existat la un moment dat ori nu există şi nu a existat la un moment dat.

(3) În cazul lipsei sau insuficienţei probelor ce ar demonstra existenţa încălcării, Centrul constată prin decizie lipsa faptei încălcării.

Articolul 80. Confidenţialitatea investigaţiei

(1) Persoanele care, în virtutea drepturilor şi atribuţiilor ce le revin în temeiul prezentei legi, au luat cunoştinţă de informaţiile investigaţiei, inclusiv alte persoane care le-au devenit cunoscute astfel de informaţii, au obligaţia să asigure confidenţialitatea acestora, fiind pasibile sancţiunilor prevăzute de legislaţie.

(2) Datele personale care au fost prelucrate în cadrul investigaţiilor Centrului sînt confidenţiale şi nu pot fi ridicate, interceptate, obţinute şi/sau utilizate în orice alt mod decît dacă subiectul de date şi-a dat consimţămîntul expres privind o astfel de prelucrare sau în condiţiile de transmitere autorizată de Centru şi nu pot fi utilizate în cazul în care ar putea înrăutăţi situaţia subiectului de date.

(3) Inspectorul de protecţie a datelor, subiectul de date sau alte persoane, care în virtutea drepturilor şi atribuţiilor ce le revin în temeiul prezentei legi, au luat cunoştinţă sau le-au devenit cunoscute informaţiile din cadrul investigaţiei nu pot fi audiaţi sau interogaţi de către alte organe sau organizaţii în ceea ce priveşte esenţa informaţiilor din cadrul investigaţiei, cu

excepţia instanţei de judecată. Informaţia, documentele şi materialele investigaţiei nu poate fi utilizată decît cu autorizaţia Centrului.

(4) Acţivităţile, actele, informaţiile şi materialele Centrului pot fi supuse doar controlului judecătoresc, cu condiţia asigurării confidenţialităţii şi securităţii acestor date.

(5) Materialele investigaţiei nu pot fi date publicităţii dacă pot genera riscuri esenţiale pentru dreptul la viaţa intimă, familială şi privată a subiectului de date. Centrul poate da publicităţii informaţii generale din materialele investigaţiei precum obiectul investigaţiei, date despre operatori, persoanele împuternicite de operator, terţii, destinatarii şi entităţile care nu sînt destinatare, privind mersul şi/sau finalitatea investigaţiei, în scopul informării societăţii.

Articolul 81. Accesul şi păstrarea materialelor investigaţiei

(1) Subiectul de date care a depus cererea sau alte persoane care sunt vizate de investigaţie pot solicita în scris sau în format electronic potrivit cerinţelor semnăturii electronice şi a documentului electronic, acces la materialele investigaţiei. Eliberarea copiilor investigaţiei se acordă gratuit o singură dată, pentru solicitările ulterioare fiind percepută o taxă, mărimea căreia se stabileşte de Centru în conformitate cu un regulament pe care îl elaborează şi îl aprobă. Taxa percepută se varsă în bugetul de stat.

(2) Până la finalizarea investigaţiei, accesul la materialele acumulate poate fi oferit doar dacă inspectorul de protecţie a datelor consideră posibil, primind autorizarea conducătorului ierarhic superior, cu respectarea prezumţiei de nevinovăţie, să nu fie afectate interesele altor persoane, de a evita obstrucţionarea şi/sau prejudicierea investigaţiei sau a acţiunilor procedurale desfăşurate în conformitate cu legea.

(3) În cazul în care materialele investigaţiei conţin informaţii atribuite la secret de stat, secret comercial, secret bancar sau secret al dosarului special, informaţii ce ţin de confidenţialitatea procesului contravenţional sau penal sau alte informaţii oficiale cu accesibilitate limitată, Centrul restricţionează accesul la acestea.

(4) În procesul examinării cererii nu se admite divulgarea informaţiilor privind viaţa intimă, familială şi privată a subiecţilor de date fără acordul scris sau în format electronic potrivit cerinţelor semnăturii electronice şi documentului electronic, în condiţiile legii.

(5) Dreptul de acces nu include accesul la documentele interne sau la corespondenţa Centrului.

(6) Accesul la materialele investigaţiei este acordat cu condiţia ca informaţia să fie folosită numai în cadrul investigaţiei efectuate de Centru sau procedurii judiciare eventual legate de aceasta.

(7) Centrul nu are obligaţia să efectueze traducerea materialelor şi informaţiilor solicitate.

(8) După finalizarea investigaţiei, materialele, care nu au fost examinate de instanţa de judecată se păstrează în arhiva Centrului pe o perioadă de 10 ani.

(9) Materialele investigaţiei care au fost examinate de instanţa de judecată se păstrează în arhiva instanţei judecătoreşti care a judecat cauza în prima instanţă.

(10) Materialele investigaţiei care conţin secret de stat se păstrează în arhiva Centrului sau a instanţei de judecată, după caz.

(11) Accesul la materialele investigaţiei care se păstrează în condiţiile prevăzute de prezentul articol se decide de către conducerea Centrului sau de o altă persoană delegată în acest sens de directorul Centrului, după caz, de preşedintele instanţei la care se păstrează acestea, cu respectarea prevederilor prezentului capitol.

Articolul 82. Emiterea şi comunicarea deciziilor

(1) La finalizarea investigaţiei, inspectorul de protecţie a datelor responsabil de investigaţie, sau, după caz, inspectorii de protecţie, conducătorul grupului prezintă prin nota motivată, concluzia referitor la rezultatele investigaţiei efectuate, cu descrierea detaliată a circumstanţelor de fapt şi de drept şi propune, după caz, măsuri de înlăturare şi corectare a neconformităţilor şi sancţiunea pecuniară ce urmează a fi aplicată, cu întocmirea deciziei.

(2) În funcţie de rezultatul şi de faptele constatate în cadrul investigaţiei Centrul, prin decizie, constată inaplicabilitatea legii sau că nu există fapta încălcării, ori poate dispune, separat sau cumulativ, următoarele:

a) rectificarea, suspendarea, blocarea, interzicerea, încetarea prelucrării şi/sau a intenţiei de prelucrare a datelor personale, inclusiv, după caz, asupra mijloacelor care sunt sau urmează să fie utilizate pentru prelucrare care nu respectă prevederile Legii privind protecţia datelor caracter personal, sau care pot genera riscuri esenţiale pentru dreptul la viaţa intimă, familială şi privată a persoanei în ceea ce priveşte colectarea, înregistrarea, organizarea, stocarea, păstrarea, restaurarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea, diseminarea sau în orice alt mod;

b) distrugerea sau ştergerea datelor personale, cu sau fără îndepărtarea sau dezinstalarea software-ului tehnic, hardware-ului, soluţiilor tehnologiei informaţionale care au servit la comiterea încălcării legislaţiei privind protecţia datelor personale;

c) repunerea în drepturi a subiecţiilor de date.

(3) Deciziile se semnează de către directorul Centrului, directorul adjunct sau de către o altă persoana responsabilă, desemnată în acest sens prin ordinul directorului Centului.

(4) Decizia se comunică persoanei vizate, în termen de 10 zile lucrătoare de la data emiterii, prin scrisoare recomandată sau în format electronic conform cerinţelor semnăturii electronice şi documentului electronic sau prin orice mijloc care să confirme recepţionarea acesteia.

(5) În cazul în care comunicarea unei decizii nu poate fi realizată în condiţiile prevăzute de alin. (4), pe motiv că persoana vizată nu a putut fi găsită sau din alte motive care pot fi atribuite persoanei sau persoanelor în cauză,

Centrul poate publica un anunţ într-un ziar de nivel naţional sau local, în care se menţionează că a fost luată o decizie care poate fi ridicată la sediul Centrului. În cazul publicării anunţului dat, după scurgerea a 5 zile din acest moment, se va considera că persoana vizată a fost informată.

Articolul 83. Executarea deciziilor Centrului

(1) Deciziile devin executorii şi urmează a fi îndeplinite în termenul menţionat în ele, cu obligaţia de a informa în scris Centrul despre măsurile întreprinse. Centrul poate stabili termenul de executare a deciziei de până la 6 luni.

(2) În cazul neexecutării în termen a deciziei Centrului, pentru măsurile stabilite la art. 82 alin. (2) lit. a); b); c), de către persoanele vizate, executorul judecătoresc efectuează executarea silită a acesteia în conformitate cu prevederile prezentei legi şi ale Codului de executare.

(3) Instanţa de judecată se va expune în toate cazurile asupra mijloacelor care au fost ridicate de Centru în rezultatul investigării, inclusiv cu privire la trasmiterea acestora către organul abilitat să le comercializeze, fără implicarea Centrului.

Articolul 84. Citarea

(1) Citaţia este individuală şi trebuie să cuprindă:

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

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

c) ora, ziua, luna şi anul, locul de prezentare a persoanei citate, menţionîndu-se consecinţele legale în caz de neprezentare;

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

(2) Persoana se citează la adresa unde locuieşte sau la adresa juridică, iar dacă aceasta nu este cunoscută, la adresa locului său de muncă.

(3) În caz de schimbare a adresei, persoana este citată la noua sa adresă numai dacă a informat Centrul despre schimbarea intervenită sau dacă Centrul determină că s-a produs o schimbare de adresă pe baza datelor obţinute.

(4) Persoana vizată, în termen de cel mult 3 zile, informează Centrul despre schimbarea domiciliului.

(5) Persoana vizată poate fi citată repetat, la sediul sau domiciliul reprezentantului legal, dacă nu s-a prezentat după prima citare legal îndeplinită.

(6) Citaţia se înmînează personal celui citat, care va semna dovada de primire.

(7) Centrul poate solicita suportul organului de poliţie privind citarea. Dacă persoana citată nu vrea să primească citaţia, refuzul de primire se consemnează într-un proces-verbal privind refuzul primirii citaţiei.

(8) În cazul în care citarea se face potrivit alin. (2) şi (5), administraţiile instituţiilor respective sînt obligate să înmîneze de îndată citaţia persoanei citate contra semnătură, certificîndu-i semnătura în dovada de primire sau indicînd motivul pentru care nu s-a putut obţine semnătura acesteia. Dovada de primire se expediază Centrului.

(9) Dacă persoana citată nu se află acasă, citaţia se înmînează soţului/soţiei, unei rude sau oricărei persoane care locuieşte cu ea ori care în mod obişnuit îi recepţionează corespondenţa. Citaţia nu poate fi înmînată unui minor sub 14 ani sau unei persoane bolnave mintal.

(10) Citarea se poate face şi prin notă telefonică sau telegrafică, prin telefax, poştă electronică ori prin orice alt sistem de mesagerie electronică în cazul în care Centrul dispune de mijloacele tehnice necesare pentru a dovedi că citaţia a fost primită sau efectuată.

Aricolul 85. Examinarea altor adresări

Adresările care nu întrunesc condiţiile statuate de prezenta lege se examinează în condiţiile altor prevedri legale, fără emiterea deciziilor.

Capitolul IX
CĂI DE ATAC, RĂSPUNDERE ŞI SANCŢIUNI

Articolul 86. Dreptul la o cale de atac judiciară eficientă împotriva actelor administrative emise de Centru

(1) Deciziile emise de Centru şi comunicate în condiţiile art. 82 alin. (4) şi (5), pot fi contestate la conducătorul ierarhic superior al persoanei care a semnat decizia sau direct în instanţa de judecată în contencios administrativ. Deciziile semnate de director se contestă direct în instanţa de judecată.

(2) Contestaţia poate fi depusă în termen de 30 zile din momentul aducerii la cunoştinţă a deciziei. Conducătorul ierarhic va examina contestaţia în termen de 30 de zile lucrătoare. Decizia emisă de conducătorul ierarhic în rezultatul examinării contestaţiei poate fi contestată în instanţa de judecată, în termen de 30 zile, din momentul aducerii la cunoştinţă a deciziei.

(3) În cazul în care subiectul de date nu a fost informat în condiţiile art. 78 alin. (28) sau cererea nu a fost examinată în conformitate cu normele specifice din prezenta lege, poate contesta acţiunile sau inacţiunile Centrului în condiţiile alin. (1).

(4) Prin derogare de la prevederile legale pînă la soluţionarea definitivă a cauzei, executarea deciziilor Centrului nu poate fi suspendată, cu excepţia cazurilor în partea ce vizează aplicarea sancţiunilor pecuniare, dispunerea distrugerii sau ştergerii datelor personale sau în cazul în care prejudiciul ar putea depăşi interesul privat sau public urmărit.

(5) Încheierea judecătorească privind suspendarea sau refuzul suspendării deciziei Centrului poate fi contestată cu recurs în termen de 15 zile. recursul împotriva încheierii se examinează în termen restrîns, care nu va depăşi 10 zile de la data depunerii cererii de recurs.

Articolul 87. Dreptul la o cale de atac judiciară eficientă împotriva unui operator sau a unei persoane împuternicite de operator

(1) Orice subiect de date are dreptul de a depune o cerere direct în instanţa de judecată, dacă pretinsa încălcare s-a desfăşurat în Republica Moldova, fără a aduce atingere drepturilor şi atribuţiilor Centrului.

(2) În cazul în care cererea se referă la exercitarea drepturilor subiecţilor de date prevăzute în Capitolul III, această cerere va fi iniţial înaintată operatorului de date sau persoanei împuternicite de operator în condiţiile legii. În cazul în care subiectul de date nu primeşte un răspuns din partea operatorului sau persoanei împuternicite de operator în timpul stabilit conform Capitolului III sau în cazul în care răspunsul sau acţiunile întreprinse de aceştea sunt considerate inadecvate sau nu rezolvă cererea, subiectul de date poate depune o cerere direct în instanţa de judecată în modul prevăzut de legislaţie, fără a aduce atingere drepturilor şi atribuţiilor Centrului.

Articolul 88. Dreptul la despăgubiri şi răspunderea

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

(2) Orice operator implicat în operaţiunile de prelucrare este răspunzător pentru prejudiciul cauzat de operaţiunile de prelucrare prin care s-au încalcă prevederile prezentei lege şi alte acte normative din domeniul protecţiei datelor personale. Persoana împuternicită de operator este răspunzătoare pentru prejudiciul cauzat de prelucrare numai în cazul în care a acţionat în afara sau în contradicţie cu instrucţiunile legale ale operatorului sau nu a respectat obligaţiile prevăzute de prezenta lege şi alte acte normative din domeniul protecţiei datelor cu caracter personal care revin în mod specific persoanelor împuternicite de operator .

(3) Operatorul sau persoana împuternicită de operator se exonerează de răspundere în temeiul alin. (2) dacă dovedeşte că nu este răspunzător în niciun fel pentru evenimentul care a cauzat prejudiciul.

(4) În cazul în care mai mulţi operatori sau mai multe persoane împuternicite de operator, sau un operator şi o persoană împuternicită de operator sunt implicaţi/te în aceeaşi operaţiune de prelucrare şi răspund, în temeiul alin. (2) şi (3), pentru orice prejudiciu cauzat de prelucrare, fiecare operator sau persoană împuternicită de operator este răspunzător/oare 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 ceilalţi operatori sau de la celelalte persoane împuternicite de operator implicate în aceeaşi operaţiune de prelucrare recuperarea acelei părţi din despăgubiri care corespunde părţii lor

de răspundere pentru prejudiciu, în conformitate cu condiţiile stabilite la alin. (2).

(6) Cererea de despăgubire se depune în instanţa judecătorească în cazul în care este stabilit operatorul sau persoana împuternicită de operator. Subiectul de date poate alege să depună cererea la instanţa de judecată în a cărei rază teritorială îşi are reşedinţa obişnuită. În cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică care acţionează în exercitarea atribuţiilor sale publice, cererea de chemare în judecată trebuie depusă în instanţa în a cărei rază teritorială se află autoritatea publică.

Articolul 89. Răspunderea administrativă pentru încălcare prevederilor prezentei legi

(1) În cazul încălcării prevederilor prezentei legi, prin decizie se aplică avertisment sau sancţiune pecuniară. Aplicarea avertismentului sau a sancţiunii pecuniare nu exclude aplicarea măsurilor de înlăturare şi corectare a neconformităţilor.

(2) Răspunderea administrativă a persoanei juridice de drept public sau drept privat nu exclude, după caz, răspunderea persoanei fizice, a persoanei cu funcţie de răspundere sau a persoanei cu funcţii de conducere pentru fapta săvîrşită.

(3) Atunci cînd se impune aplicarea unei sancţiuni pecuniare, valoarea acesteia se determină în fiecare caz în parte, luînd în consideraţie următoarele aspecte:

a) natura, gravitatea şi durata încălcării, ţinându-se seama de natura, domeniul de aplicare sau scopul prelucrării în cauză, precum şi de numărul persoanelor vizate afectate şi de nivelul prejudiciilor suferite de acestea;

b) dacă încălcarea a fost comisă intenţionat sau din neglijenţă;

c) orice acţiuni întreprinse de operator sau de persoana împuternicită de operator pentru a reduce prejudiciul suferit de subiectul de date;

d) gradul de responsabilitate al operatorului sau al persoanei împuternicite de operator ţinându-se seama de măsurile tehnice şi organizatorice implementate de aceştia în temeiul art. 30 şi 42;

e) eventualele încălcări anterioare relevante comise de operator sau de persoana împuternicită de operator;

f) gradul de cooperare cu Centru pentru a remedia încălcarea şi a atenua posibilele efecte negative ale încălcării;

g) categoriile de date personale afectate de încălcare;

h) modul în care încălcarea a fost adusă la cunoştinţa Centrului, în special, dacă şi în ce măsură operatorul sau persoana împuternicită de operator a notificat încălcarea;

i) în cazul în care au fost dispuse anterior măsuri de înlăturare şi corectare a neconformităţilor împotriva operatorului sau persoanei împuternicite de operator în cauză cu privire la acelaşi obiect, respectarea respectivelor măsuri;

j) cifra de afaceri sau venitul anual (persoană fizică) al operatorului

k) aderarea la coduri de conduită aprobate, în conformitate cu art. 45, sau la mecanisme de certificare aprobate, în conformitate cu art. 47;

l) orice alt factor agravant sau atenuant aplicabil circumstanţelor cazului, cum ar fi beneficiile financiare dobândite sau pierderile evitate în mod direct sau indirect de pe urma încălcării.

(4) În cazul în care un operator sau o persoană împuternicită de operator încalcă în mod intenţionat sau din neglijenţă, pentru aceeaşi operaţiune de prelucrare sau pentru operaţiuni de prelucrare conexe, mai multe dispoziţii din prezenta lege, cuantumul total al sancţiunii pecuniare nu poate depăşi suma prevăzută pentru cea mai gravă încălcare.

(5) Pentru încălcările următoarelor dispoziţii, în conformitate cu alin. (3), se aplică sancţiuni pecuniare de până un milion de lei, sau, în cazul unei întreprinderi, de până la 1 % din cifra de afaceri mondială totală anuală corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare:

a) obligaţiile operatorului şi ale persoanei împuternicite de operator în conformitate cu art. 8 alin. (4), 10, 30-44, 47 şi art. 48;

b) obligaţiile organismului de certificare în conformitate cu art. 47 şi 48;

c) obligaţiile organismului de monitorizare în conformitate cu art. 46.

(6) Pentru încălcarea dispoziţiilor stabilite la alin. (5) de către operator sau persoană împuternicită de operator persoană juridică de drept public se va aplica un avertisment, cu aplicarea după caz a măsurilor de înlăturare şi corectare a neconformităţilor. În cazul în care se constată faptul că operatorul sau persoană împuternicită de operator persoană juridică de drept public nu au adus la îndeplinire în totalitate măsurile de înlăturare şi corectare a neconformităţilor se va aplica o sancţiune pecuniară de până la 100 mii lei.

(7) Pentru încălcările următoarelor dispoziţii, în conformitate cu alin. (3), se aplică sancţiuni pecuniare de până la 2 milioane de lei, sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exerciţiului financiar anterior, luându-se în calcul cea mai mare valoare:

a) principiile de bază pentru prelucrare, inclusiv condiţiile privind consimţământul, în conformitate cu art. 4, 5, 8 şi 9;

b) drepturile persoanelor vizate în conformitate cu art. 17-27;

c) transferurile de date cu caracter personal către un destinatar dintr-o altă ţară sau o organizaţie internaţională, în conformitate cu art. 49-54;

d) orice obligaţii în temeiul legislaţiei naţionale adoptate în temeiul art. 12, 14, 15, 16 şi 92;

e) nerespectarea unui ordin, instrucţiuni, regulament sau a oricărui alt act administrativ sau a unei limitări temporare sau definitive asupra prelucrării, sau a suspendării fluxurilor de date, emisă de către Centru, sau neacordarea accesului.

(8) Pentru neexecutarea deciziei emise de Centru, pentru măsurile stabilite la art. 82 alin.(2) lit. a); b) şi c) se aplică, în conformitate cu alin. (3), sancţiuni pecuniare de până la 2 milioane de lei, sau, în cazul unei

întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare.

(9) Pentru încălcarea dispozițiilor stabilite la alin. (7) și (8) de către operator sau persoană împuternicită de operator persoană juridică de drept public se va aplica un avertisment cu aplicarea, după caz a măsurilor de înlăturare și corectare a neconformităților. În cazul în care se constată faptul că operatorul sau persoană împuternicită de operator persoană juridică de drept public nu au adus la îndeplinire în totalitate măsurile de înlăturare și corectare a neconformităților se va aplica o sancțiune pecuniară de până la 100 mii lei.

(10) În cazul nerespectării măsurilor dispuse sau în cazul refuzului de furnizare a tuturor informațiilor și documentelor solicitate în cadrul procedurii de investigație, Centrul poate dispune, prin decizie, aplicarea unei sancțiuni pecuniare de până la 50 mii lei pentru fiecare zi de întârziere, calculată de la data stabilită prin decizie. Calculul va fi efectuat ținîndu-se cont de continuitatea încălcării.

(11) În cazul unei încălcări ușoare și părțile s-au împăcat sau a fost retrasă cererea de către subiectul de date, iar valoarea sancțiunea pecuniară de a fi impusă ar constitui o sarcină disproporționată pentru operator persoană fizică poate fi emis un avertisment în locul unei sancțiuni pecuniare.

(12) În cazul sancțiunii pecuniare în privința organelor de ocrotire a legii, se va ține cont de prevederile aplicabile din Capitolul VII raportate la normele de trimitere enunțate supra.

(13)Termenul de atragere la răspundere administrativă pentru încălcarea prevederilor prezentei legi este de 5 ani de la momentul săvîrșirii încălcării. Încălcarea continuă se consumă în momentul încetării acțiunii sau inacțiunii încălcării sau al survenirii unor evenimente care împiedică această activitate. Încălcarea prelungită se consumă în momentul săvîrșirii ultimei acțiuni sau inacțiuni al încălcării.

(14) Persoana nu poate fi trasă la răspundere administrativă pentru încălcarea prevederilor prezentei legi și investigația încetează în următoarele cazuri:

a) nu există fapta încălcării;

b) a expirat termenul de atragere la răspundere administrativă pentru încălcarea prevederilor prezentei legi;

c) pentru aceiași faptă și privitor la aceeași persoană există o decizie/hotărîre judecătorească definitivă;

d) nu este identificat făptuitorul.

Articolul 90. Prelucrarea și accesul public la documentele oficiale

Prelucrarea datelor personale și accesul la aceste date din documentele oficiale se va efectua ținîndu-se cond de proporționalitatea și echilibrul între dreptul la viața intimă, familială și privată în legătură cu prelucrarea datelor personale și dreptul de acces la informație și la libertatea de exprimare.

Articolul 91. Dispoziţii specifice privind răspunderea adminstrativă

(1) Sumele ce reprezintă sancţiuni pecuniare aplicate de Centru se fac venit la bugetul de stat.

(2) Decizia de aplicare a sancţiunilor pecuniare trebuie să conţină termenul limită în care urmează a fi achitată sancţiunea. Termenul-limită în care urmează a fi achitată sancţiunea nu poate fi mai mare de 30 de zile de la data comunicării deciziei privind aplicarea sancţiunii.

(3) Deciziile de sancţionare, în dependenţă de caz, pot fi publicate pe pagina oficială a Centrului, cu pseudonimizarea sau anonimizarea datelor personale, dacă este cazul.

(4) În cazul în care persoanele prevăzute în decizia de sancţionare au achitat sancţiunea pecuniară în termen de 5 zile de la data notificării, acestea au dreptul la o scutire cu 25% din cuantumul sancţiunii calculate.

(5) Persoanele vizate în decizia de sancţionare vor informa Centrul cu privire la măsurile luate pentru executarea deciziei, inclusiv în privinţa măsurilor de înlăturare şi corectare a neconformităţilor şi/sau a sancţiunii pecuniare, în termenul prevăzut, cu prezentarea dovezilor în acest sens.

Articolul 92. Prelucrarea unui număr de identificare de stat

(1) Prelucrarea unui număr de identificare de stat, inclusiv prin colectarea sau dezvăluirea documentelor ce-l conţin, se poate efectua în situaţiile prevăzute de art. 5 alin. (1).

(2) Prelucrarea unui număr de identificare de stat, inclusiv prin colectarea sau dezvăluirea documentelor ce-l conţin, în scopul prevăzut de art. 5 alin. (1) lit. f), respectiv al realizării intereselor legitime urmărite de operator sau de o parte terţă se efectuează cu instituirea următoarele garanţii:

a) punerea în aplicare de măsuri tehnice şi organizatorice adecvate, pentru respectarea, în special al reducerii la minimum a datelor, precum şi pentru asigurarea securităţii şi confidenţialităţii prelucrărilor de date personale conform dispoziţiilor art. 36;

b) desemnarea unui responsabil pentru protecţia datelor în conformitate cu art. 42;

c) aderarea la un cod de conduită aprobat în condiţiile art. 45;

d) stabilirea de termene de stocare în funcţie de natura datelor şi scopul prelucrării, în conformitate cu prevederile art. 13;

e) instruirea periodică cu privire la obligaţiile ce le revin, a persoanelor care, sub directa autoritate a operatorului sau a persoanei împuternicite, prelucrează date personale.

Articolul 93. Prelucrarea datelor personale în contextul relaţiilor de muncă

În cazul în care sunt utilizate sisteme de monitorizare prin mijloace de comunicaţii electronice şi/sau prin mijloace de supraveghere video/audio la locul de muncă, prelucrarea datelor personale ale angajaţilor, în scopul

realizării intereselor legitime urmărite de angajator, este permisă numai dacă se întrunesc următoarele condiţii:

a) interesele legitime urmărite de angajator vizează activităţi de importanţă deosebită, temeinic justificate şi prevalează asupra intereselor sau drepturilor şi libertăţilor persoanelor vizate;

b) angajatorul a realizat informarea prealabilă obligatorie, completă şi în mod explicit a angajaţilor;

c) angajatorul a consultat sindicatul sau, după caz, reprezentanţii angajaţilor înainte de introducerea sistemelor de monitorizare;

d) se respectă zona rezonabilă de intimitate;

e) alte forme şi modalităţi mai puţin intruzive pentru atingerea scopului urmărit de angajator nu s-au dovedit anterior eficiente; şi

f) durata de stocare a datelor personale este proporţională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepţia situaţiilor expres reglementate de lege sau a cazurilor temeinic justificate.

Articolul 94. Prelucrarea datelor genetice şi a datelor biometrice

Prelucrarea datelor genetice şi biometrice, în scopul realizării unui proces decizional automatizat sau pentru crearea de profiluri este interzisă, cu excepţia prelucrărilor efectuate de către sau sub controlul autorităţilor publice, în limitele atribuţiilor ce le sunt conferite prin lege şi în condiţiile stabilite de legile speciale care reglementează aceste domenii, care să prevadă şi garanţii adecvate pentru persoanele vizate.

Capitolul XI
DISPOZIŢII FINALE ŞI TRANZITORII

Articolul 95. Dispoziţii finale

(1) Prezenta lege intră în vigoare la data de 02 mai 2019.

(2) La data intrării în vigoare a prezentei legi se abrogă Legea nr. 133 din 8 iulie 2011 privind protecţia datelor cu caracter personal.

Articolul 96. Dispoziţii tranzitorii

(1) Din momentul intrării în vigoare a prezentei legi, din cuantumul final al sancţiunii pecuniare aplicate de Centru în conformitate cu prevederile prezentei legi, persoanele vizate sunt obligate să achite:

a) în primul an – 30 procente din cuantumul sancţiunii pecuniare stabilite;

b) în al doilea an - 50 procente din cuantumul sancţiunii pecuniare stabilite;

d) în al treilea an – 100 procente din cuantumul sancţiunii pecuniare stabilite.

(2) Prevederile alin. (1), nu influenţează asupra criteriilor de individualizare.

(3) Plîngerile şi cauzele ale căror proceduri de examinare de către Centru nu s-au încheiat pînă la data intrării în vigoare a prezentei legi, se examinează conform normelor de procedură şi materiale prevăzute de prezenta lege. În cazul în care prezenta lege prevede o sancţiune mai gravă, încălcarea săvârşită anterior datei intrării în vigoare a prezentei legi va fi sancţionată conform dispoziţiilor actelor normative în vigoare la data săvârşirii acesteia. În situaţiile în care, potrivit prezentei legi, fapta nu mai este considerată încălcare, aceasta nu se mai sancţionează, chiar dacă a fost săvârşită înainte de data intrării în vigoare.

(4) Litigiile care la data intrării în vigoare a prezentei legi se află în proces de examinare se soluţionează în conformitate cu normele legii în vigoare la data apariţiei litigiului.

(5) Deciziile privind autorizarea sau refuzul autorizării operaţiunilor de prelucrare a datelor cu caracter personal, precum şi cele de înregistrare sau de refuz a înregistrării în calitate de operator, odată cu intrarea în vigoare a prezentei legi nu vor avea efecte juridice. Operatorii urmează să reevalueze modalitatea de prelucrare a datelor şi să aducă actele sale în concordanţă cu prezenta lege.

(6) În termen de 9 luni de la data publicării prezentei legi, Guvernul:

a) va elabora şi va prezenta Parlamentului propuneri privind aducerea legislaţiei în vigoare în concordanţă cu prezenta lege;

b) va pune actele sale normative în concordanţă cu prezenta lege;

c) va asigura punerea în concordanţă a actelor normative ale autorităţilor publice centrale cu prezenta lege.

(7) În termen de 9 luni de la data publicării prezentei legi, Centrul:

a) va elabora şi va adopta actele normative necesare punerii în aplicare a prezentei legi;

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

PREŞEDINTELE PALAMENTULUI

NOTA INFORMATIVĂ
la proiectul Legii privind protecţia datelor cu caracter personal

1. Denumirea autorului şi, după caz, a participanţilor la elaborarea proiectului

Elaborarea prezentului proiect de lege a fost iniţiată de către Centrul Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova cu participarea ulterioară a experţilor rezidenţi din cadrul proiectului Twinning *„Consolidarea capacităţilor Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova"*, finanţat de Uniunea Europeană şi implementat prin Fundaţia Germană pentru Cooperare Juridică Internaţională (IRZ) şi Ministerul Justiţiei din Letonia.

În cadrul cooperării instituţionale dintre Centru şi Consiliul Europei, la data de 8 noiembrie 2017 au fost prezentate opiniile experţilor Consiliului Europei privind modificările legislative propuse de către Centru pe vectorul protecţiei datelor cu caracter personal al Republicii Moldova.

De asemenea în cadrul proiectului Twininng *"Consolidarea capacităţilor Centrului Naţional pentru Protecţia Datelor cu Caracter Personal"*, proiectul menţionat a fost supus modificărilor, analizat şi dezbătut de către experţii din cadrul ţărilor Uniunii Europene, şi anume: Germania, Letonia, Estonia, Malta.

2. Condiţiile ce au impus elaborarea proiectului de act normativ şi finalităţile urmărite

Proiectul Legii privind protecţia datelor cu caracter personal a fost elaborat în vederea racordării cadrului juridic naţional la cadrul internaţional.

În acest sens, se menţionează că instrumentul juridic internaţional care a pus premisele reglementării proceselor automatizate de prelucrare a datelor cu caracter personal, a constituit Convenţia nr. 108 din 28.01.1981 pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, deschisă spre semnare pentru statele membre ale Consiliului Europei la Strasbourg la 28 ianuarie 1981. Acest act internaţional a fost elaborat şi instituit de comunitatea europeană, odată cu aprecierea riscurilor ce pot surveni faţă de dreptul la viaţa privată a persoanelor fizice concomitent cu automatizarea proceselor de prelucrare a datelor cu caracter personal şi a definit care sunt datele cu caracter personal, precum şi a instituit rigori vizavi de colectarea, stocarea, utilizarea, prelucrarea datele cu caracter personal care constituie componenta de bază a vieţii private.

Statul Republica Moldova a semnat Convenţia nr. 108 la 04 mai 1998, urmată de procedura ratificării prin Hotărârea Parlamentului nr.483-XIV din 02 iulie 1999, cu intrarea în vigoare începând cu data de 01 iunie 2008. Conform dispoziţiilor art. 1, 3, 4 şi 8 ale Convenţiei nr.108 şi Protocolului adiţional la această Convenţie, odată ratificate, aceste acte au devenit parte componentă a dreptului intern şi prioritare faţă de legile interne, or, dacă există neconcordanţe între pactele şi tratatele privitoare la drepturile fundamentale

ale omului la care Republica Moldova este parte şi legile ei interne, prioritate au reglementările internaţionale, în temeiul art. 4 alin. (2) din Constituţia Republicii Moldova.

În vederea implementării aquis-ului comunitar privind protecţia datelor cu caracter personal, urmare a ratificarii Convenţiei nr. 108 şi Protocolului său adiţional, Republica Moldova a formulat unele declaraţii la Convenţia respectivă şi a desemnat Centrul Naţional pentru Protecţia Datelor cu Caracter Personal în calitate de autoritate naţională competentă pentru implementarea prevederilor Convenţiei nr. 108. În acest context, prin aderarea şi ratificarea acesteia, statul Republica Moldova şi-a asumat responsabilitatea de a asigura persoanei fizice dreptul la inviolabilitatea vieţii intime, familiale şi private.

În scopul detalierii şi reglementării principiilor de protecţie a datelor cu caracter personal stabilite în Convenţia nr. 108, statele membre ale Consiliului Europei au adoptat Directiva 95/46/CE a Parlamentului European şi a Consiliului din 24 octombrie 1995 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Prevederile Directivei 95/46/CE au fost transpuse cadrul legislativ al Republicii Moldova, iniţial în Legea nr. 17 din 15.02.2007 cu privire la protecţia datelor cu caracter personal, ulterior în Legea nr.133 din 08 iulie 2011 privind protecţia datelor cu caracter personal - act regulatoriu care a asigurat continuitatea transpunerii în sistemul de drept al Republicii Moldova a prevederilor Directivei 95/46/CE, şi care, actualmente, se dovedeşte a fi depăşit.

Conform studiilor întreprinse la nivelul Comisiei Europene, Directiva 95/46/CE privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date (încă în vigoare) cât şi Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecţia datelor cu caracter personal prelucrate în cadrul cooperării poliţieneşti şi judiciare în materie penală, nu mai corespund evoluţiilor recente în domeniul metodelor de colectare a datelor, astfel că legiuitorul Uniunii a propus o politică mai cuprinzătoare şi mai coerentă în prezenţa unui Regulament general privind protecţia datelor şi a unei Directive în domeniul cooperării poliţieneşti şi judiciare în materie penală.

În opinia aceleiaşi autorităţi, obiectivele şi principiile stabilite de către reglementările actuale în domeniul protecţiei datelor cu caracter personal rămân valabile, însă punerea lor în aplicare de către statele membre s-a făcut în mod diferit, generând insecuritate juridică şi o percepţie publică generală asupra existenţei unor riscuri majore, legate în special de activităţile online.

Evoluţiile tehnologice rapide şi globalizarea au generat noi provocări pentru protecţia datelor cu caracter personal. Amploarea colectării şi a schimbului de date cu caracter personal a crescut în mod semnificativ. Tehnologia permite atât societăţilor private, cât şi autorităţilor publice să utilizeze date cu caracter personal la un nivel fără precedent în cadrul activităţilor lor. Din ce în ce mai mult, persoanele fizice fac publice la nivel mondial informaţii cu caracter personal. Acest fapt a fost demonstrat prin

incidentul masiv de securitate, ce a condus la scurgere de informaţii, prelucrare ilegală şi utilizarea datelor cu caracter personal în scop de profilare a subiecţilor de date, în vederea obţinerii de predicţii, analize etc., cu implicarea companilor „Facebook" şi „Cambridge Analytica".

Indiscutabil, tehnologia a transformat deopotrivă economia şi viaţa socială, iar revoluţia digitală promite beneficii pentru sănătate, mediu, dezvoltarea internaţională şi eficienţa economică. Însă, tehnologia nu ar trebui să dicteze valori şi drepturi.

Ţinând cont de obiectivele Uniunii Europene referitoare la o piaţă unică digitală, tehnologia de tip cloud computing, „internetul obiectelor", volumul mare de date şi alte tehnologii sunt considerate esenţiale pentru competitivitate şi dezvoltare. Modelele comerciale exploatează noi capacităţi pentru colectarea în masă, transmiterea instantanee, combinarea şi reutilizarea informaţiilor cu caracter personal în scopuri neprevăzute şi sunt justificate de politici de confidenţialitate lungi şi impenetrabile. Acest lucru supune principiile protecţiei datelor la noi presiuni, simţindu-se nevoia unei gândiri noi privind modul în care sunt aplicate.

Aceste evoluţii au impus un cadru solid şi mai coerent în materie de protecţie a datelor în spaţiul Uniunii Europene, însoţit de o aplicare riguroasă a normelor, luând în considerare importanţa creării unui climat de încredere care va permite economiei digitale să se dezvolte pe piaţa internă. Persoanele fizice trebuie să aibă control asupra propriilor date cu caracter personal, iar securitatea juridică şi practică pentru persoane fizice, operatori economici şi autorităţi publice trebuie să fie consolidată.

Pentru a se asigura un nivel consecvent şi ridicat de protecţie a persoanelor fizice şi pentru a se îndepărta obstacolele din calea circulaţiei datelor cu caracter personal în cadrul Uniunii Europene, nivelul protecţiei drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea unor astfel de date ar trebui să fie echivalent în toate statele membre. S-a constatat că aplicarea consecventă şi omogenă a normelor în materie de protecţie a drepturilor şi libertăţilor fundamentale ale persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal, trebuie să fie asigurată în întreaga Uniune Europeană.

În legătură cu ce, în anul 2016 Parlamentul European şi Consiliul au adoptat pachetul de reformă legislativă privind protecţia datelor cu caracter personal, publicat în Jurnalul Oficial al Uniunii Europene pe data de 4 mai 2016, cu intrarea în vigoare începând cu **25 mai 2018**, pachet care integrează:

1. Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE *(Regulamentul general privind protecţia datelor* - în continuare fiind utilizat acronimul GDPR, la cazul gramatical contextual);

2. Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea

datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului;

3. Directiva (UE) 2016/681 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind utilizarea datelor din registrul cu numele pasagerilor (PNR) pentru prevenirea, depistarea, investigarea și urmărirea penală a infracțiunilor de terorism și a infracțiunilor grave.

Astfel, o parte din argumentarea necesității elaborării prezentului proiect de lege este direct interconectată cu spectru de acte legislative adoptate de către Parlamentul European și Consiliul, și anume, pachetul legislativ privind protecția datelor cu caracter personal adoptat Parlamentul European și Consiliul care va fi aplicat uniform în toate țările Uniunii Europene, fără excepție.

În acest sens, Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, transpusă în Legea nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal și Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală vor fi abrogate în data de 25 mai 2018, odată cu intrarea în vigoare a pachetului legislativ enunțat supra.

Astfel, necesitatea elaborării prezentului proiect de lege derivă din importanța consolidării sistemului legislativ privind garantarea respectării dreptului constituțional – inviolabilitatea vieții intime, private și familiale, prin aducerea în concordanță a sistemului de norme juridice ale dreptului național cu normele juridice de drept comunitar european în domeniul protecției datelor cu caracter personal.

Totodată, argumentarea necesității elaborării prezentului proiect de lege, constă în asigurarea unei linii continue de compatibilitate între reglementările dreptului intern și reglementările dreptului comunitar european, în materie de protecție a datelor cu caracter personal.

Prezentul proiect va contribui la realizarea angajamentelor asumate de către Republica Moldova în raport cu Uniunea Europeană și în temeiul legislației interne și ale angajamentelor internaționale, fiind posibil transferul de date cu caracter personal între statele membre ale Uniunii Europene și/sau alte state recunoscute ca fiind state care asigură un nivel adecvat de protecție a datelor cu caracter personal, fără a fi necesare alte măsuri adiționale de securitate din partea Republicii Moldova.

Este demn de notat și de atras atenție asupra faptului că, în cadrul celei de-a 2-a reuniuni a Subcomitetului de Asociere Republica Moldova-Uniunea Europeană, pentru Justiție, Libertate și Securitate, desfășurată la data de 09 iunie 2016, Brussels-Belgia, Centrul a făcut o retrospectivă a evenimentelor, realizărilor și provocărilor în perioada 2015-2016. În premieră, la Subcomitetul

de Asociere Republica Moldova-Uniunea Europeană, pentru Justiţie, Libertate şi Securitate a participat domnul Jan Ostoja-Ostaszewski, expert în domeniul protecţiei datelor cu caracter personal din cadrul Departamentului Justiţie şi Consumatori din cadrul Comisiei Europene (DJ JUST), care a evaluat pozitiv activitatea Centrului, totodată menţionând că „Republica Moldova este campion la implementarea aspectelor ce ţin de protecţia datelor în contextul Acordului de Asociere", obţinând performanţe prin alinierea la standardele şi normele europene. În cadrul aceluiaşi dialog, domnul Jan Ostoja-Ostaszewski, reieşind din performanţele obţinute de Centru, a recomandat Centrului să promoveze cererea de aderare în calitate de membru observator în cadrul Grupului de lucru pentru protecţia datelor la ARTICOLUL 29 al Uniunii Europene.

După o serie de întrevederi şi urmare a depunerii unei munci considerabile, în cadrul şedinţei plenare din 3-4 octombrie 2017, Republica Moldova prin intermediul Centrului, a fost acceptată în calitate membru cu statut de observator în cadrul Grupului de lucru pentru protecţia datelor la ARTICOLUL 29 al Uniunii Europene. Prima şedinţă la care a participat Republica Moldova a fost la 27 - 29 noiembrie 2017. Începând cu anul 2018 Grupul de lucru pentru protecţia datelor la ARTICOLUL 29 al Uniunii Europene şi-a schimbat denumirea în Comitetul European pentru Protecţia Datelor (CEPD).

Acceptarea Republicii Moldova în calitate membru cu statut de observator în cadrul Comitetului European pentru Protecţia Datelor reprezintă o premieră şi o realizare în spaţiul estic, or, actualmente Republica Moldova este unicul stat care deţine acest statut în cadrul Comitetului European pentru Protecţia Datelor, realizare care va consolida relaţiile mutuale între Republica Moldova şi Uniunea Europeană, atât sub aspect economic cât şi sub aspect politic.

Comitetul European pentru Protecţia Datelor este organismul Uniunii Europene însărcinat cu aplicarea GDPR-lui şi începând cu data de 25 mai 2018 va fi în centrul noului sistem de protecţie a datelor personale în Uniunea Europeană. Acesta va contribui la asigurarea aplicării consecvente a legislaţiei privind protecţia datelor în întreaga Uniune Europeană şi va depune eforturi pentru a asigura cooperarea eficace între autorităţile naţionale de supraveghere a prelucrării datelor cu caracter personal. Comitetul European pentru Protecţia Datelor nu numai că va publica orientări privind interpretarea conceptelor principale ale GDPR-lui, dar şi va fi solicitat să ia decizii obligatorii în cazul unor litigii privind prelucrarea transfrontalieră, asigurând astfel o aplicare uniformă a normelor Uniunii Europene întru evitarea tratării diferite a aceluiaşi caz în diferite jurisdicţii.

Este de menţionat faptul că Republica Moldova are toate drepturile pe care le are un stat membru al Uniunii Europene *(dreptul de a face comentarii, de a participa la şedinţe, dreptul de a fi informat despre activităţile în derulare şi de a participa la dezbateri)*, cu excepţia dreptului de vot.

Prin acest for internaţional, Republica Moldova va promova interesele statului în vederea ajustării şi conformării la standardele Uniunii Europene în domeniul protecţiei datelor cu caracter personal. Totodată, se arată că, obţinerea statutului de membru observator în cadrul Comitetului European pentru Protecţia Datelor al Uniunii Europene, este o etapă importantă în vederea recunoaşterii Republicii Moldova ca stat terţ ce asigură un nivel echivalent de protecţie a datelor cu caracter personal cu Uniunea Europeană.

În vederea depunerii cererii de a fi recunoscut ca stat terţ care asigură un nivel echivalent de protecţie a datelor cu caracter personal cu cel al Uniunii Europene, a fost inserat în Planul Naţional de acţiuni pentru implementarea Acordului de Asociere Republica Moldova - Uniunea Europeană în perioada 2017-2019 aprobat prin Hotărîrea Guvernului nr. 1472 din 30.12.2016 o acţiune în acest scop, şi anume, acţiunea nr. 17 din articolul 13 *„Pregătirea pentru depunerea cererii de către Republica Moldova în calitate de stat terţ care asigură un nivel adecvat de protecţie a datelor cu caracter personal"*.

Astfel, modificarea cadrului normativ în domeniul protecţiei datelor cu caracter personal, este o etapă principală şi decisivă în vederea recunoaşterii Republicii Moldova în calitate de stat care asigură un nivel echivalent de protecţie a datelor cu catracter personal cu Uniunea Europeană.

Determinarea nivelului echivalent de protecţie a datelor este realizată printr-o decizie a Comisiei Europene, după efectuarea unei analize minuţioase a cadrului legal naţional şi expertizarea sectorială sub aspect de politici de protecţie a datelor cu caracter personal: sectorul poliţienesc, sectorul educaţional, sectorul medical, setorul social etc., urmată de emiterea unei opinii din partea Comitetului European pentru Protecţia Datelor.

În aces sens, este de reţinut că, efectele unei decizii ale Comisiei Europene privind recunoaşterea Republicii Moldova drept stat care asigură un nivel adecvat de protecţie a datelor cu caracter personal egal cu cel asigurat de ţările membre ale Uniunii Europene, va genera un spectru larg de beneficii pentru Republica Moldova, printre care: sporirea credibilităţii statului Republica Moldova, consolidarea strategiei economice, dezvoltarea mediului de afaceri, atragerea investiţiilor, etc.

Comisia Europeană a recunoscut că, la moment, prezintă un nivel adecvat de protecţie a datelor următoarele state din afara UE: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay.

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislaţiei naţionale cu legislaţia Uniunii Europene

Prezentul proiect de lege este elaborat pentru executarea următoarelor documente de politici din care derivă angajamentele asumate de către Republica Moldova în legătură cu vectorul european:

Strategia naţională în domeniul protecţiei datelor cu caracter personal pentru anii 2013–2018 şi a Planului de acţiuni privind implementarea acesteia, aprobat prin Legea nr. 229 din 10 octombrie 2013 - Obiectivul specific nr. 3

„Consolidarea capacităţilor administrative şi instituţionale ale Centrului Naţional pentru Protecţia Datelor cu Caracter Personal"

La data de 28 martie 2018 a fot aprobat Planul de acţiuni pentru implementarea Acordului de Asociere Republica Moldova - Uniunea Europeană în perioada 2017-2019. Planul actualizat înglobează prioritățile noii Agende de Asociere şi stabileşte clar sarcinile instituţiilor responsabile de implementarea acţiunilor, în conformitate cu redistribuirea competenţelor. Totodată, sunt prevăzute măsurile necesare pentru implementarea Acordului de Asociere pe parcursul celor trei ani, dar şi măsuri de ajustare a legislaţiei naţionale la standardele şi principiile europene, în conformitate cu angajamentele asumate.

Ordine în care, proiectul Planului de acţiuni pentru implementarea Acordului de Asociere Republica Moldova - Uniunea Europeană în perioada 2017-2019, la pct. 13 **„Protecţia datelor cu caracter personal"**, acţiunea nr. L6, stabileşte modificarea Legii nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal, acţiune strategică care va fi realizată prin adoptarea prezentului proiect de lege.

Prezentul proiect de lege transpune Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor) şi Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, publicate în Jurnalul Oficial al UE nr. L 119 din 4 mai 2016.

4. Principalele prevederi ale proiectului şi evidenţierea elementelor noi

Prin prezentul proiect de lege se intenţionează armonizarea cadrului legislativ intern la cadrul legislativ al dreptului comunitar european, fiind operate o serie de modificări, după cum urmează a se exemplifica:

- **Obiectul legii:** pornind de la noţiunile şi uzanţele stabilite la nivelul statelor semnatare ale Convenţiei nr. 108 pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, a fost identificată necesitatea ajustării cadrului juridic naţional în partea ce vizează obiectul de reglementare al Legii privind protecţia datelor cu caracter personal, inclusiv prin prisma dezvoltării vertiginoase a tehnologiilor informaţionale, destinate prelucrărilor de date.

Se menţionează, că la momentul elaborării Legii nr. 133 din 08 iulie 2011 privind protecţia datelor cu caracter personal, obiectul legii s-a limitat la prelucrarea datelor cu caracter personal, nu şi la mijloacele prin care se intenţionează a fi efectuate aceste prelucrări.

Drept consecinţă, în urma efectuării investigaţiilor legalităţii operaţiunilor de prelucrare a datelor cu caracter personal, Centrul în repetate rânduri s-a confruntat cu situaţii în care a dispus în privinţa datelor cu caracter personal prelucrate, însă, a fost în imposibilitate să decidă asupra mijloacelor prin intermediul cărora se efectuau aceste operaţiuni, cum ar fi, spre exemplu camerele de supraveghere video ce captau imagini din interiorul bunurilor imobile ale operatorilor. Astfel, pârghiile legale existente, care puteau fi aplicate de Centru, nu soluţionau în esenţă încălcarea, or, utilizarea acestor mijloace era posibilă şi în continuare.

De reliefat că la moment, în Republica Moldova este facil de a procura dispozitive prin care poate fi colectată informaţia despre viaţa intimă, familială şi privată, inclusiv în mod ascuns, iar asupra utilizării acestora nu pot fi dispuse careva măsuri, în conformitate cu prevederile actuale ale Legii nr. 133 din 08 iulie 2011 privind protecţia datelor cu caracter personal.

- **Latura conceptuală:** un alt pas este reprezentat de includerea unor concepte noi, cum ar fi: *date genetice, date biometrice, marketing direct, pseudonimizarea şi anonimizarea datelor cu caracter personal, creare de profiluri, operator asociat, reprezentant, întreprindere, grup de întreprindere, reguli corporatiste obligatorii, servicii ale societăţii informaţionale etc.*

Conceptul de **creare de profiluri** a fost înclus în GDPR şi în Directiva (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, respectiv transpus şi în prezentul proiect de lege, în vederea protecţiei şi implementării unor garanţii solide în raport cu efectele negative pe care le poate genera operaţiunea de creare de profiluri, unul dintre cele mai grave fiind, discriminarea.

Conceptul de **marketing direct (prospectare comercială)** reprezintă o metoda de distribuţie a produselor şi serviciilor în care sânt utilizate concepte, tehnici şi instrumente de marketing, inclusiv prin intermediul poştei, serviciilor de comunicaţii electronice sau ale altor servicii de expediere, concretizate într-un demers orientat direct către subiectul de date personale, urmărind generarea unei reacţii cuantificabile.

Proiectul face o delimitare conceptuală între pseudonimizare şi anonimizare.

Pseudonimizare reprezintă prelucrarea datelor personale într-un asemenea mod încât acestea să nu mai poată fi atribuite unui subiect de date fără a se utiliza informaţii suplimentare.

Anonimizarea reprezintă modificarea datelor personale în aşa fel încât să nu poată fi identificată sau să ducă la identificarea subiectului de date, astfel încât detaliile privind circumstanţele personale sau materiale să nu mai permită atribuirea acestora unei persoane fizice identificate sau identificabile.

Elementele novatorii le constituie stabilirea principiilor aferente prelucrării datelor personale: principiul legalităţii, echităţii şi transparenţei; principiul limitării legate de scop; principiul de minimizării datelor; principiul exactităţii; principiul limitării legate de stocare, principiul integrităţii şi confidenţialităţii.

- **Drepturile subiectului de date cu caracter personal:** în vederea consolidării drepturilor cetăţenilor în raport cu operaţiunile de prelucrare a datelor cu caracter personal care îi vizează, au fost dezvoltate drepturile existente şi extinsă sfera drepturilor subiectului de date. Astfel, noua paletă de drepturi include: *dreptul la portabilitatea datelor, dreptul la ştergerea datelor (dreptul de a fi uitat), dreptul la rectificarea datelor, etc.*

Dreptul la portabilitatea datelor are un caracter de noutate în contextul utilizării datelor personale, fiind în acelaşi sens, un aspect al dreptului de acces la date. Drept care vizează portarea datelor şi reprezintă o modalitate de realizare a circulaţiei datelor cu caracter personal, întrucât datele pot fi transferate de la un operator la altul. Operatorul căruia i-au fost furnizate datele este ţinut să nu obstaculeze transferul informaţiilor. Portarea datelor constă în deplasarea, copierea sau, după caz, transmiterea acestora, dintr-un sistem informatic în altul.

Pe dimensiunea **dreptului de a fi uitat,** se pretinde că acesta ar fi unul vital, în conjunctura în care, circulă mult prea multe informaţii personale, fără a exista posibilitatea de a fi controlate şi fără a exista o etică a utilizării informaţiilor personale care circulă în societate.

Condiţiile privind consimţământul subiectului de date: obţinerea consimţământului pentru prelucrarea datelor cu caracetr personal nu este o condiţie nouă, totuşi reforma Uniunii Europene pe dimensiunea protecţiei datelor cu caracter personal a reformat instituţia „consimţământului". Astfel, consimţământul nu va fi considerat valid dacă vine „la pachet" cu alte chestiuni, cum ar fi termenii generali din cadrul unui contract, consimţământul trebuie să poată fi distins de toate celelalte chestiuni. Altfel zis, consimţământul nu poate fi aplicat unui set deschis de activităţi, el trebuie limitat la un context specific. Consimţământul va trebui acordat printr-o acţiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoştinţă de cauză şi clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal. Dacă prelucrarea datelor se face în mai multe scopuri, consimţământul ar trebui dat pentru fiecare scop în parte.

Responsabilizarea operatorilor de date cu caracter personal: este instituită responsabilitatea operatorului de a demonstra că subiectul datelor şi-a dat consimţământul pentru prelucrarea datelor sale cu caracter personal. Totodată, responsabilitatea operatorului de a lua măsuri adecvate pentru a furniza subiectului de date orice informaţii în legătură cu prelucrarea datelor cu caracter personal ce-l vizează şi gratuitatea furnizării acestor informaţii.

- Un articol aparte din prezentul proiect de lege, şi anume art. 12, este destinat prelucrării datelor cu caracter personal şi libertatea de exprimare şi

acces la informaţie. Astfel că, prezentul proiect de lege asigură şi recunoaşte dreptul la libertatea de exprimare şi de acces la informaţie oricărei persoane. Reglementările art. 12 au scopul de a asigura o pârghie de conciliere între prelucrarea datelor cu caracter personal şi libertatea de exprimare şi dreptul de acces la informaţie.

- **Sub aspectul căilor de atac** proiectul de lege reglementează dreptul subiectului de date de a sesiza Centrul, fiind operate unele modificări în procedura de examinare: în acord cu reglementările actuale, subiectul datelor cu caracter personal care consideră că prelucrarea datelor sale nu este conformă cu cerinţele legii privind protecţia datelor cu caracter personal, poate înainta Centrului o plîngere în termen de 30 de zile din momentul depistării încălcării. Prin proiectul de lege, este extins termenul de sesizare a Centrului de către subiectul de date cu caracter personal care are suspiciuni în raport cu legalitatea prelucrării datelor sale cu caracter personal.

În aceeaşi ordine, un alt element novatoriu vizează reglementarea obligaţiei Centrului de a informa subiectul de date cu privire la progresul şi rezultatele examinării investigaţiei ori de cîte ori este necesar la cererea subiectului de date, sau la fiecare trei luni şi posibilitatea subiectul de date care, din motive temeinice şi justificate, a omis termenul de prescrepţie, de a fi repus în termen în condiţiile Codului de procedură civilă.

- **Aplicarea sancţiunilor pentru comiterea încălcărilor prevederilor Legii privind protecţia datelor cu caracter personal:** dat fiind că, din momentul intrării în vigoare a Legii nr. 208 din 21 octombrie 2011 pentru completarea şi modificarea unor acte legislative, prin care a fost modificat şi completat Codul contravenţional (prin instituirea răspunderii contravenţionale pentru încălcarea legislaţiei cu privire la protecţia datelor cu caracter personal şi abilitarea Centrului cu competenţe de organ constatator) se constată ineficienţa măsurilor punitive în vigoare la moment, care se manifestă prin caracterul îndelungat al examinării de către instanţele de judecată a cauzelor contravenţionale pornite de Centru, or, contrar prevederilor art. 454 din Codul contravenţional, circa 95 la sută din aceste cauze se examinează cu depăşirea vădită a termenului de 30 zile legal stabilit. Mai mult, circa 40 la sută din procesele-verbale cu privire la contravenţie întocmite de Centru şi expediate în instanţa de judecată au fost/sînt examinate pe parcursul câtorva ani. Totodată, în majoritatea cazurilor, examinarea îndelungată a cauzelor contravenţionale pornite de Centru, determină expirarea termenului general de prescripţie a răspunderii contravenţionale prevăzut la art. 30 din Codul contravenţional, din care motiv, deciziile instanţei judecătoreşti se rezumă la constatarea vinovăţiei persoanelor în privinţa cărora au fost pornite procese contravenţionale de comiterea faptelor prejudiciabile imputate, însă fără dispunerea sancţiunii pecuniare (amenzii).

În acelaşi timp, se arată că soluţionarea cauzelor contravenţionale prin recunoaşterea vinovăţiei contravenienţilor şi sancţionarea acestora în limitele prevăzute la art. 74^1-74^3 Cod contravenţional, se rezumă la constatarea de către

instanţa de judecată a faptelor contravenţionale comise, fără a dispune obligarea contravenientului în vederea înlăturării cauzelor ce au dus la comiterea încălcărilor vizate. Drept consecinţă, nu se soluţionează în esenţă problema care a dus la constatarea de către Centru a încălcării comise la prelucrarea datelor cu caracter personal, or, în mare parte, contravenienţii se limitează la achitarea amenzilor stabilite de instanţa de judecată (care constituie o sumă infimă în raport cu încălcarea comisă), fără a executa efectiv obligaţiile legale ce le revin - acţiuni/inacţiuni privind neexecutarea sau executarea necorespunzătoare ale cărora constituie încălcarea în fapt.

Având ca premisă acelaşi obiectiv de fortificare a competenţelor Centrului, proiectul instituie atribuţia Centrului de a efectua investigarea legalităţii operaţiunilor de prelucrare a datelor cu caracter personal efectuate prin intermediul sistemelor de evidenţă al acestor date, amplasate în încăperile şi bunurile ce aparţin persoanelor fizice. Menţionăm, că potrivit reglementărilor naţionale şi internaţionale, operator al datelor cu caracter personal poate fi şi persoana fizică, iar lipsa pârghiilor legale ce ţin de investigarea operaţiunilor de prelucrare a datelor cu caracter personal efectuate de operatori-persoane fizice creează un vid legislativ.

Însă, având în vedere mediul din Republica Moldova, în proiect, se propune un mecanism treptat de aplicare a sancţiunilor pentru a asigura o perioadă de tranziţie în vederea adaptarii de către operatorii de date la noile rigori şi standarde europene.

Astfel, prezentul proiect de lege propune aplicarea unor sancţiuni de ordin pecuniar cu variabilele: a) de până la 2 mln lei, sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exerciţiului financiar anterior; sancţiuni aplicabile prin prisma unor citerii stricte de individualizare şi racordat la gravitatea încălcării.

De menţionat, că prevederile Regulamentului 2016/679, se aplică în raport cu orice agent economic/prestator de servicii/afaceri/bussines etc., care interferează cu cetăţenii Uniunii Europene, chiar dacă aceştia se află juridic pe teritoriul Republicii Moldova vor fi obligaţi să respecte legislaţia europeană.

- **Obţinerea mandatului judecătoresc de către Centru** - accesul reprezentanţilor Centrului la domiciliul, în încăperi, terenuri şi mijloace de transport, la echipamentele de prelucrare, la programele şi aplicaţiile, precum şi la documentele, înregistrările referitoare la prelucrarea de date personale, ce aparţin, sînt în posesie sau în folosinţa persoanei fizice, în lipsa acordului scris, se va permite numai în baza mandatului judecătoresc emis în condiţiile prezentului proiect de lege şi prezentat persoanei supuse investigaţiei.

Se remarcă că această practică nu este fără precedent în legislaţia naţională, or, competenţe similare pot fi regăsite spre exemplu în Legea concurenţei nr. 183 din 11 iulie 2012. În aceeaşi ordine de idei, în conformitate cu prevederile textului modernizat al Convenţiei nr. 108 pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, adoptat la cea de-a 29-a şedinţă plenară a Comitetului consultativ al

Convenţiei, se statuează clar că în calitate de operator de date cu caracter personal se constituie şi persoana fizică, iar autorităţile naţionale de protecţie a datelor cu caracter personal urmează să dispună de pârghii suficiente în acest sens.

Cu titlu de drept comparat, se menţionează că prevederea posibilităţii efectuării investigării de către autorităţile de protecţie a datelor cu caracter personal a legalităţii operaţiunilor de prelucrare a datelor cu caracter personal, efectuate de operatori-persoane fizice, este o împuternicire răspândită în numeroase ţări ale Uniunii Europene. Spre exemplu, Autoritatea Italiană de protecţie a datelor poate efectua investigarea spaţiilor private, dacă beneficiază de consimţământul informat al persoanei inspectate sau prin mandat judecătoresc *[Secţiunea 158 a Codului Protecţiei Datelor cu Caracter Personal].*

Putem menţiona de asemenea, cazul Spaniei, unde dreptul de investigare este şi mai extins, or, articolul 125(1) al Decretului Regal 1720/2007 stipulează că inspectorii au capacitatea de a controla încăperile unde are loc prelucrarea datelor cu caracter personal, orice locaţie unde sînt situate sistemele de evidenţă a datelor cu caracter personal şi domiciliul părţii inspectate. Mai mult, nu este necesar de a avea un mandat judecătoresc, ci doar autorizaţia directorului autorităţii spaniole de protecţie a datelor.

Astfel că, pentru a nu prejudicia investigaţia sub aspect de ascundere, modificare, ştergere, distrugere a sistemelor de evidenţă a datelor personale, echipamentelor de prelucrare, programelor şi aplicaţiilor, precum şi orice document sau înregistrare referitoare la prelucrarea de date personale, Centrul poate solicita direct instanţei de judecată eliberarea mandatului judecătoresc. Mandatul judecătoresc este valabil 30 de zile de la data emiterii şi poate fi prelungit cu încă 30 de zile. În cazul solicitării unui mandat judecătoresc, instanţa de judecată va verifica dacă efectuarea investigaţiei şi măsurile care urmează a fi luate nu sînt arbitrare sau excesive, avînd în vedere obiectul investigaţiei şi gravitatea pretinsei încălcări.

-În contextul activităţilor de investigare şi de asigurare a conformităţii prelucrării datelor cu caracter personal în sectorul poliţienesc şi în vederea implementării Directivei (UE) 2016/680 a Parlamentului European şi a Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autorităţile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracţiunilor sau al executării pedepselor şi privind libera circulaţie a acestor date şi de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului, prezentul proiect de lege vine cu un capitol întreg destinat prelucrării datelor cu caracter personal de către organele de ocrotire a legii, şi anume capitolul VII, care reglementează atribuţia Centrului de a supraveghea, reglementa şi investiga modul de prelucrare a datelor personale de către organele de drept în conformitate cu prezentul proiect de lege şi Legea privind Centrul Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova.

În acest sens, se arată că anterior Centrul Naţional pentru Protecţia Datelor cu Caracter Personal nu a efectuat anumite operaţiuni de investigare a prelucrării datelor cu caracter personal în sectorul poliţienesc, atât din lipsa personalului cât şi din cauza unor divergenţe între normele legale, cu toate că, *de jure*, există premise ca Centrul să efectueze operaţiuni de investigare a prelucrării datelor cu caracter personal în sectorul poliţienesc.

Dispoziţiile art. 28 al Constituţiei Republicii Moldova reafirmă poziţia Statului care respectă şi ocroteşte viaţa intimă, familială şi privată.

Conţinutul art. 54 consacră garanţia juridică conform căreia, în Republica Moldova nu pot fi adoptate legi care ar suprima sau ar diminua drepturile şi libertăţile fundamentale ale omului şi cctăţeanului. Alin. 2 din cadrul aceluiaşi articol stabileşte că exerciţiul drepturilor şi libertăţilor nu poate fi supus altor restrîngeri decît celor prevăzute de lege, care corespund normelor unanim recunoscute ale dreptului internaţional şi sînt necesare în interesele securităţii naţionale, integrităţii teritoriale, bunăstării economice a ţării, ordinii publice, în scopul prevenirii tulburărilor în masă şi infracţiunilor, protejării drepturilor, libertăţilor şi demnităţii altor persoane, împiedicării divulgării informaţiilor confidentiale sau garantării autorităţii şi imparţialităţii justiţiei. Restrîngerea trebuie să fie proporţională cu situaţia care a determinat-o şi nu poate atinge existenţa dreptului sau a libertăţii.

Mai mult, Statul Republica Moldova prin Legea nr. 110 din 09.06.2011, a ratificat Protocolul adiţional la Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, cu privire la autorităţile de supraveghere şi fluxul transfrontalier al datelor, adoptat la Strasbourg la 8 noiembrie 2001 şi semnat de Republica Moldova la 29 aprilie 2010 (Protocol), iar potrivit art. 1 din Protocol: *„Fiecare Parte va conferi uneia sau mai multor autorităţi responsabilitatea pentru asigurarea conformităţii cu măsurile prevăzute de legislaţia sa internă, care pun în vigoare principiile, stabilite în Capitolele 2 şi 3 ale Convenţiei, precum şi în acest Protocol. Cu acest scop, autorităţile menţionate mai sus, deţin, în special, drepturi de a investiga şi interveni, precum şi dreptul de a acţiona în judecată sau de a aduce în atenţia autorităţilor judiciare competente încălcările prevederilor din legislaţia internă care pune în aplicare principiile menţionate în alin. 1 al art. 1 din acest Protocol. Fiecare autoritate de control dă curs reclamaţiilor depuse de orice persoană cu privire la protecţia drepturilor ei/lui şi libertăţilor sale fundamentale cu privire la prelucrarea datelor cu caracter personal, ce ţin de competenţa lor”.*

Centrul exercită atribuţiile sale în completă independenţă în conformitate cu prevederile art. 19 din Legea nr. 133 din 08.07.2011 privind protecţia datelor cu caracter personal, art. 1 din Legea nr. 182 cu privire la aprobarea Regulamentului Centrului Naţional pentru Protecţia Datelor cu Caracter Personal, structurii, efectivului-limită şi a modului de finanţare a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal şi prevederile art. 1 pct. 3 din Legea nrt. 271 din 07.11.2013 privind formularea unor declaraţii

ale Republicii Moldova la Convenţia pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal - Centrul Naţional pentru Protecţia Datelor cu Caracter Personal a fost investit cu competenţa exclusivă de unică Autoritate de control al prelucrării datelor cu caracter personal, care este o autoritate publică autonomă, independentă şi imparţială faţă de alte autorităţi publice.

În acelaşi context se notează că Parlamentul Rpeublicii Moldova prin Legea comunicaţiilor electronice, nr. 241-XVI din 15 noiembrie 2007, republicată în Monitorul Oficial din 17 noiembrie 2017, a atribuit Centrului în temeiul art. 71 noi competenţe de a verifica măsurile tehnice şi organizatorice corespunzătoare în vederea protejării securităţii serviciilor prestate de furnizorii de servicii de comunicaţii electronice.

Subsecvent, concomitent cu intrarea în vigoare la data de 23 februarie 2018 a Legii cu privire la prevenirea şi combaterea spălării banilor şi finanţării terorismului în partea ce vizează controlul conformităţii operaţiunilor de prelucrare a datelor cu caracter personal efectuate de autorităţile specializate în prevenirea şi combaterea terorismului, inclusiv a Serviciului Prevenirea şi Combaterea Spălării Banilor. Eset necesar de remarcat că acţiunile ce urmează a fi întreprinse de entităţile vizate în prezenta lege presupun prelucrarea unui volum exorbitant de date cu caracter personal şi se răsfrânge asupra tuturor persoanelor fizice, chiar şi care au avut o tangenţă mică cu instituţiile financiar-bancare.

O altă lege care a adus atribuţii noi Centrului este Legea nr. 120 din 21 septembrie 2017 cu privire la prevenirea şi combaterea terorismului. Activitatea de prevenire şi combatere a terorismului va fi exercitată în mod special de Serviciul de Informaţii şi Securitate care prelucrează un volum extrem de mare de date personale, iar controlul conformităţii prelucrărilor de date cu caracter personal se efectuează de către Centru.

Prin spectrul de modificări legislative, Centrul a dobândit competenţă de a investiga prelucrarea datelor cu caracter personal atribuite inclusiv la secret de stat, şi anume, cele efectuate în cadrul acţiunilor de prevenire şi investigare a infracţiunilor, al punerii în aplicare a sentinţelor de condamnare sau al altor acţiuni ce ţin de procedura penală ori contravenţională, în condiţiile legii. Competenţă care este indisolubil conexată cu capitolul VII din prezentul proiect de lege.

Capitolul VII din prezentul proiect de lege, este destinat prelucrării datelor cu caracter personal de către operatori - organe de ocrotire a legii, care au competenţe stabilite prin lege în scopul prevenirii, investigării, depistării şi/sau urmăririi penale a infracţiunilor sau executării pedepselor penale, inclusiv protejarea şi prevenirea ameninţărilor la adresa ordinii publice, securităţii de stat şi securităţii naţionale şi în cadrul dosarului sau acţiunilor speciale de investigaţie.

Prin acelaşi capitol se prevede dispoziţia conform căreia, legile speciale care reglementează domeniului de activitate a organelor de ocrotire a legii trebuie să stipuleze cel puţin obiectivele prelucrării, categoriile de date personale care urmează să fie prelucrate şi scopul prelucrării. Totodată, operatorul va fi obligat să facă distincţia clară între datele personale ale diferitelor categorii de subiecţi de date, cum ar fi bănuiţii, învinuiţii, martorii, victimele, terţii, persoanele aflate în perioada de probaţiune, condamnaţii, persoanele reţinute, arestate şi altele.

Se propune ca, organul de ocrotire a legii să ia toate măsurile necesare pentru a se asigura că datele personale care sunt inexacte, incomplete sau nu mai sunt actuale nu sunt transmise sau puse la dispoziţie. În acest scop, fiecare autoritate competentă verifică, în măsura în care este posibil, calitatea datelor personale înainte ca acestea să fie transmise sau puse la dispoziţie. În măsura în care acest lucru este posibil, în cadrul tuturor transmiterilor de date personale, se adaugă informaţii necesare care permit evaluarea gradului de exactitate, caracterul integral, gradul de fiabilitate şi de actualitate al datelor personale.

Un alt element important care a contribuit la cristalizarea competenţelor Centrului de a efectua operaţiuni de investigaţie a prelucrării datelor cu caracter personal în cadrul acţiunilor de prevenire şi investigare a infracţiunilor, al punerii în aplicare a sentinţelor de condamnare sau al altor acţiuni ce ţin de procedura penală ori contravenţională, în condiţiile legii, îl reprezintă Ghidul practic privind utilizarea datelor cu caracter personal în sectorul poliţienesc, adoptat de către Comitetul Consultativ al Convenţiei 108 pentru protecţia persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal, adoptat la data de 15 februarie 2018 la Strasbourg.

Se menţionează că Ghidul invocat are o pondere deosebită, atât sub aspect de utilitate cât şi sub aspect de comprehensivitate întrucât explică într-o manieră accesibilă faptul că *toate prelucrările de date trebuie să respecte principiile de necesitate, proporţionalitate şi limitare a scopului. Aceasta implică faptul că prelucrarea datelor cu caracter personal în cadrul poliţiei ar trebui să se bazeze pe scopuri predefinite, clare şi legitime stabilite de lege; ar trebui să fie necesar şi proporţional cu aceste scopuri legitime şi nu ar trebui să fie prelucrate într-un mod incompatibil cu aceste scopuri. Prelucrarea datelor ar trebui să se facă în mod legal, corect şi transparent. Datele personale din cadrul poliţiei ar trebui, de asemenea, să fie adecvate, relevante şi neexcesive în raport cu scopurile. În cele din urmă, acestea trebuie să fie corecte şi actualizate pentru a asigura cea mai înaltă calitate a datelor".*

Acelaşi Ghid, plasează în sarcina autorităţilor de supraveghere a prelucrării datelor cu caracter personal, în cazul Republicii Moldova, Centrul Naţional pentru Protecţia Datelor cu Caracter Personal, atribuţia de asigurare a conformităţii prelucrării datelor cu caracter personal în sectorul poliţienesc.

- Un alt element novatoriu şi esenţial vizează **evaluarea impactului asupra protecţiei datelor (DPIA)**[1]. DPIA este un proces destinat să descrie prelucrarea, să evalueze necesitatea şi proporţionalitatea acesteia şi să contribuie la gestionarea riscurilor la adresa drepturilor şi libertăţilor persoanelor vizate rezultate din prelucrarea datelor cu caracter personal, prin evaluarea acestora şi stabilirea de măsuri pentru atenuarea lor. DPIA reprezintă un instrument important pentru responsabilizare deoarece ajută operatorii de date nu numai să respecte cerinţele GDPR-ului şi să demonstreze că au fost luate măsuri adecvate pentru a asigura conformitatea cu GDPR-ul. Instrument care, este în strictă corelare cu principiul responsabilizării operatorilor de date cu caracter personal.

Se mai arată că DPIA reprezintă o abordare bazată pe risc, prevăzută de GDPR. Realizarea unei DPIA nu este obligatorie pentru fiecare operaţiune de prelucrare. DPIA este necesară numai atunci cand prelucrarea este *„susceptibilă să genereze un risc ridicat pentru drepturile şi libertăţile persoanelor fizice"*.

Prezentul proiect de lege prevede că la evaluarea impactului operaţiunilor de prelucrare efectuate de operatori sau de persoanele împuternicite de operatori, se are în vedere respectarea de către aceştia a actelor normative în domeniul protecţiei datelor personale inclusiv a codurilor de conduită, după caz.

Ordine în care, terminologia de „risc" şi „managementul riscului" va deveni una operaţională şi uzuală. Trebuie subliniat faptul că, în era tehnologiilor şi în realitatea în care riscurile prelucrării automatizate a datelor se dezvoltă cu o viteză enormă, este necesară o metodologie de gestionare a riscurilor pentru drepturile şi libertăţile persoanelor fizice, acestea trebuie identificate, analizate, estimate, evaluate, atenuate, în vederea preîntâmpinării unei încălcări masive/pe scară largă a drepturilor şi libertăţilor persoanelor fizice.

- Prezentul proiect de lege prevede că asociaţiile şi alte organisme care reprezintă categoriile de operatori sau persoane împuternicite de operatori pot pregăti **coduri de conduită** pentru a contribui la aplicarea corectă a prezentei legi, ţinând seama de caracteristicile specifice domeniilor de activitate desfăşurate de operator.

Codul de conduită trebuie să includă mecanisme care să permită unui organism care are un nivel corespunzător de expertiză în legătură cu obiectul codului să efectueze o monitorizare obligatorie a respectării dispoziţiilor sale de către operatori sau persoane împuternicite de operatori care se angajează să îl aplice fără a aduce atingere sarcinilor şi competenţelor Centrului.

---

[1] Acronim oficial al conceptului de evaluare a impactului asupra protecţiei datelor, adoptat de Grupul de lucru „Articolul 29" pentru protecţia datelor prin „Ghidul privind Evaluarea impactului asupra protecţiei datelor (DPIA) şi stabilirea dacă o prelucrare este „susceptibilă să genereze un risc ridicat" în sensul Regulamentului 2016/679", adoptat la data de 04 aprilie 2017, revizuit şi adoptat la data de 04 octombrie 2017.

- Proiectul de lege reglementează instituţia **„Reguli corporatiste obligatorii"** care reprezintă politicile în materie de protecţie a datelor cu caracter personal care trebuie respectate de un operator sau de o persoană împuternicită de operator stabilită pe teritoriul unui stat membru, în ceea ce priveşte transferurile sau seturile de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator în una sau mai multe ţări în cadrul unui grup de întreprinderi sau al unui grup de întreprinderi implicate într-o activitate economică comună. Context în care, Centrul va fi abilitat să aprobe reguli corporatiste dacă acestea sunt obligatorii şi se aplică fiecărui membru interesat al grupului de întreprinderi sau grupului de întreprinderi care desfăşoară o activitate economică comună, inclusiv angajaţilor acestora, precum şi sînt puse în aplicare de către membrii în cauză şi conferă în mod expres drepturi opozabile subiecţilor datelor în ceea ce priveşte prelucrarea datelor lor cu caracter personal.

Este notabil faptul că prevederea posibilităţii adoptării codurilor de conduită şi regulilor corporatiste obligatorii, constituie pârghii prin prisma cărora operatorii de date îşi pot demonstra caracterul conform al prelucrării datelor personale şi aderarea la un set de rigori în vederea asigurării securităţii operaţiunilor de prelucrare a datelor cu caracter personal.

- În rezultatul reglementării noţiunilor „Coduri de conduită" şi „Reguli corporatiste obligatorii", s-a modificat componenta de obligativitate a înregistrării în calitate de operator de date cu carcater personal. Astfel, prezentul proiect de lege prevede excluderea obligaţiei persoanelor fizice şi personelor juridice care prelucrează date cu carcate personal, de a se întregistra la Centru în calitate de operator de date cu caracter personal. Având în vedere necesitatea simplificării procedurii interne de notificare şi a evitării formalităţilor administrative excesive, operatorii vor fi obligaţi individual să respecte normele de securitate a datelor cu caracter personal.
- Desemnarea de către operator şi persoana împuternicită de către operator a unei persoane responsabile pentru protecţia datelor, element de progres promovat la nivelul Uniunii Europene şi reflectat în prezentul proiect de lege, care în cadrul îndeplinirii atribuţiilor, va avea obligaţia de a asigura confidenţialitatea informaţiilor la care are acces în modul prevăzut de lege, chiar şi după eliberarea din funcţie. Totodată, sunt instituite garanţii juridice pentru persoanele responsabile pentru protecţia datelor, şi anume, operatorul şi persoana împuternicită de operator se vor asigura că responsabilii de protecţia datelor nu primesc nici un fel de indicaţii în ceea ce priveşte îndeplinirea sarcinilor sale. La fel, aceştia nu pot fi demişi sau sancţionaţi de către operator sau de persoana împuternicită de operator pentru îndeplinirea legitimă a sarcinilor sale.
- Un alt element cheie constă în reglementarea cooperării internaţionale în materie de protecţie a datelor personale, datorită căreia transferul de date între statele Uniunii Europene va deveni unul liber, fără impedimente,

chestiune care într-un mod esenţial va contribui direct la intensificarea relaţiilor economice cu blocul european şi la ameliorarea imaginii Republicii Moldova pentru investiţiile străine în general.

Astfel, proiectul reglementează transmiterile transfrontaliere către un stat membru al Spaţiului Economic European care nu va necesită o autorizaţie din partea Centrului. Acelaşi lucru se va aplica atunci când Comisia Uniunii Europene a decis, pe baza unei decizii de adecvare, că o ţară terţă, un teritoriu sau unul sau mai multe sectoare specificate în respectiva ţară terţă sau o organizaţie internaţională asigură un nivel adecvat de protecţie a datelor cu caracter personal.

Proiectul de lege prevede transferul în temeiul unei decizii privind caracterul adecvat al nivelului de protecţie, care presupune transmiterea către un alt stat, pe orice suport de date sau prin orice mijloace, a datelor cu caracter personal considerate a fi prelucrate sau care sunt colectate în scopul prelucrării. Transferul de date cu caracter personal către o altă ţară sau o organizaţie internaţională se poate realiza atunci când Centru a decis că ţara, un teritoriu ori unul sau mai multe sectoare specificate din acea ţară sau organizaţia internaţională în cauză asigură un nivel de protecţie adecvat. Transferurile realizate în aceste condiţii nu necesită autorizări speciale.

În acelaşi context, proiectul de lege reglementează transmiterea transfrontalieră în baza garanţiilor adecvate, procedeu care devine operabil în absenţa unui nivel adecvat de protecţie a datelor. Operatorul sau persoana împuternicită de operator poate transfera date cu caracter personal către o altă ţară sau o organizaţie internaţională numai dacă operatorul sau persoana împuternicită de operator a oferit garanţii adecvate şi cu condiţia să existe drepturi opozabile şi căi de atac eficiente pentru subiecţii de date.

Reglementările din urmă sunt o consecinţă a integrării economice şi sociale care rezultă din funcţionarea pieţei interne a condus la o creştere substanţială a fluxurilor transfrontaliere de date cu caracter personal. Schimbul de date cu caracter personal între actori publici şi privaţi, inclusiv persoane fizice, asociaţii şi întreprinderi, s-a intensificat în întreaga Uniune Europeană. Conform dreptului Uniunii, autorităţile naţionale din statele membre sunt chemate să coopereze şi să facă schimb de date cu caracter personal pentru a putea să îşi îndeplinească atribuţiile sau să execute sarcini în numele unei autorităţi dintr-un alt stat membru.

În vederea asigurării unei implementări efective a proiectului Legii privind protecţia datelor cu caracter personal, se propune intrarea în vigoare la data de 1 martie 2019.

Impactul prezentului proiect de lege

Efectul juridic al prezentului proiect de lege va consta în consolidarea cadrului legislativ actual în domeniul protecţiei datelor cu caracter personal, dar şi armonizarea acestuia cu cadrul legislativ al Uniunii Europene.

Se notează că în realitate se atestă tendinţa majoră a companiilor de a pune un accent foarte mare pe nivelul de protecţie a datelor cu caracter personal la luarea deciziei de a se implanta economic într-o ţară. Astfel că, recunoaşterea echivalenţei în domeniul protecţiei datelor cu caracter personal între Uniunea Europeană şi Republica Moldova va constitui un garant pentru agenţii economici străini şi naţionali, dar şi pentru clienţii acestora, ale căror date stocate în Republica Moldova sunt prelucrate în condiţii adecvate de securitate şi transferate în baza unor principii şi rigori unanim recunoscute în cadrul Uniunii Europene.

În legătură cu cel din urmă considerent, se arată că armonizarea legislaţiei în domeniul protecţiei datelor cu caracter personal la legislaţia Uniunii Europene, va constitui un pas progresiv în vederea obţinerii recunoaşterii Republicii Moldova ca fiind stat care asigură un nivel adecvat de protecţie a datelor cu carcater personal. Realizarea care, va spori credibilitatea Republicii Moldova în vizorul instituţiilor financiare ale Uniunii Europene, va crea condiţii optime pentru atragerea investiţiilor şi pentru dezvoltarea unor relaţii economice durabile.

Importanţa implementării GDPR în raport cu obiectivul strategic-economic, a fost relevată şi în cadrul Studiului de impact al *Regulamentului general privind protecţia datelor cu caracter personal asupra companiilor private din Republica Moldova,* realizat în cadrul proiectului Twinning *„Consolidarea capacităţilor Centrului Naţional pentru Protecţia Datelor cu Caracter Personal al Republicii Moldova"* de către experţii rezidenţi ai Uniunii Europene.

Scopul acestui studiu a constituit, inclusiv în creşterea gradului de sensibilizare privind cazurile de aplicabilitate directă a GDPR-ului pentru companiile din Moldova şi oferirea recomandărilor pentru implementarea principiilor GDPR şi explicaţiile principalelor cerinţe ale GDPR. Se remarcă că GDPR-ul poate fi direct aplicabil oricărei companii stabilite în Republica Moldova. În plus, chiar dacă GDPR-ul se aplică direct unei companii din Moldova din cauza activităţilor pe care le desfăşoară pe piaţa Uniunii Europene, se poate aplica şi legislaţia naţională privind protecţia datelor în Republica Moldova. Astfel, fiecare companie va trebui să organizeze autoevaluarea pentru a identifica decalajul dintre practica curentă şi prelucrarea datelor cu caracter personal în cadrul companiei private din Moldova şi cerinţele GDPR.

Prin acelaşi studiu, sub aspect de dezvoltare economică s-a învederat că multe companii din Republica Moldova cooperează instituţional cu diverse companii din Uniunea Europeană oferind bunuri şi servicii. De exemplu, Biroul Naţional de Statistică a Republicii Moldova informează că în anul 2017, exporturile de mărfuri destinate ţărilor Uniunii Europene (UE–28) au însumat 1596,9 mil. dolari SUA (cu 19,9% mai mult faţă de anul 2016), deţinând o cotă

de 65,8% în total exporturi (65,1% – în anul 2016) [2]. În acest context, vor exista tot mai multe situaţii în care companiile din Republica Moldova vor fi supuse aplicabilităţii directe sau indirecte a GDPR-lui.

Pe de altă parte, nivelul de conştientizare a subiecţilor de date a importanţei dreptului la inviolabilitatea vieţii private şi a dreptului la protecţia datelor cu caracetr personal-drept care derivă din primul, se demonstrează prin majorarea numărului de plângeri parvenite în adresa Centrului, astfel, prin utilizarea metodei comparative, se arată că în anul 2016 Centrul a înregistrat 410 de plângeri şi în anul 2017 a înregistrat 554 de plângeri, ceea ce denotă o ascensiune cu 35 % în anul 2017. Dinamică, care demonstrează o creştere permanentă a conştiinţei juridice a subiecţilor faţă de datele sale cu caracter personal. Context în care, prin prezentul proiect de lege şi prin implementarea sa ulterioară, se va asigura o sensibilizare şi o cunoaştere de către subiecţi, a dreptului la protecţia datelor cu caracter personal, ce derivă din dreptul de sorginte contituţională - inviolabilitatea vieţii private, totodată şi o cunoaştere a mecanismelor de apărare a acestui drept, chestiune care, va minimiza unele încălcări admise de către operatorii de date cu caracter personal, sub riscul de a fi supuşi unei căi de atac de către subiecţii informaţi.

Pe aceeaşi notă comparativă şi statistică, se arată că pe parcursul anului 2017 au fost înregistraţi în Registrul de evidenţă a operatorilor de date 500 de operatori, întocmite 52 de procese contravenţionale şi constatate 84 de fapte contravenţionale. Însă, în perioada ianuarie-mai 2018, Centrul a înregistrat deja un număr de 314 de operatori de date, a întocmit 40 de procese contravenţionale şi a constatat 83 de fapte contravenţionale, fapt din care reiese că rezultatele obţinute pe parcursul a 4 luni din anul 2018 sunt comparabile cu rezultatele obţinute pe întreaga perioadă a anului 2017.

Deci, un alt impact al prezentului proiect de lege va consta, pe de o parte, în dezvoltarea elementelor intrinseci ale conştiinţei juridice a subiecţilor de date (spre exemplu: conştientizarea valorificării dreptului la protecţia datelor cu caracter personal, cunoaşterea mecanismelor de apărare a dreptului evocat), iar pe de altă parte, în dezvoltarea elementelor extrinseci ale conştiinţei juridice a operatorilor de date (spre exemplu comportament/caracter responsabil vizavi de operaţiunile de prelucrare a datelor cu caracter personal, o prelucrare transparentă a datelor cu caracter personal etc.).

Se mai arată că, importanţa şi impactul GDPR-ului asupra companiilor private şi a instituţiilor guvernamentale din Republica Moldova a fost discutat în cadrul unei sesiuni organizate la 25 aprilie 2018. Evenimentul a fost moderat de Consilierul Rezident de Twinning din cadrul Centrului, la care au participat mai mult de 50 de reprezentanţi ai companiilor private din Republica Moldova.În cadrul discuţiilor participanţii au aflat despre noile reglementări în domeniul protecţiei datelor prevăzute de GDPR precum şi modalităţile practice de implementare ale acestora în activitatea unei companii private.

5. Fundamentarea economico-financiară

[2] http://www.statistica.md/newsview.php?l=ro&id=5908&idc=168

Pentru implementarea prevederilor prezentului proiect de lege nu au fost identificate careva cheltuieli.

Dinpotrivă, amenzile aplicate de către Centru în ordinea stabilită, vor contribui la sporirea veniturilor bugetului de stat iar transferul liber de date va consolida obiectivul strategico-economic.

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

Proiectul se va integra perfect în sistemul legislativ în vigoare. Totuşi, pentru implementarea prevederilor acestuia, urmează:

1) În termen de 9 luni de la data publicării prezentei legi, Guvernul:

a) va elabora şi va prezenta Parlamentului propuneri privind aducerea legislaţieîn vigoare în concordanţă cu prezenta lege;

b) va pune actele sale normative în concordanţă cu prezenta lege;

c) va asigura punerea în concordanţă a actelor normative ale autorităţilor publice centrale şi cu prezenta lege;

2) Centrul în termen de 9 luni de la data publicării legii:

a) va elabora şi va adopta actele normative necesare punerii în aplicare a prezentei legi;

b) va aduce actele sale normative în concordanţă cu prevederile prezentei legi;

c) va prezenta, în comun cu Guvernul, propuneri de modificare a legislaţiei în vigoare, în scopul asigurării compatibilităţii cu prezenta lege.

Totodată, urmează a fi efectuate modificări în legile care au prevederi conexe cu domeniul protecţiei datelor cu caracter personal.

7. Avizarea şi consultarea publică a proiectului

În scopul respectării prevederilor Legii nr. 239-XVI din 13 noiembrie 2008 privind transparenţa în procesul decizional, proiectul de lege a fost plasat pe pagina web a Centrului Naţional pentru Protecţia Datelor cu Caracter Personal (directoriul „Transparenţa în procesul decizional", compartimentul „Anunţuri privind organizarea consultării publice şi proiecte de decizii".

Totodată, proiectul de lege a fost remis spre avizare organelor şi autorităţilor interesate, fiind recepţionate avize de la Ministerului Afacerilor Interne, Centrului Naţional Anticorupţie, Procuraturii Generale, Serviciului de Informaţii şi Securitate, Ministerului Sănătăţii, Muncii şi Protecţiei Sociale, Ministerului Economiei şi Infrastructurii, Agenţiei Naţionale pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei, Băncii Naţionale a Moldovei, Ministerului Finanţelor.

8. Constatările expertizei anticorupţie

Proiectul Legii a fost remis în adresa Centrului Naţional Anticorupţie în vederea efectuării expertizei anticorupţie, în conformitate cu prevederile art. 34 alin. (1) şi 35 din Legea nr. 100 din 22 decembrie 2017 cu privire la actele normative.

În urma efectuării expertizei, s-a constatat că autorul a respectat parţial rigorile de transparenţă decizională conform cerinţelor legale stabilite de Legea nr. 239/2008 privind transparenţa în procesul decizional.

Totodată în conţinutul proiectului au fost identificaţi factori de risc care pot genera apariţia unor situaţii de corupţie. Aceştia au fost analizaţi în cadrul tabelului de divergenţă la expertiza anticorupţie, CNPDCP exprimîndu-şi opinia motivată pe marginea fiecăruia din aceste obiecţii prin prisma regulamentului 679, directivei 680, directivei 681 şi legislaţiei naţionale, operînd modificări în cazurile justificate.

9. Constatările expertizei de compatibilitate

Ca urmare a evaluării proiectului de Lege privind protecţia datelor cu caracter personal, realizată de Centrul de Armonizare a Legislaţiei s-a remarcat că proiectul respectiv şi-a atins finalitatea de transpunere corespunzătoare a prevederilor Regulamentului 2016/679/UE şi ale Directivei 2016/680/UE, concluzia generală fiind că proiectul este în acord cu dreptul UE aplicabil.