

NOTA DE FUNDAMENTARE

a proiectului de lege privind protecția datelor cu caracter personal prelucrate în scopul prevenirii și combaterii infracțiunilor

1. Denumirea autorului proiectului

Proiectul de lege privind protecția datelor cu caracter personal prelucrate în scopul prevenirii și combaterii infracțiunilor a fost elaborat de Ministerul Justiției.

2. Condițiile ce au impus elaborarea proiectului

2.1. Temeiul legal și sursa proiectului

Prezentul proiect are drept scop implementarea:

- a) acțiunii nr. 28 din capitolul 23 al *Planului național de acțiuni pentru aderarea Republicii Moldova la Uniunea Europeană pe anii 2024-2027*, aprobat prin *Hotărârea Guvernului nr. 829/2023*;
- b) acțiunii nr. 211 din *Planul național de reglementări pentru anul 2025*, aprobat prin *Hotărârea Guvernului nr. 841/2024*.

2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

La 25 iulie 2024, Parlamentul Republicii Moldova a adoptat *Legea nr. 195/2024 privind protecția datelor cu caracter personal*. Acest act legislativ va intra în vigoare la 23 august 2026 și va institui noul cadru normativ general în domeniul protecției datelor cu caracter personal, asigurând transpunerea deplină în legislația națională a *Regulamentului (UE) 2016/679*.

În conformitate cu art. 2 alin. (2) lit. c) din *Legea nr. 195/2024*, acest act legislativ nu se aplică prelucrării datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmăririi penale a infracțiunilor ori al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora.

Această prevedere este identică cu cea prevăzută la art. 2 alin. (2) lit. d) din *Regulamentul (UE) 2016/679* și este determinată de faptul că, la nivelul legislației Uniunii Europene, protecția datelor cu caracter personal prelucrate în scopul prevenirii și combaterii infracțiunilor este asigurată prin intermediul unui act normativ distinct – *Directiva (UE) 2016/680*.

Instituirea unui cadru normativ special pentru reglementarea prelucrării datelor în scopul prevenirii și combaterii infracțiunilor a fost determinată de faptul că, în cazul unor astfel de prelucrări, reglementările normative trebuie, pe de o parte, să permită autorităților competente exercitarea eficientă a atribuțiilor sale de prevenire și combatere a fenomenului infracțional, iar, pe de altă parte, trebuie să asigure un nivel adecvat de protecție a datelor cu caracter personal. Din aceste considerente, *Directiva (UE) 2016/680* conține reglementări specifice ce vizează, în special:

- a) principiile și temeiul legal pentru prelucrarea datelor efectuată în scopul prevenirii și combaterii infracțiunilor;
- b) modalitatea de exercitare și limitare a drepturilor persoanelor vizate;
- c) asigurarea securității datelor cu caracter personal, în special în cadrul sistemelor informaționale automatizate;
- d) realizarea transferurilor de date către alte state sau către organizații internaționale, în vederea facilitării schimbului de informații între organele de drept;

Astfel, pentru asigurarea unui nivel înalt de protecție a datelor prelucrate în scopul prevenirii și combaterii infracțiunilor, precum și în vederea armonizării depline a legislației naționale la *acquis*-ul Uniunii Europene în acest domeniu, este imperioasă transpunerea *Directivei (UE) 2016/680* prin intermediul unui act legislativ distinct, care să intre în vigoare concomitent cu *Legea nr. 195/2024* (i.e. 23 august 2026). Or, în caz contrar, operațiunile de prelucrare a datelor efectuate în scopul prevenirii și combaterii infracțiunilor nu vor avea o reglementare normativă.

3. Obiectivele urmărite și soluțiile propuse

Obiectivul prezentului proiect constă în transpunerea deplină în legislația națională a *Directivei (UE) 2016/680*.

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

În conformitate cu art. 71 alin. (4) din *Legea nr. 100/2017 cu privire la actele normative*, la interpretarea actului normativ se ține cont de nota de fundamentare care a însoțit proiectul actului normativ și de alte documente care permit identificarea voinței autorității publice care a adoptat, a aprobat sau a emis actul normativ.

Astfel, la interpretarea prevederilor legale propuse se va ține cont de prezenta notă de fundamentare.

Adițional, pornind de la faptul că prezentul proiect de lege reprezintă o transpunere deplină a unui act normativ al Uniunii Europene (i.e. *Directiva (UE)*

2016/680), la interpretarea prevederilor din prezentul proiect de lege se va ține cont de:

- a) jurisprudența Curții de Justiție a Uniunii Europene;
- b) opiniile și ghidurile Comitetului European pentru Protecția Datelor;
- c) opiniile și ghidurile Autorității Europene pentru Protecția Datelor.

În continuare, în cadrul prezentului compartiment, vor fi descrise detaliat principalele prevederi ale proiectului, pentru stabilirea sensului exact al normelor juridice propuse.

CAPITOLUL I – DISPOZIȚII GENERALE

ARTICOLUL 1 – OBIECTUL ȘI SCOPUL LEGII

Art. 1 alin. (1), în coroborare cu art. 2 alin. (1), este cea mai importantă normă juridică din prezentul act legislativ și are o importanță crucială pentru determinarea domeniului și a modului de aplicare a legii.

Astfel, conform art. 1 alin. (1) și art. 2 alin. (1), prezenta lege se aplică în exclusivitate prelucrării datelor cu caracter personal care întrunește două criterii cumulative:

- a) prelucrarea se efectuează de către autoritățile competente, precum acestea sunt definite la art. 3 alin. (2); și
- b) prelucrarea se efectuează în scopul:
 - 1) prevenirii infracțiunilor, inclusiv al prevenirii și protejării împotriva amenințărilor la ordinea și securitatea publică;
 - 2) depistării, investigării sau urmăririi penale a infracțiunilor;
 - 3) executării pedepselor penale sau a măsurilor de siguranță.

Ambele criterii enumerate sunt strict cumulative. Astfel, în cazul în care o prelucrare a datelor nu întrunește unul din aceste criterii, se va aplica *Legea nr. 195/2024 privind protecția datelor cu caracter personal*, nu și prezenta lege.

Primul criteriu, menționat la lit. a), reprezintă „**criteriul personal**” de aplicare și determină subiecții care cad sub incidența legii. Al doilea criteriu, menționat la lit. b), reprezintă „**criteriul material**” de aplicare și determină categoriile de prelucrări care sunt reglementate de prezenta lege.

I. Criteriul personal de aplicare a legii

Prezenta lege se aplică doar prelucrării datelor efectuate de către autoritățile competente. Noțiunea de „*autoritate competentă*” este definită la art. 3 alin. (2).

Astfel, o listă detaliată a autorităților competente care intră sub incidența prezentei legi va fi oferită în contextul analizei art. 3 din prezenta notă de fundamentare.

Cu titlu general, autoritățile competente sunt entitățile împuternicite prin lege să exercite atribuții în domeniul prevenirii și combaterii fenomenului infracțional (e.g. organele de urmărire penală, procuraturile, instanțele judecătorești, etc.).

În cazul în care prelucrarea este efectuată de alte entități decât „*autoritățile competente*”, chiar dacă este întrunit criteriul material de aplicare a legii, prelucrarea este reglementată de *Legea nr. 195/2024 privind protecția datelor cu caracter personal*.

II. Criteriul material de aplicare a legii

Prezenta lege nu se aplică pentru toate operațiunile de prelucrare efectuate de autoritățile competente, ci numai în cazul prelucrărilor realizate în scopul:

- a) prevenirii infracțiunilor, inclusiv al prevenirii și protejării împotriva amenințărilor la ordinea și securitatea publică;
- b) depistării, investigării sau urmăririi penale a infracțiunilor;
- c) executării pedepselor penale sau a măsurilor de siguranță.

În cazul operațiunilor de prelucrare efectuate în alte scopuri decât cele menționate *supra*, se aplică *Legea nr. 195/2024 privind protecția datelor cu caracter personal*, cum ar fi în cazul prelucrării datelor pentru:

- managementul resurselor umane ale autorităților competente (de exemplu, concursurile de angajare; numirea în funcție; evaluarea performanțelor profesionale; remunerarea; modificarea sau încetarea raporturilor de serviciu, etc.);
- desfășurarea procedurilor administrative conform *Codului administrativ* și altor acte normative (de exemplu, examinarea și soluționarea petițiilor);
- încheierea contractelor de achiziții publice sau a contractelor de achiziții publice de valoare mică;
- organizarea și desfășurarea evenimentelor publice de către autoritățile competente (de exemplu, consultările publice, mesele rotunde, briefingurile de presă);
- perfectarea accesului în sediile autorităților competente;
- supravegherea video realizată în sediile autorităților competente;
- alte activități care nu au drept scop prevenirea sau combaterea infracțiunilor.

După cum reiese din lit. a)-c) expuse *supra*, prezenta lege se aplică doar dacă prelucrarea se efectuează în scopul prevenirii și combaterii **infracțiunilor**. Astfel,

prelucrarea datelor în contextul proceselor contravenționale de asemenea nu este reglementată de prezenta lege, dar de *Legea nr. 195/2024 privind protecția datelor cu caracter personal*.

În continuare urmează a fi examinate detaliat scopurile de prelucrare a datelor pentru care prezenta lege este aplicabilă (prevăzute la art. 1 alin. (1) lit. a)-c)).

A. Prevenirea infracțiunilor, inclusiv prevenirea și protejarea împotriva amenințărilor la ordinea și securitatea publică

Conceptul de „prevenire a infracțiunilor” este unul complex, fiind distinct de conceptul de „combatere a infracțiunilor”.¹

În timp ce combaterea infracțiunilor reprezintă o reacție a statului în raport cu un eveniment infracțional – fiind o funcție-cheie a justiției penale, realizată în cadrul unui proces penal – prevenirea infracțiunilor, pe de altă parte, reprezintă un set de măsuri cu caracter anticipativ, care sunt îndreptate spre împiedicarea comiterii infracțiunilor, precum și spre înlăturarea cauzelor și a condițiilor care generează sau favorizează comiterea infracțiunilor. După cum se remarcă în doctrină, aceste măsuri se concentrează primordial în privința potențialelor riscuri de săvârșire a infracțiunilor, decât pe un prejudiciu real care s-a produs.²

Astfel, prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii infracțiunilor se referă, în special, la prelucrarea efectuată în cadrul următoarelor activități:

1) Activitatea specială de investigații realizată în afara procesului penal

Legea nr. 59/2012 privind activitatea specială de investigații reglementează modul de realizare a acestei activități în afara procesului penal, având drept scop principal prevenirea infracțiunilor.

2) Efectuarea măsurilor de prevenire a criminalității organizate

Prelucrarea datelor în vederea realizării măsurilor prevăzute la art. 9 alin. (1), precum și la art. 9¹ din *Legea nr. 50/2012 privind prevenirea și combaterea criminalității organizate*, de asemenea va fi supusă reglementărilor prezentului proiect de lege, pentru, *inter alia*:

- a) efectuarea analizei operaționale și strategice a cauzelor, a elementelor și a circumstanțelor care favorizează crearea și activitatea grupurilor criminale organizate sau a organizațiilor

¹ În senul prezentei legi, noțiunea de „combatere a infracțiunilor” se referă la activitățile prevăzute la art. 1 alin. (1) lit. b) și c) din proiectul de lege (*i.e.* depistarea, investigarea sau urmărirea penală a infracțiunilor, precum și executarea pedepselor penale sau a măsurilor de siguranță).

² Kosta E., et al. *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, 2024, p. 53.

(asociațiilor) criminale, precum și subcultura criminală în mediul penitenciar;

- b) notificarea persoanelor care pot fi atrase în activitatea criminală organizată;
- c) monitorizarea preventivă a persoanelor care pot fi atrase în activitatea criminală organizată;
- d) identificarea, monitorizarea și documentarea deținuților adepți ai subculturii criminale în vederea diminuării activităților ilegale în mediul penitenciar;
- e) separarea deținuților în penitenciare în scopul diminuării influenței liderilor informali.

3) Analiza operațională, tactică și strategică a actelor de corupție, a actelor conexe corupției și a faptelor coruptibile

În conformitate cu art. 6² din *Legea nr. 1104/2002 cu privire la Centrul Național Anticorupție*, analiza operațională, tactică și strategică a actelor de corupție, a actelor conexe corupției și a faptelor coruptibile reprezintă activitatea analitică a Centrului, care constă în colectarea, stocarea, prelucrarea informațiilor și a datelor, precum și obținerea, utilizarea și transmiterea informațiilor analizate, efectuate în cadrul:

- a) efectuării expertizei anticorupție a proiectelor de acte normative ale Guvernului, precum și a altor inițiative legislative înregistrate în Parlament;
- b) efectuării evaluării integrității instituționale;
- c) analizei fenomenului corupției;
- d) realizării misiunii Centrului.

4) Activitatea de probațiune

În conformitate cu art. 2 din *Legea nr. 8/2008 cu privire la probațiune*, activitatea de probațiune are drept scop preîntâmpinarea săvârșirii de noi infracțiuni. Astfel, prelucrarea datelor cu caracter personal la realizarea activităților de probațiune va fi supusă reglementărilor prezentei legi.

În altă ordine de idei, precum reiese din recitalul 12 din *Directiva (UE) 2016/680*, sintagma „*inclusiv prevenirea și protejarea împotriva amenințărilor la ordinea și securitatea publică*” (prevăzută la art. 1 alin. (1) lit. a)) se referă la menținerea legii și ordinii ca atribuții ale poliției sau ale altor autorități de aplicare a legii atunci când aceasta se impune pentru a se asigura protecția împotriva amenințărilor la adresa securității publice și la adresa intereselor fundamentale ale

societății protejate prin lege și pentru prevenirea acestor amenințări, care pot conduce la o infracțiune. După cum se remarcă în recitalul 12 menționat *supra*, această sintagmă se referă în special la activitățile de prevenire a infracțiunilor cu ocazia manifestațiilor, evenimentelor sportive majore sau unor revolte.

Cu toate acestea, reamintim că în cazul inițierii proceselor contravenționale, în contextul constatării unor contravenții, se va aplica *Legea nr. 195/2024 privind protecția datelor cu caracter personal*, nu și prezenta lege.

B. Depistarea, investigarea și urmărirea penală a infracțiunilor

Art. 1 alin. (1) lit. b) prevede aplicabilitatea legii în cazul prelucrării datelor de către autoritățile competente în scopul depistării, investigării și urmării penale a infracțiunilor.

Aceste trei elemente reprezintă fazele indispensabile oricărui proces penal și sunt îndreptate spre combaterea directă a fenomenului infracțional.

Astfel, în temeiul art. 1 alin. (1) lit. b), prezenta lege se aplică prelucrării datelor cu caracter personal efectuate în cadrul unui proces penal, reglementat de *Codul de procedură penală*, inclusiv la înregistrarea sesizărilor, efectuarea investigațiilor preliminare, exercitarea atribuțiilor organelor de constatare, pornirea urmării penale și efectuarea acțiunilor de urmărire penală, dispunerea și executarea măsurilor procesuale de constrângere, efectuarea măsurilor speciale de investigații, precum și la realizarea altor acțiuni sau măsuri în cadrul unui proces penal, în scopul depistării, investigării sau urmării penale a infracțiunilor.

De asemenea, în temeiul art. 1 alin. (1) lit. b), prezenta lege se aplică prelucrării datelor cu caracter personal efectuate de către instanțele de judecată și alte autorități competente, atât la faza controlului judiciar al procedurii prejudiciare, cât și la faza judecării cauzei penale în primă instanță, în apel sau în recurs, precum și la judecarea cauzei penale pe cale extraordinară de atac.

În altă ordine de idei – deși art. 1 alin. (1) lit. b) este aplicabil primordial în cazul prelucrării datelor cu caracter personal în cadrul unui proces penal – acest temei se referă și la anumite operațiuni de prelucrare extrapenale (*i.e.* care sunt efectuate în scopul „depistării” infracțiunilor, dar în afara unui proces penal). În special, este în cazul primirii și examinării de către autoritățile competente a dezvăluirilor interne și externe de încălcare a legii, care sunt înaintate de către avertizorii de integritate. Astfel, operațiunile de prelucrare a datelor cu caracter personal, realizate de către autoritățile competente în temeiul *Legii nr. 165/2023 privind avertizorii de integritate*, vor fi reglementate de prezenta lege, precum derivă expres și din recitalul 85 din *Directiva (UE) 2019/1937*.

C. Executarea pedepselor penale sau a măsurilor de siguranță

Executarea sentințelor de condamnare reprezintă ultima etapă a unui proces penal, fiind faza finală și indispensabilă în combaterea infracțiunilor.

Astfel, în temeiul art. 1 alin. (1) lit. c), prezenta lege se aplică prelucrării datelor cu caracter personal de către autoritățile competente în scopul:

- 1) executării pedepselor penale prevăzute la art. 62 din *Codul penal*, în conformitate cu legislația execuțional-penală;
- 2) executării măsurilor de siguranță prevăzute la art. 98 din *Codul penal*, în conformitate cu legislația execuțional-penală.

ARTICOLUL 2 – DOMENIUL DE APLICARE

Alineatul (1) al acestui articol prevede că prezenta lege se aplică prelucrării datelor cu caracter personal de către autoritățile competente în scopurile prevăzute la art. 1 alin. (1).

După cum a fost menționat *supra*, art. 2 alin. (1) se aplică în directă coroborare cu art. 1 alin. (1) și determină, atât criteriul personal de aplicare a legii (subiecții care trebuie să aplice legea, *i.e.* autoritățile competente), cât și criteriul material de aplicare a legii (scopurile de prelucrare a datelor pentru care se aplică legea, *i.e.* cele descrise detaliat *supra*).

Astfel, la interpretarea art. 2 alin. (1) se aplică *mutatis mutandis* explicațiile oferite în contextul analizei art. 1 alin. (1).

În altă ordine de idei, art. 2 alin. (2) din proiect determină întinderea datelor cu caracter personal care cad sub incidența legii. Astfel, protecția persoanelor fizice în temeiul prezentei legi se aplică în ceea ce privește prelucrarea datelor cu caracter personal prin mijloace automatizate, precum și în cazul prelucrării manuale, dacă datele sunt cuprinse sau destinate să fie cuprinse într-un sistem de evidență. Dosarele sau seturile de dosare, precum și copertele acestora, care nu sunt structurate în conformitate cu criteriile specifice, nu intră sub incidența prezentei legi.

Nu în ultimul rând, în corespundere cu art. 2 alin. (3), prezenta lege nu se aplică prelucrării datelor cu caracter personal atribuite la secret de stat, care se efectuează în conformitate cu *Legea nr. 245/2008 cu privire la secretul de stat* și în măsura în care este necesar și proporțional pentru protecția securității naționale și apărării naționale.

Această prevedere este esențială pentru transpunerea adecvată a recitalului 14 din *Directiva (UE) 2016/680*, care prevede expres că această directivă nu se aplică activităților privind securitatea națională, precum și activităților agențiilor sau ale unităților specializate pe probleme de securitate națională.

Prin definiție, în conformitate cu *Legea nr. 245/2008 cu privire la secretul de stat*, secretele de stat reprezintă informațiile a căror divulgare neautorizată sau pierdere este de natură să aducă atingere securității naționale a Republicii Moldova.

Prin urmare, exceptarea aplicării prezentei legi în privința informațiilor atribuite la secret de stat este imperativă.

Se va reține că sintagma „*în măsura în care este necesar și proporțional pentru protecția securității și apărării naționale*”, prevăzută la art. 2 alin. (3) din proiect, face referire la prevederile art. 6 din *Legea nr. 245/2008 cu privire la secretul de stat*, precum și la considerentele expuse în *Hotărârea Curții Constituționale nr. 19/2015*. Astfel, art. 6 din *Legea nr. 245/2008*, în coroborare cu considerentele Curții Constituționale, reiterează necesitatea respectării principiului necesității și proporționalității la faza atribuirii informațiilor la secret de stat și la secretizarea acestora.

ARTICOLUL 3 – NOȚIUNI

În conformitate cu art. 3 alin. (1), noțiunile din prezenta lege se definesc în conformitate cu art. 4 din *Legea nr. 195/2024 privind protecția datelor cu caracter personal*. Acest lucru este firesc, or, absoluta majoritate a noțiunilor utilizate de prezenta lege sunt definite identic precum în *Legea nr. 195/2024*.

Cu toate acestea, una din noțiunile fundamentale ale prezentei legi nu este definită în *Legea nr. 195/2024* (i.e. noțiunea de „*autoritate competentă*”), iar o altă noțiune este definită puțin diferit în raport cu art. 4 din *Legea nr. 195/2024* (i.e. noțiunea de „*operator*”).

„*Autoritate competentă*”

Conform definiției expuse la art. 3, autoritățile competente se grupează în două categorii generale, prevăzute la lit. a) și b).

Astfel, în sensul lit. a), „*autoritate competentă*” este orice autoritate publică competentă în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor, de executare a pedepselor penale și a măsurilor de siguranță, inclusiv în materie de prevenire și protejare împotriva amenințărilor la ordinea și securitatea publică.

Prin urmare, sunt „*autorități competente*” următoarele autorități publice:

- organele de urmărire penală prevăzute la art. 253 alin. (1) din *Codul de procedură penală*;
- organele de constatare prevăzute la art. 273 alin. (1) din *Codul de procedură penală*;
- procuraturile (Procuratura Generală, procuraturile specializate, precum și procuraturile teritoriale);
- instanțele judecătorești de fond, apel și recurs (inclusiv judecătorul de instrucție);
- autoritățile care efectuează măsuri speciale de investigații în afara procesului penal, prevăzute la art. 6 alin. (1) din *Legea nr. 59/2012 privind activitatea specială de investigații*;
- autoritățile cu atribuții în domeniul prevenirii și combaterii criminalității organizate, prevăzute la art. 6 alin. (1) din *Legea nr. 50/2012 privind prevenirea și combaterea criminalității organizate*;
- autoritățile din cadrul sistemului administrației penitenciare (Administrația Națională a Penitenciarelor, subdiviziunile acesteia și instituțiile penitenciare);
- organele de probațiune (Inspectoratul Național de Probațiune și subdiviziunile sale teritoriale);
- alte autorități publice care execută hotărârile cu caracter penal în conformitate cu Cartea a doua, Titlul V din *Codul de executare* (e.g. art. 173-175¹ din cod);
- Agenția de Recuperare a Bunurilor Infraționale;
- instituțiile publice de expertiză judiciară, prevăzute la art. 65 alin. (2) din *Legea nr. 68/2016 cu privire la expertiza judiciară și statutul expertului judiciar*.

În altă ordine de idei, în sensul lit. b), prin „*autoritate competentă*” se înțelege și orice altă entitate împuternicită de lege să exercite competențe publice în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor, al executării pedepselor penale și a măsurilor de siguranță, inclusiv al prevenirii și protejării împotriva amenințărilor la ordinea și securitatea publică.

Această prevedere se referă la entitățile care nu au statut de autoritate publică, însă care sunt împuternicite prin lege cu atribuții publice în domeniul prevenirii și combaterii infracțiunilor, cum ar fi:

- executorii judecătorești care execută hotărârile cu caracter penal;
- experții judiciari care își desfășoară activitatea în cadrul birourilor de expertiză judiciară și efectuează expertiză judiciară în cadrul proceselor penale;

„Operator”

Spre deosebire de noțiunea din *Legea nr. 195/2024*, în sensul prezentei legi „operator” poate fi doar o „*autoritate competentă*”, care, singură sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal. În cazul în care scopurile și mijloacele de prelucrare sunt stabilite de actele normative, operatorul sau criteriile specifice pentru desemnarea acestuia sunt prevăzute de actele normative respective.

CAPITOLUL II – PRINCIPII

ARTICOLUL 4 – PRINCIPIILE PRELUCRĂRII

Art. 4 stabilește principiile diriguitoare ale regimului juridic de protecție a datelor cu caracter personal, fiind de aplicabilitate directă oricărei prelucrări care intră sub incidența prezentei legi. Astfel, toate operațiunile de prelucrare a datelor urmează a fi raportate la principiile prevăzute la art. 4, în coroborare cu alte prevederi care dezvoltă și detaliază aceste principii.

Orice prelucrare a datelor cu caracter personal trebuie să fie legală și echitabilă, precum și efectuată numai pentru scopuri specifice prevăzute de lege.

Persoanele fizice trebuie să fie informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor acestora cu caracter personal și cu privire la modul în care să își exercite drepturile respective. În special, scopurile specifice în care datele cu caracter personal sunt prelucrate trebuie să fie explicite și legitime și să fie determinate la momentul colectării datelor.

Subsecvent, datele cu caracter personal trebuie să fie adecvate și relevante pentru scopurile în care sunt prelucrate. În special, trebuie să se asigure faptul că datele cu caracter personal colectate nu sunt excesive și că nu sunt stocate mai mult timp decât este necesar pentru îndeplinirea scopului în care sunt prelucrate. Mai mult decât atât, datele cu caracter personal pot fi prelucrate doar în cazul în care scopul prelucrării nu poate fi îndeplinit, în mod rezonabil, prin alte mijloace. În vederea asigurării faptului că datele nu sunt păstrate mai mult timp decât este necesar, trebuie să se stabilească de către operator termene pentru ștergere sau revizuire periodică.

În vederea menținerii securității în ceea ce privește prelucrarea, precum și a prevenirii prelucrărilor care nu respectă prezenta lege, datele cu caracter personal trebuie prelucrate într-un mod care să asigure un nivel corespunzător de securitate și confidențialitate, inclusiv prin prevenirea accesului neautorizat la acestea sau a utilizării neautorizate a datelor și a echipamentului utilizat pentru prelucrare și luând

în considerare stadiul actual al tehnologiei disponibile, costurile punerii acesteia în aplicare în raport cu riscurile și natura datelor cu caracter personal a căror protecție trebuie asigurată.

Colectarea datelor cu caracter personal trebuie să fie efectuată în scopuri determinate, explicite și legitime în cadrul domeniului de aplicare al prezentei legi, iar prelucrarea acestora nu poate să se facă în scopuri care sunt incompatibile cu obiectivele prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau ale executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. În cazul în care datele cu caracter personal sunt prelucrate de către același sau de către un alt operator într-un scop care se încadrează în domeniul de aplicare al prezentei legi, dar este diferit de scopul în care au fost colectate, o astfel de prelucrare este permisă cu condiția ca aceasta să fie autorizată în conformitate cu dispozițiile legale aplicabile și să fie necesară și proporțională în raport cu acest alt scop.

Principiul exactității datelor trebuie aplicat luând în considerare natura și scopul prelucrării în cauză. În special în cadrul procedurilor judiciare, declarațiile care conțin date cu caracter personal se bazează, de regulă, pe o percepție subiectivă a persoanelor fizice și nu sunt întotdeauna verificabile. În consecință, acest principiu nu se aplică exactității unei declarații, ci doar faptului că o anumită declarație a fost făcută.

ARTICOLUL 5 – LEGALITATEA PRELUCRĂRII

În conformitate cu art. 5 alin. (1), prezenta lege recunoaște, în general, un singur temei legal pentru prelucrarea datelor cu caracter personal – numai dacă prelucrarea este necesară pentru exercitarea de către o autoritate competentă a unei atribuții prevăzute de actele normative, în scopurile prevăzute la art. 1 alin. (1).

Atribuțiile de prevenire și combatere a infracțiunilor trebuie să fie prevăzute expres de actele normative, cum ar fi cele reglementate de, *inter alia*, *Codul de procedură penală*, *Legea nr. 59/2012 privind activitatea specială de investigații*, *Codul de executare*, legile speciale și regulamentele de organizare și funcționare ale autorităților competente, etc.

În altă ordine de idei, în conformitate cu art. 5 alin. (2), actele normative ar trebui să prevadă, de asemenea, obiectivele prelucrării, datele care urmează să fie prelucrate și scopurile prelucrării.

ARTICOLUL 6 – PRELUCRAREA ÎN ALTE SCOPURI DECÂT CELE PREVĂZUTE LA ART. 1 ALIN. (1)

Art. 6 alin. (1) reiterează faptul că, în temeiul prezentei legi, datele cu caracter personal nu pot fi prelucrate în alte scopuri decât cele prevăzute la art. 1 alin. (1) din lege (*i.e.* în scopul prevenirii și combaterii infracțiunilor).

În cazul în care datele cu caracter personal au fost colectate inițial în scopurile prevăzute la art. 1 alin. (1), aceste date ar putea fi ulterior prelucrate în alte scopuri numai în temeiul actelor normative. Însă, în cazul dat, această prelucrare ulterioară va fi reglementată de *Legea nr. 195/2024 privind protecția datelor cu caracter personal*.

Subsecvent, art. 6 alin. (2) concretizează faptul că prelucrarea datelor cu caracter personal realizată în alte scopuri decât cele prevăzute la art. 1 alin. (1) este, *ipso facto*, reglementată de *Legea nr. 195/2024*.

În altă ordine de idei, în conformitate cu art. 6 alin. (3), în cazul în care actele normative prevăd condiții specifice de prelucrare a datelor cu caracter personal, autoritatea competentă care transmite datele respective informează destinatarul cu privire la aceste condiții și la obligația de a le respecta. Astfel de condiții ar putea include, de exemplu, interdicția de a transmite datele cu caracter personal altor destinatari sau de a le utiliza în alte scopuri decât cele pentru care au fost transmise destinatarului, sau de a informa persoana vizată în cazul unei limitări a dreptului la informare fără aprobarea prealabilă a autorității competente care a transmis datele. Obligațiile menționate se aplică, de asemenea, transferurilor realizate de autoritatea competentă care a transmis datele către destinatari din alte state sau către organizații internaționale.

ARTICOLUL 7 – PRELUCRAREA CATEGORIILOR SPECIALE DE DATE CU CARACTER PERSONAL

Datele caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale necesită o protecție specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor și libertăților fundamentale.

Categoriile speciale de date cu caracter personal pot fi prelucrate legal numai dacă prelucrarea este strict necesară și sub rezerva unor garanții adecvate pentru drepturile și libertățile persoanei vizate, în cazul în care:

1) Prelucrarea este strict necesară pentru exercitarea de către o autoritate competentă a unei atribuții prevăzute de actele normative, în scopurile prevăzute la art. 1 alin. (1)

Acest temei legal este similar cu temeiul general de prelucrare prevăzut la art. 5 alin. (1). Cu toate acestea, spre deosebire de art. 5 alin. (1), temeiul respectiv este aplicabil doar dacă prelucrarea este „*strict necesară*”. În acest sens, în *Orientările nr. 5/2022 privind utilizarea tehnologiei de recunoaștere facială în domeniul legii*, aprobate de Comitetul European pentru Protecția Datelor, se statuează următoarele:

„Prelucrarea categoriilor speciale de date, cum ar fi datele biometrice, poate fi considerată „strict necesară” (articolul 10 din LED) numai dacă atingerea adusă protecției datelor cu caracter personal și restrângerile acestora se limitează la ceea ce este absolut necesar, adică indispensabil, și exclude orice prelucrare de natură generală sau sistematică.”³

2) Prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale unei alte persoane fizice

Interesele vitale se referă la situațiile care pun viața în pericol, care pot fi legate de asistența medicală de urgență și de divulgarea informațiilor medicale confidențiale pentru a preveni o infracțiune gravă ce atentează la viața uneia sau mai multor persoane.⁴

3) Prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată

Acest temei legal trebuie interpretat în sensul în care persoana vizată a fost conștientă de faptul că datele respective vor fi disponibile publicului, și anume tuturor, inclusiv autorităților. În caz de îndoială, trebuie aplicată o interpretare restrictivă, întrucât se presupune că persoana vizată a renunțat în mod voluntar la protecția specială a datelor sensibile prin punerea lor la dispoziția publicului, inclusiv a autorităților. În situații precum publicarea datelor cu caracter personal într-o biografie, în presă sau pe un site internet public, intenția este clară.⁵

³ *Orientările nr. 5/2022 privind utilizarea tehnologiei de recunoaștere facială în domeniul legii*, Comitetul European pentru Protecția Datelor, 23 aprilie 2023, p. 6:

https://www.edpb.europa.eu/system/files/2024-05/edpb_guidelines_202304_frtlawenforcement_v2_ro.pdf

⁴ Kosta E., et al. *The EU Law Enforcement Directive (LED): A Commentary*, Oxford University Press, 2024, p. 227.

⁵ *Ibidem*, p. 228.

ARTICOLUL 8 – TERMENE PENTRU STOCARE ȘI REVIZUIRE

În conformitate cu art. 8 alin. (1), datele cu caracter personal sunt stocate numai atât timp cât sunt necesare pentru îndeplinirea scopurilor prevăzute la art. 1 alin. (1) din lege. Această prevedere coroborează cu principiul prelucrării datelor prevăzut la art. 4 alin. (1) lit. e).

Subsecvent, art. 8 alin. (2) precizează că, în cazul în care actele normative nu prevăd un termen specific și corespunzător pentru ștergerea datelor sau pentru revizuirea periodică de către operator a necesității de stocare a datelor, atunci acest termen specific și corespunzător trebuie să fie stabilit de către însăși operator.

Pentru a putea demonstra respectarea acestor prevederi, stabilirea termenului pentru ștergerea sau pentru revizuirea necesității de stocare a datelor urmează a fi documentată de către operator.

ARTICOLUL 9 – DISTINCȚIA ÎNTRE DIFERITE CATEGORII DE PERSOANE VIZATE

Prelucrarea datelor cu caracter personal în domeniul prevenirii și combaterii infracțiunilor presupune prelucrarea datelor cu caracter personal referitoare la diferite categorii de persoane. Prin urmare, trebuie să se facă o distincție clară, după caz și în măsura posibilului, între datele cu caracter personal ale diferitelor categorii de persoane vizate, cum ar fi bănușiții, învinușiții, inculpașiții, persoanele condamnate pentru comiterea unei infracțiuni, victimele și alte părți, cum ar fi martorii, persoanele care dețin informașiții sau contacte relevante, precum și complicitii suspecșiilor și ai infractorilor condamnașiți.

Această prevedere are drept scop asigurarea dreptului la prezumșiția de nevinovășție.⁶

Se va reșiține că lista categoriilor de persoane vizate enumerate la lit. a)-d) nu are caracter exhaustiv, ci exemplificativ.

ARTICOLUL 10 – DISTINCȚIA ÎNTRE DATELE CU CARACTER PERSONAL ȘI VERIFICAREA CALITĂȘII DATELOR CU CARACTER PERSONAL

Principiul exactitășții datelor trebuie aplicat luând în considerare natura și scopul prelucrării în cauză. În special, în cadrul procedurilor judiciare, declarașițiile

⁶ *Ibidem*, p. 167.

care conțin date cu caracter personal se bazează, de regulă, pe o percepție subiectivă a persoanelor fizice și nu sunt întotdeauna verificabile. În consecință, acest principiu nu trebuie să se aplice exactității unei declarații, ci doar faptului că o anumită declarație a fost făcută.

Autoritățile competente trebuie să se asigure că nu se transmit sau nu se pun la dispoziție date cu caracter personal care sunt inexacte, incomplete sau care nu mai sunt actuale. Pentru a asigura protecția persoanelor fizice și exactitatea, caracterul integral sau gradul de actualitate și fiabilitatea datelor cu caracter personal transmise sau puse la dispoziție, autoritățile competente trebuie, pe cât posibil, să adauge informațiile necesare în toate transmiterile de date cu caracter personal.

ARTICOLUL 11 – PROCESUL DECIZIONAL AUTOMATIZAT

Persoana vizată are dreptul să nu facă obiectul unei decizii care evaluează aspecte cu caracter personal referitoare la propria persoană, care se bazează exclusiv pe prelucrarea automată și care produce efecte juridice negative care privesc propria persoană sau o afectează în mod semnificativ. În orice caz, o astfel de prelucrare trebuie să facă obiectul unor garanții corespunzătoare, inclusiv o informare specifică a persoanei vizate și dreptul acesteia de a obține intervenție umană, în special de a-și exprima punctul de vedere, de a primi o explicație privind decizia luată în urma unei astfel de evaluări sau de a contesta decizia.

Este interzisă crearea de profiluri care are drept rezultat discriminarea persoanelor fizice în baza datelor cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale (*i.e.* categoriile speciale de date cu caracter personal prevăzute la art. 7).

CAPITOLUL III – DREPTURILE PERSOANEI VIZATE

ARTICOLUL 12 – DISPOZIȚII GENERALE PRIVIND COMUNICAREA ȘI MODALITĂȚILE DE EXERCITARE A DREPTURILOR PERSOANEI VIZATE

Capitolul III din prezentul proiect de lege și, în particular, art. 13-16, reglementează principalele drepturi ale persoanelor vizate în raport cu autoritățile competente care prelucrează date cu caracter personal în scopul prevenirii și combaterii infracțiunilor.

Art. 12, la rândul său, prevede un șir de dispoziții generale care reglementează unele aspecte procedurale privind modul de exercitare a drepturilor prevăzute la art. 13-16, dar și la art. 11 și 29 din lege.

Astfel, operatorul este obligat să ia măsuri rezonabile pentru a oferi persoanei vizate orice informații prevăzute la art. 13 și transmite acesteia orice comunicare în legătură cu art. 11, 14-16 și 29 referitoare la prelucrare, într-o formă concisă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Informațiile se transmit prin orice mijloace adecvate, inclusiv prin mijloace electronice. Ca regulă generală, operatorul transmite informațiile în același format în care a fost primită cererea.

În conformitate cu art. 12 alin. (3), operatorul informează în scris persoana vizată cu privire la modul în care a dat curs cererii acesteia, fără întârzieri nejustificate, **dar în cel mult o lună de la primirea cererii**. Cu toate acestea, perioada respectivă poate fi prelungită cu două luni atunci când este necesar, ținându-se cont de complexitatea și numărul cererilor. În orice caz, operatorul este obligat să informeze persoana vizată cu privire la orice astfel de prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii.

Este important de subliniat faptul că, în cazul în care operatorul are îndoieli întemeiate cu privire la identitatea persoanei fizice care înaintează cererea menționată la art. 14 sau 15, acesta poate solicita furnizarea de informații suplimentare necesare pentru a confirma identitatea persoanei vizate.

ARTICOLUL 13 – INFORMAȚII CARE SE PUN LA DISPOZIȚIA PERSONEI VIZATE SAU SE COMUNICĂ ACESTEIA

Punerea la dispoziție a informațiilor, precum și transparența în raporturile cu persoanele fizice în privința modului în care vor fi utilizate datele care le privesc, contribuie la garantarea faptului că prelucrarea legală a datelor cu caracter personal este echitabilă și că operatorii răspund pentru faptele lor.

Astfel, art. 13 alin. (1) lit. a)-e) enumeră informațiile generale care trebuie puse la dispoziție într-un mod accesibil publicului general, în special prin publicare pe pagina web oficială a autorității competente care prelucrează date în scopurile prevăzute la art. 1 alin. (1) din lege.

Subsecvent, art. 13 alin. (2) prevede informațiile care trebuie furnizate suplimentar unei anumite persoane vizate în anumite cazuri, de exemplu în situația în care datele sunt colectate direct de la persoana vizată sau indirect, fără știrea acesteia. Însă, în acest caz, comunicarea informațiilor respective poate fi amânată,

restricționată sau omisă dacă, și atât timp cât, ținând cont de drepturile fundamentale și interesele legitime ale persoanei vizate, o astfel de măsură este necesară și proporțională pentru:

- a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale ori juridice;
- b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor ori executarea pedepselor penale sau a măsurilor de siguranță;
- c) protejarea ordinii și securității publice;
- d) protejarea securității naționale;
- e) protejarea drepturilor și libertăților altor persoane.

După cum reiese din recitalul 44 al *Directivei (UE) 2016/680*, în vederea aplicării oricărei limitări în temeiul unei astfel de prevederi, operatorul trebuie să evalueze, prin intermediul unei examinări concrete și individuale a fiecărui caz, toate circumstanțele particulare.

ARTICOLUL 14 – DREPTUL DE ACCES

Art. 14 alin. (1) prevede, ca regulă generală, dreptul persoanei vizate de a avea acces la datele sale cu caracter personal, ceea ce înseamnă dreptul de a obține direct de la operator confirmarea pozitivă sau negativă cu privire la prelucrarea datelor sale cu caracter personal (cunoscut, de asemenea, ca dreptul de „acces direct” al persoanei vizate). În cazurile în care se confirmă existența prelucrării datelor, dreptul include accesul la datele cu caracter personal și la anumite informații particulare.

Esența dreptului de acces al persoanei vizate constă în obținerea confirmării temeiului juridic și în posibilitatea de a verifica legalitatea prelucrării. Prin urmare, operatorii trebuie să se asigure că informațiile furnizate sunt exacte, clare și suficiente pentru atingerea acestui scop.

Cu toate acestea, în conformitate cu art. 14 alin. (2), în vederea asigurării exercitării efective a atribuțiilor autorităților competente în domeniul prevenirii și combaterii infracțiunilor, operatorul poate limita, integral sau parțial, dreptul de acces al persoanei vizate în cazul în care și atât timp cât, ținând cont de drepturile fundamentale și interesele legitime ale persoanei vizate, o astfel de limitare este necesară și proporțională pentru:

- a) evitarea obstrucționării cercetărilor, anchetelor sau procedurilor oficiale sau juridice;

- b) a nu prejudicia prevenirea, depistarea, investigarea sau urmărirea penală a infracțiunilor ori executarea pedepselor penale sau a măsurilor de siguranță;
- c) protejarea ordinii și securității publice;
- d) protejarea securității naționale;
- e) protejarea drepturilor și libertăților altor persoane.

Precum reiese expres din recitalul 44 al *Directivei (UE) 2016/680*, în vederea limitării dreptului de acces al persoanei vizate, operatorul trebuie să evalueze, prin intermediul unei examinări concrete și individuale a fiecărui caz, toate circumstanțele particulare.

Operatorul informează în scris persoana vizată, în termenul prevăzut la art. 12 alin. (3), cu privire la refuzarea sau limitarea accesului și motivele refuzului sau ale limitării. Cu toate acestea, astfel de informații pot fi omise atunci când furnizarea lor ar contraveni unuia dintre scopurile enumerate *supra* (*i.e.* opțiunea de răspuns conform căruia operatorul nu poate „nici să confirme, nici să infirme” o anumită prelucrare de date).

Este important de precizat că operatorul este obligat să țină evidența deciziilor de limitare a dreptului de acces al persoanelor vizate, precum și să documenteze motivele de fapt și de drept pe care se întemeiază această decizie. Ulterior, informațiile respective vor fi puse la dispoziția Centrului, la cererea acestuia.

ARTICOLUL 15 – DREPTUL LA RECTIFICAREA SAU ȘTERGEREA DATELOR CU CARACTER PERSONAL ȘI LA RESTRICȚIONAREA PRELUCRĂRII

Orice persoană fizică are dreptul de a obține rectificarea datelor cu caracter personal inexacte care o privesc, mai ales când acestea se referă la fapte, precum și dreptul la ștergerea datelor în cazul în care prelucrarea datelor respective nu respectă prezenta lege. Cu toate acestea, dreptul la rectificare nu afectează, de exemplu, conținutul depozițiilor martorilor. O persoană fizică are, de asemenea, dreptul la restricționarea prelucrării atunci când această persoană contestă exactitatea datelor cu caracter personal, dar nu se poate stabili exactitatea sau inexactitatea lor, sau în cazul în care datele cu caracter personal trebuie să fie păstrate ca mijloace de probă. În special, în loc ca datele cu caracter personal să fie șterse, prelucrarea urmează să fie restricționată dacă într-un caz specific există motive întemeiate să se considere că ștergerea lor ar putea afecta interesele legitime ale persoanei vizate. În acest caz, datele restricționate pot fi prelucrate doar în scopul care a împiedicat ștergerea lor. Metodele de restricționare a prelucrării ar putea include, printre altele, transferul

datelor selectate în alt sistem de prelucrare, de exemplu în scopuri de arhivare, sau anularea accesului utilizatorilor la datele selectate. În ceea ce privește sistemele automatizate de evidență a datelor, restricționarea prelucrării datelor cu caracter personal trebuie, în principiu, asigurată prin mijloace tehnice; faptul că prelucrarea datelor cu caracter personal este restricționată trebuie indicat în sistem în așa fel încât să se înțeleagă clar că această restricționare are loc. O astfel de rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării urmează să fie comunicată destinatarilor cărora le-au fost divulgate datele și autorităților competente de la care provin datele inexacte. Operatorii trebuie, de asemenea, să nu comunice mai departe astfel de date.

ARTICOLUL 16 – EXERCITAREA DREPTURILOR DE CĂTRE PERSOANA VIZATĂ PRIN INTERMEDIUL CENTRULUI

În cazul în care operatorul refuză unei persoane vizate drepturile acesteia la informare, acces, rectificare sau ștergerea datelor ori la restricționarea prelucrării, persoana vizată are dreptul de a solicita ca Centrul Național pentru Protecția Datelor cu Caracter Personal să verifice legalitatea prelucrării.

Persoana vizată trebuie să fie informată cu privire la acest drept.

Persoana vizată urmează să fie informată de Centru cel puțin cu privire la faptul dacă toate verificările sau analizele necesare au fost efectuate. Centrul trebuie, de asemenea, să informeze persoana vizată în legătură cu dreptul de a introduce o acțiune în contencios administrativ.

CAPITOLUL IV – OPERATORUL ȘI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

SECȚIUNEA 1 – OBLIGAȚII GENERALE

Operatorul este responsabil și răspunde pentru orice prelucrare a datelor cu caracter personal efectuată de către acesta sau în numele său. În special, operatorul este obligat să pună în aplicare măsuri adecvate și eficiente și să fie în măsură să demonstreze că activitățile de prelucrare respectă prezenta lege. Măsurile respective trebuie să țină cont de natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul la adresa drepturilor și libertăților persoanelor fizice. Măsurile luate de operator trebuie să includă elaborarea și punerea în aplicare a unor garanții specifice cu privire la tratamentul datelor cu caracter personal ale persoanelor vulnerabile, în special ale copiilor.

Riscurile la adresa drepturilor și libertăților persoanelor fizice, prezentând grade diferite de probabilitate și gravitate, pot fi rezultatul unei prelucrări a datelor care ar putea genera prejudicii de natură fizică, materială sau morală, în special în cazurile în care:

- prelucrarea poate genera discriminare, furtul sau uzurparea identității, prejudiciu financiar, compromiterea reputației, pierderea confidențialității datelor protejate prin secret profesional, inversarea neautorizată a pseudonimizării sau la orice alt prejudiciu semnificativ de natură economică sau socială;
- persoanele vizate ar putea fi private de drepturile și libertățile lor sau de capacitatea de a-și exercita controlul asupra datelor lor cu caracter personal;
- datele cu caracter personal prelucrate sunt date care dezvăluie originea rasială sau etnică, opiniile politice, religia sau convingerile filozofice, ori apartenența sindicală;
- sunt prelucrate date genetice sau date biometrice pentru identificarea singulară a unei persoane sau date privind sănătatea ori privind viața sexuală și orientarea sexuală sau condamnările penale și infracțiunile ori măsurile de securitate conexe;
- sunt evaluate aspecte de natură personală, de exemplu analizarea și previzionarea unor aspecte privind randamentul la locul de muncă, situația economică, starea de sănătate, preferințele sau interesele personale, fiabilitatea sau comportamentul, localizarea sau deplasările, în scopul de a se crea sau de a se utiliza profiluri personale;
- sunt prelucrate date cu caracter personal ale unor persoane vulnerabile, în special ale copiilor;
- prelucrarea implică un volum mare de date cu caracter personal și afectează un număr larg de persoane vizate.

Probabilitatea și gravitatea riscului sunt determinate în raport de natura, domeniul de aplicare, contextul și scopurile prelucrării. Riscul trebuie să facă obiectul unei evaluări obiective, prin care să se stabilească dacă operațiunile de prelucrare a datelor prezintă un risc ridicat. Un risc ridicat este un risc deosebit de prejudiciere a drepturilor și libertăților persoanelor vizate.

Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare pentru a se asigura îndeplinirea cerințelor din prezenta lege. Punerea în aplicare a unor astfel de măsuri nu trebuie să se întemeieze doar pe considerente economice. Pentru a fi în măsură să demonstreze respectarea

prezentei legi, operatorul urmează să adopte politici interne și să pună în aplicare măsuri care să adere, în special, la principiul protecției datelor începând cu momentul conceperii și al protecției implicite a datelor. În cazul în care operatorul a realizat o evaluare a impactului asupra protecției datelor în temeiul prezentei legi, trebuie să se țină cont de rezultatele acesteia la elaborarea măsurilor și procedurilor respective. Măsurile ar putea consta, printre altele, în utilizarea pseudonimizării, cât mai curând posibil.

Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și a persoanelor împuternicite de către operator, inclusiv în ceea ce privește monitorizarea de către Centrul Național pentru Protecția Datelor cu Caracter Personal și măsurile adoptate de acesta, necesită o atribuire clară a responsabilităților stabilite prin prezenta lege, inclusiv în cazul în care un operator stabilește scopurile și mijloacele prelucrării împreună cu alți operatori sau în cazul în care o operațiune de prelucrare este efectuată în numele unui operator.

Efectuarea prelucrării de către o persoană împuternicită de către un operator trebuie să fie reglementată printr-un act juridic care să includă un contract care creează obligații pentru persoana împuternicită de către operator în raport cu operatorul și care să stipuleze, în special, că persoana împuternicită de către operator poate să acționeze numai la instrucțiunile operatorului. Persoana împuternicită de către operator va ține cont de principiul protecției datelor începând cu momentul conceperii și al protecției implicite a datelor.

În vederea demonstrării conformității cu prezenta lege, operatorul sau persoana împuternicită de către operator trebuie să păstreze evidențe ale tuturor categoriilor de activități de prelucrare aflate în responsabilitatea sa. Fiecare operator și fiecare persoană împuternicită de către operator sunt obligați de a coopera cu Centrul și de a pune la dispoziția acestuia, la cerere, aceste evidențe, pentru a putea fi utilizate în scopul monitorizării respectivelor operațiuni de prelucrare. Operatorul sau persoana împuternicită de către operator care prelucrează date cu caracter personal în sisteme de prelucrare neautomată trebuie să dispună de metode eficiente pentru a demonstra legalitatea prelucrării, a permite monitorizarea proprie și a garanta integritatea și securitatea datelor, precum înregistrări sau alte forme de evidențe.

Înregistrările trebuie păstrate cel puțin pentru operațiunile din cadrul sistemelor de prelucrare automată, precum colectarea, modificarea, consultarea, divulgarea, inclusiv transferurile, combinarea sau ștergerea. Identificarea persoanei care a consultat sau divulgat date cu caracter personal trebuie să fie înregistrată și, plecând de la identificarea respectivă, să fie posibil să se stabilească justificarea operațiunilor de prelucrare. Înregistrările pot fi utilizate numai pentru verificarea

legalității prelucrării, monitorizarea proprie, asigurarea integrității și securității datelor și pentru proceduri penale. Monitorizarea proprie include, de asemenea, proceduri disciplinare interne ale autorităților competente.

Operatorul trebuie să realizeze o evaluare a impactului asupra protecției datelor în cazurile în care operațiunile de prelucrare pot avea drept rezultat, prin natura, domeniul de aplicare sau scopurile lor, un risc ridicat la adresa drepturilor și libertăților persoanelor vizate, evaluare care va include în special măsurile, garanțiile și mecanismele preconizate în vederea asigurării protecției datelor cu caracter personal și a atestării conformității cu prezenta directivă. Evaluările impactului trebuie să acopere sistemele și procesele relevante aferente operațiunilor de prelucrare, și nu cazuri individuale.

Pentru a garanta protecția eficientă a drepturilor și libertăților persoanelor vizate, operatorul sau persoana împuternicită de către operator trebuie să se consulte cu Centrul în anumite cazuri, înainte de prelucrare.

SECȚIUNEA A 2-A – SECURITATEA DATELOR CU CARACTER PERSONAL

În vederea menținerii securității și a prevenirii prelucrărilor care încalcă prezenta lege, operatorul sau persoana împuternicită de către operator trebuie să evalueze riscurile inerente prelucrării și să pună în aplicare măsuri pentru atenuarea acestor riscuri, precum criptarea. Măsurile respective trebuie să asigure un nivel corespunzător de securitate, inclusiv de confidențialitate, luând în considerare stadiul actual al tehnologiei, costurile punerii lor în aplicare în raport cu riscurile și natura datelor cu caracter personal a căror protecție trebuie asigurată. La evaluarea riscurilor la adresa securității datelor, se va acorda atenție riscurilor pe care le prezintă prelucrarea datelor, cum ar fi distrugerea, pierderea sau modificarea accidentală sau ilegală, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod, care pot duce în special la prejudicii fizice, materiale sau morale. Operatorul și persoana împuternicită de către operator trebuie să se asigure că prelucrarea datelor cu caracter personal nu se realizează de către persoane neautorizate.

Dacă nu este soluționată la timp și într-un mod adecvat, o încălcare a securității datelor cu caracter personal poate genera prejudicii fizice, materiale sau morale persoanelor fizice, cum ar fi pierderea controlului asupra datelor lor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau uzurpare de identitate, prejudiciu financiar, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin

secret profesional sau orice alt prejudiciu important de natură economică sau socială cauzat acelei persoane fizice. Prin urmare, imediat ce a luat cunoștință de producerea unei încălcări a securității datelor cu caracter personal, operatorul este obligat să notifice încălcarea securității datelor cu caracter personal Centrului fără întârziere nejustificată și, dacă este posibil, în cel mult 72 de ore după ce a luat cunoștință de existența acesteia, cu excepția cazului în care operatorul este în măsură să demonstreze, în conformitate cu principiul responsabilității, că încălcarea securității datelor cu caracter personal nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice. Atunci când notificarea nu se poate realiza în termen de 72 de ore, aceasta va cuprinde motivele întârzierii, iar informațiile vor putea fi furnizate treptat, fără altă întârziere.

Persoanele fizice trebuie să fie notificate fără întârziere în cazul în care încălcarea securității datelor cu caracter personal este susceptibilă să genereze un risc ridicat la adresa drepturilor și libertăților persoanelor fizice, pentru a le permite acestora să ia măsurile de precauție necesare. Notificarea va descrie natura încălcării securității datelor cu caracter personal și va conține recomandări pentru persoana fizică în cauză în scopul atenuării eventualelor efecte negative. Notificarea persoanelor vizate trebuie să fie efectuată în cel mai scurt timp posibil în mod rezonabil și în strânsă cooperare cu Centrul și în conformitate cu orientările furnizate de aceasta sau de alte autorități relevante. De exemplu, necesitatea de a atenua un risc imediat de producere a unor prejudicii ar presupune notificarea cu promptitudine a persoanelor vizate, în timp ce necesitatea de a pune în aplicare măsuri corespunzătoare împotriva încălcării în continuare a securității datelor sau împotriva unor încălcări similare ale securității datelor ar putea justifica un termen mai îndelungat. În cazul în care evitarea obstrucționării cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, evitarea aducerii de prejudicii la adresa prevenirii, depistării, investigării sau urmării penale a infracțiunilor sau a executării pedepselor, a protejării securității publice, a protejării securității naționale sau a apărării drepturilor și libertăților altora nu pot fi obținute prin amânarea sau restricționarea comunicării unei încălcări a securității datelor cu caracter personal către persoana fizică în cauză, o astfel de comunicare ar putea fi omisă în circumstanțe excepționale.

SECȚIUNEA A 3-A – RESPONSABILUL CU PROTECȚIA DATELOR

Operatorul trebuie să desemneze o persoană care să îi acorde asistență pentru a monitoriza respectarea, la nivel intern, a dispozițiilor adoptate în temeiul prezentei legi, cu excepția instanțelor judecătorești în activitatea de desfășurare a justiției.

Persoana respectivă ar putea fi un membru al personalului existent al operatorului care a beneficiat de o formare specială în materie de legislație și practici privind protecția datelor pentru a dobândi cunoștințe de specialitate în domeniul respectiv. Nivelul necesar al cunoștințelor de specialitate se stabilește în special în funcție de prelucrarea efectuată asupra datelor și de gradul de protecție impus pentru datele cu caracter personal prelucrate de către operator. Îndeplinirea sarcinilor sale poate fi efectuată cu normă întreagă sau cu fracțiune de normă. Un responsabil cu protecția datelor poate fi numit în comun de mai mulți operatori, ținând seama de structura organizatorică și de dimensiunea acestora, de exemplu în caz de resurse comune în unitățile centrale. Persoana respectivă poate fi, de asemenea, numită în posturi diferite în cadrul structurii operatorilor relevanți. Persoana în cauză trebuie să acorde suport operatorului și angajaților care prelucrează date cu caracter personal, prin informarea și consilierea acestora cu privire la respectarea obligațiilor lor relevante în materie de protecție a datelor. Astfel de responsabili cu protecția datelor trebuie să fie în măsură să își îndeplinească îndatoririle și sarcinile în mod independent, în conformitate cu legislația.

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

ARTICOLELE 33-38

Transferul către un alt stat sau către o organizație internațională are loc numai în cazul în care acest transfer este necesar în scopurile prevăzute la art. 1 alin. (1) din lege, iar operatorul din alt stat sau din organizația internațională este o autoritate competentă în sensul prezentei legi.

Un transfer poate fi efectuat numai de către autoritățile competente, acționând în calitate de operatori, cu excepția cazului în care persoanele împuternicite de către operatori primesc instrucțiuni în mod expres să transfere în numele operatorilor.

Un astfel de transfer poate avea loc în cazul în care Centrul decide că statul sau organizația internațională în cauză asigură un nivel adecvat de protecție, atunci când se asigură garanții corespunzătoare ori când se aplică derogări pentru situații speciale. În cazul în care se transferă date cu caracter personal din Republica Moldova către operatori, persoane împuternicite de către operatori sau alți destinatari din alte state sau organizații internaționale, nivelul de protecție a persoanelor fizice garantat în Republica Moldova prin prezenta lege nu poate să fie diminuat, inclusiv în cazurile de transferuri ulterioare de date cu caracter personal dinspre alt stat sau

organizația internațională către operatori sau persoane împuternicite de către operatori din aceeași sau dintr-un alt stat sau organizație internațională.

Orice condiții specifice pentru transfer sunt comunicate altor state sau organizațiilor internaționale. Transferurile ulterioare de date cu caracter personal trebuie să facă obiectul autorizării prealabile de către autoritatea competentă care a realizat transferul inițial. Atunci când decide cu privire la o cerere de autorizare a unui transfer ulterior, autoritatea competentă care a realizat transferul inițial trebuie să țină cont în mod corespunzător de toți factorii relevanți, inclusiv de gravitatea infracțiunii, de condițiile specifice transferului și de scopul pentru care datele au fost transferate inițial, de natura și condițiile executării pedepsei, precum și de nivelul de protecție a datelor cu caracter personal dintr-un alt stat sau dintr-o organizație internațională către care datele cu caracter personal sunt transferate ulterior. Autoritatea competentă care a realizat transferul inițial poate aplica transferului ulterior condiții specifice. Astfel de condiții specifice pot fi descrise, de exemplu, în coduri de utilizare.

Centrul poate decide că anumite state, un teritoriu ori unul sau mai multe sectoare determinate dintr-un stat sau o organizație internațională oferă un nivel adecvat de protecție a datelor. Atunci când evaluează caracterul adecvat al nivelului de protecție, Centrul ține cont, în special, de elementele prevăzute la art. 45 alin. (2) din *Legea nr. 195/2024 privind protecția datelor cu caracter personal*. Prevederile art. 45 alin. (3)–(8) din *Legea nr. 195/2024 privind protecția datelor cu caracter personal* se aplică în mod corespunzător și în cazul emiterii deciziilor privind caracterul adecvat al nivelului de protecție în temeiul prezentei legi.

Cu toate acestea, se va reține că deciziile emise de Centru în temeiul *Legii nr. 195/2024* nu pot servi ca temei de transfer realizat în temeiul prezentului proiect de lege.

Transferurile care nu se întemeiază pe o decizie privind caracterul adecvat al nivelului de protecție sunt permise numai în cazul în care au fost prezentate garanții corespunzătoare într-un instrument cu caracter juridic obligatoriu, care să asigure protecția datelor cu caracter personal, sau în cazul în care operatorul a evaluat toate circumstanțele legate de datele transferate și, pe baza acestei evaluări, consideră că există garanții adecvate în ceea ce privește protecția datelor cu caracter personal. Astfel de instrumente cu caracter juridic obligatoriu ar putea fi, de exemplu, acorduri bilaterale cu caracter juridic obligatoriu care au fost încheiate între state și puse în aplicare în ordinea juridică a acestora și a căror respectare poate fi impusă de către persoanele vizate din respectivele state, asigurând respectarea cerințelor în materie de protecție a datelor și drepturile persoanelor vizate, inclusiv dreptul de a obține reparații efective pe cale administrativă sau judiciară. Operatorul trebuie, de asemenea, să ia în considerare faptul că transferul de date cu caracter personal va fi

supus obligațiilor de confidențialitate și principiului specificității, asigurându-se că datele nu vor fi prelucrate în alte scopuri decât cel al transferului. În plus, operatorul va lua în considerare faptul că datele cu caracter personal nu vor fi folosite pentru a solicita, a pronunța sau a executa pedeapsa cu moartea sau orice altă formă de tratament inuman. Deși aceste condiții pot fi considerate garanții adecvate care să permită transferul de date, operatorul va putea solicita garanții suplimentare.

În cazul în care nu există nicio decizie privind caracterul adecvat al nivelului de protecție sau nicio garanție adecvată, un transfer sau o categorie de transferuri poate avea loc numai în situații specifice, dacă este necesar:

- în scopul protejării intereselor vitale ale persoanei vizate sau ale unei alte persoane sau al protejării intereselor legitime ale persoanei vizate în cazul în care se prevede astfel de actele normative;
- pentru prevenirea unei amenințări imediate și grave la adresa securității publice a Republicii Moldova sau a unui alt stat;
- într-un caz specific, în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv în scopul protejării împotriva amenințărilor la adresa securității publice;
- într-un caz specific, pentru stabilirea, exercitarea sau apărarea unui drept într-o procedură administrativă, penală, judiciară sau extrajudiciară, în legătură cu scopurile prevăzute la art. 1 alin. (1) din lege.

Aceste derogări urmează a fi interpretate restrictiv și nu trebuie să permită transferuri frecvente, masive și structurale de date cu caracter personal sau transferuri la scară largă de date, ci trebuie să se limiteze la datele strict necesare. Astfel de transferuri urmează să fie documentate și să fie puse la dispoziția Centrului la cerere, în scopul monitorizării legalității transferului.

Autoritățile competente aplică acordurile internaționale bilaterale sau multilaterale în vigoare, încheiate cu alte state în domeniul cooperării judiciare în materie penală și al cooperării polițienești, în schimbul obținerii de informații relevante care să le permită să își îndeplinească sarcinile atribuite în mod legal. În principiu, acest lucru are loc prin intermediul sau cel puțin cu cooperarea autorităților competente din alte state implicate în scopul prezentei legi, uneori chiar în absența unui acord internațional bilateral sau multilateral. Cu toate acestea, în anumite cazuri individuale, procedurile obișnuite care necesită contactarea autorităților din alte state pot fi ineficiente sau inadecvate, în special din cauza faptului că transferul nu poate fi efectuat în timp util sau din cauza faptului că autoritatea din altă țară nu respectă statul de drept sau normele și standardele internaționale în materia drepturilor omului, astfel încât autoritățile competente ar putea decide să transfere datele cu caracter personal direct beneficiarilor stabiliți în statele corespunzătoare. Acesta ar

putea fi cazul atunci când există o nevoie urgentă de a transfera date cu caracter personal pentru a salva viața unei persoane care se află în pericol de a deveni victimă a unei infracțiuni sau în interesul prevenirii săvârșirii iminente a unei infracțiuni, inclusiv a terorismului.

CAPITOLUL VI – SUPRAVEGHEREA, REMEDIILE LEGALE, RĂSPUNDEREA ȘI SANCTIUNILE

ARTICOLUL 39 – COMPETENȚA CENTRULUI

În vederea asigurării respectării prevederilor prezentei legi de către autoritățile competente, Centrul Național pentru Protecția Datelor cu Caracter Personal asigură supravegherea și monitorizarea aplicării prezentei legi în vederea protejării drepturilor și libertăților fundamentale ale persoanelor fizice în legătură cu prelucrarea datelor cu caracter personal. În acest scop, Centrul exercită sarcinile și competențele prevăzute de prezenta lege, precum și cele prevăzute de Capitolele VII și VIII din *Legea nr. 195/2024 privind protecția datelor cu caracter personal*.

Astfel, Capitolele VII și VIII din *Legea nr. 195/2024* se aplică în mod corespunzător și în contextul prezentei legi.

În altă ordine de idei, Centrul nu are competența de a supraveghea operațiunile de prelucrare efectuate de instanțele judecătorești în activitatea de îndeplinire a justiției.

ARTICOLUL 40 – DREPTUL DE A DEPUNE O PLÂNGERE LA CENTRU

Orice persoană vizată are dreptul de a depune o plângere la Centru în cazul în care consideră că prelucrarea datelor cu caracter personal care o privesc încalcă prezenta lege. În acest sens, art. 72 și 73, precum și Capitolul VIII, secțiunea a 2-a din *Legea nr. 195/2024* se aplică în mod corespunzător.

ARTICOLUL 41 – DREPTUL LA REMEDII JUDICIARE

Fără a aduce atingere dreptului de a depune o plângere la Centru, orice persoană vizată are dreptul de a înainta o acțiune în contencios administrativ împotriva unui operator sau a unei persoane împuternicite de operator, în conformitate cu Codul administrativ, fără respectarea procedurii prealabile, în cazul în care consideră că drepturile de care beneficiază în temeiul prezentei legi au fost

încălcate ca urmare a prelucrării datelor sale cu caracter personal fără respectarea prezentei legi.

În acest context, persoana vizată are dreptul la despăgubiri pentru prejudiciile materiale sau morale, în conformitate cu art. 76 din *Legea nr. 195/2024*.

ARTICOLUL 42 – AMENDA

În cazul în care Centrul va constata o încălcare a prezentei legi, precum și în cazul în care operatorii sau persoanele împuternicite de operator nu vor respecta măsurile aplicate de Centru în temeiul art. 60 alin. (1) sau (2) din *Legea nr. 195/2024*, Centrul va aplica o sancțiune pecuniară sub formă de amendă în cuantum de până la 2 000 000 lei. Modul de calculare și aplicare al amenzilor se va efectua în conformitate cu art. 87 din *Legea nr. 195/2024*.

ARTICOLUL 43 – DENUNȚAREA CAZURILOR DE ÎNCĂLCARE

Acest articol oferă posibilitatea angajaților autorităților competente să semnaleze potențialele încălcări ale prezentei legi. Aceste denunțări vor fi examinate și soluționate de către Centru în conformitate cu Capitolul VIII, secțiunea a 2-a din *Legea nr. 195/2024*.

Este imperativ ca Centrul să asigure confidențialitatea identității persoanelor care denunță presupuse încălcări ale prezentei legi, pentru a nu admite din partea autorităților competente acțiuni de răzbunare în privința persoanelor în cauză.

CAPITOLUL VII – DISPOZIȚIILE FINALE ȘI TRANZITORII

ARTICOLUL 44 – DISPOZIȚII FINALE

Prezenta lege va intra în vigoare concomitent cu intrarea în vigoare a *Legii nr. 195/2024*, *i.e.* pe 23 august 2026.

Până la intrarea în vigoare a prezentei legi, vor fi efectuate modificările de rigoare ale cadrului normativ conex.

ARTICOLUL 45 – DISPOZIȚII TRANZITORII

Pentru a asigura pentru autoritățile competente o tranziție ușoară la noile prevederi normative, din momentul intrării în vigoare a prezentei legi, din cuantumul final al amenzii stabilite de Centru, se va aplica:

- a) din primul an – 10% din cuantumul amenzii stabilite;
- b) din al doilea an – 40% din cuantumul amenzii stabilite;
- c) din al treilea an – 100% din cuantumul amenzii stabilite.

Subsecvent, plângerile depuse la Centru până la data intrării în vigoare a prezentei legi se examinează și se soluționează conform normelor de procedură prevăzute de prezenta lege și *Legea nr. 195/2024 privind protecția datelor cu caracter personal* și conform normelor materiale, inclusiv celor privind răspunderea pentru încălcarea legislației privind protecția datelor cu caracter personal, prevăzute de legea în vigoare la data comiterii încălcării.

Nu în ultimul rând, cauzele civile, contravenționale sau de contencios administrativ se examinează și se soluționează în conformitate cu prevederile legii în vigoare la data apariției raportului juridic litigios.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

În vederea atingerii obiectivului trasat, opțiuni alternative nu au fost identificate.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Implementarea prevederilor proiectului de lege va avea impact în privința activităților realizate de autoritățile competente.

Prevederile *Directivei (UE) 2016/680* au fost concepute ca să instituie un regim juridic care să fie racordat la particularitățile activității de prevenire și combatere a infracțiunilor. Or, aceste activități impun reglementări speciale în partea ce vizează:

- a) principiile și temeiul legal pentru prelucrarea datelor efectuată în scopul prevenirii și combaterii infracțiunilor;
- b) modalitatea de exercitare și limitare a drepturilor persoanelor vizate;
- c) asigurarea securității datelor cu caracter personal, în special în cadrul sistemelor informaționale automatizate;
- d) realizarea transferurilor de date către alte state sau către organizații internaționale, în vederea facilitării schimbului de informații între organele de drept.

Astfel, prezentul proiect de lege va facilita activitatea autorităților competente, deoarece, pe de o parte, soluțiile juridice propuse țin cont de particularitățile activității de prevenire și combatere a infracțiunilor, iar, pe de altă parte, prevederile transpuse asigură o claritate mai înaltă a regimului de protecție a datelor în contextul activității organelor de drept.

4.2. Impactul financiar și argumentarea costurilor estimative
Implementarea prevederilor prezentului proiect de lege nu implică cheltuieli financiare suplimentare.
4.3. Impactul asupra sectorului privat
Nu este aplicabil.
4.4. Impactul social
Se implementează prevederile <i>Directivei (UE) 2016/680</i> .
4.4.1. Impactul asupra protecției datelor cu caracter personal
Se implementează prevederile <i>Directivei (UE) 2016/680</i> .
4.4.2. Impactul asupra echității și egalității de gen
Nu este aplicabil.
4.5. Impactul asupra mediului
Nu este aplicabil.
4.6. Alte impacturi și informații relevante
Nu este aplicabil.
5. Compatibilitatea proiectului cu legislația UE
5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională
Prezentul proiect de lege realizează o transpunere primară și totală a <i>Directivei (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmării 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, publicată în Jurnalul Oficial al Uniunii Europene L 119/89 din 4 mai 2016, nr. CELEX: 32016L0680.</i>

Obiectivul acestui act juridic constă în protejarea drepturilor și libertăților fundamentale ale persoanelor fizice, în special al dreptului acestora la protecția datelor cu caracter personal.

Gradul de transpunere al actului este prezentat în tabelul de concordanță, anexat la prezentul proiect de lege.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Transpunerea actului juridic european se realizează în totalitate prin intermediul prezentului proiect de lege. Pentru implementarea *Directivei (UE) 2016/680* nu este necesară transpunerea unor acte juridice delegate.

6. Avizarea și consultarea publică a proiectului

Inițierea elaborării prezentului proiect de lege a fost anunțată pe 29 decembrie 2023 ([link](#)). Adițional, a fost plasat anunț și pe platforma [particip.gov.md](#) ([link](#)). Propuneri sau recomandări nu au fost recepționate.

7. Modul de încorporare a actului în cadrul normativ existent

După adoptarea prezentului proiect de lege va fi necesară modificarea *Legii nr. 195/2024 privind protecția datelor cu caracter personal*, a *Codului de procedură penală nr. 122/2003*, a *Legii nr. 514/1995 privind organizarea judecătorească*, precum și a altor acte normative conexe.

8. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Implementarea prevederilor prezentului proiect de lege implică realizarea de către autoritățile competente și Centrul Național pentru Protecția Datelor cu Caracter Personal a măsurilor prevăzute în Capitolele II-VI din proiect, precum și a măsurilor prevăzute în Capitolele VII și VIII din *Legea nr. 195/2024 privind protecția datelor cu caracter personal*.

Secretar de stat

Eduard SERBENCO