



MINISTERUL JUSTIȚIEI
AL REPUBLICII MOLDOVA
CENTRUL DE ARMONIZARE A
LEGISLAȚIEI

str. 31 August 1989, nr. 82
MD-2012, mun. Chișinău,
tel.: 0 22 820879, fax: 0 22 820883
www.justice.gov.md

DECLARAȚIE DE COMPATIBILITATE

În baza expertizei proiectului Legii pentru modificarea și completarea unor acte legislative (Legea nr. 133/2011 privind protecția datelor cu caracter personal, Legea 355/2005 cu privire la sistemul de salarizare în sectorul bugetar, Legea 48/2012 privind sistemul de salarizare a funcționarilor publici), inclus în art. 13 "Protecția datelor cu caracter personal" din Titlul III "Justiție, libertate și securitate" al Planului Național de acțiuni pentru implementarea Acordului de Asocierie RM-UE în perioada 2017-2019 (PNAAA 2017-2019), aprobat prin Hotărârea Guvernului nr. 1472 din 30 decembrie 2016

Art. 1 din proiectul Legii pentru modificarea și completarea unor acte legislative (Legea 133/2011 privind protecția datelor cu caracter personal (redacție nouă)) **transpune:**

1. Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE), publicat în Jurnalul Oficial al UE nr. L 119 din 4 mai 2016/ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), published in the Official Journal of EU No. L 119 of 4 May 2016;

2. Directiva (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, publicat în Jurnalul Oficial al UE nr. L 119 din 4 mai 2016/ Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, published in the Official Journal of EU No. L 119 of 4 May 2016.

I. Obiectul proiectului

Proiectul Legii pentru modificarea și completarea unor acte legislative, în speță art. I care oferă redacția nouă a Legii 133/2011, își propune transpunerea la nivel național a prevederilor

Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE, precum și preluarea prevederilor 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, prin actualizarea cadrului normativ național în domeniul protecției datelor cu caracter personal, cu introducerea unor prevederi detaliate și noi referitoare la condițiile generale juridice și tehnice ce trebuie asigurate în procesul de inițiere și/sau prelucrare a datelor cu caracter personal, în vederea respectării dreptului fundamental al omului la inviolabilitatea vieții intime, familiale și private, consacrat de art. 28 din Constituția Republicii Moldova. De asemenea, Capitolul VII din proiectul național își propune fixarea prevederilor speciale referitoare la prelucrarea datelor personale de către organele de ocrotire a legii în scopul prevenirii, investigării, depistării și/sau urmării penale a infracțiunilor sau executării pedepselor penale, detenția preventivă, inclusiv protejarea și prevenirea amenințărilor la adresa ordinii publice, securității de stat și securității naționale și în cadrul dosarului sau acțiunilor speciale de investigație.

Domeniul protecției persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date, inclusiv în domeniul cooperării judiciare în materie penală și al cooperării polițienești este reglementat la nivelul legislației UE prin Regulamentul (UE) 2016/679/UE și, respectiv, Directiva 2016/680/UE, două din cele 3 acte UE care formează noul pachet legislativ al UE în domeniul prelucrării datelor cu caracter personal. Regulamentul 2016/679/UE vine să abroge și să substituie 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, act UE care a constituit obiect al transpunerii în legislația națională prin Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal (supus expertizei de compatibilitate). Directiva 2016/680/UE vine la rândul ei să abroge și să substituie 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, act UE care nu a fost transpus în legislația națională a Republicii Moldova.

Având în vedere reformarea sistemului european de protecție a datelor cu caracter personal prin noul pachet legislativ al UE în domeniul prelucrării datelor cu caracter personal, Centrul Național pentru Protecția Datelor cu Caracter Personal a inițiat un act normativ de revizuire completă a Legii 133/2011, care să reflecte evoluțiile legislației UE în domeniu și care, la momentul adopției, va constitui noul cadru legal național în domeniul protecției datelor cu caracter personal racordat la cel european.

Din punctul de vedere al transpunerii reglementărilor UE, proiectul de act normativ reglementează, în principal, următoarele aspecte relevante:

- Identificarea domeniului de aplicare al Legii, în special identificarea categoriilor de prelucrări de date care sunt afectate, precum și prelucrărilor care nu cad sub incidența Legii (art. 1 (1), art. 3 (2) și art. 2 (2) din Regulamentul 2016/679; art. 1 (1) și art. 2 din Directiva 2016/680/UE);
- Reflectarea noțiunilor specifice domeniului prelucrării datelor cu caracter personal (art. 4 din Regulamentul 2016/679 și art. 3 din Directiva 2016/680/UE);

- Stabilirea prevederilor generale privind autoritatea de supraveghere a dreptului la protecția datelor cu caracter personal (Capitolul VI din Regulamentul 2016/679/UE și Capitolul VI din Directiva 2016/680/UE)
- Descrierea condițiilor de conformitate și legalitate la prelucrarea datelor cu caracter personal (art. 5 și 6 din Regulamentul 2016/679 și art. 4 din Directiva 2016/680/UE);
- Prelucrarea condițiilor privind consimțământul persoanei vizate pentru prelucrarea datelor cu caracter personal (art. 7 din Regulamentul 2016/679);
- Inserarea normelor privind interzicerea prelucrării categoriei speciale a datelor cu caracter personal, cu excepțiile de rigoare (art. 9 din Regulamentul 2016/679 și art. 10 din Directiva 2016/680/UE);
- Stabilirea cazurilor în care prelucrarea datelor cu caracter personal nu necesită identificare (art. 11 din Regulamentul 2016/679);
- Prelucrarea normelor privind transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor persoanei vizate (art. 11 din Regulamentul 2016/679 și art. 12 din Directiva 2016/680/UE);
- Fixarea datelor ce se prezintă subiectului datelor cu caracter personal în cazul prelucrării acestora și termenilor de furnizare a acestor date (art. 13 și 14 din Regulamentul 2016/679 și art. 13 din Directiva 2016/680);
- Prelucrarea prevederilor referitoare la dreptul de acces la datele cu caracter personal al persoanei vizate (art. 15 din Regulamentul 2016/679 și art. 14 și 15 din Directiva 2016/680/UE);
- Inserarea dreptului la rectificare al subiectului datelor cu caracter personal (art. 16 din Regulamentul 2016/679);
- Fixarea dreptului la ștergerea datelor cu caracter personal și excepțiile de la acesta (art. 17 din Regulamentul 2016/679 și art. 16 din Directiva 2016/680/UE);
- Introducerea dreptului la restricționarea prelucrării datelor cu caracter personal (art. 18 din Regulamentul 2016/679);
- Stabilirea obligației de informare privind rectificarea, ștergerea datelor cu caracter personal sau restricționarea prelucrării (art. 19 din Regulamentul 2016/679);
- Reglementarea dreptului la portabilitatea datelor cu caracter personal și dreptului la opoziție al subiectului datelor cu caracter personal (art. 20 și 21 din Regulamentul 2016/679);
- Stabilirea prevederilor referitoare la procesul decizional individual automatizat (art. 22 din Regulamentul 2016/679 și art. 11 din Directiva 2016/680/UE);
- Fixarea excepțiilor și restricțiilor de la drepturile aferente prelucrării datelor cu caracter personal (art. 23 din Regulamentul 2016/679);
- Stabilirea prevederilor privind responsabilitatea operatorului de date cu caracter personal (art. 24 din Regulamentul 2016/679 și art. 19 din Directiva 2016/680/UE);
- Stabilirea obligației operatorului de a pune în aplicare a măsurilor tehnice și organizatorice adecvate de prelucrare a datelor cu caracter personal (art. 25 din Regulamentul 2016/679);
- Fixarea obligației operatorului de evaluare a impactului asupra protecției datelor cu caracter personal (art. 35 din Regulamentul 2016/679 și art. 27 din Directiva 2016/680/UE);

- Stabilirea normelor privind desemnarea responsabilului de protecția datelor în cadrul operatorului sau persoanei împuternicite, funcțiile acestuia și sarcinile (art. 37-39 din Regulamentul 2016/679 și art. 32-34 din Directiva 2016/680/UE);
- Stabilirea normelor privind operatorii asociați (art. 26 din Regulamentul 2016/679 și art. 21 din Directiva 2016/680/UE);
- Reglementarea obligațiilor operatorilor sau persoanelor împuternicite care nu au sediul în Republica Moldova (art. 27 din Regulamentul 2016/679);
- Stabilirea normelor referitoare la prelucrarea datelor de către persoana împuternicită de operator (art. 28 din Regulamentul 2016/679 și art. 22 din Directiva 2016/680/UE);
- Reglementarea modului de prelucrare a datelor sub autoritatea operatorului sau a persoanei împuternicite de acesta (art. 29 din Regulamentul 2016/679 și art. 23 din Directiva 2016/680/UE);
- Fixarea normelor privind evidența activităților de prelucrare a datelor cu caracter personal (art. 30 din Regulamentul 2016/679 și art. 24 din Directiva 2016/680/UE);
- Stabilirea normelor referitoare la securitatea prelucrării datelor cu caracter personal (art. 32-34 din Regulamentul 2016/679 și art. 29-31 din Directiva 2016/680/2018);
- Inserarea obligativității consultării autorității de supraveghere înainte de prelucrarea unor date cu caracter personal care fac parte dintr-un sistem nou de evidență a datelor (art. 36 din Regulamentul 2016/679/UE și art. 28 din Directiva 2016/680/UE);
- Prelucrarea normelor referitoare la elaborarea codurilor de conduită de către operatori (art. 40 și 41 din Regulamentul 2016/679/UE);
- Reglementarea procedurii de certificare a sistemelor de evidență a datelor cu caracter personal (art. 42, 43 și art. 51, 52 din Regulamentul 2016/679);
- Reglementarea condițiilor de depunere a reclamațiilor (art. 77 din Regulamentul 2016/679 și art. 48, 52-53 din Directiva 2016/679/UE);
- Stabilirea procedurii de transmitere transfrontalieră a datelor personale (art. 44-46 din Regulamentul 2016/679 și art. 35-39 din Directiva 2016/679/UE);
- Înstituirea normelor privind răspunderea în cazul încălcării normelor privind prelucrarea datelor cu caracter personal, în special, sancțiuni pecuniare (art. 82 și 83 din Regulamentul 2016/679 și art. 57 din Directiva 2016/680/UE).

II. Evaluarea din perspectiva compatibilității cu Dreptul UE

La nivel național, cadrul legal în vigoare în domeniul protecției datelor cu caracter personal este reprezentat de Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal (în continuare Legea 133/2011), care a asigurat transpunerea Directivei 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 și care va fi substituită de prezentul proiect de Lege la momentul adoptării și intrării în vigoare a acesteia.

În raport cu obiectul specific de reglementare, la nivelul dreptului european derivat prezintă incidență directă dispozițiile *Regulamentului (UE) 2016/679* și *Directivei 2016/680/UE*, prevederi, pe care inițiatorul proiectului național își propune să le transpună integral la nivelul legislației naționale de profil.

Regulamentul 2016/679/UE stabilește cadrul juridic unitar și uniform în aplicare la nivelul UE în ceea ce privește protecția persoanelor fizice în cadrul prelucrării datelor personale ale acestora, în vederea oferirii acestora în toate statele membre aceluiași nivel de drepturi, obligații și responsabilități opozabile din punct de vedere juridic pentru operatori și persoanele împuternicite de aceștia, pentru a asigura o monitorizare coerentă a prelucrării datelor cu caracter personal, sancțiuni echivalente în toate statele membre, precum și a institui o cooperare eficientă a autorităților de supraveghere din aceste state.

Regulamentul 2016/679/UE stabilește: principiile legate de prelucrarea datelor cu caracter personal, condițiile unei prelucrări considerate legale, condițiile privind consimțământul persoanei vizate, condițiile privind consimțământul copiilor în legătură cu serviciile societății informaționale, modalitatea de prelucrare a categoriilor speciale de date cu caracter personal, asigurarea transparenței informațiilor, a comunicărilor și a modalității de exercitare a drepturilor persoanei vizate, informațiile care se furnizează în cazul când datele cu caracter personal sunt colectate de la persoana vizată și în cazul când nu au fost obținute de la aceasta, dreptul de acces al persoanei vizate, dreptul la rectificare, dreptul la ștergerea datelor, dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, dreptul la opoziție și procesul individual automatizat responsabilitatea operatorului, operatorilor asociați, reprezentanților acestora și ai persoanelor împuternicite, evidența activităților de prelucrare, modalitățile de asigurare a securității datelor cu caracter personal, obligația operatorului de a evalua impactul asupra protecției datelor și consultarea prealabilă a autorității de supraveghere în cazul în care evaluarea a indicat anumite riscuri, funcția responsabilului cu protecția datelor în cadrul operatorului și sarcinile acestuia, elaborarea codurilor de conduită pentru aplicarea uniformă a Regulamentului, procedura de certificare a operatorilor de date cu caracter personal, transferurile de date cu caracter personal către țări terțe sau organizații internaționale, norme privind instituirea autorității de supraveghere, competența acestora și sarcinile fixate, modalitatea de cooperare între autoritățile de supraveghere, căile de atac, răspunderea și sancțiunile în cazul încălcării normelor privind prelucrarea datelor cu caracter personal.

Regulamentul 2016/679/UE introduce o serie de prevederi noi în raport cu Directiva 94/56/CE, după cum urmează:

- extinde aplicabilitatea normelor sale și asupra operatorilor sau persoanelor împuternicite de aceștia, care nu sunt stabiliți în UE, dar activitățile cărora vizează oferirea de bunuri sau servicii unor persoane vizate stabilite în UE;
- instituirea unor condiții mai stricte privind obținerea consimțământului de la persoana vizată, în speță oferirea acestuia într-o formă afirmativă, inclusiv sub formă de declarație scrisă, fiind stabilit și dreptul exprs al persoanei vizate de a-și retrage în orice moment consimțământul;
- fixarea dreptului persoanei vizate la ștergerea datelor ("dreptul de a fi uitat"), precum și a dreptului la portabilitatea datelor de la un operator la altul;
- introducerea principiilor de asigurare a protecției datelor începând cu momentul conceperii și în mod implicit ("by design" și "by default"). Aceasta constă în obligația operatorului de a pune în aplicare măsuri tehnice și organizatorice adecvate de prelucrare a datelor personale din momentul colectării acestora, cât și pe întreaga durată a prelucrării, asigurând utilizarea datelor colectate doar în scopurile pentru care persoana vizată și-a dat consimțământul;
- introducerea obligației operatorului de a efectua o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal;

- obligația operatorului de a notifica autoritatea de supraveghere în cazul încălcării securității datelor cu caracter personal și informarea persoanei vizate cu privire la această încălcare, fără întârzieri justificate și dacă este posibil în termen de cel mult 72 ore de la data luării la cunoștință de aceasta;

- noul rol al responsabilului cu protecția datelor din cadrul operatorului de date cu caracter personal, care efectuează operațiuni de prelucrare în cadrul unei autorități sau organism public și care prin natura lor, necesită o monitorizare periodică și sistematică sau datele prelucrate de aceștia fac parte din categorii speciale de date sau se referă la condamnări penale și infracțiuni;

- introducerea sistemului de certificare voluntară a operatorilor sau persoanelor împuternicite de aceștia în vederea demonstrării că operațiunile efectuate de aceștia respectă normele Regulamentului UE;

- introducerea unor sancțiuni mult mai dure, în special, amenzile administrative.

Implementarea Regulamentului 2016/679/UE reprezintă o prioritate în sensul art. 13 "Protecția datelor cu caracter personal" și Anexei I la Titlul III "Libertate, securitate și justiție" din Acordul de Asociere RM-UE.

Regulamentul 2016/679/UE nu a constituit obiect al transunerii în legislația națională a Republicii Moldova, prezentul proiect fiind exercițiul primar de transpunere a acestuia.

În ceea ce privește transpunerea sa, menționăm că proiectul național urmărește o transpunere fidelă și completă a reglementărilor UE privind protecția datelor cu caracter personal indicate la pct. I, fiind implementate corespunzător normele UE cu caracter terminologic, instituțional și material ale actului UE, inclusiv prevederile noi ale Regulamentului 2016/679/UE, care au fost evidențiate *supra*.

Astfel, proiectul național a transpus prevederile UE care se referă la: domeniul de acțiune al legii, în speță domeniile de prelucrare a datelor cu caracter personal reglementate și cele excluse (art. 2 din proiectul de Lege 133/2011); noțiunile aferente prelucrării datelor cu caracter personal (art. 3 din proiectul de Lege 133/2011); principiile aferente prelucrării datelor cu caracter personal (art. 4 din proiectul Legii 133/2011); normele referitoare la legalitatea prelucrării (art. 5 din proiectul Legii 133/2011); instituirea autorității de supraveghere a respectării dreptului la protecția datelor personale – Centrul Național pentru Protecția Datelor cu Caracter Personal (art. 6 din proiectul Legii 13/2011); condițiile privind consimțământul (art. 8 din proiectul Legii 133/2011); prelucrarea categoriei speciale de date personale (art. 9 din proiectul Legii 133/2011); stocarea și utilizarea datelor personale (art. 13 din proiectul Legii 133/2011); drepturile subiecților de date personale (art. 17 – 28 din proiectul Legii 133/2011); operatorul și persoana împuternicită de acesta (art. 29 – 36 din proiectul Legii 133/2011); norme cu referire la securitatea prelucrării (art. 37 – 49 din proiectul Legii 133/2011); modalitatea de transmitere transfrontalieră a datelor personale (art. 50 – 57 din proiectul Legii 133/2011); procedura de depunere a cererilor, examinarea și efectuarea investigațiilor, luarea deciziilor (art. 78 – 88 din proiectul Legii 133/2011); răspunderea și sancțiunile (art. 89 – 94 din proiectul Legii 133/2011), prelucrarea unor date personale specifice (art. 95 – 97 din proiectul Legii 133/2011).

Totodată, ținem să menționăm că, deși actul UE supus transunerii este un Regulament, care are aplicabilitate directă în toate statele membre UE, acesta a implicat, pentru o aplicare uniformă, elaborarea și adoptarea până la 25 mai 2018 a unor ghiduri destinate aplicării unitare a Regulamentului 2016/679/UE. Astfel, la moment, au fost adoptate 7 ghiduri finale, după cum urmează: Ghidul privind dreptul la portabilitatea datelor, raportat la art. 20 din Regulamentul 2016/679/UE, Ghidul privind responsabilul pentru protecția datelor (DPO), raportat la art. 37-39 din Regulamentul 2016/679/UE, Ghidul privind identificarea autorității de supraveghere lider a unui operator sau împuternicit, Ghidul privind notificarea încălcărilor de securitate, Ghidul privind

deciziile automate individuale și profilare, Ghidul privind consimțământul și Ghidul privind transparența în temeiul Regulamentului 2016/679/UE.

Observații privind compatibilitatea cu Regulamentul 2016/679/UE

Cu referire la art. 35 din proiectul național, în ceea ce privește evidența activităților de prelucrare și care a transpus art. 30 din Regulamentul 2016/679/UE, constatăm că alin. (5) din proiectul național exceptează de la regula ținerii evidenței de operator instituțiile de drept public sau privat cu mai puțin de 50 de angajați, or art. 30 (5) din actul UE atribuie excepția unei întreprinderi sau organizații cu mai puțin de 250 de angajați.

Observații de tehnică legislativă

Cu referire la art. 35, alin. (2) din proiectul național, care stabilește ținerea evidenței activităților de prelucrare, sintagma "fiecare operator și, după caz, persoana împuternicită de operator" se va substitui cu sintagma "fiecare persoană împuternicită de operator și, după caz, reprezentantul persoanei împuternicite" similar Rectificărilor la Regulamentul (UE) 2016/679, publicate în Jurnalul Oficial al UE nr. L 127/2 din 23 mai 2018.

Directiva 2016/680/UE are drept scop stabilirea unor norme specifice privind protecția datelor cu caracter personal și libera circulație a acestora în domeniul cooperării judiciare în materie penală și al cooperării polițienești. Astfel, actul UE stabilește norme speciale referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora.

Directiva

Directiva 2016/680/UE stabilește norme armonizate care se referă la:

- categoriile de date cu caracter personal care cad sub incidența sa;
- definițiile relevante domeniului;
- principiile referitoare la prelucrarea datelor cu caracter personal;
- drepturile persoanei vizate de prelucrarea unor date cu caracter personal;
- operatorul și persoane împuternicite de operator;
- securitatea datelor cu caracter personal;
- responsabilul cu protecția datelor;
- transferurile de date cu caracter personal către țări terțe sau organizații internaționale;
- norme-cadru privind autoritatea de supraveghere;
- căi de atac, răspundere și sancțiuni.

Totodată, *Directiva 2016/680/UE* nu împiedică statele membre să stabilească garanții mai mari în ceea ce privește prelucrarea datelor cu caracter personal decât cele fixate de ea pentru protecția drepturilor și libertăților persoanelor vizate.

Directiva 2016/680/UE abrogă și substituie Decizia-cadru 2008/977/JAI a Consiliului (care nu a constituit obiect al transunerii în legislația națională) și vine cu elemente novatorii similare cu cele ale Regulamentului 2016/679/UE, în speță, referitoare la procesul decizional automatizat (art. 11); dreptul la rectificarea și ștergerea datelor cu caracter personal (art. 16); desemnarea persoanei împuternicite de operator (art. 22); introducerea procedurii de evaluare a impactului asupra protecției datelor (art. 27); responsabilul cu protecția datelor (art. 32 – 34), etc.

Implementarea Directivei 2016/679/UE reprezintă o prioritate în sensul art. 13 "Protecția datelor cu caracter personal" și Anexei I la Titlul III "Libertate, securitate și justiție" din Acordul de Asociere RM-UE.

Directiva 2016/680/UE nu a constituit obiect al transunerii în legislația națională, prezentul proiect fiind exercițiul primar de transpunere a acesteia.

În ceea ce privește transpunerea sa, proiectul național asigură o transpunere corespunzătoare a Directivei 2016/680/UE. Astfel, proiectul național implementează normele care se referă la: domeniul de aplicare – prelucrarea de date cu caracter personal de către organele de ocrotire a legii (art. 2, alin. (2), lit. d) din proiectul Legii 133/2011); noțiunile specifice domeniului (art. 3 din proiectul Legii 133/2011); principiile prelucrării datelor cu caracter personal (art. 4 din proiectul Legii 133/2011); noime-cadru referitoare la autoritatea de supraveghere – Centrul (art. 6 din proiectul Legii 133/2011); termene pentru stocare și revizuire (art. 60 din proiectul Legii 133/2011); distincția dintre categorii diferite de subiecți de date (art. 61 din proiectul Legii 133/2011); distincția dintre datele personale în baza faptelor și datele personale în baza evaluării (art. 62 din proiectul Legii 133/2011); legalitatea prelucrării (art. 59 din proiectul Legii 133/2011); prelucrarea categoriilor speciale de date (art. 63 din proiectul Legii 133/2011); procesul individual automatizat inclusiv crearea de profiluri (art. 64 din proiectul Legii 133/2011); informații ce trebuie puse la dispoziția subiectului de date (art. 66 din proiectul Legii 133/2011); dreptul de acces al subiectului de date (art. 67 din proiectul Legii 133/2011); limitare dreptului de acces (art. 68 din proiectul Legii 133/2011); dreptul la rectificare sau la ștergerea datelor (art. 69 din proiectul Legii 133/2011); drepturile persoanei în cadrul investigațiilor și procedurilor penale (art. 66-68 din proiectul Legii 133/2011); operatorul și persoana împuternicită de acesta (art. 29 – 34 din proiectul Legii 133/2011); evidențele activității de prelucrare (art. 35 din proiectul Legii 133/2011); generarea înregistrărilor de audit (art. 72 din proiectul Legii 133/2011); obligația organului de ocrotire a legii în raport cu Centrul (art. 73 din proiectul Legii 133/2011); evaluarea impactului asupra protecției datelor (art. 41 din proiectul Legii 133/2011); securitatea datelor (art. 37 din proiectul Legii 133/2011); notificarea încălcării securității datelor personale către Centrul (art. 70 din proiectul Legii 133/2011); comunicarea încălcării securității datelor personale către subiectul de date de către organul de ocrotire (art. 71 din proiectul Legii 133/2011); responsabilul de protecția datelor (art. 43 – 45 din proiectul Legii 133/2011); transferul transfrontalier de date personale între organele de ocrotire (art. 75 din proiectul Legii 133/2011); derogări de la regula transferului în situații specifice (art. 76 din proiectul Legii 133/2011); procedura de depunere a cererilor, examinarea și efectuarea investigațiilor, luarea deciziilor (art. 78 – 88 din proiectul Legii 133/2011); răspunderea și sancțiunile (art. 89 – 94 din proiectul Legii 133/2011).

Observații privind compatibilitatea cu Directiva 2016/680/UE

Cu referire la art. 74, alin. (5) din proiectul național, care stabilește obligația operatorului de a informa subiectul de date cu caracter personal despre limitarea dreptului său de acces și care a transpus art. 15 (3) din *Directiva 2016/680/UE*, constatăm că proiectul național indică că informarea subiectului se va realiza după încetarea situației care justifică limitarea dreptului de acces, or norma UE indică informarea în scris "fără întârzieri justificate", cu posibilitatea omiterii unei astfel de informări când acest lucru ar "contraveni unuia dintre scopurile" ce justifică limitarea. În acest context, prevederea națională referitoare la momentul informării pare a fi distinctă de cea UE.

Observații de tehnică legislativă

Ținând seama de lipsa pentru Republica Moldova a calității de stat membru al UE, la art. 67, alin. (1) din proiectul național, referitor la dreptul de acces al subiectului de date cu caracter personal, la lit. c) sintagma "țări terțe" se va substitui cu cea de "alte state", iar la art. 77, alin. (2), din proiectul național referitor la definirea unui acord internațional în domeniul cooperării judiciare în materie penală și cooperării polițienești, sintagma "între statele membre și țările terțe" se va substitui cu sintagma "între Republica Moldova și alte state".

Observații privind formularea clauzei de armonizare

În vederea uniformizării clauzelor de armonizare și reflectării corecte a actelor UE transpuse și gradului lor de transpunere, potrivit exigențelor art. 31. alin. (2) din Legea nr. 100 din 22 decembrie 2016 privind actele normative și Hotărârii Guvernului nr. 1345 din 24 noiembrie 2006, **clauza de armonizare a Legii 133/2011 (redacție nouă) se va expune după partea introductivă a acesteia în următoarea redacție:** "Prezenta Lege transpune Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (Text cu relevanță pentru SEE) și 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 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, publicate în Jurnalul Oficial al UE nr. L 119 din 4 mai 2016".

Observații privind întocmirea Tabelului de concordanță

Tabelul de concordanță, care însoțește proiectul de act normativ, urmează a fi supus unor modificări pentru a corespunde cerințelor stabilite de Regulamentul privind mecanismul de armonizare a legislației Republicii Moldova și Ghidul cu privire la întocmirea Tabelelor de concordanță (Anexa I la Metodologia de Armonizare a Legislației în Republica Moldova, care poate fi accesată pe pagina electronică a Centrului de Armonizare a Legislației).

Întocmirea riguroasă a Tabelului de concordanță, precum și actualizarea acestuia potrivit concluziilor expertizei de compatibilitate este necesară pentru reflectarea exactă a realizării obligațiilor de armonizare în cadrul exercitiului de evaluare din partea UE la gradul de convergență a legislației naționale cu actele europene transpuse.

III. Concluzii

Având în vedere cele menționate, apreciem că în urma evaluării realizate, proiectul național și-a atins finalitatea propusă, asigurând transpunerea corespunzătoare a prevederilor Regulamentului 2016/679/UE și Directivei 2016/680/UE.

Facem mențiunea că analiza Centrului de Armonizare a Legislației nu are în vedere elementele de oportunitate ale soluțiilor juridice incluse în proiectul de act normativ, ci se referă strict la conformitatea acestora cu Dreptul UE aplicabil și obligațiile juridice asumate în lumina Acordului de Asociere RM – UE.


Natalia SUCEVEANU

Director

TABELUL
divergențelor rezultate din avizele prezentate de autoritățile abilitate referitor la
proiectul de lege pentru modificarea și completarea unor acte legislative

Nr. d/o	Denumirea instituției	Norma juridică la care sînt obiecții sau propuneri	Obiecția/propunerea formulată	Acceptare/argumentare neacceptări
I.	Centrul Național Anticorupție	art.2 alin.(2) lit.a)	1. Norma propusă: „<u>prelucrarea datelor cu caracter personal efectuate pe teritoriul Republicii Moldova, inclusiv informațiilor care consemnează date cu caracter personal atribuite la secret de stat, secret profesional, secret bancar, secret medical, secret comercial, secret fiscal și altor informații cu accesibilitate limitată sau operațiunilor administrative desfășurate în legătură cu gestionarea dosarului civil, contravențional sau penal, precum și mijloacelor utilizate în acest sens</u>” - art.2 alin.(2) lit.a) din proiect, contravine cadrului național în materie procesual penală. Astfel, atât Codul de procedură penală, cât și Legea nr.59/2012 privind activitatea specială de investigații stabilesc expres categoriile de subiecți care pot avea acces la materialele/informațiile în cadrul desfășurării activităților de investigare (inclusiv la materialele din dosarele penal). Astfel, art.212 din Codul procesual penal prevede expres: „<u>Confidențialitatea urmăririi penale. (1) Materialele urmăririi penale nu pot fi date publicității decât cu autorizația persoanei care efectuează urmărirea penală și numai în măsura în care ea consideră că aceasta este posibil, cu respectarea prezumției de nevinovăție, și ca să nu fie afectate interesele altor persoane și ale desfășurării urmăririi penale în condițiile Legii nr.133 din 8 iulie 2011 privind protecția datelor cu</u>	Din start, ținem să menționăm că la elaborarea avizului, Centrului Național Anticorupție (CNA) nu a luat în calcul la formularea obiecțiilor și propunerilor dispozițiile 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 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. Reiterăm că Directiva (UE) 2016/680 statuează sarcini, atribuții și garanții de care trebuie să dispună autoritatea națională de supraveghere a prelucrării datelor cu caracter personal, și anume: - Fiecare stat garantează că autoritatea sa de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor și exercitarea competențelor care le revin în conformitate cu prezenta directivă (art. 42 alin. (1)). - Statele garantează că membrii autorităților lor de supraveghere, în îndeplinirea sarcinilor și în exercitarea competențelor care le revin în conformitate cu prezenta directivă, rămân

			<i>caracter personal.”. La fel, Codul de procedură penală reglementează - „Apărarea secretului de stat în procesul penal”(a se vedea art.213 din Cod).</i> De asemenea, Legea nr.59/2012, obligă subiecții implicați în activitatea specială de investigații să respecte protecția datelor cu caracter personal în cadrul activității - art.5 „(1) <u>Persoanele care au acces la datele cu caracter personal ale persoanei supuse măsurii speciale de investigații sunt obligate să păstreze confidențialitatea datelor respective în conformitate cu prevederile Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal.</u> (2) <u>Accesul la dosarul special sau la materialele din dosar al altor persoane decât cele care investighează dosarul special este interzis, cu excepția conducătorului subdiviziunii specializate a organului respectiv, în limitele competenței, și a procurorului care a autorizat măsura specială de investigații sau a solicitat autorizarea acesteia de către judecătorul de instrucție, precum și cu excepția judecătorului de instrucție care a autorizat măsura specială de investigații.”.</u> Prin urmare, prevederile propuse la art. 2 depășește cadrul legal în vigoare și vin să compromită asigurarea realizării sarcinilor activității speciale de investigații. Astfel, la art.2 alin.(2) lit.a) optăm pentru substituirea sintagmei „inclusiv informațiilor care consemnează date cu caracter personal atribuite la secret de stat, secret profesional, secret bancar, secret medical, secret comercial, secret fiscal și altor informații cu accesibilitate limitată sau operațiunilor administrative desfășurate în legătură cu gestionarea dosarului civil, contravențional sau penal, precum și mijloacelor utilizate în acest sens;” cu sintagma „în limitele legislației în vigoare”.	independenți de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la nimeni (art. 42 alin. (2)). - Fiecare stat garantează prin lege că autorității sale de supraveghere îi revin competențe de consiliere efective pentru a oferi consiliere operatorului și de a emite avize, din proprie inițiativă sau la cerere, parlamentului național, guvernului sau, în conformitate cu dreptul său intern, altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal. - Fiecare stat membru garantează prin lege că autorității sale de supraveghere îi revin competențe de investigare efective. Respectivele competențe includ, cel puțin, competența de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal care sunt prelucrate și la toate informațiile necesare pentru îndeplinirea sarcinilor sale.(Art. 47) Mai mult, remarcăm art. 58 din noul Regulament 2016/679, care prevede competențele de investigație a autorităților de supraveghere a protecției datelor cu caracter personal prevede, inclusiv următoarele: a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale; e) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu
--	--	--	--	--

				<i>caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale;</i> <i>f) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern.</i> Un alt element important care determină competențele Centrului de a efectua operațiuni de investigație a prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, al punerii în aplicare a sentințelor de condamnare sau al altor acțiuni ce țin de procedura penală ori contravențională, în condițiile legii, îl reprezintă Ghidul practic privind utilizarea datelor cu caracter personal în sectorul polițienesc, adoptat de către Comitetul Consultativ al Convenției 108 (Consiliul Europei) pentru protecția persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal, adoptat la data de 15 februarie 2018 la Strasbourg, care urmează a fi implementat inclusiv de către CNA. Fiind remis spre implimentare pe data de 28 noiembrie 2017. Suplimentar, a se vedea Legea nr. 271 din 07 noiembrie 2013 privind formularea unor declarații ale Republicii Moldova la Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal. Astfel. Potrivit art. 1 lit. b) din actul precitat Republica Moldova nu va aplica prevederile convenției prelucrărilor de date cu caracter personal atribuite la secret de stat în modul stabilit, cu excepția celor efectuate în cadrul acțiunilor de prevenire și investigare a infracțiunilor, al punerii în executare a sentințelor de condamnare sau al altor
--	--	--	--	---

				acțiuni ce țin de procedura penală ori contravențională, în condițiile legii. La fel, potrivit art. 2 alin. (4) lit. b) al Legii privind protecția datelor cu caracter personal nr. 133 din 08 iulie 2011 domeniul de acțiune al legii se extinde inclusiv asupra prelucrării datelor cu caracter personal atribuite la secret de stat în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale în condițiile legii. Având în vedere cele menționate supra, obiecțiile formulate de CNA în partea ce vizează art.2 alin.(2) lit.a) că ar depăși cadrul legal în vigoare și ar compromite asigurarea realizării sarcinilor activității speciale de investigație, nu pot fi reținute. Un șir de organe de stat în scopul tainuirii sau limitării accesului la informații aplică secretizarea excesivă inclusiv asupra informațiilor ce țin de protecția datelor cu caracter personal – dreptul la viața privată, viața intimă a persoanei etc. Potrivit art. 8 alin. (1) al Legii cu privire la secretul de stat nu se atribuie la secret de stat și nu pot fi secretizate informațiile privind faptele de încălcare a drepturilor și libertăților omului și ale cetățeanului; faptele de încălcare a legii de către autoritățile publice și persoanele cu funcții de răspundere din cadrul acestora. În acest sens, în cazul în care a fost stabilită o încălcare a principiilor de protecție a datelor cu caracter personal Centrul trebuie să dispună de pîrghiile necesare pentru ca persoana să cunoască despre încălcarea dreptului său.
--	--	--	--	---

				Mai mult, Centrul nu este absolvit de obligația respectării normelor procesual penale și contravenționale de ridicare a obiectelor și documentelor ce conțin informații care constituie secret de stat, comercial, bancar. Nu în ultimul rând, toate dispozițiile invocate de CNA în partea ce vizează respectarea normelor de conformitate privind prelucrarea datelor cu caracter personal expuse în Legea privind protecția datelor cu caracter personal, sunt în contradicție cu argumentele expuse, or acestea denotă faptul respectării și aplicării Legii privind protecția datelor cu caracter personal, inclusiv în activitatea specială de investigație, iar supravegherea respectării conformității prelucrării datelor cu caracter personal în acest sector este pusă în temeiul legii, în sarcina Centrului național pentru Protecția Datelor cu Caracter Personal.
		art. 2 alin.(2) lit.c)	2. Cu referire la art.2 alin.(2) lit.c) din proiect, nu este clar identificat la care categorii de date cu caracter personal face referire autorul. Considerăm necesar revizuirea acestor norme în vedere stabilirii clare a domeniului de date personale ce urmează a fi prelucrate.	Nu se acceptă În cazul dat, precum și în tot textul proiectului este utilizat conceptul de „<i>date cu caracter personal</i>” care este definit la art. 3 „noțiuni principale” reprezentînd orice informație ce identifică sau duce la identificarea subiectului de date cu caracter personal. Astfel, autorul proiectului este în imposibilitate să identifice/enumere exhaustiv în acest caz și/sau în tot textul proiectului categoriile concrete de date cu caracter personal, or, avînd în vedere noțiunea expusă supra orice informație descrisă în condițiile menționate supra poate fi catalogată ca fiind date cu caracter personal.

		art.2 lit.d) alin.(2)	3. Cu referire la art.2 alin.(2) lit.d) care stabilește un alt domeniu de acțiune al proiectului și anume: <u>„prelucrarea datelor cu caracter personal de către operatori - organe de ocrotire a legii, care au competențe stabilite prin lege în scopul prevenirii, investigării, depistării și/sau urmăririi penale a infracțiunilor sau executării pedepselor penale, detenția preventivă, inclusiv protejarea și prevenirea amenințărilor la adresa ordinii publice, securității de stat și securității naționale și în cadrul dosarului sau acțiunilor speciale de investigație.”</u>, statuăm că și în cazul dat, normele propuse sunt abuzive în raport cu activitatea specială de investigații și a statutului ofițerului de urmărire penală/procurorului și ale altor organe de drept. La acest capitol, menționăm că art.3 alin.(1) din Legea nr.333 din 10.11.2006 privind statutul ofițerului de urmărire penală, prevede expres <u>„în exercitarea atribuțiilor, ofițerul de urmărire penală este independent, se supune numai legii, indicațiilor scrise ale conducătorului organului de urmărire penală, ale procurorului și hotărârilor instanței de judecată, emise în limitele competenței lor și în conformitate cu legislația în vigoare.”</u>. Orice imixtiune în activitatea ofițerului de urmărire penală este interzisă și acesta se supune doar prevederilor Cod de procedură penală și indicațiilor scrise ale procurorului și ale conducătorului organului de urmărire penală (a se analiza art.57 alin.(4) din Codul de procedură penală). Art.6 alin.(3) din Legea nr.59 din 29.03.2012 privind activitatea specială de investigații, la fel, garantează independența ofițerului de investigații <u>„Ofițerul de investigații care efectuează activitatea specială de investigații își realizează sarcinile în mod independent, cu excepția cazului când acțiunea specială de investigații</u>	Nu se acceptă Prin reglementarea în cauză, inclusiv dispozițiile cap. VII s-a trasat <u>scopul de a asigura implementarea Directivei nr. 2016/680 a Parlamentului European și 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 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, document juridic internațional prin care Uniunea Europeană a delegat dreptul de investigare a prelucrării datelor cu caracter personal efectuate în cadrul urmăririi penale, autorităților naționale de supraveghere a prelucrării datelor cu caracter personal – fapt, trecut cu vederea de către CNA. Menționăm că Centrul nu efectuează verificarea activității de urmărire penală sau a activității speciale de investigații, dar se limitează la investigarea conformității prelucrării datelor cu caracter personal.</u> Reiterăm că, clauza legală ce reglementează prelucrarea datelor cu caracter personal în sectorul polițienesc a fost instituită deja și este prevăzută la moment la art. 2 alin. (2) lit. d) Legea nr. 133. În formularea actuală domeniul de acțiune al acestei legi se extinde asupra prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale în condițiile legii.
--	--	---	--	---

		<i>este dispusă și coordonată sau este condusă în cadrul procesului penal de către procuror sau de către ofițerul de urmărire penală, în interacțiune sau în colaborare cu colaboratorii confidențiali</i>". Astfel, domeniul de reglementare propus depășește limitele legale statuate în legislația procesual penală. De asemenea, putem menționa că legalitatea desfășurării măsurilor speciale de investigații în corelație cu încălcarea respectării drepturilor omului și a libertăților fundamentale este verificată de către instanța de judecată și procuror, care autorizează sau anulează măsurile efectuate. Astfel, normele de la art.2 alin.(2) lit.d) vin să compromită asigurarea realizării sarcinilor activității speciale de investigații, reprezentând în esență, o imixtiune în activitatea acestora, precum și în activitatea ofițerilor de urmărire penală și a procurorilor. <u>Considerăm absolut necesar excluderea art.2 alin.(2) lit.d) din textul proiectului, precum și a oricăror prevederi ce vin să aducă restricții și ingerințe în activitatea specială de investigații.</u> Totodată, în aceeași ordine de idei, considerăm oportun completarea art.2 alin.(3) cu o literă nouă care să prevadă „d) prelucrării datelor cu caracter personal de către organele de drept, care au competențe stabilite prin lege, în scopul prevenirii, investigării, depistării și/sau urmăririi penale a infracțiunilor sau executării pedepselor penale, detenția preventivă, inclusiv protejarea și prevenirea amenințărilor la adresa ordinii publice, securității de stat și securității naționale și în cadrul dosarului sau acțiunilor speciale de investigație”.	În acest context, este de menționat că la 28 aprilie 2016 a fost adoptată Legea nr. 87 (publicată în Monitorul Oficial nr. 156/306 din 07.06.2016) prin care au fost operate modificări/completări la un șir de legi, fiind înserate dispoziții legale ce vizează prelucrarea datelor cu caracter personal în sectorul polițienesc, după cum urmează: 1.Cod de procedură penală. Art. 15 alin. (2) stipulează că la efectuarea acțiunilor procesuale nu poate fi acumulată fără necesitate informație despre viața privată și intimă a persoanei. La cererea organului de urmărire penală și a instanței de judecată, participanții la acțiunile procesuale sînt obligați să nu divulge asemenea informații și despre aceasta se ia un angajament în scris. <u>Prelucrarea datelor cu caracter personal în cadrul procesului penal se efectuează în conformitate cu prevederile Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal.</u> 2. Legea nr. 59 din 29.03.2012 cu privire la activitatea specială de investigație. Art. 5 alin. (1), persoanele care au acces la datele cu caracter personal ale persoanei supuse măsurii speciale de investigații sînt obligate să păstreze confidențialitatea datelor respective în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. 3. Legea nr. 320 din 27.12.2012 cu privire la Poliție și statutul polițistului Art. 16 alin. (3), prelucrarea, transmiterea și distrugerea datelor cu caracter personal deținute de Poliție se efectuează în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal.
--	--	--	--

				4. Legea nr. 1104 din 06.06.2002 cu privire la Centrul Național Anticorupție Articolul 6 lit. m), să prelucreze date cu caracter personal, inclusiv în scop de analiză informațională și strategică, în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. Avînd în vedere specificul legislației Republicii Moldova, în special, codificarea normelor de procedură penală și rigiditatea activității speciale de investigații, este necesară intervenția pentru a asigura o sincronizare în materie de protecție a datelor cu caracter personal. În același context, se notează că Parlamentul Republicii Moldova prin Legea comunicațiilor electronice, nr. 241-XVI din 15 noiembrie 2007, republicată în Monitorul Oficial din 17 noiembrie 2017, a atribuit Centrului în temeiul art. 71 noi competențe de a verifica măsurile tehnice și organizatorice corespunzătoare în vederea protejării securității serviciilor prestate de furnizorii de servicii de comunicații electronice. Subsecvent, concomitent cu intrarea în vigoare la data de 23 februarie 2018 a Legii cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului în partea ce vizează controlul conformității operațiunilor de prelucrare a datelor cu caracter personal efectuate de autoritățile specializate în prevenirea și combaterea terorismului, inclusiv a Serviciului Prevenirea și Combaterea Spălării Banilor. Este necesar a remarca că acțiunile ce urmează a fi întreprinse de entitățile vizate în prezenta lege presupun prelucrarea unui volum exorbitant de date cu caracter personal și se răsfrînge asupra tuturor persoanelor
--	--	--	--	--

				fizice, chiar și care au avut o tangență mică cu instituțiile financiar-bancare, dar nu numai. O altă lege care a adus atribuții noi Centrului este Legea nr. 120 din 21 septembrie 2017 cu privire la prevenirea și combaterea terorismului. Activitatea de prevenire și combatere a terorismului va fi exercitată în mod special de Serviciul de Informații și Securitate care prelucrează un volum extrem de mare de date personale, iar controlul conformității prelucrărilor de date cu caracter personal se efectuează de către Centru. <i>Prin spectrul de modificări legislative arătat supra, Centrul a dobândit competență de a investiga prelucrarea datelor cu caracter personal atribuite inclusiv la secret de stat etc. Astfel, Capitolul VII din prezentul proiect de lege, este destinat prelucrării datelor cu caracter personal de către operatori - organe de ocrotire a legii, care au competențe stabilite prin lege în scopul prevenirii, investigării, depistării și/sau urmăririi penale a infracțiunilor sau executării pedepselor penale, inclusiv protejarea și prevenirea amenințărilor la adresa ordinii publice, securității de stat și securității naționale și în cadrul dosarului sau acțiunilor speciale de investigație.</i> <i>Un alt element important care a contribuit la cristalizarea competențelor Centrului de a efectua operațiuni de investigație a prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, al punerii în aplicare a sentințelor de condamnare sau al altor acțiuni ce țin de procedura penală ori contravențională, în condițiile legii, îl reprezintă Ghidul practic privind utilizarea datelor cu caracter personal în sectorul polițienesc, adoptat de către Comitetul Consultativ al Convenției 108 pentru protecția persoanelor cu privire la prelucrarea automatizată a datelor cu</i>
--	--	--	--	---

				<i>caracter personal, adoptat la data de 15 februarie 2018 la Strasbourg.</i>
		art.4 alin.(2)	4. La art.4 alin.(2) din proiect <u>„Operatorul este responsabil de asigurarea conformării cu alin.(1) și poate demonstra această respectare („responsabilitate”).</u> <u>Datele personale urmează a fi prelucrate sub răspunderea operatorului, care asigură și demonstrează conformitatea fiecărei operațiuni de prelucrare cu dispozițiile prezentei legi</u>”. Consideră că norma dată este expusă într-o formă abuzivă, iar la aplicare ea va crea circumstanțe obscure/neclare pentru operatori, ceea ce reprezintă un risc de corupție. Este practic imposibil, să respecti careva cerințe dacă acestea nu sunt clar identificate/expuse pentru subiecții ce urmează a le respecta. Reglementarea oferă doar careva repere generale, precum - Datele urmează a fi: <u>„adequate, relevante”, „prelucrate într-un mod care asigură securitatea adecvată a datelor personale”, „păstrate într-o formă care permite identificarea subiectului datelor pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele”</u> etc., însă cerințele vis-a-vis de acestea sunt stabilite clar cu obligarea operatorilor de a le „demonstra”, ceea ce reprezintă o cerințe excesivă pentru operatorii din Republica Moldova.	Nu se acceptă Art. 4 alin. (1) din proiect statuează operatorilor de date ansamblul principiilor – reguli, care urmează a fi respectate la prelucrarea datelor cu caracter personal. Mai mult, atragem asupra titlului art. 4 intitulat <u>„Principiile aferente prelucrării datelor personale”</u>, or însăși dacă să pornim de la esența noțiunii de principiu acesta reprezintă un element fundamental, idee de bază pe care se întemeiază o teorie, un sistem politic etc. Prin urmare, esența art. 4 este redată sub forma unor reguli de bază și fundamentale, necesar a fi implementate și asigurate de către fiecare operator în parte. Detalierea fiecărui principiu în parte este expusă în următoarele articole din proiect. Ca de exemplu articolul 11 Minimizarea datelor prelucrate în scopul identificării subiectului de date, prevede reguli concrete în partea ce vizează respectarea acestui principiu. Deci, fiecare operator trebuie să demonstreze conformitatea fiecărei operațiuni de prelucrare cu dispozițiile prezentei legi sub răspundere proprie. Suplimentar, menționăm că stabilirea unor cerințe imperative și rectilinii pentru reglementarea exhaustivă a operațiunilor de prelucrare a datelor cu caracter personal este utopică, deoarece, prelucrarea datelor cu caracter personal este inherentă în majoritatea covârșitoare a activităților sociale, economice, culturale etc. textul legii însă nu poate cuprinde

				întreaga gamă de scenarii în care pot fi prelucrate date cu caracter personal. Astfel de machetare juridică este utilizată și în legile expuse supra, inclusiv în actele juridice europene - Regulamentul (UE) 2016/679 și art. 4 din Directiva (UE) 2016/680, care reglementează domeniul, inclusiv, în cele 28 țări membre ale UE. Mai mult, în ipoteza în care reglementarea <i>ad literam</i> în defavoarea principiilor ar fi posibilă, o astfel de conturarea juridică ar putea reprezenta cu adevărat o imixtiune în activitatea operatorilor, fie în domeniul polițienesc, bancar, medical, educațional sau altele.
		Art. 6 în corelare cu art. 81	5. Cu referire la art.6 în corelare cu art.81 din proiect - Autoritatea de supraveghere. Menționează repetat, despre necesitatea revizuirii competențelor Centrului Național pentru Protecția Datelor cu Caracter Personal care se prezintă excesive în raport cu domeniul de reglementare, precum și cu activitatea altor entități publice. Riscul acordării unui spectru larg de competențe, fără careva limite/restricții legale, începând cu: - „<u>reglementarea</u>” domeniul, - „<u>investigarea asupra respectării principiilor de protecție a datelor personale prevăzute de legislația în vigoare</u>”, în speță „<u>Centrul poate dispune prin decizie. [...] ieșirea la fața locului.</u>”, - „<u>decizia privind efectuarea investigației la fața locului se aduce la cunoștință sub semnătură persoanei, entității supuse investigației, sau reprezentantului legal. În cazul refuzului primirii și semnării deciziei se întocmește un act, în prezența unui martor sau în cazul înregistrării video și audio, în care se consemnează acest fapt</u>”, - „<u>să dispună de acces și să examineze sistemele de evidență a datelor personale, soluțiile software și</u>	Nu se acceptă Reiterăm argumentele expuse în pct. 1 și 2 din tabel. Suplimentar, este de menționat că practica internațională oferă autorităților de protecție a datelor cu caracter personal, dreptul de a avea acces la orice tip de informații, indiferent de gradul de securizare și clauza de confidențialitate, fie secret de stat, confidențialitatea urmăririi penale sau contravenționale, și de a verifica dacă prin aceste metode de colectare și utilizare a datelor, nu se încalcă drepturile omului, în special în partea ce vizează inviolabilitatea vieții intime, familiale și private. Constatăm, că practica dată este aplicată pe deplin de statele UE și nu aduce nici o ingerință în activitatea organelor de drept, ba mai mult ca atât autoritatea de supraveghere este un echilibru dintre activitățile acestor organe și drepturile omului în partea ce ține de conformitatea prelucrării datelor cu caracter personal, îmbunătățind activitate organelor de drept, astfel nu

		<u>suporturile hardware, datele personale și orice documente legate de obiectul și scopul investigației”,</u> - „<u>să intre liber în încăperi, pe terenuri sau în mijloace de transport aflate în proprietatea sau folosința subiecților de drept</u>” - „<u>să ridice, să colecteze, să obțină mijloace, copii sau extrase, sub orice formă, din sistemele de evidență și documentele care conțin date personale</u>” etc. (a se vedea norma de la art.81 din proiect), va face posibilă apariției abuzurilor din partea autorității de supraveghere - CNPDCP. Stipulează că normele propuse nu oferă și un mecanism de control/supraveghere asupra activității acestei structuri, ceea ce sporește riscul abuzurilor. Acțiunile propuse sunt identice cu cele ale organelor responsabile prin lege de desfășurarea activităților speciale de investigații, însă fără a se garanta un mecanism de coordonare și control asupra legalității acestor măsuri cu caracter procesual penal. Sub aspect comparativ, competențele acordate subiecților citați la art.6 din Legea nr.59/2012 privind activitatea specială de investigații (Ministerul Afacerilor Interne, Ministerul Apărării, Centrul Național Anticorupție, Serviciul de Informații și Securitate, Serviciul de Protecție și Pază de Stat, Serviciul Vamal și Administrația Națională a Penitenciarelor) sunt reglementate într-un mod strict, fiecare acțiune fiind autorizată și supusă unui control riguros din partea mai multor entități publice. Astfel, Codul de procedură penală la art.300 reglementează sfera de control asupra activității speciale de investigații, efectuate de judecătorul de instrucție, nemaivorbind despre alte posibilități legale oferite cetățeanului de a-și apăra drepturile și interesele personale. Totodată, Legea nr.59/2019 reglementează într-un capitol separat mecanismul de control și coordonare a activității speciale de investigații. Astfel,	este clară reticența și nedorința de modernizare a CNA și expunerea că sunt premize de elemente coruptibile. Menționăm că toate acțiunile Centrului sunt supuse controlului judecătoresc. Mai mult, toate aceste competente sunt specifice tuturor autorităților de supraveghere a prelucrării datelor cu caracter personal, fiind conferite în temeiul Convenției nr. 108 din 28 ianuarie 1981 pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Protocolului adițional la Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și 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 urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date. Astfel, în acest context art. 58 din Regulamentul (UE) 2016/679 statuează expres aceste competențe de investigare fiecare autoritate de supraveghere. În special, autoritatea de supraveghere are dreptul de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale, de a obține accesul la oricare dintre incintele operatorului și ale persoanei
--	--	---	--

			controlul asupra subiecților activității speciale de investigații este efectuat de instanțele de judecată, procuror, la fel, este supus unui control departamental și Parlamentar. Prin urmare, consideră că supravegherea activității organelor de investigație sunt suficient de mult în prezent, pentru a mai permite alte controale și supravegheri. Totodată, fără garanții legale (inclusiv procesuale) ce ar asigura monitorizarea, echitatea și imparțialitatea competențelor „autorității de supraveghere” reglementate în proiect, apreciem aceste competențe ca fiind abuzive și inacceptabile.	împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor (art. 58 alin. (1) lit. e) și lit. f)). La fel, nu pot fi reținute argumentele în partea ce vizează lipsa garanțiilor legale (inclusiv procesuale) ce ar asigura monitorizarea, echitatea și imparțialitatea competențelor „autorității de supraveghere”. Or, CNA pune la îndoială corectitudinea și conformitatea activității/statului Centrului conferit deja prin lege. În mare parte competențele date sunt expuse și astăzi, doar că într-o manieră în care se permite interpretare acestora, creînd deseori confuzii și imixiune în activitatea Centrului. Reiterăm că, la moment potrivit art. 2 alin. (2) lit. d), domeniul de acțiune al Legii privind protecția datelor cu caracter personal se extinde inclusiv asupra prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale în condițiile legii, fapt ce implică și dreptul Centrului de efectua controale a modului de prelucrare a datelor cu caracter personal în activitatea specială de investigații.. Astfel, obiecția este lipsită de suport juridic or, potrivit art. 20 din legea nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal controlul asupra respectării acestui act legislativ ține de competența Centrului Național pentru Protecția Datelor cu Caracter Personal. În partea ce ține de „abuzivitatea” competențelor, menționăm că în ipoteza depistării unor riscuri sporite la prelucrarea datelor cu caracter personal, Centrul la moment are competența de a interveni și a dispune, inclusiv: suspendarea, modificarea, încetarea
--	--	--	--	--

				operațiunilor de prelucrare a datelor. Astfel de mijloace de intervenție necesită a fi realizate operativ, or, trecerea timpului afectează posibilitatea salvagădării drepturilor și libertăților subiecților de date. Spre exemplu: Imposibilitatea intervenției asupra mijloacelor software sau hardware ar însemna în unele situații ipoteza în a curma o acțiune ilicită, care poate avea caracter transfrontalier sau ar putea prezenta indicii componenței unei infracțiuni cibernetice.
		art.12 alin.(3) și alin.(4)	6. Normele de la art.12 alin.(3) și alin.(4) sunt redactate într-un mod neclar, autorul oferind o expunere complexă. Astfel, asemenea sintagme și expuneri, precum <i>„Libertatea de exprimare și informare pot fi supuse restricțiilor prevăzute de lege și care sunt necesare într-o societate democratică”</i>, <i>„Normele prezentei legi, cu excepția competențelor Centrului [...], inclusiv nu se aplică prelucrării datelor cu caracter personal în scopuri academice, artistice, jurnalistice [...] dacă acestea sunt necesare pentru a concilia dreptul la protecția datelor personale cu libertatea de exprimare și de informare în care, în același timp: [...] c) dispozițiile prezentei legi sunt incompatibile și/sau împiedică exercitarea dreptului la libertatea de exprimare și de informare”</i>, vor crea un confuz la aplicare datorită modului general și în același timp complex de expunere. Legislația națională (Legea nr.780/2001 cu privire la actele legislative) stabilește restricții și reguli în ceea ce privește limbajul juridic în cadrul elaborării proiectelor de acte legislative. Recomandăm revizuirea acestor norme în vederea unei expuneri concise și clare pentru toți subiecții interesați.	Nu se acceptă. Ținem să menționăm că concilierea dreptului la protecția datelor cu caracter personal cu libertatea de exprimare și de informare, impune o analiză și cercetare multiaspectuală a tuturor circumstanțelor principii, în vederea indentificării unei balanțe de echilibru între aceste două drepturi fundamentale. Mai mult, în acest caz aprecierea unor asemenea limite ține inclusiv și de jurnalistul care urmează să își exercite profesia în scopul servirii interesului public, conform propriei sale cunoștiințe și în acord cu principiile prevăzute în prezentul Cod deontologic și în același timp neprejudiciind dreptul persoanei la protecția vieții intime, familiale și private. Cu referire la specificarea la alin. (4) a art. 12 a restricțiilor dreptului la libertatea de exprimare și informare, specificăm că acestea sunt reflectate atât în legislația UE cât și cea națională. Așadar art. 3 din Legea privind libertatea de exprimare prevede că: <i>„Exercitarea libertății de exprimare poate fi supusă unor restrângeri prevăzute de lege, necesare într-o societate democratică pentru securitatea națională, integritatea teritorială sau siguranța publică, pentru a apăra ordinea și a preveni infracțiunile, pentru a</i>

				<i>proteja sănătatea și morala, reputația sau drepturile altora, pentru a împiedica divulgarea de informații confidențiale sau pentru a garanta autoritatea și imparțialitatea puterii judecătorești.”</i> Prin urmare, limitările care pot fi impuse legal asupra dreptului la libertatea de exprimare nu pot depăși limitările menționate, adică trebuie să fie prevăzute de lege și să constituie, într-o societate democratică, o măsură necesară „pentru protecția ... reputației sau drepturilor altora”. Acest concept se referă la dreptul la protecția datelor cu caracter personal. Mai mult, cele invocate trebuie abordate și prin prisma proiectelor de legi care vor aduce modificări esențiale domeniului libertății de exprimare și accesului liber la informații.
		art.13 alin.(5)	7. La art.13 alin.(5) <u>„Sistemele de evidență private în care sunt prelucrate datele personale vor fi stocate în Republica Moldova sau în țările care asigură un nivel adecvat de protecție a datelor personale sau în alte țări sub responsabilitatea directă a operatorului”</u>. Considerăm că o asemenea abordare nu asigură sub nici o formă protecția datelor și aceasta derivă din modul de expunere general precum „un nivel adecvat de protecție”. Există riscul ca datele cu caracter personal din Republica Moldova să fie cu ușurință stocate în alte state, indiferent de modul de protecție, termenul de - nivel adecvat, fiind ușor interpretabil de la caz la caz. O asemenea abordare poate prezenta un pericol și sub aspectul de securitate națională, fapt care trebuie analizat în mod prioritar și foarte detaliat. Sub aspectul de securitate națională trebuie revăzute și normele de la art.32 din prezentul proiect - „Reprezentanții operatorilor sau ai persoanelor	Nu se acceptă CNPDCP a reținut îngrijorarea CNA în privința riscului care poate surveni ca datele cu caracter personal din Republica Moldova să fie stocate în alte state. Însă nu a desprins cu certitudine care ar fi propunerea concretă în acest sens. Cu referire la sistemele informaționale automatizate de stat, art. 13 alin. (4) statuează clar că „sistemele informaționale automatizate de stat, inclusiv registrele de stat în care sunt prelucrate date personale pot fi stocate fizic doar în Republica Moldova.” În cazul dat o asemenea reglementare nu prezintă un pericol sub aspectul securității statului. Totodată, remarcăm că prin prisma noțiunii de „operator”, anume operatorul stabilește scopurile și/sau mijloacele de prelucrare a datelor cu caracter personal. În acest caz operatorul răspunde de toate prelucrările de

			care nu au sediul stabilit în Republica Moldova”, care sunt redade într-un mod general și complex.	date pe care le efectuează și este responsabil pentru operațiunile sale de prelucrare a datelor. Companiile private își pot stoca datele de pretutindeni, dar trebuie să asigure un nivel adecvat de protecție a datelor cu caracter personal. Obiecțiile aduse de CNA nu sunt relevante, impunerea unor condiții irestrictive privind stocarea sistemelor de evidență private ar putea avea un impact negativ asupra companiilor private, deoarece acestea ar fi obligate să-și schimbe modelele de afaceri și locurile de activitate.
		art.21	8. Cu referire la art.21 - Dreptul la rectificare, stabilim că pe lângă cererea de rectificare depusă de către subiectul de date, acesta trebuie să anexeze și careva act justificative care ar demonstra schimbarea datelor și completarea acestora, iar acest fapt trebuie expus clar prin norme de drept. În caz contrar, la aplicare fiecare operator va fi obligat să rectifice datele deținute doar în baza unei cerere de rectificare/completare și a informațiilor expuse în mod verbal, de către subiectul de date.	Nu se acceptă. Articolul 21 din proiect, este consfințit inclusiv în Regulamentul (UE) 2016/679, <i>Articolul 16 – „Dreptul la rectificare”</i> - <i>Persoana vizată are dreptul de a obține de la operator, fără întârzieri nejustificate, rectificarea datelor cu caracter personal inexacte care o privesc. Ținându-se seama de scopurile în care au fost prelucrate datele, persoana vizată are dreptul de a obține completarea datelor cu caracter personal care sunt incomplete, inclusiv prin furnizarea unei declarații suplimentare.</i> În aceste condiții, impunerea unor obligații pe seama subiectului de date cu caracter personal, în vederea realizării dreptului la rectificare în cazurile expres statuate la art. 21 și anume: a) rectificarea datelor inexacte sau neveridice care-l vizează; b) completarea datelor incomplete care-l vizează; c) actualizarea datelor care-l vizează. - îngreunează semnificativ exercitarea dreptului în cauză

				Considerentele Regulamentul (UE) 2016/679, stipulează că statele trebuie să prevadă modalități de facilitare a exercitării de către persoana vizată a drepturilor care îi sunt conferite, inclusiv mecanismele prin care aceasta poate solicita și, dacă este cazul, obține, în mod gratuit, în special, acces la datele cu caracter personal, precum și rectificarea sau ștergerea acestora, și exercitarea dreptului la opoziție.. Operatorul ar trebui să aibă obligația de a răspunde cererilor persoanelor vizate fără întârzieri nejustificate și cel târziu în termen de o lună și, în cazul în care nu intenționează să se conformeze respectivele cereri, <u>să motiveze acest refuz.</u> <u>Suplimetar, la conturarea unor situații descrise de CNA, în ordinea art. 17 alin. (2) din proiect operatorul are dreptul de a nu da curs realizării dreptului, solicitând informații suplimentare:</u> - Operatorul facilitează exercitarea drepturilor subiectului de date în temeiul art. 20-27. În cazurile menționate la art. 10 alin. (2), operatorul nu refuză să dea curs cererii subiectului de date de a-și exercita drepturile în conformitate cu art. 20-27, <u>cu excepția cazului în care operatorul demonstrează că nu este în măsură să identifice subiectul de date.</u>
		art.24	9. La art. 24 se constată prezența unor expuneri generale, care la aplicare pot fi interpretate în mod subiectiv, fie individual în dependență de interesele urmărite. În special ne referim la sintagma „<u>cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate</u>”.	Nu se acceptă Norma prevăzută la acest articol este în corespundere cu prevederile articolul 19 din Regulamentul (UE) 2016/679, în corespundere cu care: „Obligația de notificare privind rectificarea sau ștergerea datelor cu caracter personal sau restricționarea prelucrării Operatorul comunică fiecărui destinatar cărui i-au fost divulgate datele cu caracter personal orice rectificare sau ștergere a datelor cu caracter personal sau restricționare a prelucrării efectuate în

				conformitate cu articolul 16, articolul 17 alineatul (1) și articolul 18, <u>cu excepția cazului în care acest lucru se dovedește imposibil sau presupune eforturi disproporționate. Operatorul informează persoana vizată cu privire la destinatarii respectivi dacă persoana vizată solicită acest lucru.</u>” Așadar, această obligație de comunicare decurge în cazul care se dovedește a fi imposibilă sau presupune eforturi disproporționate. Expunerea acestor impedimente, probarea imposibilității sau estimarea disproporționalității ține de obligația operatorului. <u>În această privință, în dependentă de caz se pot contura diverse motive care ar duce la imposibilitatea executării obligației statuate la acest articol, iar enumerarea unor cazuri concrete se face imposibilă.</u> <u>Or, aceasta ar putea depinde de numărul subiecților de date, numărul destinatarilor vizati, condiții tehnice etc.</u> În aceleași condiții, nu este necesară impunerea obligației de a furniza informații în cazul în care persoana vizată deține deja informațiile, în cazul în care înregistrarea sau divulgarea datelor cu caracter personal este prevăzută în mod expres de lege sau în cazul în care informarea persoanei vizate se dovedește imposibilă sau ar implica eforturi disproporționate. Acesta din urmă ar putea fi cazul în special atunci când prelucrarea se efectuează în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. În această privință, ar trebui luate în considerare numărul persoanelor vizate, vechimea datelor și orice garanții adecvate adoptate.
		art.28	10. Art.28 urmează a fi revăzut în speță alin.(1) lit.g), lit.h), lit.i), întrucât restricțiile propuse sunt redactate în mod	Nu se acceptă Restricționarea drepturilor și obligațiilor statuate la art. 28 sunt conforme Convenția europeană pentru apărarea

			general, acestea în mare parte fiind transcrise din Directivele Europene (art.23 din Directiva (UE) 2016/679 și art.16 din Directiva (UE) 2016/680).	drepturilor omului și a libertăților fundamentale, Regulamentului (UE) 2016/679 și Directivei (UE) 2016/680. Astfel, Articolul 23 din Regulamentul (UE) 2016/679, statuează că dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la articolele 12-22 și 34, precum și la articolul 5 în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la articolele 12-22, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura: a) protecția securității naționale; b) protecția securității statului; c) protecția ordinii publice; d) prevenirea, investigarea, descoperirea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa ordinii publice; e) alte obiective importante ale statului de interes general, în special un interes economic sau financiar important, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale; f) protecția independenței judiciare și a procedurilor judiciare; g) prevenirea, investigarea, depistarea și urmărirea penală a încălcărilor deontologice ale profesiilor reglementate; h) funcția de monitorizare, inspecție sau reglementare legată, chiar și ocazional, de exercitarea autorității publice în cazurile menționate la lit. a) - e) și lit. g);
--	--	--	---	--

				i) protecția subiectului de date sau a drepturilor și libertăților altora; j) punerea în aplicare a pretențiilor de drept civil. (2) În special, orice măsură legislativă menționată la alineatul (1) conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește: (a) scopurile prelucrării sau ale categoriilor de prelucrare; (b) categoriile de date cu caracter personal; (c) domeniul de aplicare al restricțiilor introduse; (d) garanțiile pentru a preveni abuzurile sau accesul sau transferul ilegal; (e) menționarea operatorului sau a categoriilor de operatori; (f) perioadele de stocare și garanțiile aplicabile având în vedere natura, domeniul de aplicare și scopurile prelucrării sau ale categoriilor de prelucrare; (g) riscurile pentru drepturile și libertăților persoanelor vizate; și (h) dreptul persoanelor vizate de a fi informate cu privire la restricție, cu excepția cazului în care acest lucru poate aduce atingere scopului restricției.
		art.35 alin.(5)	11. Nu este clară excepția stabilită la art.35 alin.(5) care prevede dreptul „instituțiilor de drept public sau privat, cu mai puțin de 50 de angajați” de a fi exceptate de laținerea unei evidențe a activităților de prelucrare a datelor cu caracter personal. Totodată, și excepția dată în continuare stabilește alte excepții „cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile	Nu se acceptă. Prin prezentul proiect de lege se transpune Regulamentului (UE) 2016/679. În acest sens remarcăm că potrivit prevederilor expuse la art. 35 alin. (5) norma în cauză este conformă dispozițiilor Regulamentului (UE) 2016/679, în conformitate cu care „Obligațiile menționate la alineatele 1 și 2 nu se aplică unei întreprinderi sau organizații cu mai puțin de 250 de angajați, cu excepția cazului în care

		<i>persoanelor vizate”, ceea ce distorsionează sensul normei, acesta fiind neclar pentru operatori la aplicare. A se revedea art.35 alin.(5) din proiect și a propune norme concise, în care să fie clar stabilit în ce circumstanțe pot fi exceptați, operatorii care dețin sub 50 de angajați, de la respectarea prevederilor legale.</i>	<i>prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10.”</i> Totuși, avînd în vedere că în Republica Moldova puțini agenți economici dispun de un staff de personal mai mare de 250 angajați s-a mers pe formula <i>mai puțin de 50 de angajați.</i> În aceste condiții nu pot reținute argumentele CNA în partea ce vizează excepția statuată în conținutul normei supra, or atunci cînd în urma unei evaluări a impactului asupra protecției datelor operatorul identifică riscuri pentru drepturile și libertățile persoanelor vizate Probabilitatea de a se materializa și gravitatea riscului pentru drepturile și libertățile persoanei vizate ar trebui să fie determinate în funcție de natura, domeniul de aplicare, contextul și scopurile prelucrării datelor cu caracter personal. Acest exercițiu urmează a fi realizat desinestătător de către fiecare operator în parte, pentru a aprecia necesitatea respectării obligațiilor de ținare/păstrare a evidenței activităților de prelucrare a datelor personale sub răspunderea lor sau de a aplica excepțiile de la alin. (5). În acest context, CNPDCP în comun cu aportul experților rezidenți din cadrul proiectului Twinning „Consolidarea capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova”, finanțat de Uniunea Europeană și implementat prin Fundația Germană pentru Cooperare Juridică Internațională (IRZ) și Ministerul Justiției din
--	--	--	---

				Letonia va elabora un manual operatorilor privind evaluarea impactului asupra protecției datelor.
		art.36 alin.(3)	12. Norma de la art.36 alin.(3) este expus într-un mod complex și ambiguu din care nu poate fi dedus cu exactitate scopul propus de aceasta. A se revedea.	Nu se acceptă Nu s-a reținut cu certitudine care prevederi urmează a fi revăzute și crează în opinia CNA loc de ambiguități, inclusiv și care ar fi propunerea înaintată în acest sens. Prin urmare, alin. (3) a art. 36 stabilește clar statutul și răspunderea pe care o poartă o altă persoană împuternicită de operator angajată de persoană împuternicită de operator. Acest articol încurajează persoana împuternicită de operator să contacteze alte persoane împuternicite prin intermediul unor angajamente contractuale sau alte acte juridice în conformitate cu legea, care oferă garanții suficiente.
		art.42 alin.(2)	13. Considerăm că termenii propuși la art.42 alin.(2) din proiect, pentru acordarea consultărilor prealabile operatorilor de către CNPDCP sunt extrem de mari și pot afecta interesele legale și activitatea per ansamblu, a operatorilor, spre exemplu: „ <u>Centrul oferă consultare în scris operatorului și, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii [...]</u> <u>Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Centrul informează operatorul și, după caz, persoana împuternicită de operator, în termen de cel mult două luni de la primirea cererii, cu privire la orice astfel de prelungire</u> ”. A se revedea termenii propuși, întrucât aceștia pot stopa, fie suspenda activitatea operatorilor.	Nu se acceptă Termenii stabiliți la acest articol sunt în strictă corespundere cu cei stabiliți în art. 36 din Regulamentul (UE) 2016/679. În aceste condiții, ținem să atragem atenția că acești termeni nu sunt extremi de mari, așa după cum a remarcat CNA, or aceștia sunt stabiliți reieșind din complexitatea examinării criteriilor necesare efectuării evaluării impactului asupra protecției datelor, aprecierii riscurilor care pot fi generate, precum și dictarea măsurilor concrete ce urmează a fi luate de operator. Alin. (2) descrie situația, în care o evaluare a impactului asupra protecției datelor arată că operațiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile și al costurilor implementării și trebuie să consulte în acest sens autoritatea de supraveghere înainte de prelucrare, care la rândul ei

				reieșind din complexitatea prelucrării necesită un termen rezonabil pentru examinare pentru a oferi o consultație adecvată operatorilor. Cu toate acestea, lipsa unei reacții din partea autorității de supraveghere în termenul respectiv ar trebui să nu aducă atingere niciunei intervenții a autorității de supraveghere în conformitate cu sarcinile și competențele sale prevăzute, inclusiv competența de a interzice operațiuni de prelucrare.
		art.46 alin.(1)	14. Cu referire la Codurile de conduită și monitorizarea acestora, menționăm că art. 46 alin.(1) nu obligă operatorii de a elabora și deține codul menționat „<i>Asociațiile și 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, ținând 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</i>”. Totodată, proiectul propune norme ce stabilesc monitorizarea respectării acestor coduri la art.45 din proiect. Mai mult ca atât, art.45 alin.(2) lit.c) prevede că aceste coduri trebuie să conțină și proceduri de gestionare a cererilor (reglementate în mod general/ambigui), ceea ce nu este caracteristic unui cod de conduită. Astfel, din proiect nu reiese clar dacă elaborarea unor asemenea coduri de conduită este obligatorie sau nu. La fel, nu este expus cu exactitate dacă elaborarea și deținerea codurilor de conduită este valabilă pentru toți operatorii sau doar pentru careva categorii, întrucât autorul operează cu termenul „<i>Asociațiile și alte organisme care reprezintă categoriile de operatori sau persoane împuternicite de operatori</i>”. Recomandăm autorului să reexamineze normele propuse la art.46 și 47 din proiect, prin prisma	Nu se acceptă Articolele menționate sunt în strictă conformitate cu prevederile art. 40, 41 din Regulamentul (UE) 2016/679. Din start, ținem să menționăm că orientări pentru implementarea unor măsuri adecvate și pentru demonstrarea conformității de către operator sau persoana împuternicită de operator, mai ales în ceea ce privește identificarea riscului legat de prelucrare, evaluarea acestuia din punctul de vedere al originii, naturii, probabilității de a se materializa și al gravității, precum și identificarea bunelor practici pentru atenuarea riscului ar putea fi oferite în special prin coduri de conduită aprobate. Așadar, art. 46 alin.(1) acordă posibilitate și nu obligă sub nici o formă <i>Asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori</i> de a elabora coduri de conduită, în limitele legii, astfel încât să se faciliteze aplicarea efectivă a prevederilor legii, luându-se în considerare caracteristicile specifice ale prelucrării efectuate în anumite sectoare și necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii. Or, norma în forma care a fost expusă,

			obiecțiilor sus-menționate și revizuirea acestora astfel, pentru a reda clar sensul și scopul propus. Ca obiecție generală asupra proiectului propus, statuăm că acesta conține numeroase expuneri cu caracter general și complex, ceea ce va permite aplicarea prevederilor în interpretare preferențială, de exemplu: „<u>Orice măsură legislativă menționată la alin. (1) din prezentul articol conține dispoziții specifice cel puțin, dacă este cazul, în ceea ce privește</u>” - art.28 alin.(2), „<u>și în dependență de situație în format scris</u>” - art.35 alin.(3), „<u>cu excepția cazului în care nu este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor fizice</u>” - art.38 alin.(1) etc. A se vedea normele expuse general.	stabilește expres și fără careva ambiguități că „<u>Asociațiile și alte organisme care reprezintă categoriile de operatori sau persoane împuternicite de operatori pot pregăti coduri de conduită...</u>” În partea ce vizează art. 47 nu s-a reținut care ar fi neclaritatea reținută de CNA, în condițiile în care această normă statuează foarte clar că monitorizarea respectării unui cod de conduită în temeiul art. 46 poate fi realizată de un organism de certificare care dispune de un nivel adecvat de expertiză în legătură cu obiectul codului și care este acreditat de Centru. Iar acesta la rândul său pentru a fi acreditat de către Centru, trebuie să întrunească mai multe condiții, una dintre care fiind instituirea unor proceduri și 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 și pentru a asigura transparența acestor proceduri și structuri pentru subiecții datelor și pentru public și a demonstrat Centrului, într-o manieră satisfăcătoare, că sarcinile și atribuțiile sale nu creează conflicte de interese.
		Capitolul VII	15. Capitolul VII „Prevederi speciale privind prelucrarea datelor personale de către organele de ocrotire a legii”, este necesar de exclus conținutul textului acestuia, cu instituirea prevederilor în proiect care să prevadă că „prezenta lege nu se aplică de către organele de ocrotire a legii prelucrărilor de date cu caracter personal efectuate în scopul prevăzut la art.2 lit.d) din lege”. În acest sens, se invocă prevederi similare ai legislației în domeniu din România, precum:	Nu se acceptă În contextul activităților de investigare și de asigurare a conformității prelucrării datelor cu caracter personal în sectorul polițienesc și în vederea implementării 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,

		<u>Legea nr.506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice</u>, care la art.1 alin.(4) statuează că „Prezenta lege nu se aplică prelucrărilor de date cu caracter personal efectuate: a) în cadrul activităților în domeniul apărării naționale și securității naționale, desfășurate în limitele și cu restricțiile stabilite de lege; b) în cadrul activităților de combatere a infracțiunilor și de menținere a ordinii publice, precum și în cadrul altor activități în domeniul dreptului penal, desfășurate în limitele și cu restricțiile stabilite de lege.” Iar, conform art.12 „(1) <u>La solicitarea instanțelor de judecată sau la solicitarea organelor de urmărire penală ori a organelor de stat cu atribuții în domeniul apărării și securității naționale, cu autorizarea prealabilă a judecătorului stabilit potrivit legii, furnizorii de servicii de comunicații electronice destinate publicului și furnizorii de rețele publice de comunicații electronice pun la dispoziția acestora, de îndată, dar nu mai târziu de 48 de ore, datele de trafic, datele de identificare a echipamentului și datele de localizare, în conformitate cu prevederile referitoare la protecția datelor cu caracter personal.</u> (2) Solicitățile privind datele prevăzute la alin. (1), formulate de către organele de stat cu atribuții în domeniul apărării și securității naționale, sunt supuse dispozițiilor art. 14, 15 și art. 17-23 din Legea nr. 51/1991 privind securitatea națională a României, republicată. (3) Solicitățile, respectiv răspunsurile, dacă sunt transmise în format electronic, se semnează cu semnătură electronică extinsă bazată pe un certificat calificat, eliberat de un furnizor de servicii de certificare acreditat. Fiecare persoană care certifică datele sub semnătură electronică răspunde, potrivit legii, pentru integritatea și securitatea acestor date. (4) Solicitățile prevăzute la alin. (1) se procesează în condiții de confidențialitate. (5) Datele de	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, prezentul proiect de lege vine cu un capitol întreg destinat prelucrării datelor cu caracter personal de către organele de ocrotire a legii, și anume capitolul VII, care reglementează atribuția Centrului de a supraveghea, reglementa și investiga modul de prelucrare a datelor personale de către organele de drept în conformitate cu prezentul proiect de lege și Legea privind Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Obecția CNA cu referire la excluderea Capitolul VII „Prevederi speciale privind prelucrarea datelor personale de către organele de ocrotire a legii” a trezit nedumerire, iar dispozițiile legiutorului românesc invocate nu sunt relevante. În acest sens, ținem să menționăm că în conformitate Articolul 1 - Obiect și obiective din Directiva (UE) 2016/680, Prezenta directivă stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. „Autoritate competentă” înseamnă: (a) orice autoritate publică competentă în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor sau de executare a pedepselor, inclusiv în materie de protejare împotriva amenințărilor la adresa securității publice și de prevenire a acestora; sau
--	--	--	---

		trafic, datele de identificare a echipamentului și datele de localizare solicitate conform alin. (1) nu fac obiectul ștergerii sau anonimizării de către furnizori, atunci când solicitarea formulată în temeiul alin. (1) este însoțită ori urmată de o notificare cu privire la necesitatea menținerii lor, în scopul identificării și conservării probelor sau indiciilor temeinice, în cadrul investigațiilor pentru combaterea infracțiunilor ori în domeniul apărării și securității naționale, atât timp cât subzistă motivele care au stat la baza solicitării, dar nu mai mult de 5 ani de la data solicitării sau, după caz, până la pronunțarea unei hotărâri definitive a instanței de judecată.” Conform proiectului, articolul 72 Generarea înregistrărilor de audit, prevede că organul de ocrotire a legii este obligat să țină evidența înregistrărilor de audit a operațiunilor de prelucrare a datelor personale în sistemele automatizate: colectare, culegere, consultare, modificare, dezvăluire, răspândirea, imprimare, transfer, combinare și ștergere. Se consideră că prevederile respective trebuie să se refere la administratorii sistemelor informaționale, care urmează să efectueze auditul operațiunilor, iar sistemele informaționale gestionate să fie dotate cu rubrici privind temeiul accesării datelor. Altfel, organele de ocrotire a legii vor fi obligate să asigure evidența în multiple registre la toate procesele de lucru cu datele, fapt ce ar implica resurse umane și timp suplimentar. Mai mult, termenul de "audit" utilizat pe tot parcursul conținutului textului proiectului (art.72, art.74 alin.(7)) este impropriu pentru domeniul de activitate reglementat prin proiect, fapt ce poate crea situații confuze și incertitudine la realizarea normelor propuse de către subiecții responsabili de implementare. Conform Legii	(b) orice alt organism sau entitate împuternicit(ă) de dreptul intern să exercite autoritate publică și competențe publice în scopul în prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. În aceste condiții, nu s-a putut reține argumentarea juridică de excludere de la prezenta lege activitatea de prelucrare a datelor cu caracter personal efectuată de către organele de ocrotire a Legii în scopul prevăzut la art.2 lit.d) din lege. Context în care, urmează a fi reliefate la moment următoarele prevederi în vigoare și de aplicare ale Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal: Articolul 2 alin. (2) lit. d) - domeniul de acțiune al acestei legi se extinde asupra prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale în condițiile legii. În partea ce vizează, invocarea unor prevederi din legislația în domeniu din România, precum <u>Legea nr.506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, care stabilește că: „Prezenta lege nu se aplică prelucrărilor de date cu caracter personal efectuate: a) în cadrul activităților în domeniul apărării naționale și securității naționale, desfășurate în limitele și cu restricțiile stabilite de lege; b) în cadrul activităților de combatere a infracțiunilor și de menținere a ordinii publice, precum și în cadrul altor activități în domeniul dreptului penal, desfășurate</u>
--	--	--	--

			nr.61/16.03.2007 privind activitatea de audit, prin "audit" se înțelege "examinare independentă a rapoartelor financiare anuale, a rapoartelor financiare anuale consolidate și a altor informații, aferente acestora, ale entității auditate pentru exprimarea unei opinii profesionale a auditorului asupra corespunderii lor, sub toate aspectele semnificative, cerințelor stabilite față de aceste rapoarte". Mai mult, nici art.3 din proiect nu definește termenul „înregistrări de audit”	<u>în limitele și cu restricțiile stabilite de lege.”, menționăm că aceasta nu are nici o relevanță cu propunerea de excludere de la prezenta lege activitatea de prelucrare a datelor cu caracter personal efectuată de către organele de ocrotire – or, prin reglementarea capitolului VII s-a trasat scopul de a asigura implementarea Directivei nr. 2016/680.</u> Reglementări similare în partea ce vizează domeniul comunicațiilor electronice, s-a reținut că art. 62¹ din Legea comunicațiilor electronice, în conformitate cu care prevede că prezentul capitol nu se aplică prelucrărilor datelor cu caracter personal efectuate: a) în cadrul acțiunilor în domeniul apărării și securității naționale, desfășurate în condițiile stabilite de lege; b) în cadrul acțiunilor de prevenire, cercetare, urmărire a infracțiunilor și de menținere a ordinii publice, precum și al altor activități în domeniul procedurii penale, desfășurate în condițiile stabilite de lege. Urmează a fi remarcat faptul, că prevederile capitolul VII din proiectul de modificare a Legii 133, precum și necesitatea implementării Directivei nr. 2016/680 a au fost discutate și dezbătute în cadrul mai multor ședințe de către experții UE cu paticiparea reprezentanților Procuraturii Generale, Ministerului Afacerilor Interne, Serviciului de Informații și Securitate, Centrului Național Anticorupție, Seviceiului Vamal, Depatamentului Instituțiilor Penitenciare etc. Cu referire la obiecția organele de ocrotire a legii de a ține evidența operațiunilor de prelucrare a datelor cu carcter personal, ținem să menționăm că la momet această obligație este una valabilă pentru toți operatorii de date. Astfel în conformitate cu cap.VIII. AUDITUL SECURITĂȚII ÎN SISTEMELE INFORMAȚIONALE DE DATE CU CARACTER
--	--	--	--	---

				PERSONAL din Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr.1123 din 14 decembrie 2010, statuează că pentru toate categoriile sistemelor informaționale de date cu caracter personal, deținătorii de date cu caracter personal organizează generarea înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal pentru evenimentele, indicate în lista corespunzătoare, supuse auditului. Prin urmare, atât Regulamentul (UE) 2016/679 cât și Directiva (UE) 2016/680 prevăd că în vederea demonstrării conformității cu legea, operatorul sau persoana împuternicită de operator ar trebui să păstreze evidențe ale activităților de prelucrare aflate în responsabilitatea sa. Fiecare operator și fiecare persoană împuternicită de operator ar trebui să aibă obligația de a coopera cu autoritatea de supraveghere și de a pune la dispoziția acesteia, la cerere, aceste evidențe, pentru a putea fi utilizate în scopul monitorizării operațiunilor de prelucrare respective.
		art.73 alin.(6)	De asemenea, cu referire la art.73 alin.(6), acesta indică la modalitatea de contestare a deciziei CNPDCP de către organele de ocrotire a legii și/sau subiectul de date. În sensul dat, norma formulată are un sens confuz referitor la procedura de contestare, pe de o parte autorul indică la instanța de contencios administrativ, iar pe de alta, examinarea cererii se efectuează în procedură specială. Codul de procedură civilă indică la procedura contenciosului administrativ, prin reglementarea condițiilor pentru exercitarea acțiunii de contencios administrativ, sesizarea instanței de contencios	Se acceptă parțial. Potrivit raționamentelor Regulamentului (UE) 2016/679 cât și Directivei (UE) 2016/680, statele membre ar trebui să aibă posibilitatea de a adopta măsuri legislative în vederea amânării, a restricționării sau a omiterii informării persoanelor vizate sau în vederea restricționării, integrale sau parțiale, a accesului la datele lor cu caracter personal, în măsura în care și atât timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate

			administrativ, judecarea cererii în instanța de contencios administrativ, și la procedura specială, respectiv fiind două proceduri distincte înaintea primei instanțe de judecată. De asemenea, norma formulată la alin.(6) privind examinarea cauzei în absența subiectului de date contravine Codului de procedură civilă, care statuează că atât în procedura contenciosului administrativ (art.279, 278 CPC), cât și în procedura specială (art.280 alin.(1)), litigiile se examinează cu prezența părților. Prin norma formulată se încalcă dreptul persoanei la justiție, la apărare și dreptul la un proces echitabil, consacrate de art.20 și 26 din Constituția Republicii Moldova, precum și de art.6 al Convenției pentru apărarea drepturilor omului și libertăților fundamentale. Astfel, toate cele invocate denotă excluderea capitolului VII din proiect.	democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice în cauză, pentru a se evita obstrucționarea cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, pentru a nu se afecta prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea pedepselor, pentru a se apăra securitatea publică sau securitatea națională ori pentru a se apăra drepturile și libertățile altor persoane. Operatorul ar trebui să evalueze, prin intermediul unei examinări concrete și individuale a fiecărui caz în parte, dacă dreptul de acces ar trebui să fie limitat parțial sau complet. În cazul în care operatorul refuză unei persoane vizate drepturile acesteia la informare, acces ori la rectificarea sau ștergerea datelor cu caracter personal sau la restricționarea prelucrării, <u>persoana vizată ar trebui să aibă dreptul de a solicita ca autoritatea națională de supraveghere să verifice legalitatea prelucrării.</u> Persoana vizată ar trebui să fie informată cu privire la acest drept. Atunci când autoritatea de supraveghere acționează în numele persoanei vizate, persoana vizată ar trebui să fie informată de către autoritatea de supraveghere cel puțin cu privire la faptul că toate verificările sau revizuirile necesare au fost efectuate de către autoritatea de supraveghere. Autoritatea de supraveghere ar trebui, de asemenea, să informeze persoana vizată în legătură cu dreptul de a introduce o cale de atac. Astfel, pentru a se evita obstrucționarea cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, pentru a nu se afecta prevenirea, investigarea, depistarea sau urmărirea penală a
--	--	--	---	--

				infracțiunilor sau executarea pedepselor, pentru a se apăra securitatea publică sau securitatea națională s-a propus o nouă redacție la norma statuată la art. 73 alin. (6) din prezentul proiect - (6) <i>Organul de ocrotire a legii și/sau subiectul de date poate contesta Decizia Centrului în instanța de contencios administrativ. Cauza se examinează în ședință închisă, în absența subiectului de date, cu participarea Centrului și a organului de ocrotire a legii.</i>
		art.58 alin.(4), art.80 alin.(1), art.81-86	16. Pe cale de consecință, normele propuse de proiect (art.58 alin.(4), art.80 alin.(1), art.81-86), care instituie pentru CNPDCP atribuții de investigații contravin cadrului normativ în vigoare, iar pentru a nu periclita activitatea instituțiilor abilitate cu acest drept, prevederile proiectului urmează a fi reformulate, prin limitarea atribuțiilor CNPDCP doar la activitatea de prevenire, reglementare, supraveghere și consultare a entităților/instituțiilor publice și cele de drept privat, în vederea prelucrării datelor cu caracter personal și instituirea normei care va prevedea că „prevederile prezentele legi nu se aplică în cazul prelucrării datelor personale de către organele de drept în scopul prevenirii, investigării, depistării și sau urmăririi penale a infracțiunilor sau executării pedepselor penale, detenția preventivă, inclusiv protejarea și prevenirea amenințărilor la adresa ordinii publice, securității de stat și securității naționale și în cadrul dosarului sau acțiunilor speciale de investigații”. Argumentele autorului cu referire la aspectul dat nu sunt justificate, ba dimpotrivă, acestea sunt camuflate prin trimiterea la Regulamentul UE 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția	Nu se acceptă Este regretabil faptul că se aduc interpretări subiective în partea ce vizează competențele Centrului în domeniul <u>investigării modului de prelucrare a datelor personale de către organele de ocrotire a legii în conformitate cu prezenta lege și Legea privind Centrul National pentru Protecția Datelor</u> cu Caracter Personal al Republicii Moldova și se omite faptul că nu se intenționează efectuarea din partea Centrului a controlului asupra activității special de investigații. Și nu în ultimul rind, s-a omis faptul că pe lângă Regulamentul (UE) 2016/679, în anul 2016 Parlamentul European și Consiliul a adoptat pachetul de reformă legislativă privind protecția 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 inclusiv:

		persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE, la care face autorul referire atât în nota informativă, cât și în Art.I din proiectul de lege, ca fiind actul care a stat la baza propunerilor legislative. În sensul dat, autorul nu a luat în considerație că „<i>Prezentul regulament nu se aplică prelucrării datelor cu caracter personal: [...] (c) de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice; (d) de către autoritățile competente în scopul prevenirii, investigării, depistării sau urmării penale a infracțiunilor, sau al executării sancțiunilor penale, inclusiv al protejării împotriva amenințărilor la adresa siguranței publice și al prevenirii acestora</i>” (art.2 din Regulamentul UE 2016/679). Prin urmare, CNPDCP nu este subiect care efectuează activitatea specială de investigații, fapt despre care am menționat și mai sus, or conform art.5 din Legea nr.59/2012, “(1) <i>Activitatea specială de investigații se efectuează de către ofițerii de investigații ai subdiviziunilor specializate din cadrul ori subordonate Ministerului Afacerilor Interne, Ministerului Apărării, Centrului Național Anticorupție, Serviciului de Informații și Securitate, Serviciului de Protecție și Pază de Stat, Serviciului Vamal și Departamentului instituțiilor penitenciare al Ministerului Justiției. (2) Se interzice efectuarea măsurilor speciale de investigații de către alte autorități decât cele prevăzute la alin.(1).</i>” Totodată, referindu-ne la activitatea specială de investigații, aceasta este o procedură reglementată de către legiuitor și are drept scop prevenirea și combaterea criminalității, asigurarea securității statului, ordinii publice, apărării drepturilor și intereselor legitime ale persoanelor, descoperirea și cercetarea infracțiunilor,	1. Directiva (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; 2. 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. Așadar, în contextul activităților de investigare și de asigurare a conformității prelucrării datelor cu caracter personal în sectorul polițienesc și în vederea implementării 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, prezentul proiect de lege vine cu un capitol întreg destinat prelucrării datelor cu caracter personal de către organele de ocrotire a legii, și anume capitolul VII, care reglementează atribuția Centrului de a supraveghea, reglementa și investiga modul de prelucrare a datelor personale de către organele de drept în conformitate cu prezentul proiect de lege și Legea privind Centrul Național pentru
--	--	--	--

			oferind instrumente specifice în acest sens cu reglementări stricte de efectuare a acestora, stabilite prin Legea nr.59/2012 privind activitatea specială de investigații și Codul de procedură penală. Analizând actele normative prenotate, acestea, în virtutea specificului activității date, stabilesc clar și fără echivoc care sunt tipurile de control și organele competente de efectua acest control, unde, CNPDCP nu se regăsește, ceea ce denotă faptul că prin proiect sunt promovate norme ce ar putea prejudicia grav interesele organelor de drept abilitate cu astfel de atribuții și periclita activitatea acestora (<i>Legea nr.59/2012 - capitolul V – Controlul și coordonarea activității speciale de investigații) trei tipuri de control. Art.38 - Controlul Parlamentar - prin intermediul Comisiei securitate națională, apărare și ordine publică; art. 39 - Controlul exercitat de procuror; art.40 - Controlul departamental.</i>) Subsidiar, se reține că a fost instituit și un organ suplimentar de coordonare a activității speciale de investigații – Consiliul de coordonare, constituit pe lângă Procurorul General. După cum am menționat și mai sus, legalitatea desfășurării măsurilor speciale de investigații în corelație cu încălcarea respectării drepturilor omului și a libertăților fundamentale, este verificată de către instanța de judecată și procuror, care autorizează sau anulează măsurile efectuate, iar odată cu aplicarea prevederilor proiectului în formula propusă, CNPDCP se va bucura de atribuții excesive în partea ce ține de controlul operațiunilor de prelucrare a datelor personale, iar acest fapt poate genera în procesul exercitării activității speciale de investigații conflicte de competențe sau conflicte ale normelor de drept în activitatea entităților înzestrate cu asemenea atribuții. De asemenea și Codul de procedură penală la art.300 reglementează sfera de control asupra activității speciale	Protecția Datelor cu Caracter Personal al Republicii Moldova. Nu pot fi reținute argumentele CNA în partea ce vizează excesivitatea competențelor Centrului în raport cu activitatea specială de investigație. Centru nu pretinde a fi subiect care efectuează activitatea specială de investigație în conformitate cu prevederile Legui nr. 59/2012. La fel, subliniem faptul că, CNPDCP nu urmărește scopul de a interveni în activitatea autorităților publice (organelor ce efectuează activitatea specială de investigații) sau private, ci de a efectua controlul legalității prelucrării datelor cu caracter personal ale subiectului de date de către entități, în calitate de operatori de date cu caracter personal, care au obligația de a asigura confidențialitatea și securitatea datelor cu caracter personal prelucrate. În același context, se notează că Parlamentul Republicii Moldova prin Legea comunicațiilor electronice, nr. 241-XVI din 15 noiembrie 2007, republicată în Monitorul Oficial din 17 noiembrie 2017, a atribuit Centrului în temeiul art. 71 noi competențe de a verifica măsurile tehnice și organizatorice corespunzătoare în vederea protejării securității serviciilor prestate de furnizorii de servicii de comunicații electronice. Subsecvent, concomitent cu intrarea în vigoare la data de 23 februarie 2018 a Legii cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului Centrul are competența de a efectua controlul conformității operațiunilor de prelucrare a datelor cu caracter personal efectuate de autoritățile specializate în prevenirea și combaterea terorismului, inclusiv a Serviciului Prevenirea și Combaterea Spălării Banilor. Este necesar a remarca că acțiunile ce urmează a fi întreprinse de entitățile
--	--	--	--	--

			de investigații, efectuate de către judecătorul de instrucție, nemaivorbind despre alte posibilități legale oferite cetățeanului de a-și apăra drepturile și interesele personale. Astfel, Centrul va avea dreptul să verifice activitatea specială de investigații efectuată de către organele de ocrotire a legii, ceea ce este inadmisibil, mai ales că această activitate este considerată secret de stat, în conformitate cu <i>Legii nr.245/2008 cu privire la secretul de stat</i> (art.7 alin.(4) lit.a), b), c)) și Hotărârii Guvernului privind aprobarea Nomenclatorului informațiilor atribuite la secret de stat nr.411/2010 (pct. 38 - 41).	vizate în prezenta lege presupun prelucrarea unui volum exorbitant de date cu caracter personal și se răsfrânge asupra tuturor persoanelor fizice, chiar și care au avut o tangență mică cu instituțiile financiar-bancare, dar nu numai. O altă lege care a adus atribuții noi Centrului este Legea nr. 120 din 21 septembrie 2017 cu privire la prevenirea și combaterea terorismului. Activitatea de prevenire și combatere a terorismului va fi exercitată în mod special de Serviciul de Informații și Securitate care prelucrează un volum extrem de mare de date personale, iar controlul conformității prelucrărilor de date cu caracter personal se efectuează de către Centru. Prin spectrul de modificări legislative arătat supra, Centrul a dobândit competență de a investiga prelucrarea datelor cu caracter personal atribuite inclusiv la secret de stat etc. Totodată, remarcăm că pe marginea activității sale CNPDCP se supune controlului Parlamentar și controlului judecătoresc. De asemenea, activitatea CNPDCP nu este exclusă de controlul din partea altor organe, conform competenței lor. Un alt element important care a contribuit la cristalizarea competențelor Centrului de a efectua operațiuni de investigație a prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, al punerii în aplicare a sentințelor de condamnare sau al altor acțiuni ce țin de procedura penală ori contravențională, în condițiile legii, îl reprezintă Ghidul practic privind utilizarea datelor cu caracter personal în sectorul polițienesc, adoptat de către Comitetul Consultativ al Convenției 108 pentru protecția persoanelor cu
--	--	--	---	---

				privire la prelucrarea automatizată a datelor cu caracter personal, adoptat la data de 15 februarie 2018 la Strasbourg. Se menționează că Ghidul invocat are o pondere deosebită, atât sub aspect de utilitate cât și sub aspect de comprehensivitate întrucât explică într-o manieră accesibilă faptul că <u>toate prelucrările de date trebuie să respecte principiile de necesitate, proportionalitate și limitare a scopului. Aceasta implică faptul că prelucrarea datelor cu caracter personal în cadrul poliției ar trebui să se bazeze pe scopuri predefinite, clare și legitime stabilite de lege; ar trebui să fie necesar și proportional cu aceste scopuri legitime și nu ar trebui să fie prelucrate într-un mod incompatibil cu aceste scopuri. Prelucrarea datelor ar trebui să se facă în mod legal, corect și transparent. Datele personale din cadrul poliției ar trebui, de asemenea, să fie adecvate, relevante și neexcesive în raport cu scopurile. În cele din urmă, acestea trebuie să fie corecte și actualizate pentru a asigura cea mai înaltă calitate a datelor</u>”. Același Ghid, plasează în sarcina autorităților de supraveghere a prelucrării datelor cu caracter personal, în cazul Republicii Moldova, Centrul Național pentru Protecția Datelor cu Caracter Personal, atribuția de asigurare a conformității prelucrării datelor cu caracter personal în sectorul polițienesc. Se arată că, prezentul Ghid deja a fost diseminat către Parlamentul Republicii Moldova spre informare, dar și către instituțiile din sistemul polițienesc, în vederea implementării acestuia.
		art.6 în corelare cu art.81	17. După cum a fost menționat mai sus, cu referire la art.6 în corelare cu art.81 din proiect, CNPDCP îi sunt instituite atribuții paralele cu cele ale organelor de drept.	Nu se acceptă

		În sensul dat, norma propusă de autor la art.81 din proiect, este abuzivă, iar inspectorii de protecție vor fi în drept să dispună de acces și să examineze sistemele de evidență a datelor personale, soluțiile software și suporturile hardware, datele personale și orice documente legate de obiectul și scopul investigației, indiferent de echipamentul și/sau suportul pe care sunt stocate datele; să intre liber în încăperi, pe terenuri sau în mijloace de transport aflate în proprietatea sau folosința subiecților de drept menționați la alin. (1) din prezentul articol; să ridice, să colecteze, să obțină mijloace, copii sau extrase, sub orice formă, din sistemele de evidență și documentele care conțin date personale; să sigileze încăperile și mijloacele, unde și prin care se efectuează prelucrarea datelor personale, mijloacele, sistemele de evidență și documentele aferente obiectului și scopului investigației, pe perioada și în măsura în care este necesar pentru desfășurarea investigației, să solicite și să primească informațiile referitoare la obiectul și scopul investigației, etc. Instituirea unor astfel de atribuții CNPDCP, identice cu cele ale organelor de drept enunțate mai sus, este inadmisibil, deoarece va genera conflicte de competențe la aplicare și comiterea abuzurilor de către inspectorii de integritate, care bucurându-se de prevederile respective vor dispune de acces la informații secrete ce constituie secret de stat, secret profesional, secret bancar, secret comercial sau a dosarului special. Or, după cum a fost menționat în repetate rânduri, nici proiectul cu privire la Centrul național pentru Protecția Datelor cu Caracter Personal, nici proiectul pentru modificarea și completarea unor acte legislative, nu prevăd mecanismul de control/supraveghere asupra activității CNPDCP și legalității acestor măsuri cu caracter procesual penal.	Un element important în procesul de asigurare a independenței reale a Centrului la exercitarea competențelor sale este reglementarea expresă prin lege a drepturilor și obligațiilor angajaților Centrului implicați în activitatea de investigare. Aceste elemente sunt determinate și de normele următoarelor instrumente juridice de drept internațional: - Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE; - 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 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 și de Recomandarea nr. R (87) 15 din 17 septembrie 1987 a Comitetului de Miniștri al Consiliului Europei ce reglementează utilizarea datelor cu caracter personal în sectorul polițienesc. De menționat că, un număr major din adresările înaintate Centrului vizează în special preținsele ilegalități admise de către organele de drept, în cadrul desfășurării urmăririi penale, măsurilor speciale de investigații, activităților operative, cauzelor contravenționale etc. Verificarea legalității colectării, utilizării și stocării datelor cu caracter personal gestionate de colaboratorii organelor de drept, impune necesitatea oferirii
--	--	--	--

			Totodată, dacă să ne referim la randamentul asupra rezultatelor activității CNPDCP cât privește atribuțiile de sancționare, în corelare cu competența excesivă ce urmează a fi atribuită conform proiectului dat cea de investigație, sunt ne semnificative, dat fiind faptul că CNPDCP nu dispune de competențe penale, iar în Codul contravențional sunt prevăzute 3 articole (<i>art. 74¹-74³</i>) de sancționare conform competenței atribuite. Astfel, se recomandă reformularea normei, prin limitarea atribuțiilor CNPDCP doar la activitatea de prevenire, reglementare, supraveghere și consultare a entităților/instituțiilor publice și cele de drept privat.	accesului la anumite informații din dosarele gestionate cu respectarea garanțiilor de confidențialitate prevăzute de legislația în vigoare, însă se constată opunere nejustificată din partea actorilor implicați, chiar dacă legislația actuală prevede o astfel de procedură, cu rezerve de interpretare. În anul 2016, un element cheie pentru domeniul protecției datelor cu caracter personal a constituit adoptarea, la 28 aprilie 2016, a Legii nr. 87 pentru modificarea și completarea unor acte legislative, prin intermediul căreia, o serie de amendamente referitoare la protecția datelor cu caracter personal au fost incluse în documentele normative ce reglementează activitatea polițienească și judecătorească în Republica Moldova (<i>exemplu, Codul de procedură penală, Codul contravențional, Legea privind statutul judecătorului, Legea cu privire la Centrul Național Anticorupție, Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, Legea cu privire la activitatea Poliției și statutul polițistului, Legea privind activitatea specială de investigații, etc.</i>). Aceste amendamente, vin să încorporeze principiile de protecție a datelor cu caracter personal în activitatea polițienească ce se referă la poliție, procuratură, instanțe de judecată etc., prin a responsabiliza personalul din sectoarele vizate implicate în prelucrarea datelor cu caracter personal. <u>Cu toate acestea, modificările date nu au fost efectuate într-o manieră, încât să permită excluderea interpretării nejustificate din partea unor organe de drept, creînd confuzie între autoritățile statului și generînd impedimente pentru angajații Centrului de a verifica legalitatea prelucrărilor de date cu caracter personal.</u>
--	--	--	--	---

				De menționat că practica internațională oferă autorităților de protecție a datelor cu caracter personal, dreptul de a avea acces la orice tip de informații, indiferent de gradul de securizare și clauza de confidențialitate, fie secret de stat, confidențialitatea urmăririi penale sau contravenționale, și de a verifica dacă prin aceste metode de colectare și utilizare a datelor, nu se încalcă drepturile omului, în special în partea ce vizează inviolabilitatea vieții intime, familiale și private. Ar fi de menționat experiența maghiară, or, în Ungaria, întru executarea controalelor, Președintele Autorității Naționale pentru Protecția Datelor și Libertății de Informație (NAIH) beneficiază de drepturi largi în domeniul investigării prelucrării informației secrete. Astfel, Vice-președintele și examinatorii beneficiază de acces la informația secretă, în cadrul operațiunilor efectuate. Spectrul întreg de atribuții vin să fortifice și să consolideze capacitățile funcționale și operaționale ale Centrului, care au consecință pentru apărarea drepturilor la viața intimă, privată și de familie a indivizilor, indiferent de rang și statut.
		alin.(12) din art.81	18. Cu referire la alin.(12) din art.81, conform art.53 alin.(1) al Legii nr.780/2001 privind actele legislative, <i>"Codul este actul legislativ care cuprinde într-un sistem unitar cele mai importante norme dintr-o anumită ramură a dreptului."</i> Intenția autorului de a reglementa prin proiect mandatul judecătoresc și drepturile și obligațiile instanței de judecată le considerăm, la fel, abuzive. Or, Codul de procedură penală este actul normativ în vigoare care reglementează mandatul judecătoresc, drepturile și obligațiile instanței de judecată care dispune sau autorizează efectuarea măsurilor	Nu se acceptă. Menționăm că prevederi similare se regăsesc în legislația Republicii Moldova există practici când autoritățile de control pot efectua controlul în domiciliul persoanei în afara unui proces penal. După cum a fost menționat supra prevederile Codului de procedură penală nu sînt aplicabile. Mandatul Judecătoresc este necesar și se eliberează doar pentru accesul reprezentanților Centrului în domiciliu posesorului legal, în lipsa

			speciale de investigații sau efectuarea altor acțiuni procesuale. Potrivit, art.1 al Codului de procedură penală, <i>"Procesul penal reprezintă activitatea organelor de urmărire penală și a instanțelor judecătorești cu participarea părților în proces și a altor persoane, desfășurată în conformitate cu prevederile prezentului cod. Procesul penal se consideră început din momentul sesizării sau autosesizării organului competent despre pregătirea sau săvârșirea unei infracțiuni."</i> Se recomandă excluderea normei.	consimțământului scris al acestuia, și nu în situațiile descrise de CNA. Mai mult, o procedură similară de eliberare a mandatului judecătoresc este prevăzută de art. 57 din Legea Concurenței nr. 183 din 11.07.2012.
		art.92	19. De asemenea, sancțiunile pecuniare prevăzute la art.92 în mărime de până la 250 000 EURO și respectiv, 5000 000 EURO, pentru încălcarea prevederilor Legii privind protecția datelor cu caracter personal sunt excesive și nu sunt bine determinate, în ce cazuri urmează a fi aplicate aceste sancțiuni, lăsând loc de interpretare și se aplică la discreția conducerii Centrului, ceea ce ar genera sancționarea neuniformă în cazuri similare. Mai mult, nota informativă nu cuprinde argumente viabile cu referire la sumele invocate, nefiind prezentate careva date din care să rezulte cuantumul stabilit, un calcul estimativ care denotă stabilirea anume a acestor sume și nu mai mici. Argumentul autorului precum că <i>„se propune un mecanism treptat de aplicare a sancțiunilor pentru a asigura o perioadă de tranziție în vederea adoptării de către operatorii de date la noile rigori și standarde europene”</i> nu constituie temei de stabilirea unor astfel de sume cu titlu de sancțiune pecuniară. Se recomandă excluderea normei.	Nu se acceptă. Urmează a menționa că noul Regulament 2016/679, la art. 83 prevede dreptul autorităților naționale de supraveghere de a aplica amenzi administrative. La moment se constată ineficiența măsurilor punitive în vigoare, care se manifestă prin caracterul îndelungat al examinării de către instanțele de judecată a cauzelor contravenționale pornite de Centru. Mai mult, soluționarea cauzelor contravenționale prin recunoașterea vinovăției contravenienților și sancționarea acestora în limitele prevăzute la art. 74¹-74³ Cod contravențional, se rezumă la constatarea de către instanța de judecată a faptelor contravenționale comise, fără a dispune obligarea contravenientului în vederea înlăturării cauzelor ce au dus la comiterea încălcărilor vizate. Într-o altă ordine de idei, urmează a menționa că noul Regulament 2016/679, la art. 83 prevede dreptul autorităților naționale de supraveghere de a aplica amenzi administrative.

				De altfel, în prezent art. 34 din Codul contravențional limitează cuantumul maxim al amenzilor pasibil a fi aplicate. Totodată, ținând cont de realitățile din Republica Moldova, în proiectul vizat se propune un mecanism treptat de aplicare a sancțiunilor pentru a nu împovăra operatorii de date și a le permite să se adapteze noilor rigori europene. Într-o altă ordine de idei, trebuie de menționat că în Republica Moldova există practici când autoritățile de control pot impune prin decizia sa sancțiuni pecuniare cum ar fi spre exemplu Consiliul concurenței, Banca Națională a Moldovei, CNPF. Nu în ultimul rând, urmează a remarca că în ordinea Legii cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, în cazul nerespectării prevederilor prezentei legi și ale actelor subordonate acestei legi, față de entitățile raportoare se aplică sancțiuni pecuniare sub formă de amendă: – în mărime dublă din valoarea beneficiului rezultat din încălcarea obligațiilor prevăzute de prezenta lege, în cazul în care beneficiul respectiv poate fi stabilit, sau în mărimea echivalentului în lei al sumei de pînă la 1000000 de euro, calculat conform cursului oficial al leului moldovenesc la data comiterii încălcării; – în mărime de pînă la echivalentul în lei al sumei de 5000000 de euro, calculat la cursul oficial al leului moldovenesc la data comiterii încălcării, sau 10% din cifra de afaceri pentru anul precedent – pentru entitățile raportoare de la art. 4 alin. (1) lit. a), c), h) și i).
II	Agencia Națională pentru Reglementare în Comunicații		Lipsa de obiecții și propuneri	

	Electronice Tehnologia Informației	și			
III	Serviciul Informații Securitate	de și	De ordin general	În conformitate cu prevederile art. 34 alin. (1) din Legea nr. 780/2001 privind actele legislative, <i>modificarea sau completarea actului legislativ reprezintă amendarea unor prevederi ale lui</i>. Totodată, examinînd redacția nouă a Legii nr. 133/2011 privind protecția datelor cu caracter personal, constatăm că autorul de fapt propune o nouă lege și nu modifică legea existentă, or conceptul „noi redacții” este substanțial diferit de redacția actuală a Legii. În acest context, urmează a promova proiectul unei legi noi, ce va abroga Legea nr. 133/2011, și nu de a expune legea veche „în redacție nouă”. La lit. a) sintagma „inclusiv informațiilor care consemnează date cu caracter personal atribuite la secret de stat”, iar la lit. d) sintagma „securității de stat și securității naționale și în cadrul dosarului sau acțiunilor speciale de investigație” de exclus. Totodată, de completat alin. (3) cu o literă nouă cu următorul conținut: „d) prelucrării datelor cu caracter personal atribuite la secret de stat în modul stabilit”. a). Deși, potrivit preambulului Legii nr. 133/2011, în redacție nouă, aceasta pune în aplicare prevederile Convenției nr. 108 și Regulamentelor (UE) 2016/679 și 2016/680 ale Parlamentului European și al Consiliului, totuși proiectul nu ține cont de anumite norme prevăzute în aceste acte internaționale. Astfel, prevederile care propunem a fi excluse, contravin art. 9 alin. 2 lit. a) din Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal din 28.01.1981, care stabilește	Se va lua în considerare propunerea întru respectarea normelor de tehnică legislativă. Nu se acceptă Din start, ținem să menționăm că SIS a omis faptul că pe lângă Regulamentul (UE) 2016/679, în anul 2016 Parlamentul European și Consiliul a adoptat pachetul de reformă legislativă privind protecția 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 inclusiv: 1. Directiva (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 urmăririi penale a infracțiunilor sau

			expres derogarea de la regimul juridic al datelor cu caracter personal în cazul prelucrării acestora pentru <u>apărarea securității statului, siguranței publice, în interesul sistemului monetar al statului sau represiunea infracțiunilor penale.</u> De asemenea, normele invocate nu corespund nici Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE. Astfel, pct. (16) din preambul expres menționează că, <u>prezentul regulament nu se aplică chestiunilor de protecție a drepturilor și libertăților fundamentale sau la libera circulație a datelor cu caracter personal referitoare la activități care nu intră în domeniul de aplicare al dreptului Uniunii, de exemplu activitățile privind securitatea națională.</u> Concomitent, menționăm că domeniul de aplicare al legii nu corespunde întru totul domeniului de aplicare al Regulamentului, în special prevederilor art. 2 alin. (2) lit. a) și d). În acest sens menționăm că art. 1 din Legea nr. 245 din 27 noiembrie 2008 cu privire la secretul de stat, definește secretul de stat ca <i>informații protejate de stat în domeniul apărării naționale, economiei, științei și tehnicii, relațiilor externe, securității statului, asigurării ordinii de drept și activității autorităților publice, a căror divulgare neautorizată sau pierdere este de natură să aducă atingere intereselor și/sau securității Republicii Moldova.</i> Astfel, regimul juridic al secretului de stat face parte din conceptul general de asigurare a securității naționale. În condițiile date, constatăm că reglementările internaționale exclud aplicabilitatea regimul juridic al protecției datelor cu caracter personal asupra secretului de stat. În consecință, se impune necesitatea	<i>al executării pedepselor și privind libera circulație a acestor date și de abrogare a Deciziei-cadru 2008/977/JAI a Consiliului;</i> 2. 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. În acest sens, ținem să menționăm că în conformitate Articolul 1 - Obiect și obiective din Directiva (UE) 2016/680, Prezenta directivă stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, <u>inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora.</u> „Autoritate competentă” înseamnă: (a) <i>orice autoritate publică competentă în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor sau de executare a pedepselor, inclusiv în materie de protejare împotriva amenințărilor la adresa securității publice și de prevenire a acestora; sau</i> (b) <i>orice alt organism sau entitate împuternicit(ă) de dreptul intern să exercite autoritate publică și competențe publice în scopul în prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora.</i> În aceste condiții, nu s-a putut reține argumentarea precum că domeniul de aplicare al legii nu corespunde
--	--	--	--	---

		reglementării similare și în legislația Republicii Moldova. Acceptarea redacției din proiect ar crea și un conflict cu privire la aplicabilitatea legii. Or, datele cu caracter personal atribuite la secret de stat ar trebuie să se subordoneze atât regimului juridic instituit de Legea prenotată, precum și regimului juridic instituit de Legea nr. 245-XVI din 27 noiembrie 2008 cu privire la secretul de stat și altor acte normative în domeniul protecției secretului de stat, ceea ce creează pericole iminente de divulgare și/sau scurgere a informațiilor atribuite la secret de stat. În acest context, menționăm că regimul juridic de protecție a secretului de stat are menirea de a asigura interesele întregii societăți, iar datele cu caracter personal vizează doar o persoană concretă, în acest caz, interesul general prevalând asupra interesului personal. Este de menționat faptul că în cadrul Conferinței din 5 iulie 2016 cu privire la Prezentarea opiniilor și recomandărilor experților Consiliului Europei cu privire la modificările cadrului legal privind protecția datelor cu caracter personal al Republicii Moldova, majoritatea experților internaționali au menționat că protecția informației atribuite la secret de stat, precum și domeniul securității naționale nu cade sub incidența reglementărilor internaționale de protecția a datelor cu caracter personal, decizia aparținând fiecărui stat în parte. De asemenea, aceștia au punctat că în majoritatea statelor din cadrul UE, aceste două mari domenii sunt exceptate de la reglementarea legislației de protecție a datelor cu caracter personal. Totodată, în scopul evitării unor eventuale abuzuri, propunem completarea art. 2 cu un alineat nou, (4), care ar institui garanții împotriva prelucrării neîntemeiate a datelor cu caracter personal atribuite la secret de stat, cu următorul conținut.	întru totul domeniului de aplicare al Regulamentului, în special prevederilor art. 2 alin. (2) lit. a) și d). Context în care, urmează a fi reliefate la moment următoarele prevederi în vigoare și de aplicare ale Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal: Articolul 2 alin. (2) lit. d) - domeniul de acțiune al acestei legi se extinde asupra prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale în condițiile legii Mai mult, Centrul a stabilit în corespundere cu GDPR, la art. 2 alin. (3) lit. b) că domeniul de acțiune al prezentei legi nu se extinde asupra prelucrării datelor cu caracter personal în cadrul activității informative (spionaj) și contrainformative (contraspionaj), agentura și sursa de informații, în condițiile legii.
--	--	--	--

		„ (4) <i>Mecanismul de evidență și control al prelucrării datelor cu caracter personal menționate la alin. (3) lit. d) al prezentului articol se stabilește prin act normativ departamental. După desecretizarea informațiilor, acestora li se aplică regimul juridic general de protecție a datelor cu caracter personal.</i>” b). Concomitent, respingerea propunerilor înaintate în prezentul aviz va denatura și conceptul de protecția a datelor cu caracter personal în cadrul activității speciale de investigații. Astfel, la adoptarea Legii nr. 59/2012, legiuitorul a creat mecanismul de protecție a informațiilor, inclusiv a datelor cu caracter personal, avînd în vedere specificul acestei activități. La art. 5 alin. (2) din Legea menționată este stabilit că „<i>accesul la dosarul special sau la materialele din dosar al altor persoane decît cele care investighează dosarul special este interzis, cu excepția conducătorului subdiviziunii specializate a organului respectiv, în limitele competenței, și a procurorului care a autorizat măsura specială de investigații sau a solicitat autorizarea acesteia de către judecătorul de instrucție, precum și cu excepția judecătorului de instrucție care a autorizat măsura specială de investigații.</i>” În același timp, ofițerului de investigații îi este impusă direct obligația de a respecta confidențialitatea datelor cu caracter personal ce au devenit cunoscute în timpul efectuării măsurii speciale de investigații (art. 11 lit. f) Legea nr.59/2012). De asemenea, art. 4 alin. (1) din Legea nr.59/2012, expres stabilește că „<i>orice persoană supusă măsurii speciale de investigații are dreptul să fie informată, după efectuarea acesteia, de către procuror sau de către judecătorul de instrucție care a autorizat măsura...</i>”. Concomitent, mecanismul de culegere,	Nu se acceptă Reiterăm că Directiva (UE) 2016/680 statuează sarcini, atribuții și garanții de care trebuie să dispună autoritatea națională de supraveghere a prelucrării datelor cu caracter personal, și anume: - Fiecare stat garantează că autoritatea sa de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor și exercitarea
--	--	---	--

		transmitere și gestionare a informațiilor, inclusiv a datelor cu caracter personal, reglementat de către Legea dată, creează un sistem integru de garanții pentru protecția informației respective. În acest context, este notoriu că Legea nr. 59/2012 respectă standardele de protecție a datelor cu caracter personal stabilite în Directiva (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 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. De asemenea, în cazul operării completării propuse în proiectul avizat, organele de ocrotire a normelor de drept, inclusiv organul de stat specializat în domeniul asigurării securității statului, vor fi obligate să informeze Centrul Național pentru Protecția Datelor cu Caracter Personal despre categoriile de date prelucrate, să fie supuse controlului de către Centru, alte interacțiuni cu CNPDCP prevăzute de Legea nr. 133/2011. Acest fapt, însă, contravine prevederilor Legii nr. 59/2012, or Centrul Național pentru Protecția Datelor cu Caracter Personal nu are competența de a controla sau monitoriza activitatea specială de investigații. Eventuala completare propusă în proiect, nu va genera nimic altceva decât o neclaritate în procesul de asigurare a protecției datelor cu caracter personal în cadrul activității speciale de investigații. Totodată, este necesar de a stabili că, prin prisma verificării protecției datelor cu caracter personal, angajații Centrului vor cunoaște formele, tactica, metodele, mijloacele și rezultatele	competențelor care le revin în conformitate cu prezenta directivă (art. 42 alin. (1)). - Statele garantează că membrii autorităților lor de supraveghere, în îndeplinirea sarcinilor și în exercitarea competențelor care le revin în conformitate cu prezenta directivă, rămân independenți de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la nimeni (art. 42 alin. (2)). - Fiecare stat garantează prin lege că autoritățile sale de supraveghere îi revin competențe de consiliere efective pentru a oferi consiliere operatorului și de a emite avize, din proprie inițiativă sau la cerere, parlamentului național, guvernului sau, în conformitate cu dreptul său intern, altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal. Mai mult, remarcăm art. 58 din noul Regulament 2016/679 prevede competențele de investigație a autorităților de supraveghere a protecției datelor cu caracter personal prevede, inclusiv următoarele competențe: a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale; e) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale; f) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de
--	--	---	---

			activității speciale de investigații desfășurată în cadrul dosarelor speciale, în particular cele ce vizează securitatea statului, fapt care excede competența unei autorități civile a statului. În acest sens menționăm că completările introduse la art. 5 din Legea nr. 59/2012 prin Legea nr. 87 din 28.04.2016, vizează doar păstrarea confidențialității datelor respective în conformitate cu prevederile Legii nr.133 din 8 iulie 2011 și nicidecum nu derogă de la normele speciale ce stabilesc modalitatea de gestionarea a informației din dosarele speciale și de control asupra activității speciale de investigații realizat de către Procuratură.	prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern. Reiterăm că, clauza legală ce reglementează prelucrarea datelor cu caracter personal în sectorul polițienesc a fost instituită la art. 2 alin. (2) lit. d) Legea nr. 133, în formularea domeniul de acțiune al acestei legi se extinde asupra prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale în condițiile legii. În acest context, este de menționat că la 28 aprilie 2016 a fost adoptată Legea nr. 87 (publicată în Monitorul Oficial nr. 156/306 din 07.06.2016) prin care au fost operate modificări/completări la un șir de legi, fiind înserate dispoziții legale ce vizează prelucrarea datelor cu caracter personal în sectorul polițienesc, după cum urmează: 1.Cod de procedură penală. Art. 15 alin. (2) stipulează că la efectuarea acțiunilor procesuale nu poate fi acumulată fără necesitate informație despre viața privată și intimă a persoanei. La cererea organului de urmărire penală și a instanței de judecată, participanții la acțiunile procesuale sînt obligați să nu divulge asemenea informații și despre aceasta se ia un angajament în scris. <u>Prelucrarea datelor cu caracter personal în cadrul procesului penal se efectuează în conformitate cu prevederile Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal.</u> 2. Legea nr. 59 din 29.03.2012 cu privire la activitatea specială de investigație. Art. 5 alin. (1), persoanele care au acces la datele cu caracter personal ale persoanei supuse măsurii speciale
--	--	--	--	--

				de investigații sînt obligate să păstreze confidențialitatea datelor respective în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. 3. Legea nr. 320 din 27.12.2012 cu privire la Poliție și statutul polițistului Art. 16 alin. (3), prelucrarea, transmiterea și distrugerea datelor cu caracter personal deținute de Poliție se efectuează în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. 4. Legea nr. 1104 din 06.06.2002 cu privire la Centrul Național Anticorupție Articolul 6 lit. m), să prelucreze date cu caracter personal, inclusiv în scop de analiză informațională și strategică, în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. Aavînd în vedere specificul legislației Republicii Moldova, în special, codificarea normelor de procedură penală și rigiditatea activității speciale de investigații, este necesară intervenția pentru a asigura o sincronizare în materie de protecție a datelor cu caracter personal. În același context, se notează că Parlamentul Republicii Moldova prin Legea comunicațiilor electronice, nr. 241-XVI din 15 noiembrie 2007, republicată în Monitorul Oficial din 17 noiembrie 2017, a atribuit Centrului în temeiul art. 71 noi competențe de a verifica măsurile tehnice și organizatorice corespunzătoare în vederea protejării securității serviciilor prestate de furnizorii de servicii de comunicații electronice. Subsecvent, remarcăm prevederile Legii cu privire la prevenirea și combaterea spălării banilor și finanțării
--	--	--	--	--

				terrorismului în partea ce vizează controlul conformității operațiunilor de prelucrare a datelor cu caracter personal efectuate de autoritățile specializate în prevenirea și combaterea terorismului, inclusiv a Serviciului Prevenirea și Combaterea Spălării Banilor. Eset necesar a remarca că acțiunile ce urmează a fi întreprinse de entitățile vizate în prezenta lege presupun prelucrarea unui volum exorbitant de date cu caracter personal și se răsfrânge asupra tuturor persoanelor fizice, chiar și care au avut o tangență mică cu instituțiile financiar-bancare, dar nu numai. O altă lege care a adus atribuții noi Centrului este Legea nr. 120 din 21 septembrie 2017 cu privire la prevenirea și combaterea terorismului. Activitatea de prevenire și combatere a terorismului va fi exercitată în mod special de Serviciul de Informații și Securitate care prelucerează un volum extrem de mare de date personale, iar controlul conformității prelucrărilor de date cu caracter personal se efectuează de către Centru. <i>Prin spectrul de modificări legislative arătat supra, Centrul a dobândit competență de a investiga prelucrarea datelor cu caracter personal atribuite inclusiv la secret de stat etc. Astfel, Capitolul VII din prezentul proiect de lege, este destinat prelucrării datelor cu caracter personal de către operatori - organe de ocrotire a legii, care au competențe stabilite prin lege în scopul prevenirii, investigării, depistării și/sau urmăririi penale a infracțiunilor sau executării pedepselor penale, inclusiv protejarea și prevenirea amenințărilor la adresa ordinii publice, securității de stat și securității naționale și în cadrul dosarului sau acțiunilor speciale de investigație.</i> <i>Un alt element important care a contribuit la cristalizarea competențelor Centrului de a efectua operațiuni de investigație a prelucrării datelor cu</i>
--	--	--	--	---

				<i>caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, al punerii în aplicare a sentințelor de condamnare sau al altor acțiuni ce țin de procedura penală ori contravențională, în condițiile legii, îl reprezintă Ghidul practic privind utilizarea datelor cu caracter personal în sectorul polițienesc, adoptat de către Comitetul Consultativ al Convenției 108 pentru protecția persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal, adoptat la data de 15 februarie 2018 la Strasbourg.</i>
IV	Ministerul Afacerilor Interne	De ordin general	Se propune, ținând cont de faptul că autorul proiectului actului normativ propune amendarea doar a Legii nr. 133 din 08 iulie 2011 cu privire la protecția datelor cu caracter personal, se impune revizuirea titlului proiectului de lege pentru modificarea și completarea unor acte legislative. Or, modificarea și completarea unor acte legislative, impune amendarea a două și mai multe proiecte de legi.	Se va lua în considerare propunerea întru respectarea normelor de tehnică legislativă.
V	Ministerul Economiei și Infrastructurii	De ordin general	Se propune ajustarea Notei Informative reieșind din faptul că Legea nr. 131/2011 se prezintă în redacție nouă și urmărește armonizarea cadrului juridic la rigorile europene, dat fiind că în Nota Informativă, autorul menționează despre necesitatea actualizării Legii nr. 133 din 08.07.2011, privind protecția datelor cu caracter personal urmare adoptării pachetului de acte europene privind protecția datelor cu caracter personal de către Parlamentul și Consiliul european (Regulamentul UE 2016/679; Directiva UE 2016/680; Directiva UE	Se va lua în considerare propunerea întru respectarea normelor de tehnică legislativă.

			2016/681 cu abrogarea Directivei 65/46/CE și Deciziei 20058/977/JAI. Se recomandă ca proiectul să fie prezentat spre avizare în formă de proiect de Lege cu privire la protecția datelor cu caracter personal în redacție nouă, cu abrogarea ulterioară a Legii actuale (nr. 133/2011), reieșind din importanța și caracterul general de aplicare a legii respective, respectându-se astfel principiul consecutivității al legiferării (art. 4, litera b) din Legea nr. 780 din 27.12.2001 privind actele legislative. Consecutiv, urmare adoptării Legii în redacție nouă, va urma modificarea cadrului juridic secundar în conformitate cu prevederile Legii noi. Deasemenea, se remarcă că în conformitate cu prevederile art. 63 alin.(1) ale Legii nr. 100 din 12.12.2017 cu privire la actele normative, care va intra în vigoare la data de 12.07.2018, în cazul în care proiectul actului normativ de modificare schimbă concepția generală ori caracterul unitar al actului, acesta urmează a fi înlocuit cu un act nou, urmînd a fi abrogat în întregime. Conform art. 21 lit. d) al Legii 100/2017, în cazul în care actul normativ este armonizat cu legislația comunitară, întru asigurarea compatibilității acestuia cu normele legislației Uniunii Europene, proiectul urmează a fi însoțit de tabelul de concordanță.	Se acceptă. Declarațiile de compatibilitate asupra proiectului au fost recepționate.
		Art. 3	Cu referire la art. 3 al proiectului Legii cu privire la protecția datelor cu caracter personal, în definițiile noțiunilor de "categorie obișnuită de date cu caracter personal", "prelucrarea datelor personale" și "sistem de evidență", autorul menționează că procesul de prelucrare a datelor personale nu se limitează doar la: nume, prenume, patronimic, nr. de identificare, etc. În acest context, sintagma "<u>nu se limitează</u>", lasă loc de	Se acceptă parțial. Autorul proiectului este în imposibilitate să identifice exhaustiv în acest caz și/sau în tot textul proiectului toate categoriile de date cu caracter personal, toate operațiunile de prelucrare a datelor cu caracter personal, toate sistemele de evidență. Autorul nu poate cuprinde și nu poate specifica în definiția noțiunilor date un domeniu atît de vast precum e prelucrarea

			interpretare, or procedurile suplimentare de prelucrare a datelor cu caracter personal pot să afecteze /să lezeze drepturile la viața privată ale persoanelor fizice. Prin urmare, se consideră relevantă reconsiderarea sintagmei în cauză prin concretizarea sensului, ori aceasta urmează a fi exclusă din text.	datelor cu caracter personal, care este specific fiecărui sector în parte fie privat sau public, fiecărui domeniu, or, cu ajutorul sintagmei "nu se limitează la", autorul prevede anume categorii care nu pot fi cuprinse de lege. Cu privire la procedurile suplimentare de prelucrare a datelor cu caracter personal, care ar putea afecta/leza drepturile la viața privată ale persoanelor fizice, CNPDCP a prevăzut căi de reglementare, astfel operatorul urmează să coordoneze cu Centrul crearea sistemului informațional, notifică sisteme noi prin care se prelucrează date cu caracter personal, iar prin sesizările primite de la cetățeni CNPDCP, poate identifica cu ușurință abaterile „în masa”, cu emiterea în acest sens a deciziilor obligative. Noțiunea de "<i>prelucrarea datelor personale</i>" a fost transpusă întocmai din Regulamentul UE 2016/679.
		Art. 30 alin.(5) lit. f)	Sintagma „orice alte informații solicitate de Centru” este incertă și interpretativă, astfel considerăm oportun după sintagma "orice alte informații solicitate de Centru,, să se completeze cu „în legătură cu prelucrarea datelor cu caracter personal,,.	Se acceptă.
		Art. 92	Se recomandă ca norma privind răspunderea administrativă pentru neîndeplinirea prevederilor legii cu privire la protecția datelor cu caracter personal, normele care prevăd sancțiunile contravenționale urmează a fi reflectate în Codul Contravențional al Republicii Moldova.	Nu se acceptă. La moment se constată ineficiența măsurilor punitive în vigoare, care se manifestă prin caracterul îndelungat al examinării de către instanțele de judecată a cauzelor contravenționale pornite de Centru. Mai mult, soluționarea cauzelor contravenționale prin recunoașterea vinovăției contravenienților și sancționarea acestora în limitele prevăzute la art. 74¹-74³ Cod contravențional, se rezumă la constatarea de către instanța de judecată a faptelor contravenționale comise, fără a dispune obligarea contravenientului în

				vederea înlăturării cauzelor ce au dus la comiterea încălcărilor vizate. Într-o altă ordine de idei, urmează a menționa că noul Regulament 2016/679, la art. 83 prevede dreptul autorităților naționale de supraveghere de a aplica amenzi administrative. De altfel, în prezent art. 34 din Codul contravențional limitează cuantumul maxim al amenzilor pasibil a fi aplicate. Totodată, ținând cont de realitățile din Republica Moldova, în proiectul vizat se propune un mecanism treptat de aplicare a sancțiunilor pentru a nu împovăra operatorii de date și a le permite să se adapteze noilor rigori europene. Într-o altă ordine de idei, trebuie de menționat că în Republica Moldova există practici când autoritățile de control pot impune prin decizia sa sancțiuni pecuniare cum ar fi spre exemplu Consiliul concurenței, Banca Națională a Moldovei, CNPF.
		De ordin general	Potrivit alin. (3) din art. 22 al Legii nr. 780 din 27.12.2001 privind actele legislative, proiectul legii în cauză urmează a fi supus, în mod obligatoriu, <i>unei expertize anticorupție</i> din partea Centrului Național Anticorupție pentru a se verifica dacă corespunde standardelor anticorupție naționale și internaționale, precum și pentru a preveni apariția de noi reglementări ce favorizează au pot favoriza corupția.	Expertiza anticorupție cu referire la proiect a fost prezentată către CNPDCP.
VI	Ministerul Finanțelor al RM			
VII	Ministerul Sănătății, Muncii și Protecției Sociale	Art. I	La propunerea de modificare/completare al art. 96 din Legea nr. 133/2011 privind protecția datelor cu caracter personal, se propune modificarea termenului de „30 de zile” în termen de „3 luni”, drept fiind un termen	Pornind de la prevederile considerentului 39) a Regulamentului UE 2016/679 al Parlamentului European și al Consiliului, perioada pentru care datele cu caracter personal sunt stocate este limitată strict la

			mai rezonabil pentru stocarea datelor în contextul relațiilor de muncă.	<u>minimum</u>. În vederea asigurării faptului că datele cu caracter personal nu sunt păstrate mai mult timp decât este necesar, ar trebui să se stabilească de către operator termene pentru ștergere sau revizuirea periodică. Deasemenea, prevederile art. 13 alin.(2) al proiectului dat, specifică că în cazul în care legislația nu prevede în mod expres condițiile și termenele pentru stocarea și utilizarea datelor personale, ele sunt stabilite de către operator . Așadar, proporționalitatea dintre scopul prelucrării și durata de stocare a datelor o stabilește însuși operatorul,(cu aprobarea Centrului), așadar acestuia îi revine sarcina de a justifica termenul rezonabil pentru stocare. Subliniem, că legislația nu prevede în mod expres termenele pentru stocare, iar norma dată nu este una restrictivă, autorul astfel a permis de a stabili desinestătător aceste termene, care urmează să fie adecvate scopului prelucrării.
		Art. III	Articolul III din proiectul de Lege prenotat, care prevede modificarea și completarea Legii nr. 48/2012 privind sistemul de salarizare a funcționarilor publici (Monitorul Oficial al Republicii Moldova, 2012, nr. 63, art. 213) se propune să fie exclus integral din proiect din considerentul că vor fi create discrepanțe vădite în materie de salarizare a funcționarilor publici. În acest sens, se reiterează argumentarea adusă de Curtea Constituțională în Hotărârea nr. 25 din 06 noiembrie 2014 privind controlul constituționalității unor prevederi ale Legii nr. 146 din 17 iulie 2014 pentru modificarea și completarea unor acte legislative (salarizarea funcționarilor publici din cadrul instanțelor judecătorești și a judecătorilor) (<i>Sesizarea nr. 52a/2014</i>)	Nu se acceptă. Actualmente angajații Centrului dispun de un sistem de salarizare net inferior plafonului de salarizare din cadrul autorităților pe care le verifică, dar și în raport cu paleta vastă de atribuții pe care le-a primit, prin mai multe acte normative : Legea comunicațiilor electronice nr. 241-XVI din 15 noiembrie 2007, Legii nr. 120 din 21.09.2017 cu privire la prevenirea și combaterea terorismului, Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului dar și prin prisma noilor modificări a Legii nr. 133 privind protecția datelor cu caracter personal, prin care Centrul va investiga operațiunile de prelucrare a datelor cu caracter personal în cadrul urmăririi penale etc. O determinantă în vederea majorării plafonului de salarizare a angajaților din cadrul Centrului, constă în

			(Monitorul oficial al Republicii Moldova, 2014, nr. 345–351, art. 41).	aceeași politică de salarizare, promovată și implementată în cadrul unor instituții care sunt susceptibile de a fi investigate de către Centru, spre exemplu: Autoritatea Națională de Integritate, Comisia Electorală Centrală, Centrul Național Anticorupție, Serviciul Prevenirea și Combaterea Banilor, Finanțării Terorismului, Serviciul Fiscal de Stat, Serviciul Vamal etc
		De ordin general	Subsidiar, se recomandă ca proiectul să fie revizuit prin prisma rigorilor normelor tehnicii legislative stipulate atât prin Legea nr. 780/2000 din 27 decembrie 2000 privind actele legislative, cât și prin normele Legii cu privire la actele normative nr. 100/2017 din 22 decembrie 2017.	Se acceptă.
	Procuratura Generală	De ordin general	20. Susținem necesitatea ajustării legislației naționale la standardele stabilite de prevederile 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 urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date. Totodată, întru respectarea normelor de tehnică legislativă, considerăm oportun adoptarea unei noi legi și respectiv abrogarea Legii nr.133 din 08.07.2011 privind protecția datelor cu caracter personal, care prin proiectul respectiv se modifică în totalitate.	Se va lua în considerare propunerea întru respectarea normelor de tehnică legislativă.
		Art. 3	21. În noțiunea de „prelucrarea datelor cu caracter personal” nu este clară, sintagma „care se efectuează asupra datelor cu caracter personal, cum ar fi, dar care nu se limitează la: ”, motiv pentru care, propunem a revedea conținutul acestei norme.	Se acceptă. Se transpune întocmai noțiunea din Regulamentul UE 2016/679: <i>Prelucrarea datelor personale - înseamnă orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de</i>

			Considerăm necesar excluderea din noțiunea „categoria specială de date cu caracter personale”, prevăzută la a textului „, precum și cele referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale”, în vederea ajustării acestei prevederi la prevederile art. 3 pct.1) al Directivei 2016/680 și asigurării eficiente a activității organelor de ocrotire a legii.	<i>date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea;</i> Nu se acceptă din considerentul că datele personale referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale necesită un nivel mai ridicat de protecție prin aplicarea măsurilor specifice și adecvate pentru a proteja drepturile fundamentale și datele cu caracter personal ale persoanelor fizice. Astfel, se impune necesitatea de a menține sau de a introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea acestor date. Totodată, atât GDPR, cât și Directiva 2016/680 oferă posibilitatea statelor, în anumite situații, de a introduce reglementări speciale. În ce privește prelucrarea datelor personale.
		Art. 6	22. La pct. 80 din preambulului Directivei 2016/680 privind protecția 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 este stipulat că „Statele membre ar trebui, de asemenea, să poată să prevadă faptul că nu este de competența autorității de supraveghere prelucrarea datelor cu caracter personal ale altor autorități judiciare independente care acționează în exercițiul funcției lor judiciare, de exemplu ministerul public. În orice caz, respectarea normelor prezentei directive de către instanțe	Nu se acceptă. Excepția prevăzută de art. 80 din textul Directivei 2016/680 Este redată în art. 6 alin. (4) din prezentul proiect: <i>(4) Centrul nu este în drept să investigheze activitățile instanțelor de judecată atunci când acționează în calitate lor judiciară. Instanțele trebuie să fie considerate acționând în calitate lor judiciară numai de către judecător în cadrul desfășurării procedurilor judiciare cu condiția existenței scopului și temeiului legal al prelucrării, cu excepția situației în care datele personale sunt colectate, dezvăluite sau prelucrate în oricare alt fel de către sau la solicitarea judecătorului</i>

			și alte autorități judiciare independente face întotdeauna obiectul unei supravegheri independente în conformitate cu articolul 8 alineatul (3) din Cartă.”. Urmează a fi menționat și faptul că în varianta originală a Directivei 2016/680 în limba engleză „ministerul public” este denumit „public prosecutor’s office”, adică „Procuratura”. Reglementări similare regăsim și la art.45 alin.(2) al Directivei 2016/680, care prevede că „...Statele membre pot să stabilească dispoziții potrivit cărora autorităților sale de supraveghere nu le revine competența să supravegheze operațiunile de prelucrare ale altor autorități judiciare independente atunci când acestea acționează în exercițiul funcției lor judiciare”. Mai mult, la pct.82 din același act normativ este menționat că „...competențele acestora (autorității de supraveghere) nu ar trebui să afecteze normele speciale de procedură penală, inclusiv cele referitoare la investigarea și urmărirea penală a infracțiunilor, sau independența justiției.”. Totodată, potrivit art. 1 al Legii cu privire la Procuratură nr. 3 din 25.02.2016, „Procuratura este o instituție publică autonomă în cadrul autorității judecătorești ...”. Astfel, pentru racordarea prevederilor proiectului de lege la standardele stabilite de Directiva 2016/680, considerăm necesar de a completa prevederile art. 6 din proiect cu un alineat nou, alin.(5), care va reglementa excepția, prevăzută de art. 80 din textul Directivei, cu referire la activitatea Procuraturii.	<i>în afara procedurilor judiciare necesare. Activitățile organizatorice și administrative de primire, repartizare, gestionare și stocare a datelor personale nu se consideră a fi acțiuni în calitate lor judiciară.</i> Totodată, considerăm că sintagma „ministerul public” nu în contextul considerentului 80 din Directiva 2016/680 poate fi tradus ca „Procuratura”, deoarece ultima, conform competenței, nu acționează în exercițiul funcției judiciare.
		Art. 58 alin.(4)	23. Propunem completarea, normei de la art. 58 alin.(4) cu următorul text: „, luând în considerare specificul de activitate a organelor de ocrotire a legii.”, așa cum articolul expus în redacția propusă de autorii proiectului nu poate fi acceptată, deoarece nu coroborează cu prevederile Directivei 2016/680, poate genera abuzuri	Se acceptă. Art. 58 alin. (4), la final s/a completat cu propoziția: „Centrul va ține cont de caracterul specific al activității acestor autorități.”

			din partea angajaților Centrului și ar putea avea efecte negative asupra activității organelor de ocrotire a legii.	
		Art. 59 alin.(2)	24. Reieșind din specificul activității organelor de ocrotire a legii, considerăm necesar de a completa art. 59 alin.(2) din proiect cu următorul text, „și/sau prelucrarea este necesară și proporțională cu acest alt scop în conformitate cu prevederile legii.”.	Urmare a revizuirii normei alin. (2) din art. 59 a fost exclus.
		Art.60	25. Art.60 a proiectului, conține reglementările ce prevăd obligația de revizuire periodică a necesității de stocare a datelor, „dar nu mai puțin de odată pe an”, considerăm excesivă această prevedere și propunem excluderea ei, întrucât Directiva 2016/680 nu stabilește careva termeni în acest sens.	Se acceptă. Sintagma „dar nu mai puțin de odată pe an” a fost exclusă.
		Art.61	26. La art.61 din proiect este necesar de a se specifica, că obligația de a face distincția dintre diferite categorii de subiecți de date se va efectua „acolo unde este posibil, sau pe cât este de posibil”, pentru coroborarea acestei norme cu prevederile art.7 al Directivei 2016/680, dar și pentru asigurarea bunei funcționări a organelor de ocrotire a legii, reieșind din specificul activității organelor de ocrotire a legii.	Se acceptă.
		Art. 62 alin.(1)	27. Din motivele expuse la pct. II. 7 (pct. 26) din aviz, propunem completarea art. 62 alin.(1) din proiect cu sintagma „acolo unde este posibil, sau pe cât este de posibil”.	Se acceptă.
		Art. 65 alin.(3)	28. Din motivele expuse la pct. II. 5, II.7 din aviz, considerăm necesar de a completa art. 65 alin.(3) din proiect cu textul „luând în considerare specificul de activitate a organelor de ocrotire a legii.”.	Nu se acceptă, din considerentul că sintagma „facilitează”, utilizată în această normă nu impune organelor de ocrotire a legii o obligație, oferindu-le posibilitatea restrîngerii drepturilor subiectului de date, în condițiile în care aceasta este justificată și constituie o măsură necesară.
		Art. 66	29. Propunem excluderea prevederii art. 66 a proiectului, care impune obligația operatorului de a pune la dispoziția subiectului de date, informațiile ce țin de prelucrarea datelor personale, din motiv că prevederile respective	Nu se acceptă. Persoanele fizice ar trebui 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

			intră în contradicție cu prevederile art. 4 alin.(1) lit. a) din proiect, care prevede că „...cerința de transparență nu se aplică prelucrării efectuate de autoritățile de ocrotire a legii...”.	exercite drepturile respective. În acest sens, însăși Directiva 2016/680 garantează prin art. 12-18 drepturile subiectului de date, inclusiv referitor la informațiile puse dispoziția persoanelor vizate. În contextul celor invocate remarcăm că art. 66 în alin. (3) din prezentul proiect prevede cazurile în care operatorul poate amâna, restricționa sau omite furnizarea de informații către subiectul de date –astfel, fiind redată condițiile în care nu se aplică cerința de transparență prevăzută la art. 4 alin.(1) lit. a) din proiect.
		Art. 73 alin.(2)	30. Considerăm necesar de a exclude din conținutul art. 73 alin.(2) textul „și legătura de cauzalitate dintre subiectul de date, calitatea acestuia și operațiunile efectuate”, precum și alin.(3), întrucât reglementările respective exced prevederile art.8 alin.(2) a Directivei 2016/680, sunt abuzive și ar putea genera abuzuri din partea angajaților Centrului. Este de menționat că, cadrul juridic existent conține reglementări ce se referă la modalitățile de restabilire a drepturilor și libertăților persoanei. Astfel, orice persoană poate contesta la procuror acțiunile, inacțiunile și actele organului de urmărire penală și ale organului care exercită activitate specială de investigații, în ordinea art. 298-2992 Cod de procedură penală, iar, în caz că nu este de acord cu rezultatul examinării plângerii sale de către procuror sau nu a primit răspuns la plângerea sa de la procuror în termenul prevăzut de lege, este în drept de a se adresa judecătorului de instrucție în baza art.313 Cod de procedură penală.	Nu se acceptă. Pentru a putea răspunde la plîngerile reclamanților Centrul trebuie să dispună de elemente de răspuns precise și cuprinzătoare, care urmează să fie furnizate de organul de ocrotire a legii. Asta nu înseamnă că se transmite dosarul complet al unei sau altei investigații, ci doar se oferă Centrului un răspuns analitic, precis și succint la întrebările adresate, cu descrierea datelor personale prelucrate, scopul, temeiul legal și legătura de cauzalitate dintre subiectul de date, calitatea acestuia și operațiunile efectuate. Reiterăm faptul că, potrivit Directivei 2016/680 statele membru garantează prin lege că autorității sale de supraveghere îi revin competențe de investigare efective. Respectivele competențe includ, cel puțin, competența de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal care sunt prelucrate și la toate informațiile necesare pentru îndeplinirea sarcinilor sale. Totodată, subliniem faptul că, CNPDCP nu urmărește scopul de a interveni în activitatea organelor de ocrotire a legii, ci de a efectua controlul legalității prelucrării datelor cu caracter personal ale subiectului de date de

				către entități, în calitate de operatori de date cu caracter personal, care au obligația de a asigura confidențialitatea și securitatea datelor cu caracter personal prelucrate.
		Art.74	31. Art.74 din proiect conține reglementări privind ținerea excepțiilor și înregistrarea acestora, este de menționat că Directivei 2016/680 nu conține asemenea norme, totodată, nota informativă aferentă proiectului de lege nu face claritate în acest sens și nu motivează în nici un fel oportunitatea operării acestor modificări, astfel, considerăm oportun excluderea articolului respectiv.	Din practică s-a constatat că în pofida faptului că organul de ocrotire a legii în temeiul art. 15 din Legea nr. 133/2011 aplică restricții drepturilor subiecților de date prevăzute la art. 12-14 , deținătorii sistemelor informaționale de stat, spre exemplu Agenția Servicii Publice nu sunt informați despre acest fapt și furnizează informații subiectului de date referitor la accesările efectuate în privința sa de organul de ocrotire a legii. În aceste circumstanțe rezumă obligația organului de ocrotire a legii, precum și a Centrului în cazul în care este sesizat de subiect, de a informa ultimul despre scopul și temeiul legal al prelucrării, fiind prejudiciată activitatea organelor de ocrotire a legii. Potrivit raționamentelor GDPR cât și Directivei (UE) 2016/680, statele membre ar trebui să aibă posibilitatea de a adopta măsuri legislative în vederea amânării, a restricționării sau a omiterii informării persoanelor vizate sau în vederea restricționării, integrale sau parțiale, a accesului la datele lor cu caracter personal, în măsura în care și atât timp cât o astfel de măsură constituie o măsură necesară și proporțională într-o societate democratică, ținând seama în mod corespunzător de drepturile fundamentale și de interesele legitime ale persoanei fizice în cauză, pentru a se evita obstrucționarea cercetărilor, a anchetelor sau a procedurilor oficiale sau judiciare, pentru a nu se afecta prevenirea, investigarea, depistarea sau urmărirea penală a infracțiunilor sau executarea pedepselor, pentru a se apăra securitatea publică sau securitatea națională ori pentru a se apăra drepturile și libertățile altor persoane.

				În cazul în care operatorul refuză unei persoane vizate drepturile acesteia la informare, acces ori la rectificarea sau ștergerea datelor cu caracter personal sau la restricționarea prelucrării, persoana vizată ar trebui să aibă dreptul de a solicita ca autoritatea națională de supraveghere să verifice legalitatea prelucrării. Persoana vizată ar trebui să fie informată cu privire la acest drept. În situația descrisă mai sus, dat fiind că, deținătorul sistemului informațional de stat nu a fost informat inițial despre faptul că în privința subiectului de date fost aplicate prevederile art. 15 alin. (1) din Legea privind protecția datelor cu caracter personal, iar ulterior se invocă aplicarea prevederilor art. 212 alin. (2) Cod de procedură penală și prevederile art. 2 alin. (2) lit. d) din Legea privind protecția datelor cu caracter personal, Centrul a venit cu soluția propusă în art. 74 din prezentul proiect. Atunci când autoritatea de supraveghere acționează în numele persoanei vizate, persoana vizată ar trebui să fie informată de către autoritatea de supraveghere cel puțin cu privire la faptul că toate verificările sau revizuirile necesare au fost efectuate de către autoritatea de supraveghere.
		Art. 78-79	32. Considerăm oportun de a substitui cuvântul „cerere”, utilizat la art. 78-79 din proiect, cu cuvântul „plângere”, întrucât noțiunea cerere semnifică o solicitare, iar cuvântul plângere reprezintă o contestare a unei pretense încălcări.	Nu se acceptă, pentru a nu se confunda cu petiția.
		Art. 83 alin.(3)	33. Art. 83 alin.(3) din proiect, prevede că „inspectorul de protecție, subiectul de date sau alte persoane, care în virtutea drepturilor și atribuțiilor ce le revin în temeiul	Nu se acceptă. Asigurarea garanțiilor este condiționată de specificul autorității, care este o contrabalantă, aceasta fiind în drept să verifice legalitatea

			prezentei legi, au luat cunoștință sau le-au devenit cunoscute informațiile din cadrul investigației nu pot fi audiați sau interogați de către alte organe sau organizații în ceea ce privește esența informațiilor din cadrul investigației, cu excepția instanței de judecată.”. Aceste prevederi sunt excesive și creează impedimente desfășurării urmăririi penale eficiente, or cauza este transmisă în instanță de către procuror doar după ce se constată că urmărirea penală este completă și există probe suficiente și legal administrate, iar în vederea colectării acestora, organul de urmărire penală și procurorul sunt împuterniciți cu atribuții de audiere a persoanelor.	operațiunilor de date cu caracter personal în diferite domenii, inclusiv în domeniul penal în această situație riscul intimidării angajaților urmează a fi diminuat prin garanții suficiente. Prin normele în cauză se urmărește scopul asigurării unor garanții suficiente, pentru angajații Centrului în partea ce ține de executarea în deplină independență și fără posibilitate de intimidare sau intervenție, inclusiv din partea organelor de drept a atribuțiilor sale.
		Art.89 alin. (6)	34. Prin prevederea de la art.89 alin. (6) din proiect, se propune stabilirea termenului obligatoriu de judecare a cererilor de contestare a deciziilor Centrului (2 luni de la data depunerii cererii), fără a se ține cont de faptul că termenii de examinare sunt clar stipulați prin Legea contenciosului administrativ, Codul de procedură civilă și Codul de procedură penală. În acest context, constatăm stabilirea disproporționată în proiect a diferitor termeni excesiv de mici în cazul drepturilor operatorilor și exagerat de mari în privința Centrului, care, în opinia noastră, urmează a fi revăzuți.	Nu se acceptă. Este un termen ce are drept scop de a nu tergiversa examinarea cererilor de contestare a deciziilor Centrului. Termenii stabiliți proiect sunt în strictă corespundere cu cei stabiliți în GDPR. În aceste condiții, ținem să atragem atenția că acești termeni nu sunt extremi de mari, așa după cum a remarcat Procuratura, or aceștia sunt stabiliți reieșind din complexitatea examinării solicitărilor depuse în adresa Centrului de către operatori sau subiecții de date.
		Art.92	16.1. Art.92 din proiect, care reglementează răspunderea pentru încălcarea Legii privind protecția datelor cu caracter personal, nu se susține, întrucât conține norme ce prevăd aplicarea sancțiunilor pecuniare sub formă de amendă, care sunt niște sancțiuni	Nu se acceptă. Urmează a menționa că noul Regulament 2016/679, la art. 83 prevede dreptul autorităților naționale de supraveghere de a aplica amenzi administrative.

			exorbitante (250.000 euro; 5 00.000 euro), depășind cu mult mărimea sancțiunilor sub formă de amendă stabilite de Legea penală, acordând, totodată, și o discreție exagerată organului de constatare, care din start generează premise pentru diferite abuzuri. Or, conform art.10 Cod contravențional: „Constituie contravenție fapta – acțiunea sau inacțiunea – ilicită, cu un grad de pericol social mai redus decât infracțiunea, săvârșită cu vinovăție, care atentează la valorile sociale ocrotite de lege, este prevăzută de prezentul cod și este pasibilă de sancțiune contravențională”. În acest sens, este relevant de menționat, că art.177 din Codul penal, prevede pentru încălcarea inviolabilității vieții personale pedeapsa maximă de 650 unități convenționale (echivalentul a 32.500 lei). Mai mult, conform art.34 alin.(2) din Codul contravențional „Amenda se aplică persoanelor fizice de la una la 500 de unități convenționale, iar persoanelor cu funcție de răspundere – de la 10 la 1500 de unități convenționale.”. Argumentele autorului, expuse în nota informativă la proiectul de lege, precum că „se constată ineficiența măsurilor punitive în vigoare la moment” nu pot fi susținute, deoarece nu au fost luate în calcul posibilitățile și nivelul economic al populației din Republica Moldova, nivelul salariului minim sau salariului mediu pe economie, rata șomajului etc. Astfel, constatăm că cuantumul amenzilor propuse nu corespund realității din statul unde urmează a fi aplicată și nu sunt în raport cu gradul de pericol social al faptei. Mai mult, în majoritatea cazurilor operatori sunt autoritățile publice, iar achitarea amenzilor urmează a fi efectuată din contul bugetelor instituțiilor publice.	La moment se constată ineficiența măsurilor punitive în vigoare, care se manifestă prin caracterul îndelungat al examinării de către instanțele de judecată a cauzelor contravenționale pornite de Centru. Mai mult, soluționarea cauzelor contravenționale prin recunoașterea vinovăției contravenienților și sancționarea acestora în limitele prevăzute la art. 741-743 Cod contravențional, se rezumă la constatarea de către instanța de judecată a faptelor contravenționale comise, fără a dispune obligarea contravenientului în vederea înlăturării cauzelor ce au dus la comiterea încălcărilor vizate. Într-o altă ordine de idei, urmează a menționa că noul Regulament 2016/679, la art. 83 prevede dreptul autorităților naționale de supraveghere de a aplica amenzi administrative. De altfel, în prezent art. 34 din Codul contravențional limitează cuantumul maxim al amenzilor pasibil a fi aplicate. Totodată, ținând cont de realitățile din Republica Moldova, în proiectul vizat se propune un mecanism treptat de aplicare a sancțiunilor pentru a nu împovăra operatorii de date și a le permite să se adapteze noilor rigori europene. Într-o altă ordine de idei, trebuie de menționat că în Republica Moldova există practici când autoritățile de control pot impune prin decizia sa sancțiuni pecuniare cum ar fi spre exemplu Consiliul concurenței, Banca Națională a Moldovei, CNPF.
--	--	--	---	---

			Subsecvent, potrivit art. 1 alin. (3) al Codului contravențional „Dacă în procesul aplicării unui alt act normativ se constată că prevederile acestuia contravin principiilor stabilite în prezentul cod, se aplică prevederile prezentului cod.”. Proiectul de lege în partea stabilirii sancțiunilor, contravine reglementărilor art.741-743 ale Codului contravențional, creând situația imposibilității de aplicare a sancțiunilor din proiect. În acest sens, este relevantă și hotărârea CtEDO pronunțată în cauza Engel și alții c. Olandei, în care Curtea a trasat câteva criterii de apreciere dacă există „acuză în materie penală”, după cum urmează: a) dacă norma care definește abaterea aparține dreptului penal în sistemul juridic al statului pârât (dacă este incriminată în Codul penal); b) ulterior trebuie examinată natura abaterii; c) în sfârșit, natura și gradul de severitate ale pedepsei care putea fi aplicată persoanei în cauză. Aceste criterii sunt alternative și nu cumulative: pentru că articolul 6 din CEDO să devină aplicabil, este suficient ca abaterea în cauză să fie, prin natura sa „penală” din punctul de vedere al Convenției sau ar trebui să facă persoana în cauză pasibilă de o sancțiune care, datorită naturii sale și gradului de severitate, ține, de obicei, de domeniul „penal.”. Raportând constatările CtEDO în cauza respectivă la prevederile din proiect, constatăm că, faptele pentru a căror săvârșire proiectul prevede posibilitatea aplicării sancțiunilor pecuniare de până la 250 000 EUR sau de până la 500 000 EUR ating gradul de severitate a unei „fapte penale”. Din aceste considerente, investigația în privința acestor fapte ar trebui să respecte toate garanțiile care sunt asigurate în cazul existenței unei acuzații în materie penală, în sensul acestei noțiuni interpretate de CtEDO în jurisprudența sa.	
--	--	--	--	--

			16.2. În conformitate cu prevederile art. 19 alin.(1) lit.e) din Legea nr. 780 din 27.12.2001 privind actele legislative, considerăm necesar de a substitui sintagma „administrativă” din textul art. 92 al proiectului, cu noțiunea de „contravențională”, care este deja utilizată în legislația națională (Codul contravențional). Alte obiecții sau propuneri nu sunt.	
	Banca Națională a Moldovei	art. 2 alin. (2) lit. c)	Consideră că norma din ultima propoziție de la art. 2 alin. (2) lit. c) ar trebui precizată în privința întinderii excepției. Or, aceasta pare să instituie o excepție de la domeniul de aplicare al legii și nu doar de la aplicarea lit. c), fapt ce reclamă, în opinia lor, completarea alin. (3) al aceluiași articol.	Nu se acceptă . Excepția în cauză se aplică în exclusivitate situațiilor descrise la art. 2 alin. (2) lit. c).
		art. 5 alin. (2)	Propune explicitarea intenției autorilor cât privește textul “sau nu se bazează pe un temei legal” de la art.5 alin.(2) din proiect, și anume dacă acesta se referă la temeiurile de legalitate enumerate la alin.(1) al aceluiași articol sau la norme speciale din alte legi. În plus, prevederea de la art.5 alin.(2) pare să pună în sarcina operatorului de date efectuarea unei evaluări proprii, în absența unui “temei legal”, oricare ar fi semnificația acestuia.	Se acceptă parțial. Norma a fost expusă într-o nouă redacție.
		art. 5 alin. (3)	La art.5 alin.(3), enumerarea care urmează după textul “fiind necesar a fi justificat...” se referă la o solicitare de date personale, prevederea fiind insuficient de clară în această privință. La același alineat, sugerăm excluderea cuvintelor “etc.” și indicarea exhaustivă a elementelor însoțitoare ale solicitării de date personale.	Nu se acceptă, solicitarea de date cu caracter personal urmează să cuprindă atât informația specificată la această normă, precum și alte informații justificative de care dispune solicitantul.
		art. 6 alin. (3)	Opinează că art.6 alin.(3) ar trebui revizuit, Centrul urmând să se bazeze pe documentele emise de instituțiile UE doar în măsura în care acestea sunt transpuse în dreptul intern.	Nu se acceptă. Prin norma în cauză se instituie un drept al Centrului de a se ghida de documentele emise de Uniunea Europeană în domeniul protecției datelor și sferei de securitate a acestora.

		art. 8 alin. (3)	La art.8 alin.(3), sugerează revizuirea cuvintelor “răspunderii părintești” din ultima propoziție, întrucât alineatul nu se referă doar la incapacitatea de exercițiu a minorului.	Se acceptă. Sintagma “răspunderii părintești” s-a substituit cu sintagma „reprezentantul legal”.
		art. 10 alin. (2)	La art.10 alin.(2) din proiect, recomandă reevaluarea trimiterii la alin.(1), întrucât cele două alineate par să reglementeze situații diferite, precum și formularea mai exactă a obligației care incumbă operatorului.	Nu se acceptă. Norma în cauză transpune în totalitate art. 11 din Regulamentul (UE) 679/2016.
		art.11 alin.(2)	La art.11 alin.(2), considerăm utilă precizarea subiectului cu drept de cerere (subiectul datelor personale, Centrul?).	Se acceptă. S-a efectuat precizarea „la cererea subiectului de date”.
		art.12	La art.12, nu este clar la ce se raportează textele “dacă acestea” (de la alin.(3)) și “și în absența intereselor” (lit.a)), iar textul “sunt incompatibile și/sau împiedică exercitarea...” poate genera probleme de aplicare, fiind neclar cui revine obligația/dreptul de a arăta o anumită incompatibilitate. Opinează că proiectul de lege ar trebui să echilibreze dreptul la protecția datelor personale și dreptul la informare/libertatea de exprimare prin efectuarea corelărilor necesare între normele juridice aplicabile celor două drepturi, eventual cu stabilirea unui principiu general de prevalență a unuia din cele două drepturi. Aceste clarificări se impun în virtutea consecințelor aplicării art.12, care la alin.(6) prevede exonerarea de răspundere pentru prelucrarea de date conform alin.(1)-(4).	Se acceptă, art. 12 alin. (3) lit. a) a fost redactat. În partea ce vizează obligația de a aprecia echilibrul între dreptul persoanei la protecția datelor în raport cu dreptul la libertatea de exprimare și informare aceasta îi revine operatorului de date care prelucra datele în scopuri academice, artistice, literare.
	Centrul Național Anticorupție expertiza anticorupție	Art.2 și art.81	Articolul 2. Domeniul material de aplicare Domeniul de acțiune al prezentei legi se extinde asupra: a) <u>prelucrării datelor</u> cu caracter personal efectuate pe teritoriul Republicii Moldova, <u>inclusiv informațiilor care consemnează date cu caracter personal atribuite la secret de stat, secret profesional, secret bancar, secret medical, secret comercial, secret fiscal și altor informații cu accesibilitate limitată sau operațiunilor administrative</u>	Nu se acceptă. Reiterăm că în prezent potrivit art. 2 alin. (4) lit. b) din Legea nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal domeniul de acțiune al legii se extinde inclusiv asupra prelucrării datelor cu caracter personal atribuite la secret de stat în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul

			desfășurate în legătură cu gestionarea dosarului civil, contravențional sau penal, precum și mijloacelor utilizate în acest sens. Articolul 81. Accesul și păstrarea materialelor investigației (3) <u>În cazul în care materialele investigației conțin informații atribuite la secret de stat</u>, secret comercial, secret bancar sau secret al dosarului special, informații ce țin de confidențialitatea procesului contravențional sau penal sau alte informații oficiale cu accesibilitate limitată, Centrul restricționează accesul la acestea. (10) <u>Materialele investigației care conțin secret de stat</u> se păstrează în arhivele instituțiilor menționate în alin. (8) și (9), în condiții speciale prevăzute de legislația în vigoare. Obiecții: Pentru început menționăm că obiecțiile înaintate în prezentul capitol va atenționa repetat asupra riscurilor identificate vis-a-vis de noua reglementare a Legii nr.133/2011 privind protecția datelor cu caracter personal, de care autorul ar trebui să țină cont. În mare parte obiecțiile date au fost evidențiate în cadrul procesului de avizare, însă asupra celor de care nu s-au acceptat Centrul Național Anticorupție, comunică repetat. În ceea ce privește domeniul de acțiune a normelor propuse la art.2 alin.(2) lit.a) din proiect invocăm că normele propuse contravin cadrului național, inclusiv celui în materie procesual penală. Conform Legii nr.245/2008, informația atribuită la secret de stat reprezintă „informații protejate de stat în domeniul apărării naționale, economiei, științei și tehnicii, relațiilor externe, securității statului, asigurării ordinii de drept și activității autorităților publice, a căror divulgare neautorizată sau pierdere este de natură să aducă atingere intereselor și/sau securității Republicii Moldova”. Astfel, făcând obiectul de reglementare al prezentului proiect, această categorie de informații (secret de stat) automat cade sub incidența tuturor normelor propuse, inclusiv în	procedurii penale sau contravenționale în condițiile legii. Avînd în vedere cele menționate supra, obiecțiile formulate de CNA în partea ce vizează art.2 alin. (2) lit. a) că ar depăși cadrul legal în vigoare și ar compromite asigurarea realizării sarcinilor activității speciale de investigație, nu pot fi reținute și nu sunt argumentate, fiind expuse niște presupuneri ce nu sunt bazate temeinic (<i>ar putea.., ar exista.., aparent... etc.</i>). Un șir de organe de stat în scopul tainuirii sau limitării acesului la informații aplică secretizarea excesivă inclusiv asupra informațiilor ce țin de protecția datelor cu caracter personal – dreptul la viața privată, viața intimă a persoanei etc. Potrivit art. 8 alin. (1) al Legii cu privire la secretul de stat, nu se atribuie la secret de stat și nu pot fi secretizate informațiile privind faptele de încălcare a drepturilor și libertăților omului și ale cetățeanului; faptele de încălcare a legii de către autoritățile publice și persoanele cu funcții de răspundere din cadrul acestora. În acest sens, în cazul în care a fost stabilită o încălcare a principiilor de protecție a datelor cu caracter personal Centrul trebuie să dispună de pîrghiile necesare pentru ca persoana să cunoască despre încălcarea dreptului său. Mai mult, Centrul nu este absolvit de obligația respectării normelor procesual penale și contravenționale de ridicare a obiectelor și documentelor ce conțin informații care constituie secret de stat, comercial, bancar. Nu în ultimul rînd, toate dispozițiile invocate de CNA în partea ce vizează respectarea normelor de conformitate privind prelucrarea datelor cu caracter personal, sunt în contradicție cu argumentele expuse, or acestea denotă obligativitatea respectării și aplicării
--	--	--	--	--

		partea ce ține de asigurarea accesului, transmiterea informației date etc. către „inspectorii de protecție a datelor cu caracter personal” a acestor date restricționate. Potrivit art. 29 din legea sus-citată „Cetățeanul căruia i s-a perfectat dreptul de acces la secretul de stat este obligat: a) să nu admită divulgarea, prin orice metodă, a secretului de stat care i-a fost încredințat sau i-a devenit cunoscut în legătură cu îndeplinirea obligațiilor funcționale; [...] d) să execute cerințele asigurării regimului secret; [...] f) să respecte alte prevederi ale legislației privind secretul de stat.”. Respectiv proiectul contravine cerințelor înaintate de Legea nr.245/2008 în partea ce vizează asigurarea accesului la datele atribuite la secret de stat. Subsidiar, menționăm că norma propusă va avea un impact direct și reprezintă o ingerință pentru activitatea speciale de investigații, acțiunile, măsurile și tehnicile cărei sunt atribuite la secret de stat, în temeiul art.7 subpct.4) din Legea nr.254/2008: „(1) În modul stabilit de prezenta lege sunt atribuite la secret de stat informațiile: [...] 4) din domeniul securității statului și asigurării ordinii de drept privind: a) efectivul, forțele, conținutul, planurile, organizarea, finanțarea și asigurarea tehnico-materială, formele, tactica, metodele, mijloacele și rezultatele activităților de informații, de contrainformații și operative de investigații; [...] b) persoanele care colaborează sau au colaborat confidențial cu organele care desfășoară activități de informații, de contrainformații și operative de investigații; c) forțele, mijloacele și metodele de asigurare a protecției de stat părții vătămate, martorilor și altor persoane care acordă ajutor în procesul penal;”. În acest context, Codul de procedură penală, cât și Legea nr.59/2012 privind activitatea specială de investigații stabilesc expres categoriile de subiecți care pot avea acces la materialele/informațiile în cadrul desfășurării activităților	Legii privind protecția datelor cu caracter personal, inclusiv în activitatea specială de investigație, iar supravegherea respectării conformității prelucrării datelor cu caracter personal în acest sector este pusă în temeiul legii, în sarcina Centrului național pentru Protecția Datelor cu Caracter Personal. Suplimentar, este de menționat că practica internațională oferă autorităților de protecție a datelor cu caracter personal, dreptul de a avea acces la orice tip de informații, indiferent de gradul de securizare și clauza de confidențialitate, fie secret de stat, confidențialitatea urmăririi penale sau contravenționale, și de a verifica dacă prin aceste metode de colectare și utilizare a datelor, nu se încalcă drepturile omului, în special în partea ce vizează inviolabilitatea vieții intime, familiale și private. Constatăm, că practica dată este aplicată pe deplin de statele UE și nu aduce nici o ingerință în activitatea organelor de drept. Mai mult ca atât, autoritatea de supraveghere este un echilibru dintre activitățile acestor organe și respectarea drepturilor omului în partea ce ține de conformitatea prelucrării datelor cu caracter personal, îmbunătățind activitatea organelor de drept, astfel nu este clară reticența și nedorința de modernizare a CNA și expunerea că sunt premize de elemente coruptibile. Menționăm că toate acțiunile Centrului sunt supuse controlului judecătoresc, controlului Parlamentar. Mai mult, toate aceste competente sunt specifice tuturor autorităților de supraveghere a prelucrării datelor cu caracter personal, fiind conferite în temeiul Convenției nr. 108 din 28 ianuarie 1981 pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Protocolului adițional la Convenția pentru protecția
--	--	---	---

			de investigare (inclusiv la materialele din dosarele penale). Astfel, art.212 din Codul procesual penal prevede expres: „Confidențialitatea urmăririi penale. (1) Materialele urmăririi penale nu pot fi date publicității decât cu autorizația persoanei care efectuează urmărirea penală și numai în măsura în care ea consideră că aceasta este posibil, cu respectarea prezumției de nevinovăție, și ca să nu fie afectate interesele altor persoane și ale desfășurării urmăririi penale în condițiile Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal.” (Legea nr.133/2011 în vigoare). La fel, Codul de procedură penală reglementează - „Apărarea secretului de stat în procesul penal” (a se vedea art.213 din cod). Legea nr.59/2012, obligă subiecții implicați în activitatea specială de investigații să respecte protecția datelor cu caracter personal în cadrul activității - art.5 „(1) Persoanele care au acces la datele cu caracter personal ale persoanei supuse măsurii speciale de investigații sunt obligate să păstreze confidențialitatea datelor 8 respective în conformitate cu prevederile Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal. (2) Accesul la dosarul special sau la materialele din dosar al altor persoane decât cele care investighează dosarul special este interzis, cu excepția conducătorului subdiviziunii specializate a organului respectiv, în limitele competenței, și a procurorului care a autorizat măsura specială de investigații sau a solicitat autorizarea acesteia de către judecătorul de instrucție, precum și cu excepția judecătorului de instrucție care a autorizat măsura specială de investigații.”. Prin urmare, prevederile propuse la art.2 depășește cadrul legal în vigoare și vin să compromită asigurarea realizării sarcinilor activității speciale de investigații. Atenționăm, că orice imixtiune în activitatea ofițerului de urmărire penală este interzisă, inclusiv la datele investigațiilor	persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și 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 urmăririi penale a infracțiunilor sau al executării pedepselor și privind libera circulație a acestor date. Astfel, în acest context art. 58 din Regulamentul (UE) 2016/679 statuează expres aceste competențe de investigare pentru autoritatea de supraveghere a datelor cu caracter personal. În special, autoritatea de supraveghere are dreptul de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale, de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor (art. 58 alin. (1) lit. e) și lit. f)). Subliniem faptul că, CNPDCP nu urmărește scopul de a interveni în activitatea autorităților publice (organelor ce efectuează activitatea specială de investigații), ci de a efectua controlul legalității prelucrării datelor cu caracter personal ale subiectului de date de către entități, în calitate de operatori de date cu caracter personal, care au obligația de a asigura confidențialitatea și securitatea datelor cu caracter personal prelucrate.
--	--	--	---	--

			(art.57 alin.(4) din Codul de procedură penală), iar ofițerii de investigații, care efectuează activitatea specială de investigații, își realizează sarcinile în mod independent, cu excepția cazului când acțiunea specială de investigații este dispusă și coordonată sau este condusă în cadrul procesului penal de către procuror sau de către ofițerul de urmărire penală, în interacțiune sau în colaborare cu colaboratorii confidențiali (art.6 alin.(3) din Legea nr.59/2012 privind activitatea specială de investigații). Obiecția dată este valabilă pentru prevederile art.81 alin.(3) și alin.(10) din proiect. Recomandări: 1) Substituirea sintagmei „inclusiv informațiilor care consemnează date cu caracter personal atribuite la secret de stat, secret profesional, secret bancar, secret medical, secret comercial, secret fiscal și altor informații cu accesibilitate limitată sau operațiunilor administrative desfășurate în legătură cu gestionarea dosarului civil, contravențional sau penal, precum și mijloacelor utilizate în acest sens;” cu sintagma „în limitele legislației în vigoare”. 2) Excluderea art.81 alin.(3) și alin.(10) din proiect.	Menționăm că, pentru majoritatea angajaților Centrului s-a perfectat dreptul de acces la secret de stat. În aceeași ordine de idei menționăm, că reieșind din atribuțiile sale legale, Centrul este în drept să investigheze orice incident de securitate, inclusiv ce ține de scurgerea unor informații ce conțin date cu caracter personal din oricare sistem informațional, chiar și ale CNA. În aceste situații Centrul este organul care efectuează investigarea. Astfel, una din atribuțiile principale ale Centrului este de a asigura securitatea datelor cu caracter personal, indiferent de modul și locul de păstrare a acestora. Obiecțiile CNA nu sunt elocvente.
		Art.2 alin.(2) lit. d)	(2) Domeniul de acțiune al prezentei legi se extinde asupra: <u>d) prelucrării datelor cu caracter personal de către operatori - organe de ocrotire a legii, care au competențe stabilite prin lege în scopul prevenirii, investigării, depistării și/sau urmăririi penale a infracțiunilor sau executării pedepselor penale, detenția preventivă, inclusiv protejarea și prevenirea amenințărilor la adresa ordinii publice, securității de stat și securității naționale și în cadrul dosarului sau acțiunilor speciale de investigație.</u> Obiecții: Cu referire la art.2 alin.(2) lit.d) care stabilește un alt domeniu de acțiune al proiectului și anume: „prelucrarea datelor cu caracter personal de către operatori - organe de ocrotire a legii, care au competențe	Nu se acceptă. Menționăm în repetate rânduri că prin reglementarea în cauză, inclusiv dispozițiile cap. VII s-a trasat <u>scopul de a asigura implementarea Directivei nr. 2016/680 a Parlamentului European și 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 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, document juridic internațional prin care Uniunea Europeană a delegat dreptul de investigare a prelucrării datelor cu caracter personal efectuate în</u>

		stabilite prin lege în scopul prevenirii, investigării, depistării și/sau urmăririi penale a infracțiunilor", statuăm că și în cazul dat, normele propuse sunt abuzive în raport cu activitatea specială de investigații și a statutului ofițerului de urmărire penală/procurorului și ale altor organe de drept. La acest capitol, menționăm că art.3 alin.(1) din Legea nr.333 din 10.11.2006 privind statutul ofițerului de urmărire penală, prevede expres „în exercitarea atribuțiilor, ofițerul de urmărire penală este independent, se supune numai legii, indicațiilor scrise ale conducătorului organului de urmărire penală, ale procurorului și hotărârilor instanței de judecată, emise în limitele competenței lor și în conformitate cu legislația în vigoare.". Orice imixtiune în activitatea ofițerului de urmărire penală este interzisă și acesta se supune doar prevederilor Cod de procedură penală și indicațiilor scrise ale procurorului și ale conducătorului organului de urmărire penală (a se analiza art.57 alin.(4) din Codul de procedură penală). Art.6 alin.(3) din Legea nr.59 din 29.03.2012 privind activitatea specială de investigații, la fel, garantează independența ofițerului de investigații „Ofițerul de investigații care efectuează activitatea specială de investigații își realizează sarcinile în mod independent, cu excepția cazului când acțiunea specială de investigații este dispusă și coordonată sau este condusă în cadrul procesului penal de către procuror sau de către ofițerul de urmărire penală, în interacțiune sau în conlucrare cu colaboratorii confidențiali". Astfel, domeniul de reglementare propus depășește limitele legale statuate în legislația procesual penală. De asemenea, putem menționa că legalitatea desfășurării măsurilor speciale de investigații în corelație cu încălcarea respectării drepturilor omului și a libertăților fundamentale este verificată de către instanța de judecată și procuror, care autorizează sau anulează măsurile	<u>cadrul urmăririi penale, autorităților naționale de supraveghere a prelucrării datelor cu caracter personal – fapt, trecut cu vederea de către CNA. Menționăm că Centrul nu efectuează verificarea activității de urmărire penală sau a activității speciale de investigații, dar se limitează la investigarea conformității prelucrării datelor cu caracter personal.</u> Reiterăm că, clauza legală ce reglementează prelucrarea datelor cu caracter personal în sectorul polițienesc a fost instituită deja și este prevăzută la moment la art. 2 alin. (2) lit. d) Legea nr. 133. În formularea actuală domeniul de acțiune al acestei legi se extinde asupra prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale în condițiile legii. În acest context, este de menționat că la 28 aprilie 2016 a fost adoptată Legea nr. 87 (publicată în Monitorul Oficial nr. 156/306 din 07.06.2016) prin care au fost operate modificări/completări la un șir de legi, fiind înserate dispoziții legale ce vizează prelucrarea datelor cu caracter personal în sectorul polițienesc, după cum urmează: 1.Cod de procedură penală. Art. 15 alin. (2) stipulează că la efectuarea acțiunilor procesuale nu poate fi acumulată fără necesitate informație despre viața privată și intimă a persoanei. La cererea organului de urmărire penală și a instanței de judecată, participanții la acțiunile procesuale sînt obligați să nu divulge asemenea informații și despre aceasta se ia un angajament în scris. <u>Prelucrarea datelor cu caracter personal în cadrul procesului penal se efectuează în conformitate cu prevederile Legii nr.133</u>
--	--	---	--

			efectuate. Astfel, normele de la art.2 alin.(2) lit.d) vin să compromită asigurarea realizării sarcinilor activității speciale de investigații, reprezentând în esență, o imixtiune în activitatea acestora, precum și în activitatea ofițerilor de urmărire penală și a procurorilor. Considerăm absolut necesar excluderea art.2 alin.(2) lit.d) din textul proiectului, precum și a oricăror prevederi ce vin să aducă restricții și ingerințe în activitatea specială de investigații. Recomandări: Excluderea art.2 alin.(2) lit.d) din textul proiectului. Totodată, considerăm oportun completarea art.2 alin.(3) cu o literă nouă care să prevadă „d) prelucrării datelor cu caracter personal de către organele de drept, care au competențe stabilite prin lege, în scopul prevenirii, investigării, depistării și/sau urmăririi penale a infracțiunilor sau executării pedepselor penale, detenția preventivă, inclusiv protejarea și prevenirea amenințărilor la adresa ordinii publice, securității de 10 stat și securității naționale și în cadrul dosarului sau acțiunilor speciale de investigație”.	<u>din 8 iulie 2011 privind protecția datelor cu caracter personal.</u> 2. Legea nr. 59 din 29.03.2012 cu privire la activitatea specială de investigație. Art. 5 alin. (1), persoanele care au acces la datele cu caracter personal ale persoanei supuse măsurii speciale de investigații sînt obligate să păstreze confidențialitatea datelor respective în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. 3. Legea nr. 320 din 27.12.2012 cu privire la Poliție și statutul polițistului Art. 16 alin. (3), prelucrarea, transmiterea și distrugerea datelor cu caracter personal deținute de Poliție se efectuează în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. 4. Legea nr. 1104 din 06.06.2002 cu privire la Centrul Național Anticorupție Articolul 6 lit. m), să prelucreze date cu caracter personal, inclusiv în scop de analiză informațională și strategică, în conformitate cu prevederile Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal. Avînd în vedere specificul legislației Republicii Moldova, în special, codificarea normelor de procedură penală și rigiditatea activității speciale de investigații, este necesară intervenția pentru a asigura o sincronizare în materie de protecție a datelor cu caracter personal. O altă lege care a adus atribuții noi Centrului este Legea nr. 120 din 21 septembrie 2017 cu privire la prevenirea și combaterea terorismului. Activitatea de prevenire și
--	--	--	---	---

				combateră a terorismului va fi exercitată în mod special de Serviciul de Informații și Securitate care prelucrează un volum extrem de mare de date personale, iar controlul conformității prelucrărilor de date cu caracter personal se efectuează de către Centru. <i>Prin spectrul de modificări legislative arătat supra, Centrul a dobândit competență de a investiga prelucrarea datelor cu caracter personal atribuite inclusiv la secret de stat etc.</i>
		Art.4	Articolul 4. Principiile aferente prelucrării datelor personale (1) Datele personale urmează a fi: [...] c) <u>adecvate, relevante și limitate</u> la ceea ce este necesar în legătură cu realizarea obiectivelor pentru care sunt prelucrate („minimizarea datelor”); d) exacte și, dacă este necesar, actualizate. <u>Trebuie să se ia toate măsurile necesare pentru a se asigura că datele personale care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse, distruse sau rectificate fără întârziere („exactitate”); [...] f) prelucrate într-un mod care asigură securitatea adecvată a datelor personale, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”); [...] (2) Operatorul este responsabil de asigurarea conformării cu alin.(1) și poate demonstra această respectare („responsabilitate”).</u> Datele personale urmează a fi prelucrate sub răspunderea operatorului, care <u>asigură și demonstrează conformitatea fiecărei operațiuni</u> de prelucrare cu dispozițiile prezentei legi. Obiecții: Pentru început menționăm că principiile stabilite la alin.(1) trebuie respectate de către toți operatorii, iar în cazul încălcării acestor principii, CNPDCP este în drept să atragă la răspundere administrativă conform art.89 din proiect. Respectarea	Nu se acceptă. Principiile protecției datelor trebuie să se aplice oricărei informații referitoare la o persoană fizică identificată sau identificabilă. Art. 4 alin. (1) din proiect statuează operatorilor de date ansamblul principiilor – reguli, care urmează a fi respectate la prelucrarea datelor cu caracter personal și reprezintă elemente fundamentale ale prelucrării datelor personale. Prin urmare, esența art. 4 este redată sub forma unor reguli de bază și fundamentale, necesar a fi implementate și asigurate de către fiecare operator în parte. Detalierea fiecărui principiu în parte este expusă în următoarele articole din proiect. Ca de exemplu articolul 11 Minimizarea datelor prelucrate în scopul identificării subiectului de date, prevede reguli concrete în partea ce vizează respectarea acestui principiu. De asemenea, art. 29 din proiectul legii, intitulat responsabilitatea operatorului, materializează clar condițiile ce urmeză a fi respectate de către operator. Deci, operatorul trebuie să fie obligat să implementeze măsuri adecvate și eficace și să fie în măsură să demonstreze conformitatea activităților de prelucrare cu prezentul regulament, inclusiv eficacitatea măsurilor. Aceste măsuri trebuie să țină seama de

		unor principii trebuie materializate prin stabilirea clară a condițiilor ce urmează a fi respectate, cu evitarea unor formulări generale impuse, precum cele evidențiate la alin.(1). Este practic imposibil, să respecti careva cerințe dacă acestea nu sunt clar identificate/expuse pentru subiecții ce urmează a le respecta. Cu referire la alin.(2) considerăm că norma dată este expusă într-o formă abuzivă, iar la aplicare ea va crea circumstanțe obscure/neclare pentru operatori, ceea ce reprezintă un risc de corupție. Atenționăm că principiile sunt idei călăuzitoare. Respectiv, alin.(2) nu corespunde denumirii articolului și domeniului reglementat de acesta. Totodată, riscul normei sporește pe măsură ce acest alineat stabilește obligativitatea demonstrării de către operatori a respectării cerințelor legale. În acest sens, atenționăm asupra principiului prezumției de nevinovăție, principiu consfințit atât de Constituția Republicii Moldova la art.21, cât și în Convenția pentru 11 apărarea drepturilor omului și a libertăților fundamentale nr.1950 din 04.11.1950, prin prisma art.6 pct.2. Subsidiar, art.375 din Codul contravențional „Prezumția de nevinovăție. (1) Persoana acuzată de săvârșirea unei contravenții se consideră nevinovată atâta timp cât vinovăția sa nu este dovedită în modul prevăzut de prezentul cod. (2) Nimeni nu este obligat să dovedească nevinovăția sa.". Astfel, sintagma „asigură și demonstrează conformitatea fiecărei operațiuni” impune obligația operatorului de a demonstra că acesta nu a încălcat prevederile legislație, la modul practic acesta trebuie să demonstreze nevinovăția, fapt ce contravine legislației naționale. Demonstrarea conformității principiilor legale se prezintă ca cerințe excesive pentru operatori și reprezintă un risc de corupție. Totodată, reglementările ambiguu vor genera imposibilitatea tragerii la răspundere a persoanelor	natura, domeniul de aplicare, contextul și scopurile prelucrării, precum și de riscul pentru drepturile și libertățile persoanelor fizice. Suplimentar, cităm mai jos prevederile Ghidului practic privind utilizarea datelor cu caracter personal în sectorul polițienesc, adoptat de către Comitetul Consultativ al Convenției 108: „Conform principiului responsabilității, poliția, ca și ceilalți operatori de date, este responsabilă de prelucrarea datelor pe care o efectuează. Aceasta implică faptul că trebuie să fie în măsură să demonstreze în orice moment că activitățile sale de prelucrare respectă normele de protecție a datelor. În plus, este necesar ca poliția să implementeze în mod activ măsuri pentru protejarea și promovarea protecției datelor în toate activitățile sale... ...Operatorul de date ar trebui să evalueze și să demonstreze dacă scopul prelucrării poate fi realizat într-un mod care are un impact mai redus asupra dreptului la viață privată și a protecției datelor și dacă prelucrarea unor categorii speciale de date nu reprezintă un risc de discriminare pentru persoana vizată. Spre regret, pînă în prezent, CNA nu a informat Centrul despre implementarea prezentului ghid.
--	--	---	--

			vinovate pentru aplicarea abuzivă a normelor propuse la art.89 din proiect. Recomandări: Excluderea art.4 alin.(2) din proiect.	
		Art.6 alin.(1), art.55 alin.(4), art.78	Articolul 6. (1) Centrul Național pentru Protecția Datelor cu Caracter Personal (în continuare - Centrul) este autoritatea publică de asigurare a dreptului la protecția datelor personale, inclusiv ce derivă din dreptul constituțional la inviolabilitatea vieții intime, familiale și private și este autoritatea învestită cu dreptul inalienabil de a efectua supravegherea, prevenirea cazurilor de încălcare a prezentei legi (prin informare, instruire, reglementare și alte acțiuni ce nu vin în contradicție cu legea), de a efectua investigarea respectării <u>principiilor</u> de protecție a datelor personale prevăzute de legislația în vigoare, precum și stabilirea politicilor în domeniul dat etc. Articolul 55. (4) <u>Centrul este competent să supravegheze, să reglementeze și să investigheze modul de prelucrare a datelor personale de către organele de ocrotire a legii în conformitate cu prezenta lege</u>. Legea privind Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova și alte acte normative. Centrul va ține cont de caracterul specific al activității acestor autorități. 78. Investigația (1) Investigația reprezintă activitatea desfășurată de către inspectorii de protecție a datelor, de conducătorii subdiviziunilor specializate din cadrul Centrului în scopul de verificare a respectării cerințelor prezentei legi și altor acte normative ce vizează domeniul protecției datelor personale de către: operatori, operatori asociați, persoane împuternicite de operatori, destinatari, precum și entități care nu sunt considerate a fi destinatari (organele de ocrotire a legii), terți, indiferent de tipul proprietății și domeniul de activitate, forma juridică de organizare. [...] (9) În cadrul investigației, inspectorii de protecție a datelor au următoarele drepturi: a) să	Nu se acceptă. Remarcăm art. 58 din noul Regulament 2016/679, care prevede competențele de investigație a autorităților de supraveghere a protecției datelor cu caracter personal prevede, inclusiv următoarele: <i>a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale;</i> <i>e) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale;</i> <i>f) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern.</i> Suplimentar, menționăm că Directiva (UE) 2016/680 statuează sarcini, atribuții și garanții de care trebuie să dispună autoritatea națională de supraveghere a prelucrării datelor cu caracter personal, și anume: - Fiecare stat garantează că autoritatea sa de supraveghere beneficiază de independență deplină în îndeplinirea sarcinilor și exercitarea competențelor care le revin în conformitate cu prezenta directivă (art. 42 alin. (1)). - Statele garantează că membrii autorităților lor de supraveghere, în îndeplinirea sarcinilor și în exercitarea competențelor care le revin în

		dispună de acces și să examineze sistemele de evidență a datelor personale, soluțiile software și suporturile hardware, datele personale și orice documente legate de obiectul și scopul investigației, indiferent de echipamentul și/sau suportul pe care sunt stocate datele; b) să intre liber în încăperi, pe terenuri sau în mijloace de transport aflate în proprietatea sau folosința subiecților de drept menționați la alin. (1) din prezentul articol; c) să ridice, să colecteze, să obțină mijloace, copii sau extrase, sub orice formă, din sistemele de evidență și documentele care conțin date personale; [...] h) să solicite sprijinul subdiviziunilor abilitate ale organelor de ocrotire a legii, care sînt obligate să acorde asistența necesară angajaților Centrului [...] Obiecții: Cu referire la art.6 în corelare cu art.78 din proiect - Autoritatea de supraveghere. Menționăm repetat, necesitatea revizuirii competențelor CNPDCP care se prezintă excesive în raport cu domeniul de reglementare, precum și cu activitatea altor entități publice. Riscul acordării unui spectru larg de competențe, fără careva limite/restricții legale, se datorează normelor proiectului ce vizează: - „reglementarea” domeniul, - „investigarea asupra respectării principiilor de protecție a datelor personale prevăzute de legislația în vigoare”, în speță „Centrul poate dispune prin decizie, [...] ieșirea la fața locului.”, - „decizia privind efectuarea investigației la fața locului se aduce la cunoștință sub semnătură persoanei, entității supuse investigației, sau reprezentantului legal. În cazul refuzului primirii și semnării deciziei se întocmește un act, în prezența unui martor sau în cazul înregistrării video și audio, în care se consemnează acest fapt”, - „să dispună de acces și să examineze sistemele de evidență a datelor personale, soluțiile software și suporturile hardware, datele	conformitate cu prezenta directivă, rămân independenți de orice influență externă directă sau indirectă și nici nu solicită, nici nu acceptă instrucțiuni de la nimeni (art. 42 alin. (2)). - Fiecare stat garantează prin lege că autorității sale de supraveghere îi revin competențe de consiliere efective pentru a oferi consiliere operatorului și de a emite avize, din proprie inițiativă sau la cerere, parlamentului național, guvernului sau, în conformitate cu dreptul său intern, altor instituții și organisme, precum și publicului, cu privire la orice aspect legat de protecția datelor cu caracter personal. - Fiecare stat membru garantează prin lege că autorității sale de supraveghere îi revin competențe de investigare efective. Respectivele competențe includ, cel puțin, competența de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal care sunt prelucrate și la toate informațiile necesare pentru îndeplinirea sarcinilor sale.(Art. 47) Este de menționat, că legislația și practica internațională oferă autorităților de protecție a datelor cu caracter personal, dreptul de a avea acces la orice tip de informații, indiferent de gradul de securizare și clauza de confidențialitate, fie secret de stat, confidențialitatea urmăririi penale sau contravenționale, și de a verifica dacă prin aceste metode de colectare și utilizare a datelor, nu se încalcă drepturile omului, în special în partea ce vizează inviolabilitatea vieții intime, familiale și private. Constatăm, că practica dată este aplicată pe deplin de statele UE și nu aduce nici o ingerință în activitatea organelor de drept, ba mai mult ca atît autoritatea de
--	--	--	---

		personale și orice documente legate de obiectul și scopul investigației", - „să intre liber în încăperi, pe terenuri sau în mijloace de transport aflate în proprietatea sau folosința subiecților de drept", - „să ridice, să colecteze, să obțină mijloace, copii sau extrase, sub orice formă, din sistemele de evidență și documentele care conțin date personale" etc. (a se vedea norma de la art.78 din proiect), va admite apariția la aplicare, abuzurilor din partea autorității de supraveghere - CNPDCP. Totodată, este important de stipulat că normele propuse nu oferă și un mecanism de control/supraveghere asupra activității acestei structuri, ceea ce sporește riscul abuzurilor. Acțiunile propuse sunt identice cu cele ale organelor responsabile prin lege de desfășurarea activităților speciale de investigații, însă fără a se garanta un mecanism de coordonare și control asupra legalității acestor măsuri cu caracter procesual penal. Se constată că proiectul oferă o reglementare diferită și individualizată a procesului de investigare efectuat de către CNPDCP, în comparație cu procedura legală prevăzută de legislația procesual penală, aplicabilă tuturor organelor de drept în atribuțiile cărora intra efectuarea măsurilor speciale de investigație. Sub aspect comparativ, competențele acordate subiecților citați la art.6 din Legea nr.59/2012 privind activitatea specială de investigații (Ministerul Afacerilor Interne, Ministerul Apărării, Centrul Național Anticorupție, Serviciul de Informații și Securitate, Serviciul de Protecție și Pază de Stat, Serviciul Vamal și Administrația Națională a Penitenciarelor) sunt reglementate într-un mod strict, fiecare acțiune fiind autorizată și supusă unui control riguros din partea mai multor entități publice. Astfel, Codul de procedură penală la art.300 reglementează sfera de control asupra activității speciale de investigații, efectuate de judecătorul de instrucție, nemaivorbind despre alte posibilități legale	supraveghere este un echilibru dintre activitățile acestor organe și drepturile omului în partea ce ține de conformitatea prelucrării datelor cu caracter personal, îmbunătățind activitate organelor de drept, astfel nu este clară reticența repetată și nedorința de modernizare a CNA și expunerea că sunt premise de elemente coruptibile. Menționăm că, toate acțiunile Centrului sunt supuse controlului judecătoresc, controlului parlamentar. La fel, nu pot fi reținute argumentele în partea ce vizează lipsa garanțiilor legale (inclusiv procesuale) ce ar asigura monitorizarea, echitatea și imparțialitatea competențelor „autorității de supraveghere”. Or, CNA pune la îndoială corectitudinea și conformitatea activității/statului Centrului conferit deja prin lege. În mare parte competențele date sunt expuse și astăzi, doar că într-o manieră în care se permite interpretarea acestora, creînd deseori confuzii și imixiune în activitatea Centrului. Reiterăm că, la moment potrivit art. 2 alin. (2) lit. d), domeniul de acțiune al Legii privind protecția datelor cu caracter personal se extinde inclusiv asupra prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale în condițiile legii, fapt ce implică și dreptul Centrului de efectua controale a modului de prelucrare a datelor cu caracter personal în activitatea specială de investigații. Astfel, obiecția invocată este lipsită de suport juridic or, potrivit art. 20 din Legea nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal, controlul asupra respectării acestui
--	--	--	---

		oferite cetățeanului de a-și apăra drepturile și interesele personale. Totodată, Legea nr.59/2019 reglementează într-un capitol separat mecanismul de control și coordonare a activității speciale de investigații. Astfel, controlul asupra subiecților activității speciale de investigații este efectuat de instanțele de judecată, procuror, la fel, este supus unui control departamental și Parlamentar. În acest context, proiectul nu oferă garanții similare pentru autoritatea de supraveghere, enunțată la art.6 din proiect, ceea ce face posibilă stabilirea unor proceduri cu caracter procesual penal, însă într-o interpretare diferită și condiții diferite (excesive și discreționare) decât cele generale prevăzute de cadrul legal național. La acest capitol, Codul de procedură penală, prevede expres la art.2 alin.(4) „Normele juridice cu caracter procesual din alte legi naționale pot fi aplicate numai cu condiția includerii lor în prezentul cod.” Admiterea multiplelor forme de supraveghere, pe lângă controlul prevăzut de Codul procesual penal asupra procesului de investigare a infracțiunilor/contravențiilor și asupra măsurilor speciale de investigații vor crea impedimente în realizarea actului justiției, deoarece apare un nou subiect (organ de control) competențele căruia nu sunt clar reglementate, fie sunt excesive și discreționare. În speță, orice intervenție în aceste măsuri, din exterior (precum se propune la art.78 din proiect) reprezintă o ingerință directă în procesul de investigație a infracțiunilor și poate afecta considerabil mersul anchetei. Art.5 alin.(2) din Legea nr.59/2012 stipulează expres că „accesul la dosarul special sau la materialele din dosar al altor persoane decât cele care investighează dosarul special este interzis, cu excepția conducătorului subdiviziunii specializate a organului respectiv, în limitele competenței, și a procurorului care a autorizat măsura specială de investigații sau a solicitat autorizarea	act legislativ ține de competența Centrului Național pentru Protecția Datelor cu Caracter Personal. În partea ce ține de „abuzivitatea” competențelor, menționăm, că în ipoteza depistării unor riscuri sporite la prelucrarea datelor cu caracter personal, Centrul la moment are competența de a interveni și a dispune, inclusiv: suspendarea, modificarea, încetarea operațiunilor de prelucrare a datelor. Astfel de mijloace de intervenție necesită a fi realizate operativ, or, trecerea timpului afectează posibilitatea salvării drepturilor și libertăților subiecților de date. Spre exemplu: Imposibilitatea intervenției asupra mijloacelor software sau hardware ar însemna în unele situații neputința de a curma o acțiune ilicită, care poate avea caracter transfrontalier sau ar putea prezenta indicii componente unei infracțiuni cibernetice.
--	--	---	---

		acesteia de către judecătorul de instrucție, precum și cu excepția judecătorului de instrucție care a autorizat măsura specială de investigații". În aceeași ordine de idei, se invocă art.3 alin.(1) din Legea nr.333 din 10.11.2006, privind statutul ofițerului de urmărire penală, conform căruia, „în exercitarea atribuțiilor, ofițerul de urmărire penală este independent, se supune numai legii, indicațiilor scrise ale conducătorului organului de urmărire penală, ale procurorului și hotărârilor instanței de judecată, emise în limitele competenței lor și în conformitate cu legislația în vigoare.". În cazul în care CNPDCP își asumă sarcinile organelor de control, menționate mai sus, în partea ce ține de controlul operațiunilor de prelucrare a datelor personale în procesul exercitării activității speciale de investigații, se vor crea confuzii la aplicarea legilor. Astfel, Centrul va avea dreptul să verifice activitatea specială de investigații efectuată de către subiecții acesteia, ceea ce este inadmisibil, mai ales că această activitate este considerată secret de stat, în conformitate cu prevederile cu art.7, alin.(4), lit.a), b), c) a Legii nr.245/2008 cu privire la secretul de stat și corespunzător conform pct.38-41 la Hotărârea Guvernului nr. 411/2010. Prin urmare, drepturile expuse la art.78, precum și cumulul de competențe propus la art.6 din proiect depășește grav cadrul legal național și reprezintă o imexiune directă în activitatea ofițerului de urmărire penală, care este interzisă conform legislației (art.57 alin.(4) din CPP). Recomandări: Sub aspectul competențelor, atribuțiilor și drepturilor acordate CNPDCP-lui prin proiect considerăm absolut necesar excluderea tuturor prevederilor ce pot aduce atingere activității speciale de investigație, precum și modificarea proiectului, după cum urmează: 1) Revizuirea art.6 prin excluderea unui cumul de competențe excesive în domeniul protecției datelor cu	
--	--	---	--

			caracter personal. 2) Excluderea art.55 alin.(4) din proiect 3) Excluderea art.77-85 din proiect, precum și excluderea tuturor normelor ce aduc atingere măsurilor speciale de investigații reglementate prin Legea nr.59/2012 și Codul de procedură penală.	
		Art.20 alin.(5), art.21, art.62 alin.(4)	Articolul 20. (5) Subiectul de date are dreptul să obțină la cerere, gratuit și fără întârzieri nejustificate, accesul fizic la datele personale stocate care îl privesc și care sunt prelucrate în sistemele de evidență, în măsura în care acest drept ar putea fi susceptibil de a aduce atingere cerințelor de securitate asigurate sau din punct de vedere tehnic nu este posibil a fi realizat. Articolul 21. Dreptul la rectificare Subiectul de date are dreptul de a obține de la operator, la cerere și fără întârziere nejustificată: Articolul 62. (4) Operatorul informează în scris persoana vizată cu privire la modul în care a dat curs cererii acesteia, fără întârzieri nejustificate. Obiecții: Autorul nu impune o limită legală ce ar garanta termenul real și justificat, în care operatorii trebuie să întreprindă anumite acțiuni reglementate de norme. Astfel, se atestă prezența unor norme expuse general, care riscă să fie interpretate și aplicate în mod diferit, în raport cu fiecare operator. Considerăm că pentru a asigura drepturile și interesele tuturor părților implicate (subiecții de date, operatorii) trebuie să se specifice un termen limită (apreciat ca fiind justificat: X zile lucrătoare) în cadrul căreia operatorul va fi obligat să prezinte datele solicitate sau să realizeze alte acțiuni propuse de norme. În caz contrar, CNPDCP va putea stabili și aprecia diferențiat, în dependență de interese această întârzierea justificată/nejustificată, ceea ce reprezintă un factor de corupție, materializat prin abuz de serviciu sau din contra favoritism. Totodată, reglementările ambigue vor genera imposibilitatea tragerii la răspundere a persoanelor	Nu se acceptă. Obiecțiile invocate nu pot fi reținute. Atragem atenția că prezentul proiect prevede termeni reali și concreți în limitele cărora operatorul trebuie să întreprindă anumite acțiuni de realizare a drepturilor subiectului de date. În acest sens, stipulăm dispozițiile prevăzute la <i>Articolul 17. Transparența informațiilor, a comunicărilor și a modalităților de exercitare a drepturilor subiectului de date</i> (3) Operatorul furnizează subiectului de date informații privind acțiunile întreprinse în urma unei cereri în temeiul art. 20-27, fără întârzieri nejustificate și, în orice caz, în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Operatorul informează subiectul de date cu privire la prelungire, în termen de o lună de la primirea cererii, prezentând și motivele întârzierii. În cazul în care subiectul de date introduce o cerere în format electronic cu semnătură electronică, informațiile sunt furnizate în format electronic acolo unde este posibil, cu excepția 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 și în termen de cel mult o lună de la primirea cererii, cu privire la motivele pentru care nu s-au luat măsuri și la posibilitatea de a depune cerere la Centru și/sau să utilizeze o cale judiciară.

			vinovate pentru aplicarea abuzivă a normelor propuse în proiect. Recomandări: Stabilirea clară și expresă în norme a unui termen, ce va substitui formularea „fără întârziere nejustificată”.	
		Art.28	Articolul 28 Restricții (1) Drepturile și obligațiile prevăzute la art. 17-27 și la art. 38, precum și la art. 4, în măsura în care prevederile acestuia corespund drepturilor și obligațiilor prevăzute la art. 17-27, pot fi restricționate de un act legislativ când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică pentru: [...] h) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității publice în cazurile menționate la lit. a) - e) și lit. g); i) protecția subiectului de date sau a drepturilor și libertăților altora; Obiecții: Art.28 urmează a fi revăzut, în speță alin.(1) lit.h), lit.i), întrucât restricțiile propuse sunt redactate în mod general cu multiple trimiteri la alte articole din proiect fapt ce complică și mai mult înțelegerea textului propus, precum și limita acestor restricții. Atenționăm că aceste restricții au fost preluate din în mare parte din Directivele Europene (art.23 din Directiva (UE) 2016/679 și art.16 din Directiva (UE) 2016/680), însă atenționăm că transpunerea textului unei directive în forma sa generală, fără o concretizare prin prisma actelor legislative naționale, fără o evaluare clară a cadrului național și fără stabilirea unei coerențe între acestea două, riscă să creeze confuzii la aplicare. În primul rând, aceste norme, la fel și alte reglementări din prezentul proiect (art.12, 21 etc. din proiect) comportă un caracter declarativ, autorul operând cu termeni generali, în al doilea rând expunerile generale lasă posibilitatea interpretării normei și aplicării acesteia într-o formulă preferențială. Astfel, se atestă în	Nu se acceptă. Prin prezentul articol se impun restricții în privința unor principii specifice, în privința dreptului la informare, a dreptului de acces la datele cu caracter personal și de rectificare sau ștergere a acestora, în privința dreptului la portabilitatea datelor, a dreptului la opoziție, a deciziilor bazate pe crearea de profiluri, precum și în privința comunicării asupra unei prelucrări a datelor cu caracter personal persoanei vizate și a anumitor obligații conexe ale operatorilor, în măsura în care acest lucru este necesar și proporțional într-o societate democratică pentru a se garanta siguranța publică, inclusiv protecția vieții omului, în special ca răspuns la prevenirea, investigarea și urmărirea penală a infracțiunilor sau executarea pedepselor, inclusiv protejarea împotriva amenințărilor la adresa siguranței publice sau împotriva încălcării eticii în cazul profesiilor reglementate și prevenirea acestora, alte obiective importante de interes public general, în special un interes economic sau financiar important, menținerea de registre publice din motive de interes public general, prelucrarea ulterioară a datelor cu caracter personal arhivate pentru a transmite informații specifice legate de comportamentul politic în perioada regimurilor fostelor state totalitare, protecția persoanei vizate sau a drepturilor și libertăților unor terți, inclusiv protecția socială, sănătatea publică și scopurile umanitare. Aceste restricții ar trebui să fie conforme cu cerințele prevăzute de Carta și de Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale.

			cazul prezentului proiect că nu s-a ținut cont de prevederile legislației naționale. La fel, și multiplele trimiteri interne ca în cazul prezentei norme va complica și mai mult înțelegerea voinței legiuitorului. Conform art.54 din Legea nr.100/2017 "(1) Textul proiectului actului normativ se elaborează în limba română, cu respectarea următoarelor reguli: a) conținutul proiectului se expune într-un limbaj simplu, clar și concis, pentru a se exclude orice echivoc, cu respectarea strictă a regulilor gramaticale, de ortografie și de punctuație; b) într-o frază este exprimată o singură idee; c) terminologia utilizată este constantă, uniformă și corespunde celei utilizate în alte acte normative, în legislația Uniunii Europene și în alte instrumente internaționale la care Republica Moldova este parte, cu respectarea prevederilor prezentei legi". Prin urmare, restricțiile trebuie stabilite într-o formă concisă, pentru a fi clare tuturor subiecților interesați la aplicare, precum și pentru a se evita orice interpretare preferențială a normelor de drept. Recomandări: Reexaminarea art.28, astfel încât proiectul să prevadă clar și concis restricțiile legale la prelucrarea datelor cu caracter personal.	Restricțiile statuate la art. 28 sunt conforme cu Convenția europeană pentru apărarea drepturilor omului și a libertăților fundamentale, Regulamentul (UE) 2016/679 și Directiva (UE) 2016/680. Totodată, articolul 23 din Regulamentul (UE) 2016/679, statuează că dreptul Uniunii sau dreptul intern care se aplică operatorului de date sau persoanei împuternicite de operator poate restricționa printr-o măsură legislativă domeniul de aplicare al obligațiilor și al drepturilor prevăzute la articolele 12-22 și 34, precum și la articolul 5 în măsura în care dispozițiile acestuia corespund drepturilor și obligațiilor prevăzute la articolele 12-22, atunci când o astfel de restricție respectă esența drepturilor și libertăților fundamentale și constituie o măsură necesară și proporțională într-o societate democratică, pentru a asigura: a) protecția securității naționale; b) protecția securității statului; c) protecția ordinii publice; d) prevenirea, investigarea, descoperirea sau urmărirea penală a infracțiunilor sau executarea sancțiunilor penale, inclusiv protejarea împotriva amenințărilor la adresa ordinii publice; e) alte obiective importante ale statului de interes general, în special un interes economic sau financiar important, inclusiv în domeniile monetar, bugetar și fiscal și în domeniul sănătății publice și al securității sociale; f) protecția independenței judiciare și a procedurilor judiciare; g) prevenirea, investigarea, depistarea și urmărirea penală a încălcărilor deontologice ale profesiilor reglementate;
--	--	--	---	---

				h) funcția de monitorizare, inspectare sau reglementare legată, chiar și ocazional, de exercitarea autorității publice în cazurile menționate la lit. a) - e) și lit. g); i) protecția subiectului de date sau a drepturilor și libertăților altora; j) punerea în aplicare a pretențiilor de drept civil.
		Art.32	Reprezentanții operatorilor sau ai persoanelor care nu au sediul stabilit în Republica Moldova (1) În cazul aplicării art.2 alin.(2) lit.c) din prezenta lege, operatorii sau persoanele împuternicite de operatori care nu au sediul stabilit <u>în Republica Moldova desemnează în scris un reprezentant în Republica Moldova sau într-un stat membru UE care va fi responsabil pentru Republica Moldova.</u> (2) <u>Obligația prevăzută la alin.(1) din prezentul articol nu se aplică: a) prelucrării care are un caracter ocazional, care nu include, pe scară largă, prelucrarea unor categorii speciale de date și care este puțin susceptibilă de a genera un risc pentru drepturile și libertățile persoanelor, ținând cont de natura, contextul, domeniul de aplicare și scopurile prelucrării.</u> Obiecții: În norma propusă la alin.(1) nu este clar statuată ce presupune împuternicirea unui reprezentant (în Republica Moldova sau într-un stat membru UE) care urmează a fi responsabil pentru operatorul cu sediul în afara Republicii Moldova. Proiectul oferă o reglementare generală din care nu putem distinge competențele de bază, limitele și responsabilitățile reprezentantului menționat. La fel, nu este clar cum se va stabili procedura desemnării. Totodată, excepția de la alin.(2) este expusă într-un mod general, datorită formulărilor „care nu include, pe scară largă, prelucrarea unor categorii speciale de date și care este puțin susceptibilă de a genera un risc pentru drepturile și libertățile persoanelor”. În limitele propuse se pot încadra o mare parte a	Nu se acceptă. În partea ce vizează definirea reprezentantului, specificăm că aceasta este definită la art. 3 din proiect, astfel <i>reprezentant</i> - înseamnă persoană fizică sau juridică stabilită în 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 privește obligațiile care le revin în temeiul prezentei legi. Astfel, reprezentantului îi revine competențele, limitele și responsabilitățile operatorului sau persoanei împuternicite de operator care l-a desemnat să acționeze în numele acestuia. Totodată, operatorul desinestătător decide asupra modalității de desemnare a reprezentantului său, însă acesta trebuie să fie desemnat în mod explicit, printr-un mandat scris al operatorului (ordin, decizie, contract, etc.) sau al persoanei împuternicite de operator, să acționeze în numele acestuia (acesteia) în ceea ce privește obligațiile lor în temeiul prezentului regulament. Desemnarea unui astfel de reprezentant nu aduce atingere responsabilității sau răspunderii operatorului sau a persoanei împuternicite de operator în temeiul prezentei legi. Un astfel de reprezentant ar trebui să își îndeplinească sarcinile în conformitate cu mandatul primit de la operator sau de la persoana împuternicită de operator, inclusiv să coopereze cu autoritățile de supraveghere competente în ceea ce

			circumstanțelor, care pot fi tratate ca „nu ocupă o scară largă de date”, fapt pentru care nu necesită delegarea unui reprezentant. În cadrul supravegherii datelor cu caracter personal, autoritatea responsabilă de asemenea va fi în drept să stabilească această excepție, fără careva limite legale, apreciind fiecare caz la propria convingere - când prelucrarea este ocazională sau când aceasta „nu include, pe scară largă, prelucrarea unor categorii speciale de date”. Incluzând asemenea abordări generale la categoria excepții de la normă, implică riscuri de corupție, datorită posibilității stabilirii în mod preferențial a regulii de aplicare. Totodată, reglementările ambigui vor genera imposibilitatea tragerii la răspundere a persoanelor vinovate pentru aplicarea abuzivă a normelor propuse în proiect. Recomandări: Completarea cu norme suplimentare care să reglementeze detaliat aspectele de desemnare a unui reprezentat. Alin.(2) lit.a) trebuie expus într-o formulă limitativă a cazurilor în care operatorul nu este obligat să desemneze un reprezentant.	privește orice acțiune întreprinsă pentru a asigura respectarea prezentei legi. Cu referire la obiecțiile formulate privind ambiguitatea, menționăm că prevederile statuate sunt în strictă conformitate cu prevederile art. 27 din Regulamentul (UE) 2016/679. Neînțelegerea prevederilor legale prevăzute în proiect de către autorul expertizei nu pot fi considerate ca reglementări ambigui, iar invocarea riscurilor de corupție este nejustificată. Recomandările privind necesitatea prevederii unui mecanism de desemnare a reprezentatului operatorului nu sunt temeinice.
		Art.35 alin.(5)	(5) Obligațiile menționate la alin.(1) și (2) nu se aplică instituțiilor de drept public sau privat, cu mai puțin de 50 de angajați, <u>cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date</u>, astfel cum se prevede la art.9 alin.(1), sau date personale referitoare la condamnări penale și infracțiuni, astfel cum se menționează la art.3. Obiecții: Nu este clară excepția stabilită la art.35 alin.(5) care prevede dreptul „instituțiilor de drept public sau privat, cu mai puțin de 50 de angajați” de a fi exceptate de la ținerea unei evidențe a activităților de prelucrare a datelor cu caracter personal. Totodată, și excepția dată în continuare stabilește alte excepții „cu excepția cazului în	Nu se acceptă. Prezentul proiect de lege transpune Regulamentul (UE) 2016/679. Pentru a se lua în considerare situația specifică a microîntreprinderilor și a întreprinderilor mici și mijlocii, regulamentul în cauză include o derogare pentru organizațiile cu mai puțin de 250 de angajați în ceea ce privește păstrarea evidențelor, luând în considerare necesitățile specifice ale microîntreprinderilor și ale întreprinderilor mici și mijlocii în aplicarea prezentului regulament. În acest sens remarcăm că potrivit prevederilor expuse la art. 35 alin. (5) norma în cauză este conformă dispozițiilor Regulamentului (UE) 2016/679, în conformitate cu care „<i>Obligațiile menționate la alineatele 1 și 2 nu se aplică unei întreprinderi sau</i>

			care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate", ceea ce distorsionează sensul normei, acesta fiind neclar pentru operatori la aplicare. În mod repetat, atenționăm că stabilirea unor excepții expuse general, acordă reglementării un caracter coruptibil, în speță: autorității responsabile de supravegherea datelor cu caracter personal de a stabili, fără careva limite legale, când un operator cu mai puțini de 50 de angajați va corespunde cerințelor de la art.35 și când nu. Acestuia i se acordă dreptul de a aprecia fiecare caz în mod independent și la propria convingere. Incluzând asemenea abordări generale la categoria excepții de la normă, implică riscuri de corupție, datorită posibilității stabilirii în mod preferențial a unor reguli de aplicare. Totodată, reglementările ambigui vor genera imposibilitatea tragerii la răspundere a persoanelor vinovate pentru aplicarea abuzivă a normelor propuse în proiect. Recomandări: A se revedea art.35 alin.(5) din proiect și a propune norme concise, în care să fie clar stabilit în ce circumstanțe pot fi exceptați, operatorii care dețin sub 50 de angajați, de la respectarea prevederilor legale.	<i>organizații cu mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10."</i> În acest sens, avînd în vedere că în Republica Moldova puțini agenți economici dispun de un staff de personal mai mare de 250 angajați s-a mers inițial pe formula <i>mai puțin de 50 de angajați</i>, iar ulterior a fost redactată, fiind prevăzut un număr <i>de mai puțin de 20 de angajați</i>. Considerăm că norma dată este expusă într-o formă clară și într-un limbaj accesibil și nu crează careva confuzii de înțelegere a normei.
		Art.41	Articolul 41. Consultarea prealabilă Obiecții: Considerăm că termenii propuși la art.42 alin.(2) din proiect, pentru acordarea consultărilor prealabile operatorilor de către CNPDPC sunt extrem de mari și pot afecta interesele legale și activitatea per ansamblu, a operatorilor, spre exemplu: „Centrul oferă consultare în scris operatorului și, după caz, persoanei împuternicite de operator, în cel mult opt săptămâni de la primirea cererii [...]”. Această perioadă poate fi prelungită cu șase săptămâni, ținându-se seama de complexitatea prelucrării prevăzute. Centrul informează operatorul și, după caz, persoana împuternicită de operator, în termen	Nu se acceptă. Evaluarea impactului asupra protecției datelor este un proces destinat să descrie prelucrarea, să evalueze necesitatea și proporționalitatea acesteia și să contribuie la gestionarea riscurilor la adresa drepturilor și libertăților persoanelor vizate rezultate din prelucrarea datelor cu caracter personal, prin evaluarea acestora și stabilirea de mpsuri pentru atenuarea lor. Evaluarea impactului reprezintă un instrument important pentru responsabilizare deoarece ajută operatorii de date nu numai să respecte cerințele prezentei legi, ci și să demonstreze că au fost luate măsuri adecvate pentru a asigura conformitatea cu

			de cel mult două luni de la primirea cererii, cu privire la orice astfel de prelungire". După cum s-a specificat în obiecțiile anterioare vis-a-vis de obligativitatea operatorilor de a acționa „fără întârzieri nejustificate” (obiecția de la pct.5 cap.III al prezentului raport), în redacția dată deja se prezintă viceversa CNPDCP stabilește termeni exagerați de lungi pentru executarea atribuțiilor/responsabilităților ce le revin. Considerăm că acordarea unei consultații în termen ce depășește 30 de zile lucrătoare, deja este o prelungire exagerată, care permite tergiversarea timpului și nicidecum nu contribuie la responsabilizarea angajaților acestei structuri. Recomandări: A se revedea termenii propuși, întrucât aceștia pot stopa, fie suspenda activitatea operatorilor, în temeiuri neîntemeiate/subiective.	prezenta lege. Cu alte cuvinte, evaluarea impactului asupra protecției datelor reprezintă un process pentru construirea și demonstrarea conformității. Termenii prevăzuți în acest articol sunt prevăzuți de Regulamentul (UE) 2016/679, ținând cont de necesitatea evaluării multilaterale a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. În aceste condiții, acești termeni sunt stabiliți reieșind din complexitatea examinării criteriilor necesare efectuării evaluării impactului asupra protecției datelor, aprecierii riscurilor care pot fi generate, precum și dictarea măsurilor concrete ce urmează a fi luate de operator. Alin. (2) descrie situația, în care o evaluare a impactului asupra protecției datelor arată că operațiunile de prelucrare implică un risc ridicat, pe care operatorul nu îl poate atenua prin măsuri adecvate sub aspectul tehnologiei disponibile și al costurilor implementării și trebuie să consulte în acest sens autoritatea de supraveghere înainte de prelucrare, care la rândul ei reieșind din complexitatea prelucrării necesită un termen rezonabil pentru examinare pentru a oferi o consultație adecvată operatorilor.
		Cap.VII potrivit proiectului de lege	Capitolul VII „ Prevederi speciale privind prelucrarea datelor personale de către organele de ocrotire a legii”. Art.55 Domeniul de aplicare al capitolului. Art.69 Generarea înregistrărilor de audit. Art.70 Obligația organului de ocrotire a legii de în raport cu atribuțiile Centrului. Art.71 Ținerea excepțiilor și înregistrarea acestora. Art.74 Transferuri de date personale către alți destinatari în afara Republicii Moldova. (4) Organul de ocrotire a legii informează Centru, cu privire la transferurile efectuate în temeiul prezentului articol până	Nu se acceptă. Orice prelucrare a datelor cu caracter personal trebuie să fie legală, echitabilă și transparentă față de persoanele fizice în cauză, iar prelucrarea trebuie să fie făcută numai pentru scopuri specifice prevăzute de lege. Acest lucru nu împiedică, în sine, autoritățile de aplicare a legii să desfășoare activități precum investigațiile sub acoperire sau supravegherea video. Totodată, persoanele fizice trebuie să fie informate cu privire la riscurile, normele, garanțiile și drepturile în materie de prelucrare a datelor acestora cu

			la efectuarea transferului sau în termen de două zile de la efectuarea transferului, în caz contrar Centru va constata încălcarea principiilor de protecție a datelor personale și prevederile prezentei norme. Obiecții: În ceea ce privește efectuarea unor investigații asupra organelor de drept, stabilite în prezentul capitol, recomandăm autorului să revadă argumentele invocate la pct.4 cap.III din prezentul raport de expertiză anticorupție, ele fiind valabile și pentru prezentul capitol. Conform proiectului, articolul 69 Generarea înregistrărilor de audit, prevede că organul de ocrotire a legii este obligat să țină evidența înregistrărilor de audit a operațiunilor de prelucrare a datelor personale în sistemele automatizate: colectare, culegere, consultare, modificare, dezvăluire, răspândirea, imprimare, transfer, combinare și ștergere. Se consideră că prevederile respective trebuie să se refere la administratorii sistemelor informaționale, care urmează să efectueze auditul operațiunilor, iar sistemele informaționale gestionate să fie dotate cu rubrici privind temeiul accesării datelor. Altfel, organele de ocrotire a legii vor fi obligate să asigure evidența în multiple registre la toate procesele de lucru cu datele, fapt ce ar implica resurse umane și timp suplimentar. La fel, art.70 și 71 din proiect stabilește multiple raportări și evidențe vis-a-vis de prelucrarea datelor cu caracter personal, fapt ce implică multiple resurse pentru a asigura toate aceste cerințe care sunt într-o măsură excesivă și deviază de la atribuțiile de bază pe care trebuie să pună accent organele de investigație. Unele prevederi de la art.71 sunt expuse într-un mod confuz din care nu poate fi destins cu exactitate scopul legiuitorului, aici ne referim la formularea „(4) Neaplicarea excepțiilor, omiterea termenului de prelungire a excepțiilor sau depășirea acestora, exclude posibilitatea aplicării excepțiilor pe aceleași temeiuri de	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. 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. Datele cu caracter personal trebuie prelucrate doar în cazul în care scopul prelucrării nu poate fi îndeplinit, în mod rezonabil, prin alte mijloace. Excluderea organelor de ocrotire a legii de la domeniul de aplicare a prezentei lei ar constitui o încălcare flagrantă a drepturilor persoanelor vizate privind prelucrarea datelor cu caracter personal, drept garantat prin acte internaționale și naționale. În contextul activităților de investigare și de asigurare a conformității prelucrării datelor cu caracter personal în sectorul polițienesc și în vederea implementării 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 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, prezentul proiect de lege vine cu un capitol întreg destinat prelucrării datelor cu caracter personal de către organele de ocrotire a legii, și anume capitolul VII, care reglementează atribuția Centrului de supraveghere, reglementa și investiga
--	--	--	--	---

			drept.". Astfel, în mod repetat, atenționăm că normele trebuie să corespundă cerințelor stabilite la art.54 din Legea nr.100/2017 privind actele normative. Toate formulările ambigui, în special cele ce care fac referire la careva cerințe, trebuie expuse exact pentru a elimina orice interpretare abuzivă la aplicare (în special recomandăm a se revedea art.67 alin.(2), 68 alin.(3) alin.(4), art.71 alin.(4) art.74 alin.(1) lit.c) și d) din cap.VII al proiectului), în caz contrar proiectul implică riscuri de coruptibilitate. Totodată, reglementările ambiguu vor genera imposibilitatea tragerii la răspundere a persoanelor vinovate pentru aplicarea abuzivă a normelor propuse în proiect. Recomandări: Excluderea conținutului textului capitolului VII din proiect și includerea unei norme, precum: „Prezenta lege nu se aplică de către organele de ocrotire a legii prelucrărilor de date cu caracter personal efectuate în scopul prevăzut la art.2 alin.(2) lit.d) din lege”.	modul de prelucrare a datelor personale de către organele de drept în conformitate cu prezentul proiect de lege și Legea privind Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova. Obecția CNA cu referire la excluderea Capitolul VII „<i>Prevederi speciale privind prelucrarea datelor personale de către organele de ocrotire a legii</i>” a trezit nedumerire, iar dispozițiile legiutorului românesc invocate nu sunt relevante. În acest sens, ținem să menționăm că în conformitate Articolul I - Obiect și obiective din Directiva (UE) 2016/680, Prezenta directivă stabilește normele referitoare la protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora. „Autoritate competentă” înseamnă: (a) <i>orice autoritate publică competentă în materie de prevenire, depistare, investigare sau urmărire penală a infracțiunilor sau de executare a pedepselor, inclusiv în materie de protejare împotriva amenințărilor la adresa securității publice și de prevenire a acestora; sau</i> (b) <i>orice alt organism sau entitate împuternicit(ă) de dreptul intern să exercite autoritate publică și competențe publice în scopul în prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora.</i> În aceste condiții, nu s-a putut reține argumentarea juridică de excludere de la prezenta lege activitatea de
--	--	--	---	--

				prelucrare a datelor cu caracter personal efectuată de către organele de octrotire a Legii în scopul prevăzut la art.2 lit.d) din lege. Context în care, urmează a fi reliefate la moment următoarele prevederi în vigoare și de aplicare ale Legii nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal: <i>Articolul 2 alin. (2) lit. d) - domeniul de acțiune al acestei legi se extinde asupra prelucrării datelor cu caracter personal în cadrul acțiunilor de prevenire și investigare a infracțiunilor, punerii în executare a sentințelor de condamnare și al altor acțiuni din cadrul procedurii penale sau contravenționale în condițiile legii.</i> Remarcăm faptul că, în cazul excluderii Capitolului VII de la aplicabilitatea legii privind protecția datelor cu caracter personal, urmează a fi modificate declarațiile depuse de Republica Moldova la Convenția nr. 108, cu notificarea Secretarului General al Consiliului Europei. În partea ce ține de transmiterea transfrontalieră, atragem atenția că orice transmitere transfrontalieră de către CNA, fără autorizarea Centrului este ilegală cu excepția cazurilor statuate de art. 32 din Legea 133/2016 (cu consimțământul subiectului datelor cu caracter personal; în baza prevederilor unei legi speciale sau ale unui tratat internațional; dacă aceasta este necesară pentru a proteja viața, integritatea fizică sau sănătatea subiectului datelor cu caracter personal etc.) pe când prevederile din proiectul dat acordă o marjă de acțiune organelor de drept extrem de mare punând aceste autorități pe picior de egalitate cu autoritățile din UE. Considerăm că autorul expertizei nu a intrat în esența modificărilor propuse și importanța acestora pentru activitatea organelor de drept și a dat o apreciere confuză și nejustificată a normelor statuate în acest capitol.
--	--	--	--	--

					Capitolul VII este o transpunere a Directivei 2016/680 și stabilește, inclusiv excepțiile care vor fi utilizate de organele de drept în activitatea lor, creînd un cadru normativ viabil și clar în scopul excluderii unor abuzuri din partea organelor de drept și apărarea drepturilor și libertăților fundamentale ale omului, apărare prin convenții internaționale. În cadrul controalelor efectuate, Centrul nu o singură dată a constatat că prelucrarea datelor cu caracter personal de către organele de drept a fost un abuzivă, fiind efectuată în lipsa unui temei legal. Remarcăm că în aceste situații Deciziile Centrului, urmare a contestării, nu au fost anulate de instanța de judecată, astfel fiind supuse controlului judecătoresc. De altfel, o mare parte din decizii prin care au fost constatate încălcări, nu au fost contestate în instanță de organele de drept, acestea fiind de acord cu concluziile și soluțiile Centrului.
		Art.89		Articolul 89. Răspunderea administrativă pentru neîndeplinirea prevederilor prezentei legi (4) Pentru încălcările următoarelor dispoziții, în conformitate cu alin. (2), se aplică sancțiuni pecuniare de până la 250 000 EUR, calculat la cursul oficial al leului moldovenesc la data comiterii încălcării, sau, în cazul unei întreprinderi, de până la 2 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare: a) obligațiile operatorului și ale persoanei împuternicite de operator în conformitate cu art. 8 alin. (4), 10, 30-44, 47 și alin. 48; b) obligațiile organismului de certificare în conformitate cu art. 47 și 48; c) obligațiile organismului de monitorizare în conformitate cu art. 46. (5) Pentru încălcările următoarelor dispoziții, în conformitate cu alin. (2), se aplică sancțiuni pecuniare de până la 500 000 EUR, calculat la cursul oficial al leului moldovenesc la data	Nu se acceptă. Urmează a menționa că noul Regulament 2016/679, la art. 83 prevede dreptul autorităților naționale de supraveghere de a aplica amenzi administrative. La moment se constată ineficiența măsurilor punitive în vigoare, care se manifestă prin caracterul îndelungat al examinării de către instanțele de judecată a cauzelor contravenționale pornite de Centru. Mai mult, soluționarea cauzelor contravenționale prin recunoașterea vinovăției contravenienților și sancționarea acestora în limitele prevăzute la art. 74¹-74³ Cod contravențional, se rezumă la constatarea de către instanța de judecată a faptelor contravenționale comise, fără a dispune obligarea contravenientului în vederea înlăturării cauzelor ce au dus la comiterea încălcărilor vizate.

			comiterii încălcării, sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare: a) principiile de bază pentru prelucrare, inclusiv condițiile privind consimțământul, în conformitate cu art. 4, 5, 8 și 9; b) drepturile persoanelor vizate în conformitate cu art. 17-27; c) transferurile de date cu caracter personal către un destinatar dintr-o altă țară sau o organizație internațională, în conformitate cu art. 49-54; d) orice obligații în temeiul legislației naționale adoptate în temeiul art. 12, 14, 15, 16 și 92. (6) Pentru neexecutarea deciziei, ordinului, instrucțiunii sau oricărui alt act administrativ emis de Centru, se aplică, în conformitate cu alin. (2) din prezentul articol, sancțiuni pecuniare de până la 500 000 EUR, calculat la cursul oficial al leului moldovenesc la data comiterii încălcării, sau, în cazul unei întreprinderi, de până la 4 % din cifra de afaceri mondială totală anuală corespunzătoare exercițiului financiar anterior, luându-se în calcul cea mai mare valoare. Obiecții: De asemenea, sancțiunile pecuniare prevăzute la art.89 în mărime de până la 250 000 EURO și respectiv, 5000 000 EURO, pentru încălcarea prevederilor Legii privind protecția datelor cu caracter personal sunt excesive și nu sunt bine determinate, în ce cazuri urmează a fi aplicate aceste sancțiuni, lăsând loc de multiple interpretări. După cum am menționat anterior, luând în ansamblu modul de reglementare general (preluat exact din textul directivelor europene), cerințele impuse operatorilor (la fel general reglementate), procedura „investigării” și sancțiunile pecuniare propuse din care 25% vine în bugetul instituțional, riscă să creeze un mecanism de control abuziv al tuturor subiecților ce operează cu datele cu caracter personal, precum și	Într-o altă ordine de idei, urmează a menționa că noul Regulament 2016/679, la art. 83 prevede dreptul autorităților naționale de supraveghere de a aplica amenzi administrative. De altfel, în prezent art. 34 din Codul contravențional limitează cuantumul maxim al amenzilor pasibil a fi aplicate. Totodată, ținând cont de realitățile din Republica Moldova, în proiectul vizat se propune un mecanism treptat de aplicare a sancțiunilor pentru a nu împovăra operatorii de date și a le permite să se adapteze noilor rigori europene. Într-o altă ordine de idei, trebuie de menționat că în Republica Moldova există practici când autoritățile de control pot impune prin decizia sa sancțiuni pecuniare cum ar fi spre exemplu Consiliul concurenței, Banca Națională a Moldovei, CNPF. Nu în ultimul rând, urmează a remarca că în ordinea Legii cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, în cazul nerespectării prevederilor prezentei legi și ale actelor subordonate acestei legi, față de entitățile raportoare se aplică sancțiuni pecuniare sub formă de amendă: – în mărime dublă din valoarea beneficiului rezultat din încălcarea obligațiilor prevăzute de prezenta lege, în cazul în care beneficiul respectiv poate fi stabilit, sau în mărimea echivalentului în lei al sumei de până la 1000000 de euro, calculat conform cursului oficial al leului moldovenesc la data comiterii încălcării; – în mărime de până la echivalentul în lei al sumei de 5000000 de euro, calculat la cursul oficial al leului moldovenesc la data comiterii încălcării, sau 10% din cifra de afaceri pentru anul precedent – pentru entitățile raportoare de la art. 4 alin. (1) lit. a), c), h) și i).
--	--	--	--	--

			aplicarea sancțiunilor pecuniare în mod abuziv. Totodată, amenziile propuse vor spori interesul angajaților de a constata încălcări, în mod nelimitativ, stabilind neconformități datorită cerințelor stabilite în mod general/neclar, în tot textul proiectului. În lipsa unor cerințe clar reglementate și în raport cu sancțiunile propuse pentru încălcarea acestora, normele propuse la art.89 aduc atingere directă drepturilor fundamentale ale omului consacrate de Constituția Republicii Moldova, prin prisma art.23 alin.(2) care garantează expres - Dreptul fiecărui om de a-și cunoaște drepturile și îndatoririle „Statul asigură dreptul fiecărui om de a-și cunoaște drepturile și îndatoririle. În acest scop statul publică și face accesibile toate legile și alte acte normative.”. În acest sens, atenționăm că proiectul oferă o reglementare generală a temeiurilor pentru care operatorii sunt pasibili de răspundere administrativă (art.89 alin.(2), (4), (5), (6)). La fel, nu sunt oferite limite clare la aprecierea amenzii, CNPDCP „acordând o atenție sporită” unor factori expuși la fel general, ceea ce acordă un risc sporit de corupție întregului proiect. Potrivit, Hotărârii Curții Constituționale nr.26 din 23.11.2010 „Pentru a corespunde celor trei criterii de calitate - accesibilitate, previzibilitate și claritate - norma de drept trebuie să fie formulată cu suficientă precizie, astfel încât să permită persoanei să decidă asupra conduitei sale și să prevadă, în mod rezonabil, în funcție de circumstanțele cauzei, consecințele acestei conduite. În caz contrar, cu toate că legea conține o normă de drept care aparent descrie conduita persoanei în situația dată, persoana poate pretinde că nu-și cunoaște drepturile și obligațiile. Într-o astfel de interpretare, norma ce nu corespunde criteriilor clarității este contrară art.23 din Constituție [...]”. Totodată, nota informativă nu cuprinde argumente viabile cu referire la sumele invocate, nefiind prezentate	Atragem atenția că CNA în calitate de autor al Legii cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, nu a prevăzut în conținutul acesteia nici o garanție sau procedură de aplicare a sancțiunilor, în comparație cu proiectul prezentei legi elaborate de Centru (art. 89 alin. (2)), care este obligatoriu pentru determinarea cuantumului sancțiunii. Toate obiecțiile CNA sunt subiective și neîntemeiate. În concluzie menționăm, că conținutul proiectului de lege este unul previzibil și nu există criterii care ar demonstra elemente de coruptibilitate, fiind total compatibil cu Directiva nr. 2016/680 și Regulamentul (UE) 2016/679. Totodată, admitem că este o lege complexă, care necesită o atenție deosebită pentru înțelegere și aplicare. În viziunea Centrului normele consemnate în proiectul de lege nu sunt ambigui, fiind proporționale scopurilor propuse și corespund relațiilor economice din RM, iar orice obstrucționare privind adoptarea și implementarea acestei legi va atrage împiedicarea dezvoltării relațiilor economice cu alte state, atragerii investițiilor, recunoașterii RM în calitate de stat care asigură un nivel de protecție adecvat de protecție a datelor, condamnării RM la CEDO în partea ce ține de asigurarea protecției drepturilor și libertăților fundamentale ale persoanei fizice în ceea ce privește prelucrarea datelor cu caracter personal, în special a dreptului la inviolabilitatea vieții intime, familiale și private.
--	--	--	---	---

			careva date din care să rezulte cuantumul stabilit, un calcul estimativ care denotă stabilirea anume a acestor sume și nu mai mici. Argumentul autorului precum că „se propune un mecanism treptat de aplicare a sancțiunilor pentru a asigura o perioadă de tranziție în vederea adoptării de către operatorii de date la noile rigori și standarde europene” nu constituie temei justificativ pentru stabilirea mărimii sancțiunii pecuniare, precum este propus în proiect. De asemenea, cu referință la reglementările europene, argumentele invocate nu pot fi acceptată, deoarece la stabilirea unei sancțiuni trebuie să se țină cont de principiul proporționalității și rezonabilității, de contextul social al Republicii Moldova, gravitatea încălcării și alte aspecte. În acest sens, însăși Directiva nr.2016/680 al Parlamentului European și a Consiliului din 27.04.2016 consacră la art.57 principiul proporționalității „Statele membre definesc normele privind sancțiunile aplicabile în cazurile de încălcare a dispozițiilor adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a se asigura că acestea sunt puse în aplicare. Sancțiunile prevăzute trebuie să fie eficace, proporționale și disuasive”. Totodată, nu este clară ce presupune sintagma „în cazul unei întreprinderi”, deoarece avem mai multe forme de organizare ale persoanelor juridice (întreprindere de stat, municipală, societate pe acțiuni etc.) și nu este clar dacă termenul dat se vor răsfrânge asupra tuturor persoanelor juridice ce vor activa și vor obține/produce în urma activității date un profit. Recomandări: Reformularea articolului 89 astfel, încât să corespundă realității social-economice a Republicii Moldova și aspectelor menționate mai sus. Sancțiunile propuse în proiect nu sunt oportune. A se revedea termenul de „întreprinderi”, întrucât se impune o concretizare în acest sens.	
--	--	--	---	--

	Ministerul Finanțelor	La Art. I	Se propune de exclus alin. (26) al articolului 81, dat fiind că nu constituie obiectul unei legi. Privind prevederile articolului 92 alineatele (4)-(6) considerăm oportun ca sancțiunile propuse să fie stabilite în moneda națională, dat fiind conform art. 130 din Constituție, moneda națională este leul moldovenesc. Articolul 94 se propune de exclus din proiectul dat de lege, deoarece prevederile acestuia nu reprezintă obiectul de reglementare a legii menționate. Dispozițiile respective se conțin în prevederile Codului Contravențional nr.218/2008, iar amenzile constatate de către Centru se varsă integral la bugetul de stat. Conform articolului 17 alin.(3) al „<i>Legii finanțelor publice și responsabilității bugetar-fiscale nr.181 din 25 iulie 2014</i>, se interzice stabilirea prin alte acte normative decât legea/decizia bugetară a unor sume sau cote procentuale din buget sau din produsul intern brut destinate anumitor domenii, sectoare sau programe. Astfel, prevederile alineatului 1 referitor la vărsarea a 25 la sută din amenzi în bugetul centrului contravin legislației în vigoare.	1) Cu referire la obiecțiile aduse la art. 81 alin. (26) din proiect, considerăm că acestea sunt irelevante nefiind aduse careva argumente justificate, pentru a sesiza esența obiecției înaintate. 2) Cu privire la stabilirea sancțiunilor, expuse în art. 92 alin. (4)-(6), în moneda națională, atragem atenția asupra faptului că aplicarea amenzilor se va efectua în MDL. Nu în ultimul rând, consemnăm că, conform prevederilor art. 89 din proiectul legii sancțiunea va fi aplicată în MDL, calculată în dependență de valoarea euro la data comiterii abaterii. În aceste condiții, considerăm că norma în cauză este conformă prevederilor legale invocate. Totodată, menționăm că o astfel de modalitate de stabilire a amenzilor în euro a fost remarcată în Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului nr. 308 din 22 decembrie 2017. 3) Cu referire la obiecțiile aduse la art. 94, relatăm că CNPDCP nu va aplica amenzi conform prevederilor Codului Contravențional. Amenzile administrative fac parte și sînt obiectul Legii privind protecția datelor cu caracter personal și vor fi aplicate pentru încălcarea legislației în domeniu. Această situație reiese și din prevederile noului Regulament 2016/679, care la art. 83 prevede dreptul autorităților naționale de supraveghere de a aplica amenzi administrative. La moment se constată ineficiența măsurilor punitive în vigoare, care se manifestă prin caracterul îndelungat al examinării de către instanțele de judecată a cauzelor contravenționale pornite de CNPDCP. Mai mult, soluționarea cauzelor contravenționale prin recunoașterea vinovăției contravenienților și sancționarea acestora în limitele prevăzute la art. 74¹-74³ Cod contravențional, se rezumă la constatarea de
--	--------------------------	-----------	--	---

				către instanța de judecată a faptelor contravenționale comise, fără a dispune obligarea contravenientului în vederea înlăturării cauzelor ce au dus la comiterea încălcărilor vizate. De altfel, în prezent art. 34 din Codul contravențional limitează cuantumul maxim al amenzilor pasibil a fi aplicate. Totodată, ținând cont de realitățile din Republica Moldova, în proiectul vizat se propune un mecanism treptat de aplicare a sancțiunilor pentru a nu împovăra operatorii de date și a le permite să se adapteze noilor rigori. O practică analogică există deja fiind statuată în Legea Concurenței nr. 183 din 11 iulie 2012, în Legea cu privire la Banca Națională a Moldovei nr. 548-XIII din 21 iulie 1995, în Legea privind Comisia Națională a Pieței Financiare nr. 192-XIV din 12 noiembrie 1998, etc. 4) Totodată remarcăm, că obiecția în legătură cu vărsarea a 25 % din amenzile stabilite pentru încălcarea legislației cu privire la protecția datelor cu caracter personal în bugetul CNPDCP este irelevantă și nu are un substrat juridic. Subliniem că, asemenea procedură este prevăzută în activitatea mai multor autorități, spre exemplu Inspectoratul General al Poliției (IGP) din cadrul Ministerului Afacerilor Interne reține un anumit procent din amenzi, care ulterior sînt folosite în scopul stimulării financiare a agenților constatați din cadrul IGP, reglementările fiind stipulate în Hotărîrea Guvernului nr. 172 din 22 martie 2017. În urma acumulării unor resurse financiare suplimentare, CNPDCP va avea posibilități mai ample în vederea implementării politicilor în domeniul protecției datelor cu caracter personal, ca de exemplu:
--	--	--	--	---

				angajarea experților din domeniu, efectuarea vizitelor cu scopul schimbului de experiență, dotarea tehnico-materială a CNPDCP, organizarea instruirilor, promovarea și sensibilizarea domeniului protecției datelor cu caracter personal în rândul cetățenilor etc.
		La Art. II	Articolul II urmează a fi exclus în întregime din următoarele considerente: Modificarea vizează introducerea unui spor pentru eficiență în activitate în mărime de 1,5 din salariul lunar pentru persoanele cu funcții de demnitate publică și funcționarii publici cu statut special; majorarea gradelor de salarizare pentru funcțiile actuale de funcționari publici, ce, în consecință, va genera costuri suplimentare neprevăzute în buget. În același timp, actualmente Ministerul Finanțelor definitivează proiectul noii legi privind sistemul unitar de salarizare în sectorul bugetar, care se preconizează a fi pusă în aplicare începând cu 1 ianuarie 2019. Luând în considerare, că modificările pentru Legea nr. 355/2005 și Legea nr. 48/2012 se propun a fi implementate din 1 martie 2019, se consideră inoportună intervenția în actele normative menționate, odată ce acestea vor fi abrogate din momentul adoptării legii noi.	Actualmente angajații CNPDCP dispun de un sistem de salarizare net inferior plafonului de salarizare a angajaților din cadrul autorităților pe care le verifică. Cu toate acestea Parlamentul Republicii Moldova, începând cu septembrie 2017 până în iulie 2018 a adoptat un set de acte normative prin care a extins competențele și atribuțiile exercitate de către CNPDCP, fiind adoptate Legea comunicațiilor electronice, nr. 241-XVI din 15 noiembrie 2007 (republicată și modificată), Legea nr. 120 din 21 septembrie 2017 cu privire la prevenirea și combaterea terorismului, Legea nr. 308 din 22 decembrie 2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, Legea nr. 142 din 19 iulie 2018 cu privire la schimbul de date și interoperabilitate. În aceste condiții, noile atribuții stabilite CNPDCP prin actele normative precitate schimbă esențial paleta activităților de investigare și de asigurare a conformității prelucrării datelor cu caracter personal, ținând cont de faptul că autoritățile supuse controlului prelucrează un volum enorm de date cu caracter personal care sunt atribuite, inclusiv la secret de stat, comercial, bancar, profesional etc.

				Spre regret odată cu adoptarea noilor acte normative nu s-au prevăzut și surse pentru implementarea acestora, nu au fost evaluate posibilitățile CNPDCP de a efectua un control eficient și calitativ în raport cu complexitatea atribuțiilor, numărul de angajați, salarizarea adecvată. Un alt aspect important de menționat sunt și noile modificări și completări propuse de proiectele de legi elaborate, potrivit cărora CNPDCP va investiga operațiunile de prelucrare a datelor cu caracter personal în cadrul prevenirii, investigării, depistării și/sau urmăririi penale a infracțiunilor sau executării pedepselor penale, detenția preventivă, inclusiv protejarea și prevenirea amenințărilor la adresa ordinii publice, securității de stat și securității naționale și în cadrul dosarului sau acțiunilor speciale de investigație. Majorarea sistemului de salarizare a angajaților din cadrul CNPDCP, reiese și din politica de sporire a sistemului de salarizare a funcționarilor din cadrul tuturor instituțiilor care sunt susceptibile de a fi investigate de către CNPDCP, cum ar fi, dar care nu se limitează la: Autoritatea Națională de Integritate, Comisia Electorală Centrală, Serviciul de Prevenire și Combaterea Spălării Banilor, Centrul Național Anticorupție, Serviciul Vamal, Serviciul Fiscal etc. Atragem atenția asupra faptului că inițial norma de la art. 4 alin. (2) din proiect nu s-a regăsit
--	--	--	--	---

					în proiectul Legii cu privire la CNPDCP. Acesta a fost introdus în urma recomandărilor domnului Bernhard Bannasch, expert a Comisiei Europene din cadrul proiectului Twinning „<i>Consolidarea capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova</i>”, finanțat de Uniunea Europeană prin intermediul Fundației Germană pentru Cooperare Juridică Internațională (IRZ) și Ministerul Justiției din Letonia, în cadrul prezentării Raportului Misiunii cu trecerea pe agendă a observațiilor și recomandărilor la proiectul de Lege privind Centrul Național pentru Protecția Datelor cu Caracter Personal, care a notat că, resursele umane sunt o condiție pentru impactul real al oricărei autorități de supraveghere a prelucrării datelor cu caracter personal, iar remunerarea adecvată a angajaților CNPDCP, inclusiv și a celor cu funcții de demnitate publică, trebuie să fie echivalent cu nivelul de remunerare a unui judecător din cadrul Curții Constituționale. La data de 14 mai 2018, Comisia securitate națională, apărare și ordine publică a Parlamentului Republicii Moldova (în continuare Comisia), prin Decizia privind rezultatele audierii raportului de activitate al Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova pentru perioada 2017 a subliniat că, în comparație cu anul 2016, se
--	--	--	--	--	---

				constată o creștere semnificativă a volumului și complexității sarcinilor funcționale ale CNPDCP. În aceeași ordine, Comisia a notat că deși prin Legea nr. 156 din 20 iulie 2017 a fost majorat efectivul-limită de personal al CNPDCP, menținerea specialiștilor existenți și angajarea în serviciu a unor profesioniști noi rămâne a fi dificilă din cauza sistemului de salarizare neatractiv stabilit pentru funcționarii din cadrul Centrului. Pe finalul constatărilor, Comisia, luând în considerație importanța asigurării unui nivel adecvat al protecției datelor cu caracter personal în Republica Moldova, <u>a recomandat CNPDCP să întreprindă toate acțiunile necesare în vederea soluționării problemelor aferente personalului, sistemului de salarizare și cadrului normativ regulator adecvat, pentru eficientizarea controalelor legalității prelucrării datelor cu caracter personal inițiate de Centru.</u> Considerentele enunțate supra constituie o motivare fermă, dar și o necesitate imperioasă de modificare a cadrului legal în vederea majorării plafonului de salarizare al funcționarilor din cadrul CNPDCP.
--	--	--	--	---

422, 421

Partnership for Good Governance



**Avizul de specialitate privind
conformitatea legilor referitoare la
protecția datelor cu caracter personal din Republica
Moldova
cu Convenția CoE pentru protejarea persoanelor față de
prelucrarea automatizată a datelor cu caracter personal
(Convenția 108)
și alte standarde europene**

de către

Maria Michaelidou și Nevena Ruzić, experți ai Consiliului Europei

2017

Acest document a fost elaborat în cadrul unui proiect co-finanțat de către Uniunea Europeană și Consiliul Europei. Opiniile exprimate în prezentul document nu pot fi considerate, în niciun caz, ca reflectând poziția oficială a uneia dintre părți.

Analiză de specialitate cu privire la legislația privind protecția datelor din Republica Moldova

Analiză de specialitate cu privire la legislația privind protecția datelor din Republica Moldova

**Aviz privind
conformitatea legilor referitoare la protecția datelor cu
caracter personal din Republica Moldova
cu Convenția CoE pentru protejarea persoanelor față de
prelucrarea automatizată a datelor cu caracter personal
(Convenția 108)**

Întocmit de
Maria Michaelidou, expertă a Consiliului Europei

5 octombrie 2017

Introducere

Mi s-a solicitat să prezint o analiză de specialitate a legilor revizuite privind protecția datelor din Moldova în cadrul programului comun Parteneriat pentru o bună guvernare (PBG) al Uniunii Europene/Consiliului Europei.

Trebuie menționat faptul că în mai 2016, Consiliul Europei a prezentat două analize juridice privind aceleași legi (legea privind protecția datelor și proiectul de lege privind CNPDPC). Au fost furnizate comentarii privind conformitatea legislației naționale și a noului proiect legislativ și au fost făcute recomandări privind modul de asigurare a conformității depline a acestora cu standardele Consiliului Europei.

Prezenta analiză examinează proiectul de lege privind protecția datelor cu caracter personal, astfel cum a fost revizuit în luna aprilie și apoi în luna august (?) 2017 (numită în continuare „legea revizuită privind protecția datelor”), care modifică legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal și proiectul de lege privind Centrul Național pentru Protecția Datelor cu Caracter Personal, elaborat în aprilie 2017 și revizuit în septembrie 2017 (numit în continuare „proiect de lege privind CNPDPC”).

Prezentul aviz se bazează pe Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (numită în continuare „Convenția 108”) și pe protocolul său adițional. Câteva dintre recomandările Consiliului Europei, în special cea privind crearea de profiluri, au fost, de asemenea, luate în considerare la analiza dispozițiilor legilor privind protecția datelor. Versiunea modernizată a Convenției mai sus menționate (numită în continuare „Convenția 108 modernizată”) a constituit, de asemenea, bază pentru analiză, deoarece va deveni regulă în viitorul apropiat.

În final, avizul ia în considerare, unde este cazul, Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestora și de abrogare a Directivei 95/46/CE (numit în continuare RGPD).

Analiza urmărește ordinea articolelor, astfel cum este prevăzută în Convenția 108 și, după caz, Convenția 108 modernizată.

Aș dori să subliniez faptul că studiul a fost efectuat cu foarte puține cunoștințe anterioare, dacă au existat, privind contextul politic și legislativ din Republica Moldova. Orice omisiune sau interpretare greșită este responsabilitatea exclusivă a autorului. În general, comentariile exprimate în prezentul raport trebuie înțelese ca

posibile probleme, fiind necesare discuții ulterioare cu autoritățile naționale și nu pot fi, în niciun caz, considerate ca având un caracter concludent.

Obiect și scop

Scopul Convenției 108 este de a asigura pentru fiecare persoană, indiferent de naționalitatea sau reședința acesteia, respectarea drepturilor și a libertăților fundamentale și, în special, dreptul acesteia la viața privată în legătură cu prelucrarea datelor cu caracter personal cu privire la persoana în cauză.

Articolul 1 din legea revizuită privind protecția datelor prevede faptul că „*scopul legii este de a asigura dreptul la protecția datelor cu caracter personal, care derivă din dreptul intangibil constituțional la intimitate, viață de familie și viață privată*”.

Legea revizuită privind protecția datelor nu definește clar în domeniul său de aplicare faptul că legea se aplică fiecărei persoane, indiferent de naționalitatea sau reședința acesteia. Nu poate fi găsită nicio referire la noțiunea de persoană fizică sau individ în articolul 2 din legea revizuită privind protecția datelor, care tratează domeniul de aplicare.

Scopul și domeniul de aplicare al legii reprezintă puncte principale. Se propune să se analizeze din nou formularea articolului 1 și să se stipuleze faptul că „*scopul legii este de a asigura dreptul la protecția datelor cu caracter personal, pentru fiecare persoană, indiferent de naționalitatea sau reședința acesteia*”.

Definiții

Definițiile în temeiul articolului 3 din legea revizuită privind protecția datelor sunt compatibile cu standardele prevăzute prin Convenția 108, iar noțiunile esențiale de „date cu caracter personal”, „prelucrarea datelor” și „operator” sunt compatibile cu Convenția 108 și Convenția modernizată. Cu toate acestea, două concepte trebuie analizate și comentate în continuare.

1) Crearea de profiluri

Legea revizuită privind protecția datelor definește crearea de profiluri ca fiind orice formă de prelucrare automată a datelor cu caracter personal, care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a revizui sau a prevedea aspecte legate de performanța la locul de muncă, situația economică, sănătate, preferințe personale, interese, veridicitate, comportament, locația persoanei fizice în cauză sau călătoriile acesteia.

La nivelul Consiliului Europei, definiția creării de profiluri este furnizată în Recomandarea CM/Rec(2010)13 și se spune că este „o tehnică automată de prelucrare a datelor, care constă în aplicarea unui «profil» (adică a unui set de date

care caracterizează o categorie de persoane) unei persoane, în special pentru a lua decizii cu privire la aceasta sau pentru analizarea sau prezicerea preferințelor, comportamentelor și atitudinilor sale personale”.

Deși definiția prevăzută în legea revizuită privind protecția datelor este similară cu definiția CoE, lipsesc criteriile referitoare la „procesul de luare a deciziilor”. Deși crearea de profiluri nu este utilizată exclusiv pentru a lua decizii asupra unei persoane, adesea, o consecință indirectă a creării de profiluri va duce la luarea unei decizii cu privire la o persoană. Scopul principal al reglementării utilizării funcției de creare de profiluri este de a oferi persoanei vizate dreptul de a se opune acestor decizii atunci când prevalează interesele legitime.

2) Destinatar

Legea revizuită privind protecția datelor definește destinatarul ca fiind persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism căruia îi sunt divulgate date cu caracter personal „fără a solicita acest lucru, indiferent dacă sunt sau nu terțe părți”.

În ceea ce privește partea subliniată a definiției, trebuie remarcat faptul că nici proiectul Convenției 108 modernizate, nici RGPD nu introduce un astfel de concept în raport cu destinatarul. Conform raportului explicativ al proiectului Convenției 108 modernizate, „destinatar” este o persoană sau o entitate care primește date cu caracter personal sau căreia i-au fost puse la dispoziție date cu caracter personal. În funcție de circumstanțe, destinatarul poate fi operator sau persoană împuternicită de către operator. Spre exemplu, o întreprindere trimite anumite date referitoare la angajații săi către un departament guvernamental care le va procesa în calitate de operator în scopuri fiscale. Aceasta le poate trimite către o companie care oferă servicii de stocare, acționând astfel în calitate de persoană împuternicită de către operator.

Acest lucru implică faptul că divulgarea datelor cu caracter personal către un destinatar, indiferent dacă destinatarul este operator sau persoană împuternicită de către operator, este o operațiune de prelucrare care necesită o bază juridică și să respecte cerințele Convenției. Nu este clar care ar fi valoarea adăugată a definirii destinatarului ca fiind o persoană căreia îi sunt divulgate date cu caracter personal, *fără a solicita acest lucru*.

Domeniu de aplicare

Convenția 108 se aplică la orice prelucrare a datelor care se efectuează atât de către sectorul privat, cât și de cel public, precum și la prelucrarea datelor de către organele

Analiză de specialitate cu privire la legislația privind protecția datelor din Republica Moldova

judecătorești și autoritățile de punere în aplicare a legii. Aceasta protejează persoanele de abuzuri care pot fi asociate cu prelucrarea datelor cu caracter personal.

1) Aplicarea legii

Conform dispozițiilor din articolul 2 al legii revizuite privind protecția datelor, domeniul de aplicare prevede că legea se aplică prelucrării datelor cu caracter personal în cadrul activităților efectuate de către operatorii (*operatori de date?*) stabiliți pe teritoriul Republicii Moldova, prelucrării datelor cu caracter personal în misiuni diplomatice și oficii consulare în Republica Moldova și prelucrării datelor cu caracter personal de către operatorii stabiliți în afara teritoriului Republicii Moldova, prin intermediul mijloacelor aflate în teritoriu.

Legea revizuită privind protecția datelor se aplică în continuare secretului de stat, secretului profesional, secretului bancar, secretului comercial sau dosarelor speciale, confidențialității procedurilor civile sau penale sau altor informații și nu poate fi invocată cu încălcarea regimului juridic al acestei legi (articolul 2 alineatul (2) litera (d) din legea revizuită).

Nu este clar dacă legea revizuită privind protecția datelor se aplică atât sectorului public, cât și celui privat. Articolul 3 din legea revizuită privind protecția datelor, care definește operatorul ca fiind persoana fizică sau juridică *în temeiul dreptului public sau privat*, poate implica faptul că legea acoperă prelucrarea datelor efectuată atât de sectorul public, cât și de cel privat. Cu toate acestea, domeniul de aplicare material al legii reprezintă un punct principal și se propune să se precizeze în mod specific în articolul 2 dacă legea acoperă ambele sectoare.

2) Excepții și limitări

Articolul 2 alineatul (3) din legea revizuită privind protecția datelor prevede posibilitatea de a exclude anumite activități din aplicarea legii. După cum a fost prevăzut anterior, scopul și domeniul de aplicare al legii sunt dispozițiile fundamentale. Prin urmare, trebuie acordată o atenție specială oricărei scutiri de la aplicarea legii.

Legea revizuită privind protecția datelor propune excluderea din lege a „prelucrării datelor cu caracter personal în cadrul activităților de informații (spionaj) și contrainformații (contraspionaj), referitoare la agenți și surse de informații”. Această scutire la nivel global ridică preocupări serioase.

Dreptul fundamental la protecția datelor cu caracter personal în temeiul articolului 8

Analiză de specialitate cu privire la legislația privind protecția datelor din Republica Moldova

din CEDO nu este un drept absolut. Acesta trebuie luat în considerare în raport cu alte drepturi. Cu toate acestea, limitările față de acest drept fundamental sunt reglementate strict. Articolul 52 alineatul (1) din Carta UE recunoaște posibilitatea de a prevedea limitări atâta timp cât aceste limitări sunt prevăzute prin lege, respectă esența dreptului la protecția datelor și, supuse principiului proporționalității, sunt necesare pentru a îndeplini obiectivele de interes general recunoscute de către Uniune sau nevoia de protecție a drepturilor și libertăților altor persoane.

Convenția 108 prevede că, în principiu, nu se pot face excepții de la dispozițiile referitoare la calitatea datelor, categoriile speciale de date și măsurile de protecție suplimentare pentru subiecții datelor. Cu toate acestea, ar putea fi prevăzute excepții pentru aceste dispoziții numai atâta timp cât sunt prevăzute prin lege și constituie o măsură necesară într-o societate democratică în interesul:

- de a proteja securitatea statului, siguranța publică, interesele monetare ale statului sau suprimarea infracțiunilor penale;
- de a proteja persoana vizată sau drepturile și libertățile altor persoane.

După cum s-a menționat anterior, este permis, în anumite condiții, să se prevadă limitări la aplicarea anumitor dispoziții ale legii privind protecția datelor. Excluderea pur și simplu a aplicării legii privind protecția datelor unui anumit sector nu este în conformitate cu cerințele care se referă la instaurarea unei limitări și deschide ușa către abuzuri.

Mai mult, în ceea ce privește excluderea operațiunilor care implică prelucrarea și transmiterea transfrontalieră a datelor cu caracter personal referitoare la făptuitori sau victime ale unui genocid, război sau alte infracțiuni comise împotriva umanității (art. 2(3)(b) din legea revizuită privind protecția datelor), trebuie remarcat faptul că o astfel de scutire nu este prevăzută în Convenția 108, și nici în proiectul Convenției 108 modernizate.

Se recomandă cu insistență eliminarea alineatului (3), litera (b), care exclude de la aplicarea legii prelucrarea datelor cu caracter personal în cadrul activităților de informații (spionaj) și contrainformații (contraspionaj).

Calitatea datelor și caracterul legitim al prelucrării

Principiile enunțate la articolul 5 din Convenția 108 privind calitatea datelor sunt implementate în cadrul articolului 4 (cerințe pentru conformitatea și legalitatea prelucrării datelor cu caracter personal), iar articolul 5 din legea revizuită privind protecția datelor (condiții referitoare la consimțământ) este, în general, conform cu articolul 5 din Convenția 108 și proiectul Convenției modernizate. Cu toate acestea, s-ar putea ridica o observație.

Alineatul 2 litera (e) din articolul 4 se referă la o sarcină care servește unui interes legitim sau rezultă din exercitarea competențelor autorității publice investite în operator. Conceptul de „interes legitim” este tratat în cadrul articolului 4 alineatul (2) litera (f) și trebuie distins în mod clar de cerințele din articolul 4 alineatul (2) litera (e). Conceptul de interes legitim poate fi interpretat în sens larg și, din acest motiv, ar trebui să se solicite un test de echilibrare: interesele legitime ale operatorului (sau ale terțelor părți) trebuie să fie echilibrate față de interesele sau drepturile și libertățile fundamentale ale persoanei vizate. Un astfel de echilibru nu este abordat în articolul 4 alineatul (2) litera (e). Mai mult, un interes trebuie să fie suficient de clar articulat pentru a permite efectuarea testului de echilibrare față de interesele și drepturile fundamentale ale persoanei vizate.

Înțeleg că articolul 4 alineatul (2) litera (e) este relevant atât pentru sectorul public, cât și pentru cel privat. Pentru a fi în concordanță cu principiile Convenției 108 și cu dispozițiile RGPD, articolul 4, alineatul (2) litera (e) trebuie să se refere la *interesul public* și nu la *interesul legitim*. Astfel, acesta ar trebui să acopere două situații. Prima, ar trebui să acopere situații în care însuși operatorul are o autoritate oficială sau o sarcină de interes public (dar nu neapărat și o obligație juridică de prelucrare a datelor), iar prelucrarea este necesară pentru exercitarea acelei autorități sau efectuarea acelei sarcini. A doua, ar trebui să acopere situații în care operatorul nu are o autoritate oficială, dar o terță parte i-a solicitat să aibă o astfel de autoritate pentru a divulga date.

Categoriile speciale de date

Categoriile speciale de date sunt enumerate în cadrul articolului 3 din legea revizuită privind protecția datelor și cuprind „date care divulgă originea rasială sau etnică, opinii politice, credințe religioase sau filozofice sau apartenența socială și prelucrarea datelor genetice, a datelor biometrice pentru identificarea unică a unei persoane fizice, a datelor referitoare la sănătate sau a datelor referitoare la viața sexuală sau orientarea sexuală a unei persoane fizice și a datelor referitoare la condamnări, măsuri de constrângere procedurală sau sancțiuni impuse prin dreptul civil”. Această definiție pare în concordanță cu categoriile speciale de date cu caracter personal prevăzute în articolul 6 din proiectul Convenției 108 modernizate.

Cerințele pentru prelucrarea categoriilor speciale de date prevăzute în articolele 6 și 7 din legea revizuită privind protecția datelor, în ansamblu, îndeplinesc cerința prevăzută în Convenția 108 cu privire la calitatea dreptului intern în furnizarea unor măsuri de protecție corespunzătoare pentru prelucrarea acestor date. Majoritatea cerințelor pot fi comparate cu cele prevăzute în articolul 9 din RGPD. Acestea fac apel la un comentariu.

Articolul 6 alineatul (2) litera (g) permite prelucrarea categoriilor speciale de date în cazul în care *prelucrarea este necesară pentru a asigura securitatea statului, cu*

condiția ca aceasta să fie efectuată cu respectarea drepturilor persoanei vizate și a altor măsuri de protecție prevăzute de această lege. O astfel de scutire poate fi interpretată în sens larg și nu delimitează în mod strict și exhaustiv temeiurile juridice de prelucrarea a datelor sensibile. Articolul 9 alineatul (2) litera (g) din RGPD este mai restrictiv, deoarece permite prelucrarea categoriilor speciale de date atunci când este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate. Cerințele subliniate nu sunt prevăzute în articolul specific al proiectului de lege.

Securitatea datelor

Articolul 29 din legea revizuită privind protecția datelor aplică principiile securității datelor prevăzute în articolul 7 din Convenția 108 și proiectul Convenției 108 modernizate. Cu toate acestea, articolul 30 din legea revizuită privind protecția datelor pare să introducă excepții privind confidențialitatea datelor cu caracter personal și anume:

Articolul 30. Confidențialitatea datelor cu caracter personal

(1) Persoanele care au acces la date cu caracter personal trebuie să asigure confidențialitatea datelor respective, cu excepția următoarelor cazuri:

- a) prelucrarea se referă la date publicate în mod voluntar și vădit de către persoana vizată;
- b) datele cu caracter personal au fost depersonalizate;
- c) datele cu caracter personal au fost trecute sub pseudonim, pentru a evita riscul de încălcare a intangibilității vieții intime, de familie și private;
- d) existența unor temeiuri juridice pentru divulgare, în temeiul acestei legi.

Astfel de excepții nu sunt prevăzute în cadrul articolului 7 din Convenția 108, și nici în cadrul articolului 9 care tratează excepțiile și restricțiile. Introducerea excepțiilor privind confidențialitatea datelor pare să fie problematică.

Persoanele care au acces la date cu caracter personal trebuie să asigure confidențialitatea acestora în orice circumstanță. Condițiile pentru divulgarea datelor către terțe părți vor fi evaluate pe baza condițiilor prevăzute în cadrul articolului 5 din Convenție (Capitolul II din legea revizuită privind protecția datelor). Excepțiile prevăzute la articolul 30 din legea revizuită privind protecția datelor pot duce la incertitudine juridică în ceea ce privește secretul profesional și privind măsurile corespunzătoare care ar trebui luate pentru a garanta confidențialitatea și securitatea datelor. Acest lucru poate duce ulterior la incertitudine juridică în ceea ce privește condițiile pentru divulgarea datelor cu caracter personal către terțe părți. Spre exemplu, scutirea prevăzută la articolul 30 alineatul (1) litera (d), care se referă la temeiurile juridice pentru divulgarea datelor către terțe părți, nu ia în considerare principiile de limitare a scopului și de reducere a datelor.

Măsuri de protecție suplimentare - drepturile persoanei vizate

Articolele de la 11 la 20 din legea revizuită privind protecția datelor tratează drepturile persoanelor vizate și, în special, transparența prelucrării, dreptul la acces și rectificare, dreptul de ștergere (dreptul de a fi uitat, în temeiul RGPD), dreptul la restricționarea prelucrării, dreptul la portabilitate și dreptul de a se opune. În ansamblu, dispozițiile articolelor de la 11 la 20 din legea revizuită privind protecția datelor sunt în

concordanță cu articolul 8 din Convenție și proiectul Convenției 108 modernizate. Cu toate acestea, modificările propuse ridică unele observații:

- a) În timp ce drepturile persoanelor vizate în legea revizuită privind protecția datelor au fost consolidate și au fost introduse drepturi noi (dreptul la portabilitate, dreptul de ștergere și dreptul de a restricționa prelucrarea), se pare că dreptul la o cale de atac nu este prevăzut în versiunea revizuită a legii. Legea originală privind protecția datelor prevede un astfel de drept în articolul 18.
- b) Articolul 20 din legea revizuită privind protecția datelor tratează procesul individual de luare a deciziilor, inclusiv crearea de profiluri. Alineatele (1), (2) și (3) din acest articol sunt în conformitate cu Convenția 108 și Recomandarea CM/Rec(2010)13 privind crearea de profiluri. De asemenea, sunt în concordanță cu Regulamentul UE 2016/679. Cu toate acestea, formularea alineatului (4) este imprecisă. Nu este clar dacă interzicerea prelucrării datelor sensibile în contextul creării de profiluri este generală sau dacă este permisă cu acordul persoanei vizate. Referirea la articolul 9 în acest alineat este, de asemenea, neclară, dat fiind faptul că articolul 9 din legea revizuită privind protecția datelor tratează libertatea de exprimare.

Sugestie: punerea alineatului (4) în acord cu CM/Rec(2010)13 privind crearea de profiluri, care prevede faptul că „colectarea și prelucrarea datelor sensibile în contextul creării unor profiluri este interzisă, cu excepția cazului în care aceste date sunt necesare în scopul juridic și specific al prelucrării, atâta timp cât dreptul intern asigură măsuri de protecție adecvate. Atunci când se impune consimțământul, acesta trebuie să fie explicit în cazul în care prelucrarea se referă la date sensibile”.

Obligații suplimentare

Capitolul IV din legea revizuită privind protecția datelor (articolele de la 22 la 32) tratează obligațiile operatorului și ale persoanei împuternicite de către operator.

Articolul 23 prevede, în special, obligația operatorului de a se asigura că cerințele de protecție a datelor sunt integrate în etapa de arhitectură și de proiectare a sistemului de operațiuni de prelucrare a datelor, prin măsuri tehnice și organizaționale (protecția datelor prin proiectare). Acesta stabilește măsurile care trebuie luate de către operator pentru a implementa principiile de protecție a datelor, cum ar fi reducerea datelor și trecerea sub pseudonim. Acesta stipulează, de asemenea, obligația operatorului de a implementa măsuri tehnice și organizaționale corespunzătoare pentru a se asigura că, în mod implicit, sunt prelucrate numai datele cu caracter personal care sunt necesare pentru fiecare scop specific de prelucrare. Aceste dispoziții sunt conforme cu articolul 8 bis alineatul (3) din proiectul Convenției 108 modernizate.

Articolul 24 din legea revizuită privind protecția datelor prevede obligația operatorului și a persoanei împuternicite de către operator de a examina impactul posibil al prelucrării datelor intenționate asupra drepturilor și libertăților fundamentale ale persoanelor vizate înainte de începerea prelucrării (evaluarea impactului protecției datelor - EIPD). Mai mult, articolul 24 reglementează operațiuni specifice de prelucrare care necesită efectuarea unei astfel de evaluări înainte de activitățile de prelucrare și stabilește metodologia pentru efectuarea EIPD. Dispozițiile articolului 24 sunt conforme cu articolul 8 bis alineatul (2) din proiectul Convenției 108 modernizate.

Conform alineatului 1 al articolului 8 bis din Convenția 108 modernizată, *operatorii și, după caz, persoanele împuternicite de către operatori trebuie să ia toate măsurile corespunzătoare pentru a respecta obligațiile Convenției și a putea să demonstreze, în special autorității de supraveghere, că prelucrarea datelor sub controlul acestora este în conformitate cu dispozițiile Convenției*. Raportul explicativ al proiectului Convenției modernizate clarifică faptul că măsurile corespunzătoare pe care operatorul și persoana împuternicită de către operator le pot lua pentru a asigura conformitatea includ: instruirea angajaților, stabilirea procedurilor de notificare corespunzătoare și desemnarea unui „ofițer de protecție a datelor” însărcinat cu mijloacele necesare pentru a-și îndeplini mandatul. Articolele de la 25 la 27 din legea revizuită privind protecția datelor cu privire la desemnarea și atribuțiile „ofițerului de protecție a datelor” și articolul 32 privind evidența activităților de prelucrare de către operator par să îndeplinească cerințele articolului 8 bis alineatul (1) din proiectul Convenției 108 modernizate.

Deși, în ansamblu, Capitolul IV din legea revizuită privind protecția datelor îndeplinește cerințele articolului 8 bis din proiectul Convenției 108 modernizat, una dintre dispozițiile sale ridică o observație:

Articolul 31 din legea revizuită privind protecția datelor prevede că:

(1) Prelucrarea datelor cu caracter personal de către persoane care lucrează în baza unui contract de muncă legal sub autoritatea operatorului sau a persoanei împuternicite de către operator reprezintă operațiuni de prelucrare a datelor cu caracter personal efectuate de către operator.

(2) În cazul în care prelucrarea datelor cu caracter personal menționate la alineatul (1) din acest articol este efectuată în alte scopuri decât cele stabilite de către operator, chiar dacă persoana în cauză este angajată într-un contract de muncă legal cu operatorul de date cu caracter personal (operator?), acea persoană acționează în calitate de operator de date cu caracter personal în raport cu prelucrarea.

Dispozițiile subliniate ridică preocupări. Având în vedere relația de subordonare dintre angajator și angajați, dispozițiile acestui articol implică riscul de a permite operatorilor să atribuie angajaților responsabilitatea unei încălcări a securității datelor și să nu fie sancționați pentru acest lucru. Conform articolului 7 din Convenție, operatorul trebuie să ia măsurile de securitate necesare pentru a proteja datele împotriva utilizării sau a divulgării neautorizate. *Dacă un angajat utilizează date în alte scopuri decât cele stabilite de către operator*, operatorul trebuie să rămână răspunzător și trebuie să fie obligat să demonstreze că au fost luate măsuri de protecție pentru a proteja utilizarea ulterioară a datelor.

Scutiri și restricții

Articolul 21 alineatul (1) prevede excepții cu privire la exercitarea unor drepturi ale persoanelor vizate și stabilește scopuri pentru care pot fi utilizate aceste scutiri. Scopurile includ: *apărare națională, securitatea statului și menținerea ordinii publice, protecția drepturilor și a libertăților persoanelor vizate sau a altor persoane, protecția independenței judiciare și a procedurilor judiciare, prevenirea, investigarea, detectarea și urmărirea penală a încălcărilor etice în cazul profesiilor reglementate, protecția drepturilor și a libertăților subiectului sau a altor persoane, punerea în aplicare a cererilor de despăgubire în temeiul dreptului civil dacă, prin aplicarea acestora, prejudiciul este cauzat eficienței acțiunii sau obiectivului urmărit în exercitarea competențelor juridice ale autorităților publice.*

În ansamblu, derogările prevăzute în cadrul articolului 21 alineatul (1) sunt conforme cu scutirile stipulate în cadrul articolului 9 din Convenția 108.

Deși sunt enumerate scopuri legitime similare în cadrul articolului 9 din Convenția 108, legea revizuită privind protecția datelor nu prevede testul în trei părți: derogările trebuie prevăzute de lege, să respecte esența drepturilor și libertăților fundamentale și să constituie o măsură necesară și proporțională într-o societate democratică pentru anumite interese legitime.

Legea revizuită privind protecția datelor propune extinderea listei de derogări enumerate în cadrul legii inițiale privind protecția datelor și sunt posibile noi derogări, și anume *pentru protejarea independenței judiciare și a procedurilor judiciare, prevenirea, investigarea, detectarea și urmărirea penală a încălcărilor etice în cazul profesiilor reglementate și punerea în aplicare a cererilor de despăgubire în temeiul dreptului civil.* Convenția 108 permite, în anumite condiții, să se prevadă limitări ale aplicării unor anumite prevederi în scopul prevenirii, investigării și urmăririi penale a infracțiunilor. Dacă o *încălcare etică* constituie o infracțiune în cadrul sistemului judiciar din Moldova, într-un astfel de caz, trimiterea la încălcările etice din articolul 21 alineatul (1) este în conformitate cu Convenția 108.

Fluxuri transfrontaliere de date

Transferul datelor cu caracter personal către altă parte contractantă la Convenția 108 trebuie să nu aibă restricții. Legislația CoE permite ca dreptul intern să accepte transferul de date către statele care nu sunt contractante, dacă statul sau organizația destinatară asigură un nivel adecvat de protecție pentru transferul de date intenționat. Legislația UE prevede același principiu.

Articolul 12 din proiectul Convenției 108 modernizate specifică faptul că un nivel corespunzător de protecție poate fi asigurat prin legea statului respectiv sau prin măsuri de protecție standardizate ad hoc sau aprobate. Pe lângă situațiile anterioare, alineatul (4) din articolul 12 permite părților să facă derogări de la principiul impunerii unui nivel corespunzător de protecție și să permită un transfer către un destinatar care nu asigură o astfel de protecție. Astfel de derogări sunt permise numai în situații limitate: cu acordul persoanei vizate sau cu un interes specific și/sau în cazul în care există interese legitime predominante prevăzute de lege și/sau transferul constituie o măsură necesară și proporțională pentru libertatea de exprimare într-o societate democratică. Astfel de derogări trebuie să respecte principiile necesității și proporționalității.

Capitolul IX din legea revizuită privind protecția datelor acoperă transmiterea transfrontalieră a datelor cu caracter personal către alte țări

1) Transferuri către țări care asigură un nivel adecvat de protecție

Legea revizuită privind protecția datelor definește în articolul 3 prelucrarea transfrontalieră a datelor cu caracter personal ca fiind „prelucrarea datelor cu caracter personal care implică un element străin, cu participarea unei persoane fizice sau juridice guvernate de dreptul public sau privat, care se află în alt stat”.

Alineatul (3) din articolul 48 stabilește ca regulă faptul că transmiterea transfrontalieră a datelor cu caracter personal către orice țară este supusă autorizării de către autoritatea de supraveghere (Centrul). Ulterior, s-a făcut distincția între țările care asigură un nivel adecvat de protecție și cele care nu asigură un nivel adecvat de protecție. Excepții de la această regulă se fac în alineatul (7), care permite transmiterea datelor fără autorizarea Centrului atunci când „transferul datelor cu caracter personal se realizează în temeiul dispozițiilor unei legi speciale sau a unui tratat internațional ratificat de către Republica Moldova, în special dacă transferul este realizat cu scopul de a preveni sau a investiga infracțiuni”.

Trimiterea transmiterii transfrontaliere de date cu caracter personal către autorizarea Centrului poate fi considerată o măsură de protecție suplimentară. Cu toate acestea, acest articol nu face nicio distincție între părțile și non-părțile la Convenția 108. După cum s-a menționat mai sus, transferul de date cu caracter personal către altă parte contractantă la Convenția 108 trebuie să fie fără restricții. (Articolul 12 din Convenția 108).

Raportul explicativ al proiectului Convenției modernizate clarifică faptul că diferite elemente ale transferului trebuie examinate la evaluarea nivelului de protecție, cum ar fi: tipul datelor; scopul și durata prelucrării pentru care sunt transferate datele; respectarea statului de drept de către țara destinației finale; normele juridice generale și sectoriale aplicabile în statul sau organizarea în cauză; și normele profesionale și de securitate care se aplică acolo.

Evaluarea caracterului adecvat al nivelului de protecție este prevăzută în cadrul alineatului (4) din articolul 48 și ia în considerare „condițiile în care sunt transmise datele cu caracter personal, în special natura acestora, scopul și durata prelucrării evenimentelor de prelucrare propuse, țara de destinație, legislația și normele profesionale, precum și măsurile de securitate respectate în țara de destinație”.

Articolul 48 alineatul (4) este în concordanță cu cerințele Convenției 108.

2) Transferuri către țări care nu asigură un nivel adecvat de protecție

Când nu este asigurat un nivel adecvat de protecție, Centrul poate totuși să autorizeze transmiterea dacă clauzele contractuale prevăd „garanții suficiente cu privire la protecția și exercitarea drepturilor persoanelor vizate” (alineatul (6) din articolul 48). Articolul 48 alineatul (6) este în concordanță cu cerințele Convenției 108.

Alineatul (9) din articolul 48 stabilește condiții suplimentare care permit transmiterea datelor cu caracter personal către statele care nu asigură un nivel adecvat:

- a) cu acordul persoanei vizate;
- b) în cazul în care este necesar să se încheie sau să se realizeze un acord sau un contract între persoana vizată și operator sau între operator și o terță parte în interesul persoanei vizate;
- c) dacă este necesară protejarea vieții, integrității fizice sau sănătatea persoanei vizate;
- d) dacă transmiterea are loc dintr-un registru destinat informării publicului general și deschis consultării publice sau a oricărei persoane care dovedește un interes legitim, în măsura în care cerințele legale au fost îndeplinite pentru consultare în anumite cazuri;
- e) atunci când este necesară satisfacerea unui interes public major, cum ar fi apărarea națională, securitatea statului sau ordinea publică, pentru buna desfășurare a procedurilor penale sau pentru a constata, a exercita sau a apăra un drept în instanță,

Analiză de specialitate cu privire la legislația privind protecția datelor din Republica Moldova

cu condiția ca datele cu caracter personal să fie prelucrate în legătură cu acest scop și numai pentru perioada necesară pentru atingerea acestui scop.

Ca o observație preliminară, trebuie remarcat faptul că corelația dintre alineatul (9) și alineatele de la (3) la (6) este neclară. Derogările stabilite în alineatul (9) sunt supuse autorizării Centrului? Pentru aceste derogări se aplică condiții suplimentare?

În articolul său 49, RGPD permite transferul de date în temeiul unor derogări similare, cu condiția ca „transferul să nu fie repetitiv, să se refere numai la un număr limitat de persoane vizate, să fie necesar în scopul exercitării intereselor legitime majore urmărite de către operator asupra cărora nu prevalează interesele sau drepturile și libertățile persoanei vizate, iar operatorul să fi evaluat toate circumstanțele aferente transferului de date și, pe baza acestei evaluări, să fi prezentat garanții corespunzătoare în ceea ce privește protecția datelor cu caracter personal”.

Acestea sunt clarificări importante pentru a se evita incertitudinea juridică și o lipsă a previzibilității pentru persoanele care se supun legii moldovenești privind protecția datelor. De asemenea, acestea sunt condiții principale pentru a fi conform cu Convenția 108 și cu legislația UE.

Pe lângă observațiile principale de mai sus, dispozițiile articolului 48 alineatul (9) ridică următoarele observații în lumina dispozițiilor din articolul 12 alineatul (4) din Convenția 108 modernizată menționată mai sus.

Articolul 48 alineatul (9) din legea revizuită privind protecția datelor permite transferul de date cu consimțământul persoanei vizate (punctul (a)). Acesta nu oferă nicio indicație suplimentară privind calificarea consimțământului. Articolul 3 din legea revizuită definește consimțământul *ca fiind orice exprimare liberă, specifică, informată și lipsită de ambiguitate a voinței persoanei vizate, prin care aceasta acceptă, într-o declarație sau acțiune neechivocă, prelucrarea datelor sale cu caracter personal*. Convenția 108 modernizată specifică faptul că consimțământul ca bază juridică pentru transferul de date către părți care nu sunt contractante trebuie să fie *explicit, specific, liber, iar persoana vizată trebuie să fie informată cu privire la riscurile care decurg din absența unor măsuri de protecție corespunzătoare*. Consimțământul definit în legea revizuită privind protecția datelor trebuie să fie lipsit de ambiguitate, ceea ce nu corespunde cerinței unui consimțământ explicit pentru fluxurile transfrontaliere de date în temeiul proiectului Convenției modernizate. Mai mult, articolul 48 alineatul (9) litera (a) menționează explicit obligația operatorului de a informa persoana vizată cu privire la riscurile care decurg din absența unor măsuri de protecție corespunzătoare.

Articolul 48 alineatul (9) din legea revizuită privind protecția datelor permite, în plus, transferul de date pentru încheierea unui contract între persoana vizată și operator. Această derogare nu este prevăzută în cadrul articolului 12 alineatul (4) din proiectul

Analiză de specialitate cu privire la legislația privind protecția datelor din Republica Moldova

Convenției modernizate. Mai mult, transferul de date pe baza contractului este deja prevăzut în cadrul articolului 48 alineatul (6).

3) Libera circulație a datelor cu caracter personal

În cele din urmă, legea revizuită privind protecția datelor autorizează în articolul 48 alineatul (8) libera circulație a datelor cu caracter personal în scopuri jurnalistice, artistice sau literare, cu condiția ca datele să fie făcute publice în mod voluntar și vădit de către persoana vizată sau să fie cu privire la o persoană publică în funcția sa oficială.

Această derogare pare să fie în conformitate cu Convenția 108 și cu proiectul Convenției modernizate, în timp ce prelucrarea datelor a făcut apel public pentru precauție în evaluarea proporționalității și a bazei juridice a noii prelucrări

Autoritate de supraveghere

Prezenta secțiune evaluează competențele, independența și capacitățile autorității de supraveghere din Moldova, și anume Centrul Național pentru Protecția Datelor cu Caracter Personal (numit în continuare „Centrul”). Aceasta va acoperi Capitolul VI din legea revizuită privind protecția datelor, art. 35-47, care instituie Centrul ca organism de supraveghere independent și stabilește procedurile pentru desfășurarea activității sale în condițiile prevăzute în articolele de la 37 la 47. Acesta va acoperi în continuare proiectul de lege privind CNPDPC, elaborat în aprilie 2017 și revizuit în august 2017, care prevede obiectivele, organizarea, atribuțiile, competențele, garanțiile, precum și alte aspecte legate de activitatea Centrului.

Evaluarea se realizează pe baza a cinci domenii principale de acțiuni și obiective ale autorităților de supraveghere instituite în temeiul articolului 12 bis din proiectul Convenției modernizate: 1) independența; 2) promovarea conformității cu legea; 3) competențe de punere în aplicare; 4) acordarea de asistență pentru persoanele vizate în exercitarea drepturilor acestora; 4) mecanisme de sancțiuni și căi de atac.

1) Independența

Diferite dispoziții din proiectul de lege privind CNPDPC prevăd garanții adecvate în ceea ce privește independența autorității de supraveghere:

Articolul 2 alineatul (2) stipulează în mod specific faptul că „Centrul este o autoritate publică autonomă și imparțială, instituită independent de alte autorități publice, persoane fizice și juridice. În timpul activității sale, Centrul respectă numai legea”.

Mai mult, articolul 4 prevede garanții specifice care contribuie la asigurarea independenței, cum ar fi independența financiară a Centrului (tratată în detaliu în cadrul art. 5), interzicerea influențării Centrului în îndeplinirea atribuțiilor sale și exercitarea competenței și posibilitatea de a fi tras la răspundere în acest caz.

Conform articolului 14, directorul Centrului, care se ocupă de gestionarea acestuia cu ajutorul directorului adjunct, este desemnat de către Parlament cu majoritatea deputaților aleși, pentru un mandat de cinci ani. Directorul poate fi ales pentru două mandate consecutive. Directorul adjunct este desemnat de către Parlament la propunerea directorului pentru un mandat de cinci ani.

Articolele 5, 9, 10 și 20 asigură infrastructura și resursele umane, tehnice și financiare corespunzătoare, necesare pentru efectuarea eficientă a sarcinilor Centrului și exercitarea competențelor sale.

Articolul 16 prevede garanții specifice în ceea ce privește atribuțiile și acțiunile directorului și ale directorului adjunct de a nu se angaja în nicio funcție incompatibilă cu atribuțiile și competențele acestora în timpul mandatului.

Dispozițiile de mai sus sunt conforme cu criteriul de independență prevăzut în cadrul Convenției 108.

Cu toate acestea, una dintre dispozițiile proiectului de lege privind CNPDPC trebuie clarificată:

Articolul 11 sugerează instituirea unui Consiliu Consultativ învestit cu autoritatea de a consulta și a consilia Centrul. Mandatul și competențele exacte ale Consiliului Consultativ nu sunt prevăzute în acest articol care, cu toate acestea, prevede la alineatul (4) *faptul că statutul de membru și regulamentul de organizare și funcționare a Consiliului Consultativ se aprobă de către directorul Centrului*. Trebuie remarcat faptul că componența Consiliului Consultativ include un membru al Comisiei pentru securitate națională, apărare și ordine publică și un reprezentant al personalului președintelui Republicii Moldova. Se recomandă ca *Regulamentul de organizare și funcționare a Consiliului Consultativ* să fie suficient de clar pentru a oferi garanții adecvate în ceea ce privește independența autorității de supraveghere în chestiunile care se referă la aspectele legate de autoritatea executivă și de poliție și securitatea națională.

2) Promovarea conformității cu legea

Centrul va primi o misiune educațională, astfel cum s-a propus în articolul 7 din proiectul de lege privind CNPDPC prin instituirea unui Centru de instruire. Acest lucru reprezintă o implementare satisfăcătoare a articolului 12 alineatul (2) litera (e) din proiectul convenției 108 modernizate și va spori rolul Centrului în promovarea gradului

de conștientizare publică. Pagina web a acestuia arată faptul că este oarecum activ în îndeplinirea misiunii sale de promovare a conformității și gradului de conștientizare. Acesta a emis deja recomandări specifice, cum ar fi instrucțiunile privind prelucrarea datelor cu caracter personal în procesul electoral și, de asemenea, instrucțiunile pentru sectorul poliției. Acestea sunt indicații pozitive ale faptului că Centrul este activ în rolul său.

3) Competențe de punere în aplicare

Articolele de la 36 la 47 din legea revizuită privind protecția datelor propune acordarea competenței Centrului de a furniza autorizații pentru anumite operațiuni de prelucrare a datelor cu caracter personal, de a controla legalitatea prelucrării și de a desfășura investigații. Procedurile pentru autorizații, reclamații și inspecții sunt bine detaliate în cadrul Capitolului VII și prevăd competențe adecvate de investigare și intervenție.

Pe lângă acest lucru, Centrul dispune de mai multe competențe de intervenție și consultare, pentru a emite decizii și a îndeplini funcțiile legate de transferul de date către țări terțe. Competențele și funcțiile descrise în articolul 8 din proiectul de lege privind CNPDPC sunt în concordanță cu cerințele Convenției 108 și ale proiectului Convenției modernizate, cu o singură excepție:

se pare că legea revizuită privind protecția datelor și proiectul de lege privind CNPDPC nu stipulează competențe cu privire la capacitatea de se angaja în proceduri juridice sau de a aduce în atenția autorităților judiciare competente încălcări ale dispozițiilor.

4) Acordarea de asistență pentru persoanele vizate în exercitarea drepturilor acestora

Proiectul convenției 108 modernizat solicită în mod specific autorității de supraveghere să ofere asistență persoanelor vizate, ceea ce include, în special, tratarea reclamațiilor.

Procedura pentru primirea și soluționarea reclamațiilor prevăzută în cadrul articolului 37 din legea revizuită privind protecția datelor ridică o preocupare importantă. Conform alineatului (1), reclamațiile persoanei vizate trebuie depuse la operator sau la persoana împuternicită de către operator și nu direct la Centru. Persoana vizată poate să se adreseze Centrului numai dacă nu este satisfăcută de rezultatul unei reclamații revizuite de către operator. Această procedură restrânge și limitează drepturile persoanei vizate. În sectorul ocupării forței de muncă, spre exemplu, având în vedere relația dintre angajator și angajați, procedura propusă în cadrul articolului 37 poate împiedica angajații să-și exercite drepturile și să depună o reclamație direct la angajatorul acestora. Mai mult, în caz de încălcare a securității datelor, acțiunile

operatorului pot satisface reclamantul, dar Centrul va fi lipsit de puterea sa de a impune o sancțiune, dacă este necesar.

Competența Centrului de a examina reclamații nu este prevăzută în cadrul articolului 8 din proiectul de lege privind CNPDPC. Deși este abordată pe larg în Capitolul VI din legea revizuită, trebuie stipulat în mod specific și în cadrul articolului 8.

5) Mecanisme de sancțiuni și căi de atac

Propunerea legii revizuite privind protecția datelor prevede mecanisme de sancțiuni și căi de atac corespunzătoare, care sunt conforme cu proiectul Convenției 108 modernizate.

Articolul 44 din legea revizuită privind protecția datelor autorizează Centrul să impună rectificarea, suspendarea, blocarea, interzicerea/încheierea operațiunilor de prelucrare și, de asemenea, distrugerea/ștergerea datelor cu caracter personal, cu posibilitatea de a solicita distrugerea software-ului și a hardware-ului care a fost utilizat pentru încălcarea legislației.

Mai mult, în temeiul articolului 49 din legea revizuită, Centrul este autorizat să impună sancțiuni pecuniare pentru operatori în cazul unei încălcări a legii. Legea revizuită propune creșterea amenzilor pentru încălcarea legii, de la 1 000 MDL până la 5 milioane MDL pentru anumite încălcări.

Regimul de sancțiuni din legea moldovenească privind protecția datelor, astfel cum a fost revizuită, este în conformitate cu cerințele Convenției 108 și ale proiectului Convenției modernizate.

**Avizul de specialitate privind
conformitatea legilor din Republica Moldova referitoare la
protecția datelor cu caracter personal
cu Convenția CoE pentru protejarea persoanelor față de
prelucrarea automatizată a datelor cu caracter personal
(Convenția 108)**

Întocmit de

Nevena Ruzic, expert al Consiliului Europei

Septembrie 2017

Rezumat

Analiza proiectului de lege privind protecția datelor cu caracter personal și a proiectului de lege privind Centrul Național pentru Protecția Datelor cu Caracter Personal din Republica Moldova arată că acestea sunt, în mare măsură, în conformitate cu dispozițiile și standardele prevăzute prin Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108) și protocolul său adițional cu privire la autoritățile de supraveghere și fluxurile transfrontaliere ale datelor, precum și cu proiectul convenției modernizate pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal. Cu toate acestea, analiza evidențiază dispoziții prin care o astfel de conformitate ar putea fi îmbunătățită și sugerează modificări ale legislației propuse. La sfârșitul acestei analize este prezentată lista recomandărilor specifice.

Introducere

Scopul acestei analize este acela de a furniza constatări concrete, comentarii și sugestii, după caz, cu privire la conformitatea legislației naționale, precum și a noii legislații propuse, cu convențiile și standardele CoE.

Analiza urmează ordinea articolelor astfel cum este stabilită în Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (numită în continuare Convenția 108) și protocolul său adițional. După caz, analiza se referă, de asemenea, la proiectul convenției modernizate pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (numit în continuare proiectul convenției modernizate), ținându-se cont în mod specific de intenția prezentă de modificare a legislației naționale existente.

Expertul a primit traducerile în limba engleză ale proiectului de lege privind protecția datelor cu caracter personal și proiectul de lege privind Centrul Național pentru Protecția Datelor cu Caracter Personal din Republica Moldova.

Cadrul juridic al Consiliului Europei luat în considerare în scopul acestei analize este următorul: Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (Convenția 108) și protocolul său adițional, referitor la autoritățile de supraveghere și fluxurile transfrontaliere de date (protocol adițional, CETS 181), precum și proiectul Convenției modernizate pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal.

Este important de subliniat faptul că expertul a emis un aviz privind o versiune anterioară a proiectului legislativ în luna mai 2016. Acest aviz a fost comandat și de către Consiliul Europei. Este important de subliniat faptul că expertul a emis un aviz

privind o versiune anterioară a proiectului legislativ în luna mai 2016. Acest aviz a fost comandat și de către Consiliul Europei.

Obiect și scop (articolul 1 din Convenția 108)

Articolul 1 din proiectul de lege privind protecția datelor cu caracter personal (numită în continuare Legea PD) prevede faptul că „scopul acestei legi este de a asigura dreptul la protecția datelor cu caracter personal, care derivă din dreptul intangibil constituțional la intimitate, viață de familie și viață privată”.

Deși articolul nu cuprinde o referire specifică la o persoană, prin urmare, nicio referire la naționalitatea persoanei, acesta trebuie să fie auto-concludent cu privire la faptul că acoperă orice persoană și drepturile sale, indiferent de naționalitate. Mai ales că acesta se bazează pe garanții constituționale, iar acestea trebuie să se refere la fiecare persoană.

Mai mult, articolul 3 alineatul (4) definește „persoana vizată” ca fiind „persoana fizică identificată sau care poate fi identificată prin date cu caracter personal”.

Notă: un comentariu similar a fost furnizat în avizul anterior.

Atât Convenția 108, cât și proiectul Convenției modernizate¹ se referă la protecția fiecărei persoane, *indiferent de naționalitatea sau reședința acesteia*.

Sugestie:

Îmbunătățiți nivelul de precizie cu privire la irelevanța naționalității și a reședinței fie în articolul 1, fie în articolul 3 alineatul (4), în cazul în care acesta din urmă este mai convenabil datorită formulării articolului 1.

Definiții (articolul 2 din Convenția 108)

a) Date cu caracter personal (articolul 2 litera (a) din Convenția 108)

Conform articolului 3 alineatul (1) din Legea PD, datele cu caracter personal reprezintă orice informație care identifică sau care duce la identificarea persoanei vizate. Pot exista două categorii de date cu caracter personal: „comune și speciale”. Articolul oferă, apoi, în detaliu ce fel de date trebuie considerate ca fiind comune și care ca fiind speciale.

¹ Textul consolidat al Convenției modernizate din septembrie 2016

„Categorია specială de date” este un concept adoptat atât în Convenția 108, cât și în proiectul Convenției 108 modernizate. Lista prevăzută în Legea PD nu se potrivește cu lista cuprinsă în Convenția 108 modernizată.

Cu toate acestea, lista de date care trebuie considerate „comune” nu pare doar redundantă, ci și neclară și ar putea duce la incertitudini juridice. Spre exemplu, datele comune sunt, de asemenea, „una sau mai multe particularități legate de identitatea fizică, psihologică, economică, culturală sau socială a persoanei fizice în cauză”. Nu este clar dacă, spre exemplu, datele biometrice ar putea fi considerate ca fiind o particularitate legată de identitatea fizică sau, ca un alt exemplu, originea etnică ca fiind identitatea sa culturală, deși ultimul proiect cuprinde o definiție separată a datelor biometrice.

Comentariu:

Comparativ cu articolul 2 litera (a) din Convenția 108, conform căruia „datele cu caracter personal” denotă orice informații privind persoana fizică identificată sau identificabilă („persoană vizată”), precum și cu definiția prevăzută în proiectul Convenției modernizate la articolul 2 litera (a), definiția datelor cu caracter personal este mai detaliată. Acest lucru nu este un impediment, atâta timp cât prevederea nu poate fi formulată ca acoperind „identificarea persoanelor prin metode foarte sofisticate”, așa cum s-a explicat în Expunerea de motive a Convenției 108. (NOTĂ: comentariul este luat aproape textual din avizul din 2016)

Definiția categoriei comune de date cu caracter personal cuprinde exemple care ar putea să intre cu ușurință în definiția „categoriei speciale”.

Sugestie:

- Evitați interpretarea potențială a formulării articolului 3 alineatul (1) din Legea PD „care duce la identificarea persoanei vizate” ca fiind aplicabilă oricăror date. (NOTĂ: Aceeași sugestie a fost furnizată în avizul din 2016).

- Revizuiți definiția „categorie comună” de date cu caracter personal din articolul 3 al Legii PD, pentru a evita incertitudinea juridică.

b) Fișier automatizat (articolul 2 litera (b) din Convenția 108)

Nu există dispoziții privind definirea noțiunii de „fișier automatizat”.

c) Prelucrare automată (articolul 2 litera (c) din Convenția 108)

Nu există dispoziții privind definiția noțiunii de „prelucrare automată”, dar articolul 3 alineatul (11) din Legea PD cuprinde o definiție a unui „sistem de arhivare”.

Notă: În cadrul articolului 2 litera (b), prelucrarea automată este presupusă.

d) Operator (articolul 2 litera (d) din Convenția 108)

Definiția „operatorului” este prevăzută în articolul 3 alineatele (8) și (9) din Legea PD. Conform definiției respective, un operator este „o persoană fizică sau juridică de drept

public sau privat, inclusiv autoritatea publică, orice altă instituție, organizație sau persoană autorizată care, în mod direct sau prin persoana împuternicită de către operator, stabilește scopurile și/sau mijloacele de prelucrare a datelor cu caracter personal, prelucrează sau intenționează să prelucreze astfel de date". În continuare, conceptul de „operator asociat” înseamnă „doi sau mai mulți operatori care determină împreună scopul și mijloacele de prelucrare a datelor cu caracter personal”.

O astfel de definiție este mai detaliată în comparație cu cea prevăzută în Convenția 108.

Notă: Articolul 2 litera (c) din proiectul Convenției modernizate include noțiunea de operatori comuni.

Comentariu:

formularea „prin intermediul persoanei împuternicite de către operator” nu este clară aici. Acest lucru ar putea fi o chestiune de traducere. Cu toate acestea, acest lucru ar putea fi oarecum confuz în ceea ce privește rolul persoanei împuternicite de către operator în „determinarea scopului prelucrării datelor cu caracter personal”.

Sugestie:

Revedeți formularea „prin intermediul persoanei împuternicite de către operator” din articolul 3 alineatul (8) din Legea PD.

Definiții reluate în proiectul Convenției modernizate

Proiectul Convenției modernizate include definiții suplimentare, cum ar fi cele ale destinatarului și ale persoanei împuternicite de către operator.

Destinatar

Articolul 3 alineatul (11) din Legea PD definește destinatarul ca fiind persoana fizică sau juridică, autoritatea publică, agenția sau orice alt organism căruia îi sunt divulgate date cu caracter personal *fără a solicita acest lucru*, indiferent dacă sunt sau nu terțe părți.

Proiectul Convenției modernizate se referă la toate persoanele *căroră le sunt divulgate date sau le sunt puse la dispoziție*. Prin urmare, nu în mod specific, astfel cum se poate citi din proiectul de lege, „destinatar involuntar”.

Sugestie:

Definiți „destinatar” în art. 3 al. (11) în concordanță cu definiția furnizată în proiectul Convenției 108 modernizate.

Persoana împuternicită de către operator

Conform art. 3 al. (10) din Legea PD, persoana împuternicită de către operator este o persoană fizică sau juridică în temeiul dreptului public sau privat, inclusiv o autoritate publică, agenție sau orice altă entitate care prelucrează date cu caracter personal în

numele operatorului. Ca o regulă, persoana împuternicită de către operator trebuie să fie o persoană fizică sau juridică diferită de operator.

O astfel de definiție este în conformitate cu cea prevăzută în proiectul Convenției modernizate. A doua propoziție poate părea inutilă; totuși, aceasta ar putea fi o chestiune de stiluri juridice diferite.

Domeniu de aplicare (articolul 3 din Convenția 108)

Astfel cum prevede articolul 2 din *Legea PD*, domeniul de aplicare al legii este larg. Acesta cuprinde cerințe juridice și tehnice generale referitoare la „intenția/începerea de a prelucra și/sau prelucrarea datelor cu caracter personal, inclusiv mijloacele utilizate sau intenționate pentru a fi utilizate în prelucrare”. În ceea ce privește teritoriul, acesta acoperă toate activitățile „efectuate de către operatori (SIC) pe teritoriul Republicii Moldova”, precum și misiunile diplomatice și oficiile consulare și de către „operatorii” stabiliți în afara granițelor naționale, dar pe teritorii unde dreptul intern din Republica Moldova este aplicabil în temeiul dreptului public internațional. De asemenea, se aplică și prelucrării datelor cu caracter personal de către „operatorii” stabiliți în afara teritoriului Republicii Moldova, prin mijloacele aflate pe teritoriu, exceptând cazurile în care astfel de mijloace sunt utilizate numai cu scopul de a transmite date.

Comentariu:

cuvântul „operator” lipsește din lista de definiții a art. 3 din Legea PD. Dacă acest cuvânt se referă la orice persoană care se ocupă de date cu caracter personal (adică operator, persoana împuternicită de către operator, terță parte și destinatar), definiția acestuia este necesară în această lege.

Sugestie:

Includeți definiția „operatorului” în art. 3 din Legea PD dacă acesta se referă la orice persoană care se ocupă de date cu caracter personal (adică operator, persoana împuternicită de către operator, terță parte și destinatar).

Domeniul de aplicare acoperă, de asemenea, informații confidențiale, cum ar fi secretul de stat, secretul profesional, secretul bancar, secretul comercial sau dosarele speciale, confidențialitatea procedurilor civile sau penale sau a altor informații și „nu poate fi invocată cu încălcarea regimului juridic al acestei legi”. Deși se poate presupune că intenția este de a acoperi orice informație referitoare la o persoană, scopul acestei dispoziții nu pare a fi exact pentru expert. Aceasta poate fi o chestiune de traducere sau, în caz contrar, trebuie oferite clarificări esențiale în ceea ce privește „orice altă informație”.

Comentariu: formularea art. 2 al. (2) lit. (d) din Legea PD trebuie reexaminată.

Sugestie:

Examinați dacă ar fi necesară reformularea art. 2 al. (2) lit. (d) din Legea PD din motive de claritate

Art. 2 al. (3) lit. (a) din Legea PD prevede faptul că legea nu se va aplica prelucrării datelor cu caracter personal de către persoane fizice numai pentru nevoile personale și familiale ale acestora, cu condiția ca drepturile persoanelor vizate să nu fie încălcate.

Proiectul Convenției modernizate se referă la *activități gospodărești și personale*.

Comentariu:

Deși formularea art. 2 al. (3) lit. (a) din Legea PD nu este echivalentă cu formularea din proiectul Convenției modernizate, aceasta nu o contrazice.

Cu privire la excluderea din sfera de aplicabilitate (a legii), Legea PD exclude aplicarea operațiunilor de prelucrare și transmitere transfrontalieră a datelor cu caracter personal ce se referă la făptuitorii sau victimele crimelor de genocid, ale crimelor de război și ale crimelor împotriva umanității (art. 2 alineatul (4) litera (c)).

Deși în Convenția 108 sau proiectul Convenției modernizate nu se prevede o astfel de excludere, aceasta nu este incompatibilă.

Calitatea datelor (articolul 5 din Convenția 108)

Art. 4 din Legea PD este în conformitate cu art. 5 din Convenția 108, precum și articolul 5 din proiectul Convenției modernizate.

În plus, mai multe principii sunt elaborate cu mai multe detalii.

Cu toate acestea, anumite formulări din articolul 4 alineatul (3), care prevede condiții pentru prelucrarea legală, pot părea neclare, redundante sau pot duce chiar la incertitudini juridice.

În temeiul articolului 4 alineatul (3) litera (b), „transmiterea datelor legate de executarea unui contract de către alt operator sau persoană împuternicită de către operator poate avea loc numai cu consimțământul persoanei vizate sau atunci când contractul este transmis în condițiile prevăzute de lege.” Nu este clar în care situație s-ar aplica acest lucru. În cazul în care acesta acoperă cesiunea de datorii, ar presupune notificarea debitorului pentru consimțământul privind transferul de date cu caracter personal? Dacă răspunsul este afirmativ, dispoziția necesită modificări.

Sugestie:

Reexaminați formularea art. 4 al. (3) lit. (b) din Legea PD

În temeiul sub-alineatului c, prelucrarea este legală dacă este necesară pentru a îndeplini obligația juridică a operatorului. Având în vedere că noțiunea de „obligație juridică” acoperă cazurile când prelucrarea este necesară pentru executarea unui contract, dacă această dispoziție se referă la prelucrarea exactă atunci când este prevăzută de lege ca act legislativ, aceasta trebuie clarificată.

Sugestie:

Clarificați termenul „obligație juridică” în articolul 4 alineatul (3) litera (c) din Legea PD

Categorii speciale de date (articolul 6 din Convenția 108)

Art. 3 din Legea PD prevede definiția categoriilor speciale de date cu caracter personal (consultați comentariul de mai sus). Articolul 6 din Legea PD prevede condițiile în care este permisă prelucrarea unei categorii speciale de date.

Cu toate acestea, articolul 6 din Legea PD nu prevede măsuri de protecție corespunzătoare, astfel cum se prevede în art. 6 din Convenția 108, precum și în art. 6 al. (2) din proiectul Convenției modernizate, conform căruia este necesar să se prevadă măsuri de protecție corespunzătoare specifice și suplimentare.

În pofida acestui fapt, articolul 23 prevede datoria de a implementa măsuri de protecție „în mod implicit din etapa de proiectare”. Cu toate acestea, nu este inclus, în special, riscul de discriminare, astfel cum se subliniază în proiectul Convenției modernizate.

Sugestie:

Precizați necesitatea pentru măsuri de protecție complementare în cazurile care se permite prelucrarea datelor dintr-o categorie specială.

Securitatea datelor (articolul 7 din Convenția 108)

Capitolul V din Legea PD (art. 33-34) reglementează confidențialitatea și securitatea prelucrării datelor cu caracter personal. Articolul 33 alineatul (4) vizează impunerea obligației de a raporta Centrului o încălcare a securității datelor, în calitate de autoritate de protecție a datelor. Acesta este în concordanță cu proiectul Convenției modernizate.

Măsuri de protecție suplimentare pentru persoana vizată (articolul 8 din Convenția 108)

a) Dreptul la informații (articolul 8 litera (a) din Convenția 108)

Art. 11 și 12 din Legea PD stipulează obligația de a oferi persoanei vizate informații cu privire la identitatea operatorului sau a persoanei împuternicite de către operator, scopul colectării datelor, precum și informații suplimentare, cum ar fi: destinatarii sau categoriile de destinatari ai datelor cu caracter personal, existența dreptului la acces, corectare sau obiecție, precum și condițiile în temeiul cărora pot fi exercitate astfel de drepturi.

Cel mai recent proiect din articolul 12 alineatul (1) nu cuprinde obligația de a oferi persoanelor vizate informații cu privire la categoriile de date cu caracter personal care urmează să fie colectate. Această dispoziție nu este în conformitate cu art. 7 bis al. (1) din proiectul Convenției modernizate.

Sugestie:

Includeți obligația operatorului de a oferi persoanelor vizate informații cu privire la categoriile de date colectate și prelucrate.

b) Dreptul la acces (articolul 8 litera (b) din Convenția 108)

Dreptul de acces la date cu caracter personal, astfel cum este prevăzut în art. 13 din Legea PD este în concordanță cu art. 8 al. (2) din Convenția 108.

Pe lângă atribuțiile stabilite în cadrul Convenției 108, operatorul are obligația de a oferi informații către persoanele vizate într-o formă inteligibilă, care nu necesită cunoștințe specifice într-un anumit domeniu și astfel încât să nu fie necesar niciun echipament suplimentar, care corespunde cu „comunicarea într-o formă inteligibilă a datelor prelucrate” în temeiul art. 8 lit. (b) din proiectul Convenției modernizate.

c) Dreptul la rectificare și ștergere (articolul 8 litera (c) din Convenția 108)

Art. 14 din Legea PD este în conformitate cu art. 8 lit. (c) din Convenția 108.

d) Dreptul la o cale de atac (articolul 8 litera (d) din Convenția 108)

Dreptul la o cale de atac este cuprins în mai multe articole.

Articolul 37 și 38 din Legea PD definește procedura de reclamație. Dacă acest lucru este suficient, adică dacă există un tarif/o taxă procedurală/ă, cât de formală sau complicată este procedura depinde de o lege procedurală națională și nu poate fi evaluat de către expert.

Excepții și restricții (articolul 9 din Convenția 108)

Legea PD prevede excepții de la exercitarea unor drepturi pe baza prelucrării datelor cu caracter personal în scopuri statistice și de cercetare istorică sau științifică.

Art. 9 din Legea PD stipulează excepții în scopul libertății de exprimare și a dreptului de acces la informații. Ultimul proiect creează incertitudini, iar expertul nu înțelege sensul alineatului 2.

Art. 21 din Legea PD stipulează excepții în scopuri de apărare națională, securitate a statului și menținerea ordinii publice, protecția drepturilor și libertăților persoanelor vizate sau a altor persoane, protecția independenței judiciare și a procedurilor judiciare, prevenirea, investigarea, detectarea și urmărirea penală a încălcărilor etice în cazul profesiilor reglementate, protecția drepturilor și a libertăților subiectului sau a altor persoane, punerea în aplicare a cererilor de despăgubire în temeiul dreptului civil dacă, prin aplicarea acestora, prejudiciul este cauzat eficienței acțiunii sau obiectivului urmărit în exercitarea competențelor juridice ale autorităților publice. Deși mai detaliate, aceste excepții intră sub incidența celor două condiții ale testului tripartit din Convenția Europeană - prevăzut de legea pentru protecția interesului legitim. Cu toate acestea, a treia condiție - măsura necesară într-o societate democratică - nu este clar definită, cu excepția perioadei de prelucrare a datelor, adică nu există teste suplimentare privind proporționalitatea pentru a evalua dacă toate datele sau numai câteva date cu caracter personal sunt necesare pentru a proteja interesul predominant.

Sugestie:

Oferiți măsuri de protecție suplimentare pentru dreptul persoanelor vizate în art. 21 din Legea PD, nu numai pentru a asigura faptul că datele sunt prelucrate excepțional în intervalul de timp limitat, dar și pentru a permite reexaminarea prelucrării în timpul perioadei stabilite.

Sanctiuni și căi de atac (articolul 10 din Convenția 108)

Art. 49 din Legea PD stipulează răspunderea pentru încălcarea legii cu referire la răspunderea specifică. După cum se pare, Legea PD furnizează lista de contravenții. Acest lucru nu ar trebui să excludă răspunderea dreptului civil.

Fluxuri transfrontaliere de date (articolul 12 din Convenția 108 și articolul 2 din protocolul adițional)

Capitolul VII din Legea PD (art. 48) reglementează transmiterea transfrontalieră a datelor cu caracter personal.

Condiția, precum și scutirile de la regula generală conform căreia autoritatea națională de protecție a datelor trebuie să autorizeze transferul de date, nu sunt în contradicție cu Convenția 108 și proiectul Convenției modernizate.

Autoritate de supraveghere (articolul 1 din protocolul adițional)

Centrul Național de Protecție a Datelor cu Caracter Personal este un organism de supraveghere. Cu toate acestea, este mai degrabă o autoritate asumată, deoarece instituirea acesteia nu este prevăzută de Legea PD, și nici nu este definită ca o autoritate de protecție a datelor. În tot cuprinsul Legii PD, Centrul Național pentru Protecția Datelor cu Caracter Personal este menționat în diferite proceduri. Deși acest lucru poate face parte dintr-un stil juridic special, este neobișnuit să nu se prevadă instituirea unui astfel de organism în baza principalei legi privind protecția datelor (astfel cum este cazul cu actuala Lege moldovenească privind protecția datelor). Instituirea, competențele și atribuțiile autorității naționale de protecție a datelor sunt prevăzute în proiectului de lege privind Centrul Național pentru Protecția Datelor cu Caracter Personal din Republica Moldova.

Următoarea listă a cerințelor Consiliului Europei pentru un organism de supraveghere privind protecția datelor este oferită în ordinea dispozițiilor din cadrul articolului 12 bis din proiectul Convenției modernizate.

a) Competențe de investigare și intervenții

În temeiul articolului 25, Centrul are competențe de examinare.

b) Funcții privind transferuri de date

Consultați mai sus (flux transfrontalier de date).

c) Competențe de a emite decizii în ceea ce privește încălcarea și impunerea sancțiunilor administrative

Aceste competențe sunt prevăzute în Legea PD

Analiză de specialitate cu privire la legislația privind protecția datelor din Republica Moldova

d) Competența de a se angaja în proceduri juridice

Nu a fost găsită o referire specifică la această competență.

Sugestie:

Precizați competența Centrului Național de Protecție a Datelor cu Caracter Personal de a se angaja în proceduri juridice

e) Promovarea gradului de conștientizare

Centrul cooperează cu „mass-media, asociațiile civile și instituțiile de același fel din străinătate” în temeiul art. 8 al. (1) lit. (n).

f) Consultare cu privire la propuneri pentru orice măsură legislativă sau administrativă referitoare la date cu caracter personal

Articolul 6 alineatul (3) stipulează faptul că proiectele legilor de reglementare care intră sub incidența competenței Centrului sunt supuse examinării Centrului. Cu toate acestea, nu este prevăzută nicio obligație de a respecta comentariile acestuia.

În temeiul art. 8 al. (1) lit. (f), Centrul are datoria de a elabora proiectele actelor legislative și de reglementare necesare pentru implementarea legislației referitoare la protecția datelor cu caracter personal și de a transmite astfel de proiecte către entități cu inițiative legislative. Este neclar modul în care va fi evaluată și tratată neconformitatea cu o astfel de atribuție.

g) Tratarea cererilor și reclamațiilor

Această competență este prevăzută în Legea PD în cadrul Capitolului VI „Autorizarea prelucrării datelor cu caracter personal”

h) Independență și imparțialitate

Articolele 2-4 prevăd faptul că Centrul este un organism apolitic, nefiind susținut de un partid politic.

i) Resurse adecvate

Articolul 5 definește finanțarea activităților Centrului.

j) Membri care urmează să fie supuși obligației de confidențialitate

Articolul 22 stipulează obligația de a păstra secretele de stat și alte secrete, precum și confidențialitatea informațiilor.

k) Deciziile pot face obiectul unui recurs înaintat în instanță

Această competență este prevăzută în Legea PD în cadrul articolului 44 alineatul (5).

l) Cooperarea cu alte autorități de protecție a datelor

În cadrul art. 8 al. (1) lit. (n) aceasta este prevăzută ca fiind cooperare cu „instituții de același fel din străinătate”.

Analiză de specialitate cu privire la legislația privind protecția datelor din Republica Moldova

Concluzii și recomandări

În lumina comentariilor și sugestiilor făcute mai sus, expertul concluzionează prin prezentul că proiectul de lege privind protecția datelor nu este incompatibil cu Convenția 108 (și protocolul său adițional), și nici cu dispozițiile viitoare din cadrul proiectului Convenției modernizate. Expertul dorește să remarce că a fost făcută o mare îmbunătățire de la proiectul de lege privind protecția datelor cu caracter personal pe care aceasta a avut ocazia să îl examineze, iar multe dintre observațiile sale au fost luate în considerare și aplicate.

Cu toate acestea, câteva dispoziții ar trebui încă să fie aliniate pentru a fi pe deplin în conformitate cu standardele relevante. Comentariile concrete sunt subliniate în analiză.

Urmând ordinea apariției acestora în această analiză, recomandările sunt:

- Îmbunătățiți nivelul de precizie cu privire la irelevanța naționalității și a reședinței fie în articolul 1, fie în articolul 3 alineatul (4), în cazul în care acesta din urmă este mai convenabil datorită formulării articolului 1.
- Evitați interpretarea potențială a formulării articolului 3 alineatul (1) din Legea PD „care duce la identificarea persoanei vizate” ca fiind aplicabilă oricăror date.
- Revizuiți definiția „categorie comună” de date cu caracter personal din articolul 3 al Legii PD, pentru a evita incertitudinea juridică.
- Revedeți formularea „prin intermediul persoanei împuternicite de către operator” din articolul 3 alineatul (8) din Legea PD.
- Definiți termenul „destinatar” în art. 3 al. (11) în concordanță cu definiția furnizată în proiectul Convenției modernizate.
- Includeți definiția „operatorului” în art. 3 din Legea PD dacă acesta se referă la orice persoană care se ocupă de date cu caracter personal (adică operator, persoana împuternicită de către operator, terță parte și destinatar).
- Examinați dacă ar fi necesară reformularea art. 2 al. (2) lit. (d) din Legea PD din motive de claritate.
- Reexaminați formularea art. 4 al. (3) lit. (b) din Legea PD.
- Clarificați termenul „obligație juridică” în articolul 4 alineatul (3) litera (c) din Legea PD.
- Precizați necesitatea pentru măsuri de protecție complementare în cazurile care permit prelucrarea datelor dintr-o categorie specială.
- În articolul 12, includeți obligația operatorului de a oferi persoanei vizate informații cu privire la categoriile de date colectate și prelucrate.
- Oferiți măsuri de protecție suplimentare pentru dreptul persoanelor vizate în art. 21 din Legea PD, nu numai pentru a asigura faptul că datele sunt prelucrate excepțional în intervalul de timp limitat, dar și pentru a permite reexaminarea prelucrării în timpul perioadei stabilite.

- Precizați competența Centrului Național de Protecție a Datelor cu Caracter Personal de a se angaja în proceduri juridice.



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

22.02.2018

**Analiza divergențelor
a legii privind protecția datelor cu caracter personal a Republicii Moldova (Legea)
din perspectiva conformității acesteia cu Regulamentul General privind protecția
datelor (GDPR)**

Titlul complet al Regulamentului:

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

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
Domeniul de aplicare a excepției pentru aplicarea Legii este mai extins decât în GDPR - prevede că Legea nu se aplică persoanelor fizice și juridice (în Lege definiți ca "operatori") care prelucrează datele cu caracter personal pentru nevoile personale și familiale. Dar o restrânge prin regula că în aceste cazuri excepționale nu ar trebui să fie încălcate drepturile subiecților de date cu caracter personal (2.a).	Scopul GDPR nu se aplică prelucrării datelor cu caracter personal de către o persoană fizică în cursul unei activități pur personale sau de uz casnic și astfel fără legătură cu o activitate profesională sau comercială. Activitățile personale sau gospodărești ar putea include corespondența și deținerea adreselor sau a rețelelor sociale și a activităților online întreprinse în contextul unor astfel de activități. Cu toate acestea, GDPR se aplică operatorilor sau persoanelor împuternicite de operatori care oferă mijloacele de prelucrare a datelor personale pentru astfel de activități personale sau de uz casnic. Acțiune: să se prevadă că legislația nu se aplică prelucrării datelor personale de către o persoană fizică în cursul unei activități pur personale sau gospodărești, fără restricții. (Articolul 2 (2.c) din GDPR)
Legea prevede că nu se aplică infracțiunilor specifice - genocid, crime împotriva umanității și crime de război -, însă legea se aplică și altor infracțiuni (penale sau administrative) (2.c, 2.2.d).	Acțiune: să se prevadă că legea nu se aplică tuturor infracțiunilor - prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, detectării sau urmăririi penale a infracțiunilor sau executării de sancțiuni penale, inclusiv salvagardarea și prevenirea amenințărilor la adresa siguranței publice și a liberei circulații a acestor date. (Datele personale prelucrate de autoritățile publice în cadrul GDPR, atunci când sunt utilizate în acest scop, sunt reglementate de Directiva (UE) 2016/680 a Parlamentului European și a Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, investigării, detectării sau urmăririi penale a infracțiunilor sau executării de sancțiuni penale și liberei circulații a acestor date și de abrogare a Deciziei-cadru 2008/977 / JAI a Consiliului). (Articolul 2 (2.d) din GDPR)
Legea nu prevede că prelucrarea datelor cu caracter personal ale persoanelor vizate care sunt în Republica Moldova de către un operator sau o persoană împuternicită de către operator care nu este stabilită în Republica Moldova ar trebui, de asemenea, să se prevadă în această	Pentru a se asigura că persoanele fizice nu sunt private de protecția la care au dreptul în temeiul legii, prelucrarea datelor cu caracter personal a subiecților de date care se află în Republica Moldova de către un operator sau o persoană împuternicită de către un operator care nu este stabilit în



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
Lege în care activitățile de prelucrare sunt: 1) legate de furnizarea de bunuri sau de servicii persoanelor vizate, indiferent dacă sunt legate de o plată sau nu; 2) atunci când se referă la monitorizarea comportamentului subiecților de date, în măsura în care comportamentul lor are loc în Republica Moldova (2.2.c).	Republica Moldova ar trebui să fie obiectul acestei legi, în care activitățile de prelucrare sunt legate de furnizarea de bunuri sau de servicii acestor persoane, indiferent dacă sunt legate de o plată. Prelucrarea datelor cu caracter personal ale subiecților de date care se află în Republica Moldova de către un operator sau o persoană împuternicită de către operator care nu este stabilită în Republica Moldova ar trebui, de asemenea, să facă obiectul Legii atunci când este legată de monitorizarea comportamentului acestor subiecți de date în măsura în care comportamentul lor are loc în Republica Moldova. Acțiune: în Lege ar trebui să se precizeze că prelucrarea datelor cu caracter personal ale subiecților de date care se află în Republica Moldova de către un operator sau o persoană împuternicită de către operator care nu este stabilită în Republica Moldova ar trebui, de asemenea, să fie obiectul Legii în care activitățile de prelucrare sunt: 1) legate de furnizarea de bunuri sau de servicii persoanelor vizate, indiferent dacă sunt legate de o plată sau nu; 2) atunci când se referă la monitorizarea comportamentului subiecților de date, în măsura în care comportamentul lor are loc în Republica Moldova (2.2.c).
Legea nu prevede că persoana fizică identificabilă poate fi identificată printr-un nume; localizare; un identificator online; factor specific genetice persoanei fizice (3).	Datele personale care au fost supuse unei pseudonimii, care ar putea fi atribuite unei persoane fizice prin utilizarea unor informații suplimentare, ar trebui considerate a fi informații privind o persoană fizică identificabilă. Pentru a determina dacă o persoană fizică este identificabilă, trebuie să se țină cont de toate mijloacele care pot fi utilizate în mod rezonabil, fie de către operator, fie de către o altă persoană pentru a identifica persoana fizică direct sau indirect. Acțiune: în Lege ar trebui să se precizeze toate criteriile posibile prin care persoana fizică poate fi identificată - este necesar să se completeze definiția datelor cu caracter personal cu criterii suplimentare prin care pot fi identificate persoane fizice identificabile, cum ar fi un nume; localizare; un identificator online; factor specific genetice persoanei fizice. (Articolul 4 alineatul (1) din GDPR)
Legea nu prevede că anumite categorii speciale de date cu caracter personal includ date care dezvăluie calitatea de membru al sindicatelor, date genetice, date biometrice în scopul identificării unice a unei persoane fizice și date referitoare la orientarea sexuală a persoanei fizice. (3)	Datele personale care, prin natura lor, sunt deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale - printre altele, date care dezvăluie calitatea de membru al sindicatelor, date genetice, date biometrice în scopul identificării unice a unei persoane fizice și date privind orientarea sexuală a persoanei fizice - merită protecția specifică, deoarece contextul procesării acestora ar putea crea riscuri semnificative pentru drepturile și libertățile fundamentale. Acțiune: dat fiind faptul că definiția categoriilor speciale de date cu caracter personal nu include toate categoriile speciale de date cu caracter personal, este necesar să se includă în definiția categoriilor speciale de date cu caracter personal date care



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	dezvăluie calitatea de membru al sindicatelor, date genetice, date biometrice în scopul identificării unice a unei persoane fizice și date referitoare la orientarea sexuală a persoanei fizice. (Articolul 9 alineatul (1) din GDPR)
Legea nu conține o definiție a restricționării prelucrării datelor (3).	Acțiune: dat fiind că definiția prelucrării datelor cu caracter personal nu include o astfel de activitate ca "restricție", ar fi recomandabil să se ia în considerare necesitatea includerii în lege a definiției de restricționare a prelucrării. (Articolul 4 alineatul 3 din GDPR)
Legea nu conține o definiție a profilării (3).	Persoanele fizice pot fi asociate cu identificatori online furnizați de dispozitivele lor, aplicații, instrumente și protocoale (adrese de protocol internet, identificatori de cookie-uri) sau alți identificatori, cum ar fi etichetele de identificare a frecvențelor radio. Acest lucru poate lăsa urme care, în special atunci când sunt combinate cu identificatori unici și alte informații primite de pe servere, pot fi folosite pentru a crea profiluri ale persoanelor fizice și pentru a le identifica. Acțiune: este necesar să se definească în lege o definiție a profilării (ceea ce înseamnă orice formă de prelucrare automată a datelor cu caracter personal care constă în utilizarea datelor cu caracter personal pentru a evalua anumite aspecte personale referitoare la o persoană fizică, în special pentru a analiza sau anticipa aspecte cu privire la performanța persoanei fizice la locul de muncă, situația economică, sănătatea, preferințele personale, interesele, fiabilitatea, comportamentul, locația sau mișcările). (Articolul 4 alineatul (4) din GDPR)
Legea nu prevede norme aplicabile procesării datelor cu caracter personal în cadrul unei anchete, în conformitate cu legea Republicii Moldova, de către autoritățile publice care pot primi aceste date (3).	Autoritățile publice cărora li se dezvăluie date cu caracter personal în conformitate cu o obligație legală pentru exercitarea misiunii lor oficiale nu ar trebui considerați destinatari în cazul în care primesc date cu caracter personal care sunt necesare pentru a efectua o anchetă specială de interes general, în conformitate cu legislația Republicii Moldova. Cererile de dezvăluire transmise de autoritățile publice ar trebui să fie întotdeauna în scris, motivate și ocazionale și nu ar trebui să se refere la întregul sistem de depozitare sau să conducă la interconectarea sistemelor de evidență. Prelucrarea datelor cu caracter personal de către aceste autorități publice ar trebui să respecte normele aplicabile privind protecția datelor în conformitate cu scopurile prelucrării. Acțiune: ar fi de dorit să se menționeze în lege că prelucrarea datelor cu caracter personal în cadrul unei anumite anchete, în conformitate cu legea Republicii Moldova, de către autoritățile publice care pot primi aceste date trebuie să fie în conformitate cu regulile aplicabile privind protecția datelor în funcție de scopurile prelucrării. (Articolul 4 alineatul 9 din GDPR)



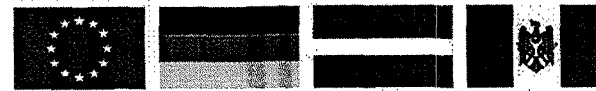
EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
Legea limitează gama autorităților publice cărora le sunt dezvăluite datele cu caracter personal în conformitate cu o obligație legală pentru exercitarea misiunii lor oficiale (3).	Legea ar trebui să acopere toate autoritățile publice posibile la care sunt dezvăluite datele cu caracter personal în conformitate cu obligația legală de a-și exercita misiunea oficială. Acțiune: în plus față de autoritățile publice enumerate în lege, ar trebui să fie enumerate autorități publice, cum ar fi autoritățile fiscale și vamale, unitățile de investigații financiare, autoritățile administrative independente sau autoritățile pieței financiare responsabile cu reglementarea și supravegherea piețelor valorilor mobiliare. (Articolul 4 alineatul 9 din GDPR)
Legea nu conține o definiție a încălcării datelor cu caracter personal. (3)	Acțiune: deoarece încălcarea datelor cu caracter personal poate avea consecințe grave, este necesar să se includă în lege definiția încălcării datelor cu caracter personal. (Articolul 4 alineatul 12 din GDPR)
Legea nu conține o definiție a datelor genetice (3).	Acțiune: deoarece datele genetice sunt una dintre datele personale sensibile, ar fi necesar să includem în lege definiția datelor genetice. Datele genetice ar trebui să fie definite ca date personale referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice care rezultă din analiza unei probe biologice de la persoana fizică în cauză, în special acidul cromozomic, deoxiribonucleic (ADN) sau acidul ribonucleic (ARN) sau din analiza unui alt element care să permită obținerea de informații echivalente. (Articolul 4 alineatul 13 din GDPR)
Legea nu conține o definiție a datelor biometrice (3).	Acțiune: deoarece datele biometrice sunt una dintre datele personale sensibile, ar fi necesar să se includă în lege definiția datelor biometrice care să o definească ca date personale care rezultă din prelucrarea tehnică specifică referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a acelei persoane fizice, cum ar fi imaginile faciale sau datele dactiloscopice. (Articolul 4 alineatul 14 din GDPR)
Legea nu conține o definiție a datelor privind sănătatea (3).	Acțiune: dat fiind că datele referitoare la sănătate sunt una dintre categoriile de date personale sensibile, ar fi necesar să se includă în lege definiția datelor privind sănătatea. Datele personale referitoare la sănătate ar trebui să includă toate datele referitoare la starea de sănătate a unui subiect de date care prezintă informații referitoare la starea de sănătate fizică sau psihică trecută, actuală sau viitoare a persoanei vizate: informații despre persoana fizică colectată în cursul înregistrării sau furnizării de servicii de sănătate acestei persoane fizice; un număr, un simbol sau o atribuire particulară unei persoane fizice pentru identificarea unică a persoanei fizice în scopuri de sănătate; informații derivate din testarea sau examinarea unei părți corporale sau a unei substanțe corporale, inclusiv din date genetice și probe biologice; și orice informații referitoare, de exemplu, la o boală, handicap, risc de boală, antecedente



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	medicale, tratament clinic sau starea fiziologică sau biomedicală a persoanei vizate, independent de sursa ei, de exemplu de la un medic sau alt profesionist medical, dispozitiv medical sau un test de diagnostic in vitro. (Articolul 4 alineatul 15 din GDPR)
Legea nu conține o definiție a locației de bază (3).	Acțiune: este necesar să se definească (enumere) criterii specifice prin care să se determine sediul principal. Principalul sediu a unui operator în Republica Moldova ar trebui să fie locul administrației sale centrale în Republica Moldova. Sediul principal a unui operator în Republica Moldova ar trebui stabilit în funcție de criterii obiective și ar trebui să implice exercitarea efectivă și reală a activităților de conducere, determinând deciziile principale cu privire la scopurile și mijloacele de prelucrare prin intermediul unor aranjamente stabile. Sediul principal al persoanei împuternicite de operator ar trebui să fie locul administrației sale centrale în Republica Moldova sau, dacă nu are o administrație centrală în Republica Moldova, ar trebui să fie locul unde se petrec principalele activități de prelucrare în Republica Moldova. (Articolul 4 alineatul 16 din GDPR)
Legea nu conține o definiție a reprezentantului. (3)	Acțiune: să se ofere o definiție a reprezentantului, așa cum este prevăzută în articolul 4 alineatul (17) din GDPR.
Legea nu conține o definiție a regulilor corporative obligatorii (3).	Deoarece este foarte ca întreprinderile să aibă sucursale, întreprinderi controlate, subdiviziuni teritoriale, este necesar ca toate să aibă o politică comună de protecție a datelor cu caracter personal (linii directoare) care să fie respectate de un operator sau o persoană împuternicită de operator stabilit pe teritoriul Republicii Moldova pentru transferuri sau un set de transferuri de date cu caracter personal către un operator sau o persoană împuternicită de operator din una sau mai multe țări terțe, în cadrul unui grup de întreprinderi sau al unui grup de companii care desfășoară o activitate economică comună. Acțiune: în Lege trebuie să existe o definiție a regulilor corporative obligatorii. (Articolul 4 alineatul 20 din GDPR)
Legea nu conține o definiție a prelucrării transfrontaliere (3).	Acțiune: în zilele în care are loc globalizarea, este necesar să se descrie ce este procesarea transfrontalieră. (Articolul 4 alineatul 23 din GDPR)
Legea nu conține o definiție a obiecțiilor pertinente și motivate, dar rezultă parțial din paragraful 1 al articolului 16 din lege. (3)	Acțiune: considerați necesitatea de a defini obiecții relevante și motivate. Deoarece este important să se afirme că obiecțiile relevante și motivate sunt cele care demonstrează clar semnificația riscurilor prezentate de proiectul de decizie în ceea ce privește drepturile și libertățile fundamentale ale persoanelor vizate și, după caz, fluxul liber de date cu caracter personal în cadrul Republicii din Moldova. (Articolul 4 alineatul (24) din GDPR)
Legea nu include principiul transparenței (4.1.a)	Principiile protecției datelor ar trebui să se aplice oricărei informații referitoare la o persoană fizică identificată sau



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	identificabilă și este important ca datele cu caracter personal să fie prelucrate în mod transparent în raport cu persoana vizată. Principiul transparenței impune ca orice informație și comunicare referitoare la prelucrarea datelor cu caracter personal să fie ușor accesibile și ușor de înțeles și să fie utilizat un limbaj clar și simplu. Acest principiu se referă, în special, la informarea persoanelor vizate cu privire la identitatea operatorului și la scopul prelucrării datelor și alte informații care să asigure o prelucrare corectă și transparentă a datelor și să asigure respectarea drepturilor persoanelor fizice în cauză și dreptul lor de a obține confirmarea și comunicarea privind datele personale care sunt prelucrate. Acțiune: în lege trebuie precizat că datele cu caracter personal trebuie prelucrate în mod transparent în raport cu persoana vizată. (Articolul 5 alineatul 1.a din GDPR)
Legea nu enumeră toate posibilele baze legitime care se vor aplica în urma prelucrării datelor cu caracter personal (-)	Pentru ca prelucrarea să fie legală, datele cu caracter personal ar trebui să fie prelucrate în baza legii, prevăzute de lege, inclusiv necesitatea respectării obligației legale la care este supus operatorul sau a necesității executării unui contract pe care persoana vizată este parte sau pentru a lua măsuri la cererea persoanei vizate înainte de a încheia un contract. Acțiune: să se prevadă reguli conform cărora prelucrarea datelor cu caracter personal ar trebui să fie legală și să se aplice cel puțin una dintre bazele legitime și ulterior, să se ia în considerare lista cu toate bazele legitime posibile (Articolul 6 alineatul (1) din GDPR)
Legea nu prevede o regulă conform căreia consimțământul persoanei cu caracter personal ar trebui să fie dat în scopuri specifice (punctul 5.1)	În cazul în care prelucrarea se bazează pe consimțământul persoanei vizate, o declarație de consimțământ pre-formulată de către operator trebuie să fie furnizată într-o formă inteligibilă și ușor accesibilă, folosind un limbaj clar și simplu și nu trebuie să conțină clauze abuzive. Pentru comunicarea consimțământului, persoana vizată trebuie să cunoască cel puțin identitatea operatorului și scopul prelucrării datele cu caracter personal. Acțiune: să se prevadă norme în care persoana vizată acordă consimțământul pentru prelucrarea datelor sale cu caracter personal în scopuri specifice. (Articolul 6 alineatul 1.a din GDPR)
Legea nu evidențiază un subiect specific de date - copil (5.5.e)	Acțiune: deoarece copiii sunt mai puțin protejați ca adulții, ar fi recomandabil să se ia în considerare necesitatea de a evidenția persoana vizată - copilul a cărui interese ar trebui să fie primare față de alte interese ale persoanelor vizate. (Articolul 6 (1f) din GDPR)
Legea nu precizează condițiile pe care trebuie să le îndeplinească operatorul, dacă dorește să proceseze date personale în alt scop decât cele pentru care au fost colectate datele cu caracter personal și nu se bazează pe	Prelucrarea datelor cu caracter personal în alte scopuri decât cele pentru care datele cu caracter personal au fost inițial colectate ar trebui să fie permisă numai în cazul în care



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
consimțământul persoanei vizate (5.5.f).	prelucrarea este compatibilă cu scopurile pentru care datele cu caracter personal au fost inițial colectate. Pentru a stabili dacă un scop de prelucrare ulterioară este compatibil cu scopul pentru care datele cu caracter personal sunt colectate inițial, operatorul ar trebui să țină seama în special de: orice legătură între aceste scopuri și scopul prelucrării preconizate; contextul în care au fost colectate datele cu caracter personal, în special așteptările rezonabile ale persoanelor vizate bazate pe relația lor cu operatorul cu privire la utilizarea ulterioară a acestora; natura datelor cu caracter personal; consecințele prelucrării ulterioare preconizate pentru persoanele vizate; precum și existența unor garanții adecvate atât pentru operațiunile de prelucrare inițiale, cât și pentru cele preconizate. Acțiune: ar fi recomandabil să se ia în considerare necesitatea de a furniza condiții care ar trebui îndeplinite de operator dacă dorește să proceseze date personale pentru un alt scop decât cel pentru care au fost colectate datele cu caracter personal și nu se bazează pe consimțământul persoanei vizate. (Articolul 6 alineatul 4 din GDPR)
Legea nu prevede condiții aplicabile consimțământului copilului în legătură cu serviciul societății informaționale. (-)	Copiii merită o protecție specifică în ceea ce privește datele lor personale, deoarece aceștia ar putea să fie mai puțin conștienți de riscurile, consecințele și garanțiile în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal. O astfel de protecție specifică ar trebui să se aplice, în special, în cazul utilizării datelor cu caracter personal ale copiilor în scopul comercializării sau creării profilurilor de personalitate sau de utilizare și colectare de date cu caracter personal în ceea ce privește copiii atunci când folosesc serviciile oferite direct unui copil. Acțiune: să se ofere condiții care să permită consimțământul copilului în legătură cu serviciul societății informaționale. (Articolul 8 din GDPR)
Legea nu prevede că categoriile speciale de date cu caracter personal pot fi procesate ori de câte ori instanțele judecătorești acționează în calitatea lor judiciară. (-)	Acțiune: ar fi recomandabil să se ia în considerare necesitatea de a prevedea că categoriile speciale de date cu caracter personal pot fi prelucrate ori de câte ori instanțele judecătorești acționează în calitatea lor judiciară. (Articolul 9 (2.f) din GDPR)
Legea nu prevede excepția că pot fi prelucrate categorii speciale de date cu caracter personal dacă acest lucru este necesar din motive de interes public considerabil. (6.1.)	<i>Articolul 9 (4) din GDPR oferă libertatea de alegere și afirmă că statele pot menține sau introduce alte condiții, inclusiv limitări, în ceea ce privește prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea.</i> Acțiune: să se ia în considerare necesitatea de a face excepție faptul că anumite categorii speciale de date cu caracter personal pot fi prelucrate dacă este necesar și din motive de interes public considerabil. (Articolul 9 (4.g) din GDPR)



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
Legea nu prevede excepția că categoriile speciale de date cu caracter personal pot fi prelucrate dacă sunt necesare în scopul arhivării în scopuri de interes public, în scopuri științifice sau istorice de cercetare sau în scopuri statistice, bazate pe legea statului, proporționale cu scopul urmărit; esența dreptului la protecție a datelor și să prevadă măsuri adecvate și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate. (6.1.)	<i>Articolul 9 (4) din GDPR oferă libertatea de alegere și afirmă că statele pot menține sau introduce alte condiții, inclusiv limitări, în ceea ce privește prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea.</i> Acțiune: să ia în considerare necesitatea de a face excepție faptul că categorii speciale de date cu caracter personal pot fi prelucrate dacă este necesar în scopuri de arhivare, în interes public, în scopuri științifice sau istorice de cercetare sau în scopuri statistice bazate pe legea statului, proporționale cu scopul urmărit, respectă esența dreptului la protecția datelor și prevăd măsuri adecvate și specifice pentru a proteja drepturile fundamentale și interesele persoanei vizate. (Articolul 9 (4.j) din GDPR)
Legea nu prevede condiții pentru prelucrarea datelor cu caracter personal care nu necesită identificare. (-)	În cazul în care datele cu caracter personal prelucrate de un operator nu permit operatorului să identifice o persoană fizică, acesta nu ar trebui să obțină informații suplimentare pentru a identifica persoana vizată numai în scopul respectării oricărei dispoziții din lege. Cu toate acestea, operatorul nu trebuie să refuze să ia informații suplimentare furnizate de persoana vizată pentru a susține exercitarea drepturilor sale. Identificarea ar trebui să includă identificarea digitală a persoanei vizate, de exemplu prin intermediul unui mecanism de autentificare, cum ar fi aceleași acreditări, utilizat de persoana vizată pentru a vă conecta la serviciul on-line oferit de controlorul de date. Acțiune: să se prevadă condiții pentru prelucrarea datelor cu caracter personal care nu necesită identificare. (Articolul 11 din GDPR)
Legea nu prevede condiții de informare, comunicare și modalități transparente pentru exercitarea drepturilor persoanei vizate.	Principiul transparenței impune ca orice informație adresată publicului sau persoanei vizate să fie concisă, ușor accesibilă și ușor de înțeles și să fie folosită o limbă clară și, dacă este cazul, vizualizată. Acest lucru are o relevanță deosebită în situațiile în care proliferarea actorilor și complexitatea tehnologică a practicilor îngreunează persoana vizată să cunoască și să înțeleagă dacă, de cine și în ce scop sunt colectate date cu caracter personal care îi privesc, cum ar fi în cazul publicității online. Având în vedere că copiii merită o protecție specifică, orice informație și comunicare, în cazul în care prelucrarea este adresată unui copil, ar trebui să fie într-un limbaj atât de clar încât copilul să poată înțelege cu ușurință. Acțiune: să ofere condiții de informare, comunicare și modalități transparente pentru exercitarea drepturilor persoanei vizate: ar trebui prevăzute modalități de facilitare a exercitării drepturilor persoanelor vizate în temeiul legii, inclusiv mecanisme de solicitare și, dacă este cazul, de obținere, în mod gratuit, în special, accesul, rectificarea sau ștergerea datelor cu caracter personal și exercitarea dreptului de opoziție. De asemenea, operatorul ar trebui să ofere mijloacele pentru ca cererile să fie făcute electronic, în special în cazul în care datele



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	cu caracter personal sunt prelucrate prin mijloace electronice. Operatorul ar trebui să fie obligat să răspundă la cererile persoanei vizate fără întârzieri nejustificate și cel târziu în termen de o lună și să motiveze dacă operatorul nu intenționează să se conformeze unor astfel de solicitări. (Articolul 12 din GDPR)
Legea nu prevede că operatorul trebuie să furnizeze și datele de contact ale operatorului, nu numai identitatea. (12.1.1).	Principiile procesării corecte și transparente impun ca persoana vizată să fie informată cu privire la existența operațiunii de prelucrare și la scopurile acesteia. Operatorul ar trebui să furnizeze persoanei vizate orice alte informații suplimentare necesare pentru a asigura procesarea corectă și transparentă, ținând cont de circumstanțele specifice și de contextul în care sunt prelucrate datele cu caracter personal. Acțiune: să se prevadă că operatorul trebuie să furnizeze și detaliile sale de contact. (Articolul 13 (1a) din GDPR)
Legea nu prevede că operatorul trebuie să furnizeze detaliile de contact ale inspectorului de protecția datelor, după caz. (-)	Acțiune: să se prevadă că operatorul trebuie să furnizeze, dacă este cazul, datele de contact ale inspectorului de protecția datelor. (Articolul 13 (1.b) din GDPR)
Legea nu prevede că operatorul trebuie să furnizeze baza legală pentru prelucrare. (12.1.2).	Acțiune: să se prevadă că operatorul trebuie să furnizeze baza legală pentru prelucrare. (Articolul 13 (1c) din GDPR)
Legea nu prevede că operatorul trebuie să furnizeze informații cu privire la interesele legitime urmărite de operator sau de un terț (în cazul în care prelucrarea se bazează pe articolul 5 alineatul (5) litera (e) din lege.	Acțiune: să se prevadă că operatorul trebuie să furnizeze informații cu privire la interesele legitime urmărite de operator sau de o parte terță (în cazul în care prelucrarea se bazează pe articolul 5 alineatul (5) litera (e) din lege. (Articolul 13 (1.d) din GDPR)
Legea nu oferă o listă detaliată care include "dreptul de intervenție asupra datelor" și nu prevede că persoana vizată are dreptul la portabilitatea datelor. (12.1.3.b)	Acțiune: 1) este necesar să se furnizeze o listă detaliată care include "dreptul de intervenție asupra datelor" - de exemplu, să se precizeze că persoana vizată are dreptul la rectificare sau ștergere a datelor cu caracter personal sau la restricționarea prelucrării cu privire la persoana vizată; 2) să prevadă că persoana vizată are dreptul la portabilitatea datelor. (Articolul 13 alineatul (2) litera (b) din GDPR)
Legea nu prevede că operatorul va furniza persoanei vizate informații cu privire la faptul dacă furnizarea de date cu caracter personal este o cerință legală sau contractuală sau o cerință necesară pentru a încheia un contract. (12.1.3.c)	Acțiune: să se prevadă că operatorul furnizează persoanei vizate informații cu privire la faptul dacă furnizarea de date cu caracter personal este o cerință legală sau contractuală sau o cerință necesară pentru a încheia un contract. (Articolul 13 (2.e) din GDPR)
Legea nu prevede că operatorul trebuie să furnizeze persoanei vizate informația privind intenția sa de a transfera date cu caracter personal către o țară terță sau organizație internațională, făcând trimitere la garanțiile corespunzătoare sau adecvate și mijloacele prin care să obțină o copie a acestora sau unde aceste date au fost puse la dispoziție (acolo unde este	Acțiune: să se prevadă că operatorul trebuie să furnizeze persoanei vizate informația privind intenția sa de a transfera date cu caracter personal către o țară terță sau organizație internațională, trimiterea la garanțiile corespunzătoare sau adecvate și mijloacele prin care să obțină o copie a acestora sau unde aceste date au fost puse la dispoziție (acolo unde este



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
la dispoziție (acolo unde este cazul). (-)	cazul). (Articolul 13 (1f) din GDPR)
Legea nu prevede ca operatorul, în momentul obținerii datelor cu caracter personal, să furnizeze persoanei vizate informațiile suplimentare necesare pentru a asigura procesarea corectă și transparentă. (-)	Principiile procesării corecte și transparente impun ca persoana vizată să fie informată cu privire la existența operațiunii de prelucrare și la scopurile acesteia. Operatorul ar trebui să furnizeze persoanei vizate orice alte informații suplimentare necesare pentru a asigura procesarea corectă și transparentă, ținând cont de circumstanțele specifice și de contextul în care sunt prelucrate datele cu caracter personal. Acțiune: să se prevadă că, în momentul obținerii datelor cu caracter personal, operatorul furnizează persoanei vizate informațiile suplimentare necesare pentru a asigura procesarea corectă și transparentă. (Articolul 13 alineatul 2 din GDPR)
Legea nu prevede că operatorul va furniza persoanei vizate informații cu privire la perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru stabilirea acestei perioade. (-)	Acțiune: să se prevadă că operatorul furnizează persoanei vizate informații cu privire la perioada pentru care datele cu caracter personal vor fi stocate sau, dacă acest lucru nu este posibil, criteriile utilizate pentru stabilirea acestei perioade. (Articolul 13 (2a) din GDPR)
Legea nu prevede că operatorul va furniza persoanei vizate informații cu privire la existența dreptului de retragere a consimțământului în orice moment, fără a afecta legalitatea procesării bazate pe consimțământ înainte de retragerea sa, atunci când prelucrarea se bazează pe articolul 5 alineatul (1) litera) sau art. 6 alin. (1) lit. a) din lege.	Acțiune: să se prevadă că operatorul furnizează persoanei vizate informații cu privire la existența dreptului de retragere a consimțământului în orice moment, fără a afecta legalitatea prelucrării pe baza consimțământului înainte de retragerea sa, atunci când prelucrarea se bazează pe articolul 5 alineatul (1) litera sau al articolului 6 alineatul (1) litera (a) din lege. (Articolul 13 (2.c) din GDPR)
Legea nu prevede că operatorul va furniza persoanei vizate informații cu privire la dreptul de a depune o plângere la o autoritate de supraveghere. (-)	Acțiune: să se prevadă că operatorul furnizează persoanei vizate informații cu privire la dreptul de a depune o plângere la o autoritate de supraveghere. (Articolul 13 (2.d) din GDPR)
Legea nu prevede că operatorul va furniza persoanei vizate informații cu privire la existența unui proces decizional automat, inclusiv a profilului, precum și informații relevante despre logica implicată, precum și semnificația și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată. (-)	Persoana vizată trebuie informată cu privire la existența unui profil și la consecințele acestuia. Acțiune: să se prevadă că operatorul furnizează persoanei vizate informații cu privire la existența unui proces decizional automat, inclusiv profilarea și informații relevante cu privire la logica implicată, precum și semnificația și consecințele preconizate ale unei astfel de procesări pentru persoana vizată. (Articolul 13 (2.f) din GDPR)
Legea nu prevede că în cazul în care operatorul intenționează să prelucreză în continuare datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, operatorul ar trebui să informeze persoana vizată înainte de această prelucrare ulterioară cu privire la acest alt scop și alte informații necesare.	În cazul în care operatorul intenționează să proceseze datele cu caracter personal în alt scop decât cel pentru care acestea au fost colectate, operatorul ar trebui să informeze persoana vizată înainte de această prelucrare ulterioară cu privire la acest alt scop și alte informații necesare. Acțiune: să se prevadă că atunci când operatorul intenționează să prelucreză în continuare datele cu caracter personal în alt scop decât cel pentru care au fost colectate datele cu caracter personal, operatorul informează persoana vizată înainte de această prelucrare ulterioară privind scopul și alte informații



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	suplimentare relevante menționate la articolul 13 alineatul (2) din GDPR. (Articolul 13 alineatul 3 din GDPR)
Legea nu prevede o condiție detaliată care ar trebui să fie îndeplinită de către operator care furnizează persoanei vizate informații în cazul în care datele cu caracter personal nu au fost obținute de la persoana vizată.	Acțiune: să se furnizeze o condiție detaliată care ar trebui să fie îndeplinită de către operator care furnizează persoanei vizate informații cu privire la care nu au fost obținute date cu caracter personal de la persoana vizată. (Articolul 14 alineatul 3 din GDPR)
Legea nu prevede că, în cazul în care operatorul intenționează să prelucreză în continuare datele cu caracter personal într-un alt scop decât cel pentru care au fost obținute datele cu caracter personal, operatorul informează persoana vizată înainte de această prelucrare ulterioară privind scopul și orice informații suplimentare relevante.	Acțiune: să se prevadă că, în cazul în care operatorul intenționează să prelucreză în continuare datele cu caracter personal în alt scop decât cel pentru care au fost obținute datele cu caracter personal, operatorul informează persoana vizată înainte de această prelucrare ulterioară privind scopul și orice informații suplimentare relevante, astfel cum se menționează la articolul 14 alineatul (2) din GDPR. (Articolul 14 alineatul (4) din GDPR)
Legea nu prevede că, în cazurile menționate la articolul 12 alineatul (3) litera (b) din lege, operatorul va lua măsurile adecvate pentru a proteja drepturile și libertățile și interesele legitime ale subiectului vizat, inclusiv punerea informațiilor la dispoziția publicului.(12.3.b)	Acțiune: să se prevadă că, în cazurile menționate la articolul 12 alineatul (3) litera (b) din lege, operatorul va lua măsurile adecvate pentru a proteja drepturile și libertățile și interesele legitime ale persoanei vizate, inclusiv punerea informațiilor la dispoziția publicului. (Articolul 14 (5.b) din GDPR)
Legea nu prevede că, în cazul în care datele personale nu au fost obținute de la persoana vizată, operatorul are dreptul să nu aplice articolul 12 alineatul (2) din lege în cazul în care datele cu caracter personal trebuie să rămână confidențiale sub rezerva obligației de păstrare a secretului profesional reglementate de o lege, inclusiv o obligație legală de păstrare a secretului. (-)	Acțiune: ar fi necesar să se considere că în cazul în care nu au fost obținute date cu caracter personal de la persoana vizată, operatorul are dreptul să nu aplice articolul 12 alineatul (2) din lege în cazul în care datele cu caracter personal trebuie să rămână confidențiale, obligația secretului profesional reglementată de o lege, inclusiv obligația legală de păstrare a secretului. (Articolul 14 (5.d) din GDPR)
Legea nu prevede că persoana vizată are dreptul de a obține de la operator informații despre existența unui proces automat de luare a deciziilor, inclusiv profilarea, precum și importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată. (13.1.c)	Acțiune: să se prevadă că persoana vizată are dreptul de a obține de la operator informații despre existența unui proces automat de luare a deciziilor, inclusiv profilarea, precum și semnificația și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată. (Articolul 15 (1.b) din GDPR)
Legea nu oferă o listă detaliată care include "dreptul de intervenție asupra datelor". (13.1.e)	Acțiune: este necesar să se furnizeze o listă detaliată care include "dreptul de intervenție asupra datelor" - de exemplu, să se precizeze că persoana vizată are dreptul de a solicita rectificării sau ștergerii de date de către operator sau restricționarea prelucrării datelor cu caracter personal cu privire la persoana vizată sau să se opună acestei prelucrări. (Articolul 15 (1.e) din GDPR)
Legea nu prevede că persoana vizată are dreptul să obțină de la operator informații despre perioada prevăzută pentru care vor fi stocate datele cu caracter personal sau, dacă nu este posibil, criteriile utilizate pentru a determina această perioadă (dacă este posibil). (-)	Acțiune: să se prevadă că persoana vizată are dreptul să obțină de la operator informații despre perioada prevăzută pentru care vor fi stocate datele cu caracter personal sau, dacă nu este posibil, criteriile utilizate pentru a determina această perioadă (dacă este posibil).



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	(Articolul 15 (1.d) din GDPR)
Legea nu prevede că persoana vizată are dreptul de a obține de la operator informații despre dreptul de a depune o plângere la o autoritate de supraveghere. (-)	Acțiune: să se prevadă că persoana vizată are dreptul de a obține de la operator informații despre dreptul de a depune o plângere la o autoritate de supraveghere. (Articolul 15 (1f) din GDPR)
Legea nu prevede că persoana vizată are dreptul de a fi informată cu privire la garanțiile corespunzătoare, în cazul în care datele cu caracter personal sunt transferate unei țări terțe sau unei organizații internaționale. (-)	Acțiune: să se prevadă că persoana vizată are dreptul de a fi informată cu privire la măsurile de protecție adecvate, în cazul în care datele cu caracter personal sunt transferate unei țări terțe sau unei organizații internaționale. (Articolul 15 alineatul 2 din GDPR)
Legea nu prevede ca operatorul să furnizeze o copie a datelor cu caracter personal în cursul perioadei de prelucrare. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă pe baza costurilor administrative. În cazul în care persoana vizată depune cererea prin mijloace electronice și dacă persoana vizată nu solicită altfel, informațiile se furnizează în formă electronică utilizată în mod obișnuit. De asemenea, Legea nu prevede că dreptul de a obține o copie menționată nu va afecta negativ drepturile și libertățile celorlalți. (-)	Acțiune: 1) să se prevadă că operatorul va furniza o copie a datelor cu caracter personal în cursul perioadei de prelucrare. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă pe baza costurilor administrative. În cazul în care persoana vizată depune cererea prin mijloace electronice și dacă persoana vizată nu solicită altfel, informațiile se furnizează în formă electronică utilizată în mod obișnuit; 2) să se prevadă că dreptul de a obține o copie menționată nu afectează în mod negativ drepturile și libertățile altora. (Articolul 15 alineatul 3 din GDPR)
Legea nu prevede condiții detaliate privind dreptul persoanei vizate de a fi uitată (are dreptul de a obține de la operator o ștergere a datelor cu caracter personal care o privesc fără întârzieri nejustificate și operatorul are obligația de a șterge personal fără întârzieri nejustificate în cazul în care se aplică unul dintre motivele specifice). (14 litera)	Persoana vizată ar trebui să aibă un "drept de a fi uitată" în cazul în care păstrarea unor astfel de date încalcă legea la care este supus operatorul. În special, persoana vizată ar trebui să aibă dreptul de a șterge datele sale cu caracter personal și de a nu mai fi prelucrate în cazul în care datele cu caracter personal nu mai sunt necesare în legătură cu scopurile pentru care sunt colectate sau prelucrate în alt mod, consimțământul acestuia sau obiectează la prelucrarea datelor cu caracter personal care îl privesc sau în cazul în care prelucrarea datelor sale cu caracter personal nu respectă în alt mod prezentul regulament. Acest drept este relevant în special în cazul în care persoana vizată și-a dat consimțământul fiind copil și nu era pe deplin conștientă de riscurile implicate de prelucrare și mai târziu dorește să elimine aceste date cu caracter personal, în special pe internet. Persoana vizată ar trebui să poată exercita acest drept, chiar dacă acesta nu mai este copil. Cu toate acestea, păstrarea în continuare a datelor cu caracter personal ar trebui să fie legală atunci când este necesar, pentru exercitarea dreptului la libertatea de exprimare și de informare, pentru respectarea unei obligații legale, pentru îndeplinirea unei sarcini în interes public sau în exercitarea autorității publice care revine operatorului, pe motive de interes public în domeniul sănătății publice, în scopuri de arhivare în interesul public, în scopuri de cercetare științifică sau istorică sau în scopuri statistice sau pentru stabilirea, exercitarea sau apărarea unor revendicări legale. Acțiune: să furnizeze condiții detaliate privind dreptul persoanei vizate de a fi uitată - să aibă dreptul de a obține de la operator o ștergere a datelor cu caracter personal care o privesc fără întârzieri nejustificate și operatorul are obligația de a șterge



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	datele cu caracter personal fără întârzieri nejustificate, în cazul în care unul dintre motivele specifice se aplică în conformitate cu articolul 17 alineatul (1) din GDPR. (Articolul 17 alineatul (1) din GDPR)
Legea nu prevede o obligație imperioasă a operatorului față de alți operatori care prelucrează datele cu caracter personal pe care persoana vizată le-a solicitat să le ștergă (pentru a ajunge la dreptul persoanei vizate de a fi uitată). (14.b)	Pentru a consolida dreptul de a fi uitat în mediul online, dreptul de ștergere ar trebui să fie extins astfel încât un operator care a făcut publice datele personale ar trebui să fie obligat să informeze operatorii care prelucrează astfel de date cu caracter personal pentru a șterge orice link-uri, copii sau replicări ale acestor date personale. Procedând astfel, operatorul respectiv trebuie să ia măsuri rezonabile, ținând seama de tehnologia disponibilă și de mijloacele de care dispune, inclusiv de măsurile tehnice, pentru a informa operatorii care prelucrează datele cu caracter personal privind solicitarea persoanei vizate. Acțiune: să se impună operatorului o obligație mai imperativă (așa cum este prevăzută la articolul 17 alineatul (2) din GDPR) în ceea ce privește operatorii care prelucrează datele cu caracter personal pe care persoana vizată le-a solicitat să le ștergă (pentru a ajunge la dreptul persoanei vizate de a fi uitată). (Articolul 17 alineatul 2 din GDPR)
Legea nu prevede dreptul persoanelor vizate de a restricționa prelucrarea. (-)	Metodele prin care se limitează prelucrarea datelor cu caracter personal ar putea include, printre altele, mutarea temporară a datelor selectate într-un alt sistem de procesare, transformarea datelor personale selectate în imposibilitatea de a fi utilizate de către utilizatori sau eliminarea temporară a datelor publicate de pe un site web. În sistemele automatizate de arhivare, restricționarea prelucrării ar trebui în principiu să fie asigurată prin mijloace tehnice, astfel încât datele cu caracter personal să nu facă obiectul unor operațiuni ulterioare de prelucrare și să nu poată fi modificate. Faptul că prelucrarea datelor cu caracter personal este restricționată ar trebui să fie clar indicată în sistem. Acțiune: asigurarea dreptului persoanei vizate de a restricționa prelucrarea. (Articolul 18 din GDPR)
Legea nu prevede obligația operatorului de a informa persoana vizată despre destinatarii cărora le-au fost comunicate datele cu caracter personal, în cazul în care persoana vizată solicită. (14.b)	Acțiune: obligația operatorului de a informa persoana vizată cu privire la destinatarii cărora le-au fost comunicate datele cu caracter personal în cazul în care persoana vizată solicită. (Articolul 19 din GDPR)
Legea nu prevede dreptul persoanei vizate asupra portabilității datelor. (-)	Persoana vizată ar trebui să aibă permisiunea de a primi date cu caracter personal care o privesc pe care le-a furnizat unui operator într-un format structurat, utilizat în mod obișnuit, interoperabil și să îl transmită altui operator. Acest drept ar trebui aplicat în cazul în care persoana vizată a furnizat datele cu caracter personal pe baza consimțământului său sau prelucrarea este necesară pentru executarea unui contract. Nu ar trebui să se aplice atunci când prelucrarea se bazează pe un motiv juridic diferit de consimțământ sau contract. Prin natura sa, acest drept nu ar trebui exercitat împotriva operatorilor care prelucrează date cu caracter personal în exercitarea atribuțiilor lor publice.



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	Dreptul persoanei vizate de a transmite sau primi date cu caracter personal care îi privesc nu ar trebui să creeze o obligație pentru operatorii de a adopta sau de a menține sisteme de prelucrare compatibile din punct de vedere tehnic. În cazul în care, într-un anumit set de date cu caracter personal, mai mulți subiecți de date sunt vizati, dreptul de a primi datele cu caracter personal nu trebuie să aducă atingere drepturilor și libertăților altor persoane vizate. În cazul în care acest lucru este fezabil din punct de vedere tehnic, persoana vizată ar trebui să aibă dreptul de a transmite datele personale direct de la un operator la altul. Acțiune: furnizați dreptul persoanei vizate la portabilitatea datelor. (Articolul 20 din GDPR)
Legea nu prevede că datele cu caracter personal nu vor mai fi prelucrate în cazul în care persoana vizată obiectează pentru prelucrare în scopuri de marketing direct. (-)	Acțiune: să se prevadă că datele cu caracter personal nu vor mai fi prelucrate în cazul în care persoana vizată obiectează pentru prelucrare în scopuri de marketing direct. (Articolul 21 alineatul (3) din GDPR)
Legea nu prevede că, cel târziu, în momentul primei comunicări cu persoana vizată, dreptul menționat la paragrafele 1 și 2 ale articolului 16 din lege va fi adus în mod explicit în atenția persoanei vizate și va fi prezentat clar și separat de orice alte informații. (16.1 și 16.2)	Dreptul persoanei vizate la obiecție ar trebui să fie adus în mod explicit în atenția persoanei vizate și prezentat în mod clar și separat de orice alte informații. Acțiune: să se prevadă că, cel târziu, în momentul primei comunicări cu persoana vizată, dreptul la care se face referire în paragrafele 1 și 2 ale articolului 16 din lege va fi adus în mod explicit în atenția persoanei vizate și va fi prezentat clar și separat de orice alte informații. (Articolul 21 alineatul (4) din GDPR)
Legea nu prevede că, în contextul utilizării serviciilor societății informaționale, persoana vizată își poate exercita dreptul de a se opune prin mijloace automatizate, utilizând specificații tehnice. (16.1).	Acțiune: să se prevadă că, în contextul utilizării serviciilor societății informaționale, persoana vizată își poate exercita dreptul de a se opune prin mijloace automate prin utilizarea specificațiilor tehnice. (Articolul 21 alineatul 5 din GDPR)
Legea limitează dreptul persoanei vizate la anumite aspecte personale, cum ar fi performanța sa la locul de muncă, bonitatea, comportamentul sau alte aspecte similare, dar GDPR oferă acest drept tuturor aspectelor care produc efecte juridice asupra persoanei vizate sau îi afectează în mod semnificativ. (17.1).	Persoana vizată ar trebui să aibă dreptul de a nu fi obiectul unei decizii care poate include o măsură care să evalueze aspectele sale personale care se bazează exclusiv pe prelucrarea automatizată și care produce efecte juridice care o privesc sau o afectează în mod semnificativ. O astfel de prelucrare include "profilare" care constă în orice formă de prelucrare automată a datelor cu caracter personal care evaluează aspectele personale legate de o persoană fizică, în special pentru a analiza sau prezice aspecte privind performanța persoanei vizate la locul de muncă, situația economică, sănătatea, interesele, fiabilitatea sau comportamentul, localizarea sau mișcările, în cazul în care produce efecte juridice care oprivesc sau, în mod similar, o afectează în mod semnificativ. Acțiune: în locul restricției, persoana vizată are dreptul să solicite anularea, în totalitate sau în parte, a oricărei decizii individuale care produce efecte juridice privind drepturile și libertățile sale și care se bazează exclusiv pe prelucrarea



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	automată a datelor destinate să evalueze anumite aspecte personale legate de ea, cum ar fi performanța sa la locul de muncă, bonitatea, comportamentul sau alte aspecte similare pentru a asigura o reglementare mai amplă - că persoana vizată are dreptul de a nu face obiectul unei decizii bazate exclusiv pe prelucrarea automată, profilare, care produce efecte juridice care o privesc sau o afectează în mod semnificativ. (Articolul 22 alineatul (1) din GDPR)
Legea nu prevede că o persoană poate fi supusă deciziei de tipul celor prevăzute la articolul 17 alineatul (1) din lege dacă această decizie se bazează pe acordul explicit al persoanei vizate. (17,2).	Acțiune: să se prevadă că o persoană poate fi supusă deciziei de tipul celor menționate la articolul 17 alineatul (1) din lege dacă această decizie se bazează pe acordul explicit al persoanei vizate. (Articolul 22 (2.c) din GDPR)
Legea nu prevede condiții pentru operatorul de date care ar trebui îndeplinite în cazurile prevăzute la paragraful 2 al articolului 17 din lege. (17.)	Acțiune: să se prevadă condiții pentru operatorul de date, așa cum prevede articolul 22 alineatul (3) și articolul 22 alineatul (4) din GDPR (Articolul 22 alineatul (3) și articolul 22 alineatul (4) din GDPR)
Articolul 15 din lege care prevede restricții nu prevede restricții prevăzute la articolul 23 din GDPR. (-)	Restricțiile privind principiile specifice și drepturile la informare, accesul la și rectificarea sau ștergerea datelor cu caracter personal, dreptul la portabilitate a datelor, dreptul de a se opune, deciziile bazate pe profilare, precum și comunicarea unei încălcări a datelor cu caracter personal unui subiect de date iar anumite obligații aferente ale operatorilor pot fi impuse prin lege, în măsura în care este necesar și proporțional într-o societate democratică, pentru a proteja securitatea publică, inclusiv protecția vieții umane, în special ca răspuns la dezastrele naturale sau provocate de om, prevenirea, investigarea și urmărirea penală a infracțiunilor penale sau executarea sancțiunilor penale, inclusiv protejarea și prevenirea amenințărilor la adresa siguranței publice sau încălcarea eticii pentru profesiile reglementate, alte obiective importante de interes public general ale statului, în special un interes economic sau financiar important a statului, păstrarea registrelor publice păstrate din motive de interes public, prelucrarea ulterioară a datelor cu caracter personal arhivate pentru a furniza informații specifice legate de comportamentul politic în cadrul fostelor regimuri de stat sau de protecția persoanei vizate sau a drepturilor și libertăților altora, inclusiv protecția socială, sănătatea publică și scopurile umanitare. Acțiune: ar fi recomandabil să se ia în considerare necesitatea de a prevedea restricții stabilite la articolul 23 din GDPR. (Articolul 23 din GDPR)
Legea nu are un capitol separat (secțiuni, articole) care stabilește obligațiile și condițiile pentru operatori și persoana imputernicită de operator. (-) Există unele reguli în Hotărârea de Guvern nr. 1123, dar nu este suficient conform GDPR - Hotărârea Guvernului nr. 1123 nu are obligații și condiții detaliate și exhaustive pentru operatori și persoanele care sunt imputernicite de	Acțiune: să fie prevăzut un capitol separat (secțiuni, articole) care să stabilească obligațiile și condițiile generale pentru operatori și persoanele imputernicite de către operatori, așa cum este prezentat în Capitolul IV al GDPR. (Capitolul IV al GDPR)



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
către operatori. Și chiar mai mult aceste reguli ar trebui să fie prevăzute în lege în loc de decizie a Guvernului. <i>Inclusiv:</i> ⏚	<i>Inclusiv:</i> ⏚
Legea nu prevede cerințe specifice pentru protecția datelor începând cu momentul conceperii și în mod implicit. (-)	Pentru a putea demonstra conformitatea cu legea, operatorul ar trebui să adopte politici interne și să pună în aplicare măsuri care să îndeplinească, în special, principiile protecției datelor începând cu momentul conceperii și protecția datelor în mod implicit. Astfel de măsuri ar putea consta, printre altele, în minimizarea prelucrării datelor cu caracter personal, pseudonimizarea datelor cu caracter personal cât mai curând posibil, transparența în ceea ce privește funcțiile și prelucrarea datelor cu caracter personal, care să permită persoanei vizate să monitorizeze prelucrarea datelor, permițând operatorului să creeze și să îmbunătățească caracteristicile de securitate. Acțiune: să se prevadă cerințe specifice pentru protecția datelor, începând cu momentul conceperii și în mod implicit. (Articolul 25 din GDPR)
Legea nu prevede reguli pentru operatori asociați.	Protecția drepturilor și libertăților persoanelor vizate, precum și responsabilitatea și răspunderea operatorilor și persoanelor imputernicite de operatori, inclusiv în ceea ce privește monitorizarea prin intermediul măsurilor autorităților de supraveghere, necesită o alocare clară a responsabilităților prevăzute de lege, inclusiv în cazul în care un operator determină scopurile și mijloacele de procesare împreună cu alți operatori sau în cazul în care o operațiune de prelucrare este efectuată în numele unui operator. Acțiune: să se prevadă reguli pentru operatori asociați. (Articolul 26 din GDPR)
Legea nu prevede reguli pentru reprezentanții operatorilor sau a persoanelor imputernicite de către operatori care nu sunt stabiliți în Republica Moldova.	În cazul în care un operator sau o persoană imputernicită de către un operator care nu este stabilit în Republica Moldova prelucrează date cu caracter personal ale persoanelor vizate care se află în Republica Moldova ale căror activități de prelucrare sunt legate de oferirea de bunuri sau de servicii, indiferent dacă plata persoanei vizate este necesară pentru aceste persoane vizate în Republica Moldova sau pentru monitorizarea comportamentului lor, în măsura în care comportamentul lor are loc în Republica Moldova, operatorul sau persoana care este imputernicită de către operator ar trebui să desemneze un reprezentant, cu excepția cazului în care prelucrarea este ocazională, nu include prelucrarea la scară largă a unor categorii speciale de date cu caracter personal sau prelucrarea datelor cu caracter personal referitoare la condamnări penale și infracțiuni și este puțin probabil să ducă la un risc pentru drepturile și libertățile persoanelor fizice, ținând seama de natura, contextul, și scopurile prelucrării sau dacă operatorul este o autoritate sau un organism public. Reprezentantul ar trebui să acționeze în numele operatorului sau al persoanei imputernicite de către



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	operator și poate fi abordat de autoritatea de supraveghere. Reprezentantul ar trebui să fie desemnat în mod explicit printr-un mandat scris al operatorului sau a persoanei împuternicite de către operator de a acționa în numele său cu privire la obligațiile care îi revin în temeiul legii. Desemnarea unui astfel de reprezentant nu afectează responsabilitatea sau răspunderea operatorului sau a persoanei împuternicite de către operator conform legii. Un astfel de reprezentant ar trebui să-și îndeplinească sarcinile în conformitate cu mandatul primit de la operator sau de la persoana împuternicită de către operator, inclusiv prin cooperarea cu autoritățile de supraveghere competente cu privire la orice acțiune întreprinsă pentru a asigura respectarea legii. Reprezentantul desemnat ar trebui să fie obiectul unei proceduri de executare în cazul nerespectării de către operatorul sau prelucrătorul. Acțiune: să se prevadă reguli pentru reprezentanții operatorilor sau ale persoanelor împuternicite de către operatori care nu sunt stabiliți în Republica Moldova. (Articolul 27 din GDPR)
Legea nu prevede că persoana împuternicită de operator nu trebuie să angajeze un altă persoană împuternicită fără o autorizație scrisă specifică sau generală a operatorului. În cazul autorizației scrise generale, persoana împuternicită de operator informează operatorul despre modificările intenționate privind adăugarea sau înlocuirea altor persoane împuternicite, oferind astfel operatorului posibilitatea de a se opune unor astfel de modificări. (-)	Acțiune: să se prevadă că persoana împuternicită de operator nu trebuie să angajeze un altă persoană împuternicită fără o autorizație scrisă specifică sau generală a operatorului. În cazul autorizației scrise generale, persoana împuternicită de operator informează operatorul despre modificările intenționate privind adăugarea sau înlocuirea altor persoane împuternicite, oferind astfel operatorului posibilitatea de a se opune unor astfel de modificări. (Articolul 28 alineatul (2) din GDPR)
Legea nu stabilește reguli detaliate care trebuie incluse în contract sau în actul juridic (cum ar fi obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile persoanelor vizate și obligațiile și drepturile operatorului). (30.3).	Executarea prelucrării de către o persoană împuternicită de către operator ar trebui să fie reglementată de un contract sau de un alt act juridic care să lege persoana împuternicită de către operator la operator, stabilind obiectul și durata prelucrării, natura și scopul prelucrării, tipul de prelucrare datele cu caracter personal și categoriile persoanelor vizate, ținând cont de sarcinile și responsabilitățile specifice ale persoanei împuternicite de către operator în contextul prelucrării care trebuie efectuată și de riscul pentru drepturile și libertățile persoanei vizate. Acțiune: să se prevadă norme detaliate care trebuie incluse în contract sau în actul juridic (cum ar fi obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile persoanelor vizate și obligațiile și drepturile operatorului). (Articolul 28 alineatul (3) din GDPR)
Legea nu prevede că instrucțiunile operatorului vor fi documentate. De asemenea, legea nu prevede că, în cazul transferurilor de date cu caracter personal către o țară terță sau o	Acțiune: 1) să se asigure că instrucțiunile de la operator sunt documentate; 2) să se prevadă că, în cazul transferurilor de date cu caracter personal către o țară terță sau o organizație internațională, ar



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
organizație internațională, ar trebui să existe și instrucțiuni documentate de la operator către persoana împuternicită de către operator și că într-un astfel de caz, persoana împuternicită informează operatorul despre această cerință legală înainte de prelucrare, cu excepția cazului în care legea interzice aceste informații din motive de interes general importante. (30.3.a)	trebuie să existe și instrucțiuni documentate de la operator către persoana împuternicită și că într-un astfel de caz, persoana împuternicită informează operatorul cu privire la această cerință juridică înainte de prelucrare, cu excepția cazului în care legea interzice astfel de informații din motive de interes public importante. (Articolul 28 (3.a) din GDPR)
Legea nu prevede direct că persoana împuternicită care este guvernată de un contract sau de un alt act juridic trebuie să se asigure că persoanele autorizate să proceseze datele cu caracter personal s-au angajat să păstreze confidențialitatea sau că au o obligație legală confidențială corespunzătoare. (-)	Acțiune: să se prevadă în mod direct că persoana împuternicită care este guvernată de un contract sau de un alt act juridic se asigură că persoanele autorizate să proceseze datele cu caracter personal s-au angajat să păstreze confidențialitatea sau că au obligația legală de confidențialitate (Articolul 28 (3.b) din GDPR)
Legea nu stabilește reguli care trebuie stipulate, în special, în contract sau în actul juridic. (-)	Acțiune: stabilirea unor norme care trebuie stipulate, în special, în contract sau în actul juridic (Articolul 28 alineatul (3) din GDPR)
Legea nu prevede că contractul sau celălalt act juridic prevăzut la paragraful 3 al articolului 30 din lege trebuie să fie în scris, inclusiv în formă electronică. (-)	Acțiune: să se prevadă că contractul sau celălalt act juridic menționat la articolul 30 alineatul (3) din lege trebuie să fie în scris, inclusiv în formă electronică. (Articolul 28 (9) din GDPR)
Legea nu prevede că, dacă o persoană împuternicită de operator încalcă legea prin stabilirea scopurilor și a mijloacelor de procesare, persoana împuternicită este considerată operator în ceea ce privește prelucrarea respectivă.	Acțiune: să se prevadă că, în cazul în care o persoană împuternicită încalcă legea prin stabilirea scopurilor și a mijloacelor de procesare, persoana împuternicită este considerată operator în ceea ce privește prelucrarea respectivă. (Articolul 28 (10) din GDPR)
Legea prevede o însărcinare sarcină administrativă destul de mare pentru operator – acesta personal sau prin reprezentant notifică Centrul despre activități de prelucrare a datelor cu caracter personal. În plus, această notificare prevăzută de lege nu înseamnă că operatorii vor respecta cerințele privind protecția datelor și vor asigura implementarea acestora. Mai mult, secțiunea III a Hotărârii Guvernului nr.1123 prevede că fiecare deținător de date cu caracter personal (operatorul și / sau persoana împuternicită), pe baza activității specifice, elaborează și organizează punerea în aplicare a dispozițiilor privind documentele care stabilesc politica de securitate a datelor cu caracter personal. Aceasta este o măsură care oferă rezultate mai bune decât notificarea menționată. (23.1). Legea nu prevede ca operatorul sau persoana împuternicită să țină o evidență a activităților de prelucrare pe cont propriu și în scris, inclusiv în formă electronică. (23.1).	Pentru a demonstra conformitatea cu legea, operatorul sau persoana împuternicită ar trebui să țină evidența activităților de prelucrare aflate sub responsabilitatea sa. Fiecare operator și persoană împuternicită ar trebui să fie obligată să coopereze cu autoritatea de supraveghere (Centrul) și să pună la dispoziție aceste înregistrări, la cerere, pentru a putea monitoriza operațiunile de prelucrare. Acțiunea: 1) este necesar să se evalueze dacă operatorul personal sau prin persoana împuternicită trebuie să notifice Centrul cu privire la prelucrarea activităților de date cu caracter personal (este o povară administrativă destul de mare și această notificare nu înseamnă că operatorii vor respecta cerințele privind protecția datelor și asigurarea implementării acestora) sau poate că ar fi de ajuns ca operatorul să țină o evidență a activităților de procesare și Centrul poate verifica aceste înregistrări în orice moment; 2) să se asigure că operatorul sau persoana împuternicită înregistrează o evidență a activităților de prelucrare, în scris, inclusiv în formă electronică; 3) este necesar să se evalueze necesitatea de a prevedea norme de politică de securitate a datelor cu caracter personal în Lege în locul hotărârii Guvernului; 4) în cele din urmă, deoarece GDPR nu furnizează registrul deținătorilor de date cu caracter personal, ar fi necesar să se



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	elimine articolul 28 din lege. (Articolul 30 din GDPR)
Legea nu prevede că persoana împuternicită, într-o evidență a activităților de prelucrare, trebuie să dețină și informațiile despre fiecare operator în numele căruia persoana împuternicită acționează, fie în numele operatorului sau al reprezentantului persoanei împuternicite. (23.2.a)	Acțiune: că persoana împuternicită, într-o evidență a activităților de prelucrare, trebuie să dețină și informațiile despre fiecare operator în numele căruia persoana împuternicită acționează, fie în numele operatorului sau al reprezentantului persoanei împuternicite. (Articolul 30 (2a) din GDPR)
Legea nu prevede că acea persoană împuternicită în registrul activităților de prelucrare trebuie să dețină și informații despre categoriile de prelucrare efectuate în numele fiecărui operator. (23.2.c)	Acțiune: să se asigure că acea persoană împuternicită în registrul activităților de prelucrare trebuie să dețină și informații despre categoriile de prelucrare efectuate în numele fiecărui operator. (Articolul 30 (2.b) din GDPR)
Legea nu prevede obligația concretă că, în cazul transferurilor de date cu caracter personal către o țară terță sau către o organizație internațională, trebuie deținută o evidență a activităților de prelucrare, de asemenea, informații privind documentația garanțiilor adecvate. (23.3).	Acțiune: obligația concretă că, în cazul transferurilor de date cu caracter personal către o țară terță sau către o organizație internațională, trebuie deținută o evidență a activităților de prelucrare, de asemenea, informații privind documentația garanțiilor adecvate. (Articolul 30 (2.c) din GDPR)
Legea nu prevede că înregistrarea activităților de prelucrare nu se aplică unei întreprinderi sau unei organizații care angajează mai puțin de 250 de persoane, cu excepția cazului în care prelucrarea pe care o desfășoară poate avea drept consecință un risc pentru drepturile și libertățile persoanelor vizate; prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date - date cu caracter personal care dezvăluie originea rasială sau etnică, opinii politice, credințe religioase sau filosofice sau apartenența la un sindicat și date genetice, date biometrice în scopul identificării unice a unei identități naturale persoană, date privind sănătatea sau date privind viața sexuală sau orientarea sexuală a unei persoane fizice. (23.4 și 23.5).	Acțiune: să se prevadă excepții potrivit cărora înregistrarea activităților de prelucrare nu se aplică unei întreprinderi sau unei organizații care angajează mai puțin de 250 de persoane, cu excepția cazului în care prelucrarea pe care o desfășoară poate avea drept consecință un risc pentru drepturile și libertățile persoanelor vizate; procesarea nu este ocazională sau prelucrarea include categorii speciale de date - date cu caracter personal care dezvăluie originea rasială sau etnică, opinii politice, credințe religioase sau filosofice sau apartenența la un sindicat și date genetice, date biometrice în scopul identificării unice a unei identități naturale persoană, date privind sănătatea sau date privind viața sexuală sau orientarea sexuală a unei persoane fizice. (Articolul 30 alineatul (5) din GDPR)
Legea include o excepție care nu este prevăzută în GDPR. (23.5).	Acțiune: este necesar să se evalueze dacă este cu adevărat necesar să se prevadă excepția că nu se aplică un registru al activităților de prelucrare atunci când prelucrarea se efectuează în scopul de a ține un registru destinat să informeze publicul sau orice altă persoană care dovedește un interes legitim, prelucrarea se limitează la datele necesare păstrării registrului menționat și care este obiectivul acestei excepții - este important de reținut că GDPR nu oferă o astfel de excepție. (Articolul 30 din GDPR)
Legea include o excepție care nu este prevăzută în GDPR. (23.6).	Acțiune: este necesar să se evalueze dacă este cu adevărat necesar să se prevadă că Centrul are dreptul de a stabili alte excepții atunci când nu se aplică o evidență a activităților de prelucrare și care este obiectivul acestui drept - este important de reținut că GDPR nu oferă o astfel de excepție. (Articolul 30 din GDPR)



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
Legea nu prevede obligația generală ca operatorul și persoana împuternicită și, după caz, reprezentanții acestora, să coopereze, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor sale. (20.3.?)	Acțiune: este necesar să se evalueze necesitatea de a prevedea obligația generală că operatorul și persoana împuternicită și, dacă este cazul, reprezentanții acestora, să cooperează, la cerere, cu autoritatea de supraveghere în îndeplinirea sarcinilor sale. (Articolul 31 din GDPR)
Legea prevede condiții de securitate destul de generale (comparativ cu GDPR) care ar trebui să fie puse în aplicare de operator și nu prevede că aceste măsuri de securitate vor include, printre altele, pseudonimizarea și criptarea datelor cu caracter personal; capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și reziliența în curs a sistemelor și serviciilor de prelucrare; abilitatea de a restabili în timp util disponibilitatea și accesul la datele cu caracter personal în cazul unui incident fizic sau tehnic și un proces de testare, evaluarea periodică a eficacității măsurilor tehnice și organizatorice pentru asigurarea securității prelucrării. (30.1).	Operatorul trebuie să fie obligat să implementeze măsuri adecvate și eficiente și să poată demonstra conformitatea activităților de prelucrare cu legea, inclusiv eficacitatea măsurilor. Aceste măsuri trebuie să țină seama de natura, scopul, contextul și scopurile prelucrării și riscul pentru drepturile și libertățile persoanelor fizice. Acțiune: să se prevadă condiții de securitate mai detaliate care ar trebui să fie puse în aplicare de către operator, printre altele pseudonimizarea și criptarea datelor cu caracter personal; capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și reziliența în curs a sistemelor și serviciilor de prelucrare; capacitatea de a restabili în timp util disponibilitatea și accesul la datele cu caracter personal în cazul unui incident fizic sau tehnic și un proces de testare, evaluarea periodică a eficacității măsurilor tehnice și organizatorice pentru asigurarea securității procesării (Articolul 32 din GDPR).
Deoarece Legea nu prevede existența unui cod de conduită aprobat, nu este prevăzut ca codul de conduită să poată fi folosit ca element prin care să se demonstreze măsurile tehnice și organizatorice adecvate pentru a asigura un nivel de securitate. (-)	<i>Este o libertate de a alege ca codul de conduită să fie aprobat și că codul de conduită poate fi folosit ca element prin care să se demonstreze măsurile tehnice și organizatorice adecvate pentru a asigura un nivel de securitate. (nu este obligatorie)</i> Acțiune: să ia în considerare necesitatea de a prevedea ca codul de conduită să poată fi folosit ca element prin care să se demonstreze măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate. (Articolul 32 alineatul (3) din GDPR)
Legea nu prevede că operatorul și persoana împuternicită trebuie să ia măsuri pentru a se asigura că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite care are acces la datele cu caracter personal nu le prelucreează, cu excepția instrucțiunilor operatorului, în care acesta care trebuie să facă acest lucru prin legea Republicii Moldova. (-)	Acțiune: să se prevadă că operatorul și persoana împuternicită trebuie să ia măsuri pentru a se asigura că orice persoană fizică care acționează sub autoritatea operatorului sau a persoanei împuternicite care are acces la datele cu caracter personal nu le prelucreează, cu excepția instrucțiunilor operatorului, în care acesta care trebuie să facă acest lucru prin legea Republicii Moldova. (Articolul 32 alineatul (4) din GDPR)
Legea nu prevede obligația operatorului de a notifica încălcările privind datele cu caracter personal autorității de supraveghere și persoanei vizate și nu prevede cerințe pentru această notificare. (-)	O încălcare a datelor cu caracter personal poate, dacă nu este abordată în mod corespunzător și în timp util, duce ulterior la daune fizice, materiale sau morale persoanelor fizice. Din acest motiv, ar trebui să se verifice dacă au fost puse în aplicare toate măsurile tehnologice și organizatorice adecvate pentru a stabili imediat dacă a avut loc o încălcare a datelor cu caracter personal și pentru a informa prompt autoritatea de supraveghere și persoana vizată. La stabilirea unor norme detaliate privind formatul și



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	procedurile aplicabile notificării încălcărilor datelor cu caracter personal, ar trebui să se țină seama în mod corespunzător de circumstanțele acestei încălcări, inclusiv dacă datele cu caracter personal au fost sau nu protejate prin măsuri tehnice de protecție adecvate, limitând în mod efectiv probabilitatea fraudei de identitate sau alte forme de utilizare incorectă. Acțiune: să se prevadă obligația operatorului de a notifica autoritatea de supraveghere privind încălcarea datelor cu caracter personal și cerințele pentru notificarea respectivă. (Articolul 33 și articolul 34 din GDPR)
Legea nu prevede obligația operatorului de a efectua o evaluare a impactului operațiunilor de prelucrare avute asupra protecției datelor cu caracter personal atunci când un tip de prelucrare poate duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice. (-) În schimb, Legea prevede că organismul de supraveghere - Centrul trebuie să stabilească faptul că prelucrarea este susceptibilă să ducă la un risc ridicat pentru drepturile și libertățile persoanelor fizice și va efectua o verificare prealabilă. Deoarece Legea (art. 24 alin. (1)) prevede că organul de supraveghere - Centrul stabilește că prelucrarea poate duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice și va efectua o verificare prealabilă, Legea nu prevede: (1) organismul de supraveghere stabilește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței unei evaluări a impactului privind protecția datelor; (2) conținutul unei evaluări a impactului protecției datelor; (3) conformitatea cu codurile de conduită aprobate de controlorii sau de prelucrătorii relevanți trebuie luată în considerare în evaluarea impactului operațiunilor de prelucrare efectuate de operatori sau de către persoanele împuternicite, în special în scopul unei evaluări a impactului privind protecția datelor; (4) că operatorul solicită opiniile persoanelor vizate sau ale reprezentanților acestora cu privire la prelucrarea intenționată, fără a aduce prejudiciu protecției intereselor comerciale sau publice sau securității operațiunilor de prelucrare (după caz); (5) scutirea în cazul în care nu se efectuează o evaluare a impactului; (6) operatorul efectuează o revizuire pentru a evalua dacă prelucrarea se efectuează în conformitate cu evaluarea impactului protecției datelor cel puțin atunci când există o schimbare a riscului reprezentat de operațiunile de prelucrare; (7) că operatorul consultă autoritatea de supraveghere înainte de prelucrare în cazul în care o evaluare a impactului privind protecția datelor indică faptul că prelucrarea ar conduce la un risc ridicat în absența	În cazul în care operațiunile de prelucrare pot duce la un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul ar trebui să fie responsabil de efectuarea unei evaluări a impactului privind protecția datelor pentru a evalua, în special, originea, natura, particularitatea și gravitatea din acest risc. Rezultatul evaluării ar trebui luat în considerare la stabilirea măsurilor adecvate care trebuie luate pentru a demonstra că prelucrarea datelor cu caracter personal respectă legea. În cazul în care o evaluare a impactului privind protecția datelor indică faptul că operațiunile de prelucrare implică un risc ridicat pe care operatorul nu îl poate atenua prin măsuri adecvate din punctul de vedere al tehnologiei disponibile și al costurilor de punere în aplicare, trebuie să aibă loc o consultare a autorității de supraveghere înainte de prelucrare. Acțiunea: 1) să se prevadă obligația operatorului de a efectua o evaluare a impactului operațiunilor de prelucrare avute asupra protecției datelor cu caracter personal atunci când un tip de prelucrare poate conduce la un risc ridicat pentru drepturile și libertățile ale persoanelor fizice; 2) să se asigure că organismul de supraveghere stabilește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței unei evaluări a impactului privind protecția datelor; (Articolul 35 alineatul (4) și articolul 57 alineatul (1k) din GDPR) 3) să furnizeze un conținut al unei evaluări a impactului privind protecția datelor; (4) să se asigure că conformitatea cu codurile de conduită aprobate de operatori sau de persoanele împuternicite este luată în considerare în evaluarea impactului operațiunilor de prelucrare efectuate de acești operatori sau persoane împuternicite, în special în scopul unei evaluări a impactului protecției datelor; (4) să se asigure că operatorul solicită punctul de vedere al persoanelor vizate sau al reprezentanților acestora cu privire la prelucrarea intenționată, fără a aduce prejudiciu protecției intereselor comerciale sau publice sau securității operațiunilor de prelucrare (după caz); 5) acordarea unei scutiri atunci când nu se efectuează o evaluare a impactului; 6) să se prevadă că operatorul efectuează o revizuire pentru a evalua dacă prelucrarea este efectuată în conformitate cu



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
măsurile luate de operator pentru a atenua riscul și tipurile de informații operatorul trebuie să furnizeze autorității de supraveghere; 1) (8) că autoritatea de supraveghere furnizează operatorului și, după caz, persoanei împuternicite, avizul scris, în cazul în care autoritatea de supraveghere consideră că prelucrarea preconizată ar conduce la un risc ridicat ar încălca legea, în special atunci când operatorul a a identificat sau a atenuat insuficient riscul.	evaluarea impactului protecției datelor cel puțin atunci când există o schimbare a riscului reprezentat de operațiunile de prelucrare; (Articolul 35 din GDPR) 7) să se prevadă că operatorul consultă autoritatea de supraveghere înainte de prelucrare în cazul în care o evaluare a impactului privind protecția datelor indică faptul că prelucrarea ar conduce la un risc ridicat în absența măsurilor luate de operator pentru a reduce riscul și tipurile de informații operatorul trebuie să furnizeze autorității de supraveghere; 8) să se prevadă că autoritatea de supraveghere trebuie să furnizeze un aviz scris în favoarea operatorului și, dacă este cazul, operatorului, atunci când autoritatea de supraveghere consideră că prelucrarea intenționată ar conduce la un risc ridicat ar încălca legea, în special atunci când controlorul nu a identificat sau a atenuat insuficient riscul. (Articolul 36 alineatul (2) și articolul 57 alineatul (1) din GDPR (Articolul 36 (1) - 36 (3) din GDPR)
Legea nu prevede că datele cu caracter personal care pot prezenta riscuri specifice pentru drepturile și libertățile persoanelor includ și o monitorizare sistematică a unei zone accesibile publicului la scară largă. (24,2).	Acțiune: să se prevadă că datele cu caracter personal care pot prezenta riscuri specifice pentru drepturile și libertățile persoanelor includ și o monitorizare sistematică a unei zone accesibile publicului la scară largă. (Articolul 35 (3.c) din GDPR)
Legea nu prevede nicio regulă pentru inspectorul pentru protecția datelor. Există o definiție a persoanei responsabile de politica de securitate a datelor cu caracter personal și a unor puncte din Hotărârea de Guvern nr. 1123, însă nu este suficient conform GDPR - Hotărârea Guvernului nr.1123 nu conține o listă detaliată și exhaustivă a sarcinilor persoanei responsabile de politica de securitate a datelor cu caracter personal (inspectorul pentru protecția datelor) și chiar mai mult aceste norme ar trebui să fie prevăzute în lege și nu în hotărârea de guvern. (3., 17-19.)	În cazul în care prelucrarea este efectuată de o autoritate publică, cu excepția instanțelor judecătorești sau a autorităților judiciare independente atunci când acționează în calitate de judecătorească, în cazul în care, în sectorul privat, prelucrarea este efectuată de un operator al cărui activități principale constau în operațiuni de prelucrare care necesită operațiuni regulate și monitorizarea sistematică a persoanelor vizate la scară largă sau în cazul în care activitățile esențiale ale operatorului sau ale prelucrătorului constau în prelucrarea la scară largă a categoriilor speciale de date cu caracter personal și a datelor privind condamnările penale și infracțiunile, legislația și practicile privind protecția datelor ar trebui să îi ajute pe controlori sau pe procesatori să monitorizeze respectarea internă a legii. Nivelul necesar de cunoștințe de specialitate ar trebui determinat în special în funcție de operațiunile de prelucrare a datelor efectuate și de protecția necesară pentru datele personale prelucrate de controlori sau de procesatori. Acești inspectori de protecție a datelor, indiferent dacă sunt sau nu angajați ai operatorului, ar trebui să fie în măsură să-și îndeplinească sarcinile și sarcinile în mod independent. Acțiune: să se prevadă în lege normele și sarcinile specifice pentru inspectorul de protecție a datelor în conformitate cu secțiunea 4 din capitolul IV din GDPR și să se elimine definiția persoanei responsabile pentru politica de securitate a datelor cu caracter personal menționată la punctul 3 din Hotărârea Guvernului nr. 1123 și să se elimine punctele 17-19 din Hotărârea Guvernului nr.1123
Legea nu prevede existența unui cod de conduită aprobat. (-)	Asociațiile sau alte organisme care reprezintă categorii de operatori sau persoane împuternicite ar trebui să fie încurajați să



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
	elaboreze coduri de conduită, în limitele legii, pentru a facilita aplicarea efectivă a legii, ținând seama de caracteristicile specifice prelucrării efectuate în anumite sectoare și nevoile specifice ale microîntreprinderilor și întreprinderilor mici și mijlocii. La elaborarea unui cod de conduită sau la modificarea sau extinderea unui astfel de cod, asociațiile și alte organisme care reprezintă categorii de controlori sau prelucrători ar trebui să consulte părțile interesate relevante, inclusiv persoanele vizate, dacă este posibil, și să țină seama de observațiile primite și de punctele de vedere exprimate ca răspuns la astfel de consultări. Ghidul privind punerea în aplicare a măsurilor adecvate și demonstrarea respectării de către operatorul de date sau de către persoana împuternicită, în special în ceea ce privește identificarea riscului legat de prelucrare, evaluarea acestora în ceea ce privește originea, natura, probabilitatea și gravitatea și identificarea celei mai bune practici de atenuare a riscului ar putea fi furnizate în special prin intermediul unor coduri de conduită aprobate. Acțiune: este necesar să se evalueze necesitatea de a prevedea existența unui cod de conduită aprobat. Și dacă va exista o astfel de reglementare care să prevadă că codul de conduită poate fi folosit ca element prin care să se demonstreze măsuri tehnice și organizatorice adecvate pentru a asigura un nivel adecvat de securitate. <i>Este o libertate de a alege dacă codul de conduită să fie aprobat folosit ca element prin care să se demonstreze măsurile tehnice și organizatorice adecvate pentru a asigura un nivel adecvat de securitate. (nu este obligatorie)</i> (Articolul 40-41 din GDPR)
Legea nu prevede reguli de certificare. <i>Este un drept de a alege dacă statul și autoritatea de supraveghere ar trebui să încurajeze instituirea mecanismelor de certificare a protecției datelor și a sigiliilor și mărcilor de protecție a datelor, în scopul de a demonstra că operațiunilor de prelucrare de către operatori și persoanele împuternicite sunt în conformitate cu legea.</i>	Pentru a spori transparența și conformitatea cu legea, ar trebui stabilite mecanisme de certificare și sigilii și mărci de protecție a datelor, care să permită persoanelor vizate să evalueze rapid nivelul protecției datelor cu privire la produsele și serviciile relevante. Acțiune: este necesar să se evalueze necesitatea de a prevedea că ar trebui să existe mecanisme de certificare a protecției datelor și sigilii și mărci de protecție a datelor, în scopul de a demonstra conformitatea cu legea a operațiunilor de prelucrare de către operatori și persoanele împuternicite de către operatori. <i>Este un drept de a alege dacă statul și autoritatea de supraveghere ar trebui să încurajeze instituirea mecanismelor de certificare a protecției datelor și a sigiliilor și mărcilor de protecție a datelor, în scopul de a demonstra că operațiunilor de prelucrare de către operatori și persoanele împuternicite sunt în conformitate cu legea. (nu este obligatorie)</i> (Articolele 42-43, articolul 57 (1.n) - 1.q; Articolul 58 (1.c) și articolul 58 (2.h) din GDPR)



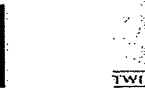
EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
Legea nu prevede că obligația de păstrare a secretului profesional al conducerii Centrului și al angajaților se va aplica, în special, la raportarea de către persoane fizice a încălcărilor legii. (29.3).	Acțiune: să se prevadă că obligația de păstrare a secretului profesional al conducerii Centrului și al angajaților se aplică, în special, raportării de către persoane fizice a încălcărilor legii. (Articolul 54 alineatul (2) din GDPR)
Legea nu prevede că Centrul va efectua o revizuire periodică a deciziei de autorizare, care va lua în considerare toate evoluțiile relevante din țara terță sau organizația internațională a căreia i-au fost transferate date cu caracter personal. (32.3).	Acțiune: evaluarea necesității de a prevedea că Centrul va efectua o revizuire periodică a deciziei de autorizare, care va lua în considerare toate evoluțiile relevante din țara terță sau organizația internațională a căreia i-au fost transferate date cu caracter personal. (Articolul 45 alineatul 3 din GDPR)
Legea nu prevede în mod expres că una dintre condițiile pe care Centrul le ia în considerare este dreptul efectiv și aplicabil al persoanelor vizate și căile de atac eficiente din punct de vedere administrativ și judiciar al persoanelor vizate ale căror date cu caracter personal sunt transferate; precum și existența și funcționarea eficientă a uneia sau mai multor autorități independente de supraveghere din țara terță sau la care o organizație internațională este subiect, precum și angajamentele internaționale pe care le-a încheiat țara terță sau organizația internațională în cauză sau alte obligații sau instrumente care rezultă din convențiile obligatorii din punct de vedere juridic. (32.4).	Țara terță ar trebui să asigure o supraveghere independentă eficientă a protecției datelor și ar trebui să prevadă mecanisme de cooperare cu autoritățile de protecție a datelor ale statelor, iar persoanele vizate ar trebui să beneficieze de drepturi efective și executorii și de acțiuni administrative și judiciare eficiente. Acțiune: să se prevadă că și condițiile pe care Centrul le ia în considerare sunt: 1) drepturile efective și aplicabile ale persoanelor vizate și căile de atac administrative și judiciare efective pentru persoanele vizate ale căror date cu caracter personal sunt transferate; 2) existența și funcționarea eficientă a uneia sau mai multor autorități independente de supraveghere din țara terță sau a căror organizație internațională este supusă, cu responsabilitatea de a asigura și de a asigura respectarea normelor de protecție a datelor, inclusiv competențe adecvate de aplicare, pentru asistarea și consilierea persoanelor vizate în exercitarea drepturilor lor și pentru cooperarea cu autoritățile de supraveghere ale statelor; și (3) angajamentele internaționale pe care le-a încheiat țara terță sau organizația internațională în cauză sau alte obligații care rezultă din convenții sau instrumente juridice obligatorii, precum și din participarea sa la sisteme multilaterale sau regionale, în special în ceea ce privește protecția datelor cu caracter personal. (Articolul 45 alineatul 2 din GDPR)
Legea nu prevede ca Centrul să inițieze consultări cu țara terță sau organizația internațională care nu asigură un nivel adecvat de protecție. (32.5).	Acțiune: este necesar să se evalueze necesitatea de a se asigura că Centrul inițiază consultări cu țara terță sau organizația internațională care nu asigură un nivel adecvat de protecție. (Articolul 45 alineatul 6 din GDPR)
Legea nu indică cu ce ar putea fi furnizate garanțiile corespunzătoare. (32.6).	Acțiune: a indica faptul că garanțiile adecvate pot fi furnizate prin orice instrument menționat la articolul 46 alineatele (2) și (3) din GDPR. (Articolul 46 alineatul 2, articolul 46 alineatul 3 din GDPR)
Legea nu prevede că, înainte de consimțământul subiectului datelor personale, acesta trebuie să fie informat despre riscurile posibile ale unor astfel de transferuri pentru persoana vizată, din cauza lipsei unei decizii de adevărate și a garanțiilor. (32.9.a)	Acțiune: să se prevadă că, înainte de consimțământul persoanei vizate, aceasta trebuie să fie informată cu privire la riscurile posibile ale unor astfel de transferuri pentru persoana vizată, din cauza lipsei unei decizii de adevărate și a garanțiilor. (Articolul 49 alineatul 1.a din GDPR)



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
Legea nu prevede o listă de excepții în cazul în care transferul către o țară terță sau o organizație internațională poate avea loc în conformitate cu articolul 49 alineatul (1) punctele 2-4 din GDPR. (-)	Acțiune: a evalua necesitatea furnizării unei liste de excepții în cazul în care transferul către o țară terță sau la o organizație internațională poate avea loc în conformitate cu articolul 49 alineatul (1) punctele 2-4 din GDPR și să se prevadă că operatorul sau persoana împuternicită trebuie să documenteze evaluarea și garanțiile corespunzătoare ale acestor excepții. (-) (Articolul 49 alineatul (6) din GDPR)
Legea nu prevede că, dacă transferul se face dintr-un registru, transferul nu implică toate datele personale sau întreaga categorie de date cu caracter personal conținute în registru. (32.9.d)	Acțiune: să se prevadă că, dacă transferul este efectuat dintr-un registru, transferul nu implică toate datele personale sau întreaga categorie de date cu caracter personal conținute în registru. (Articolul 49 alineatul (2) din GDPR)
Legea nu prevede că art. 32 alin. (9) lit. a) și b) nu se aplică activităților desfășurate de autoritățile publice în exercitarea atribuțiilor lor publice. (-)	Acțiune: să se prevadă că articolul 32 alineatul (9) literele (a) și (b) nu se aplică activităților desfășurate de autoritățile publice în exercitarea competențelor lor publice. (Articolul 49 alineatul (3) din GDPR)
Legea nu prevede că interesul public menționat la art. 32 alin. (9) lit. e) este recunoscut în legea Republicii Moldova. (32.9.e)	Acțiune: este necesar să se evalueze necesitatea de a prevedea că interesul public menționat la articolul 32 alineatul (9) litera (e) este recunoscut în legislația Republicii Moldova. (Articolul 49 alineatul (4) din GDPR)
Articolul 21 alineatul (3) din lege și anexa I alineatul II punctul 4 din Legea nr.182 duplicate.	Acțiune: Este necesar să se evalueze necesitatea dublării acestor reguli în ambele legi.
Legea nu prevede că membrii autorității de supraveghere (directorul și directorul adjunct), în exercitarea atribuțiilor lor în conformitate cu legea, rămân în afara influenței externe, directe sau indirecte, și nici nu vor căuta și primi instrucțiuni de la nimeni. <i>În general, aceasta derivă din articolul 19 alineatul (1), din articolul 22 alineatul (1) și din articolul 22 alineatul (3) din lege.</i>	Acțiune: să se prevadă în mod direct că membrii autorității de supraveghere (directorul și directorul adjunct), în să-și îndeplinească sarcinile și să-și exercite atribuțiile în conformitate cu legea, rămân în afara influenței externe, directe sau indirecte și nici nu vor căuta și primi instrucțiuni de la nimeni. (Articolul 52 alineatul (2) din GDPR)
Legea nu prevede că autoritatea de supraveghere - Centrul nu trebuie să fie competent să supravegheze operațiunile de procesare a instanțelor care acționează în calitatea de judecător. (-)	Acțiune: să se prevadă că autoritatea de supraveghere - Centrul nu trebuie să fie competent să supravegheze operațiunile de procesare a instanțelor care acționează în calitatea lor judiciară. (Articolul 55 alineatul (3) din GDPR)
Legea nu prevede că una dintre îndatoririle Centrului este de a promova conștientizarea și înțelegerea publică a riscurilor, regulilor, garanțiilor și drepturilor legate de prelucrare. Activitățile adresate în mod specific copiilor ar trebui să primească o atenție deosebită. (20,1).	Acțiune: să se prevadă că una dintre atribuțiile Observatorului este de a promova conștientizarea și înțelegerea publică a riscurilor, a regulilor, a garanțiilor și a drepturilor legate de prelucrare. Activitățile adresate în mod specific copiilor vor primi o atenție deosebită. (Articolul 57 (1.b) din GDPR)
Legea nu prevede că una dintre atribuțiile Centrului este de a consilia parlamentul național, guvernul și alte instituții și organe cu privire la măsurile administrative privind protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor. (20.1.j))	Acțiune: să se prevadă că una dintre atribuțiile Centrului este de a consilia parlamentul național, guvernul și alte instituții și organe nu numai în ceea ce privește măsurile legislative, ci și cele administrative privind protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor. (Articolul 57 (1.c) din GDPR)
Legea nu prevede obligația Centrului de a adopta clauze contractuale standard pentru contractele dintre operator și persoana împuternicită de operator. (-)	Acțiune: să se acorde Comisiei sarcina de a adopta clauze contractuale standard pentru contractele încheiate între operator și persoana împuternicită de operator. (Articolul 57 (1j) din GDPR)
Deoarece Legea nu prevede că ar trebui să existe un cod de conduită aprobat și nu prevede norme de certificare, nu	Acțiune: dacă în Lege vor fi prevăzute norme privind codul de conduită și certificare, este necesar să se îndeplinească



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
există sarcini pentru centru în acest domeniu. (-)	atribuțiile Centrului în acest domeniu. (Articolul 57 (1.m) - 57 (1.r) din GDPR) <i>N.B. Codul de conduită și certificarea sunt de alegere.</i>
Legea nu prevede ca Centrul să țină evidența internă a încălcărilor prezentului regulament și a măsurilor luate în conformitate cu articolul 26 din lege. (-)	Acțiune: să se acorde Comisiei sarcina de a ține evidența internă a încălcărilor prezentului regulament și a măsurilor luate în conformitate cu articolul 26 din lege. (Articolul 57 (1.u) din GDPR)
Legea nu prevede că autoritatea de supraveghere facilitează depunerea plângerilor depuse de persoana vizată sau de un organism, organizație sau asociație care reprezintă interesele persoanei vizate prin măsuri precum un formular de depunere a reclamațiilor care poate fi completat și electronic, fără a exclude alte mijloace de comunicare.	Acțiune: să se prevadă că autoritatea de supraveghere facilitează depunerea plângerilor depuse de persoana vizată sau de un organism, o organizație sau o asociație care reprezintă interesele persoanei vizate prin măsuri precum un formular de depunere a plângerilor care poate fi completat și electronic, fără a exclude alte mijloace de comunicare. (Articolul 57 alineatul (2) din GDPR)
Legea nu prevede autoritatea Centrului de a emite avertismente unui operator sau unei persoane împuternicite de către operator care presupune că operațiunile de prelucrare intenționate ar putea încălca prevederile legii sau să emită reproșuri unui operator sau unei persoane împuternicite de către operator în cazul în care operațiunile de prelucrare au încălcat prevederile Legii. (-)	În cazul unei încălcări minore sau în cazul în care amenda care ar putea fi impusă ar constitui o sarcină disproporționată pentru o persoană fizică, se poate emite o mustrare în locul unei amenzi. Cu toate acestea, ar trebui acordată o atenție deosebită naturii, gravității și duratei încălcării, caracterului intenționat al încălcării, acțiunilor întreprinse pentru diminuarea prejudiciului suferit, gradului de răspundere sau oricărei încălcări anterioare relevante, modului în care încălcarea a devenit cunoscută autorității de supraveghere, respectarea măsurilor dispuse împotriva operatorului sau persoanei împuternicite de către operator, respectarea unui cod de conduită și orice alt factor agravant sau atenuant. Singura opțiune în ceea ce privește legea (articolul 26 alineatul (4)) este aceea că, în urma controlului efectuat, se atestă încălcări constatate, <u>Centrul emite o decizie privind suspendarea operațiunilor de prelucrare a datelor cu caracter personal</u> , care conține instrucțiuni pentru aducerea datelor cu caracter personal prelucrate în conformitate cu prevederile prezentei legi. În unele cazuri, această opțiune este prea disproporționată și nu este eficientă. Acțiune: acordarea competențelor Centrului de a emite: 1) avertismentele adresate unui operator sau unei persoane împuternicite de către operator precum că operațiunile de prelucrare intenționate ar putea încălca prevederile Legii; (Articolul 58 (2a) din GDPR) 2) reproșează unui operator sau unei persoane împuternicite de către operator dacă operațiunile de prelucrare au încălcat prevederile Legii. (Articolul 58 (2b) din GDPR)
Legea nu prevede împuternicirea Centrului de a obliga operatorul sau persoana împuternicită de către operator să se conformeze cererilor persoanei vizate de a-și exercita drepturile în temeiul legii. (-)	Acțiune: să împuternicească Centrul cu sarcina de a ordona operatorului sau persoanei împuternicite de către operator să respecte cererile persoanei vizate de a-și exercita drepturile în conformitate cu legea. (Articolul 58 (2.c) din GDPR)
Legea nu prevede împuternicirea Centrului de a ordona operatorului să comunice o încălcare a datelor cu caracter personal persoanei vizate. (-)	Acțiune: să împuternicească Centrul să ordone operatorului să comunice persoanei vizate o încălcare a datelor cu caracter personal. (Articolul 58 (2.e) din GDPR)
Legea nu prevede împuternicirea Centrului de a ordona rectificarea datelor cu caracter personal care nu au fost	Acțiune: să împuternicească Centrul pentru a ordona: 1) rectificarea datelor cu caracter personal care nu au fost



EU Twinning Project
Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova
MD 13ENPI JH0317 (MD/29)

Situația curentă ("ce este")	Viitorul în conformitate cu GDPR ("ce ar trebui să fie")
prelucrate în conformitate cu legea și notificarea acestor acțiuni către destinatarii cărora i-au fost dezvăluite datele cu caracter personal. (26.4.-26.6.)	prelucrate în conformitate cu legea; 2) notificarea acestor acțiuni destinatarilor cărora le-au fost comunicate datele cu caracter personal. (Articolul 58 (2.g) din GDPR)
Legea nu prevede reguli pentru următorul tip de reprezentare a persoanelor vizate. (-)	În cazul în care un subiect de date consideră că drepturile sale în temeiul Legii sunt încălcate, acesta ar trebui să aibă dreptul de a mandata un organism, organizație sau asociație non-profit care este constituită în conformitate cu legea Republicii Moldova, are obiective atutare care sunt de interes public și activează în domeniul protecției datelor cu caracter personal de a depune o plângere în numele său în fața unei autorități de supraveghere, să își exercite dreptul la o cale de atac în numele persoanelor vizate sau, dacă prevăzute într-o lege a Republicii Moldova, își exercită dreptul de a primi despăgubiri în numele persoanelor vizate. Acțiune: să se prevadă norme de reprezentare a persoanelor vizate așa cum se prevede la articolul 80 din GDPR. (Articolul 80 din GDPR)
Legea nu prevede direct că operatorul sau persoana împuternicită de operator este scutit de răspundere în conformitate cu articolul 33 dacă dovedește că nu este în niciun fel responsabil pentru cauza care a cauzat prejudiciul. (33.)	Acțiune: să se evalueze necesitatea de a asigura în mod direct că operatorul sau persoana împuternicită este scutit de răspundere în temeiul articolului 33 dacă dovedește că nu este în niciun fel responsabil pentru cauza care a cauzat prejudiciul. (Articolul 82 alineatul (3) din GDPR) <i>Dar rezultă din contextul articolului 33 că operatorul sau prelucrătorul este răspunzător numai pentru încălcarea legii (deci, dacă nu încalcă legea, ei sunt scutiți de răspundere.)</i>
Codul infracțiunilor administrative (articolele 74 ¹ , 74 ² și 74 ³) nu prevede amenzi administrative care sunt eficiente, proporționale și disuasive. De asemenea, nu prevede amenzi administrative foarte detaliate, așa cum este prevăzut la articolul 83 alineatul (2) din GDPR.	Fiecare autoritate de supraveghere ar trebui să fie împuternicită de a impune amenzi administrative pentru încălcarea legii. Codul infracțiunilor administrative ar trebui să indice încălcările și limita superioară admisibilă și criteriile de stabilire a amenzilor administrative aferente, care ar trebui stabilite de autoritatea competentă de supraveghere în fiecare caz în parte, ținând seama de toate circumstanțele relevante ale situației specifice, în special în ceea ce privește natura, gravitatea și durata încălcării, precum și consecințele acesteia și măsurile luate pentru a asigura respectarea obligațiilor prevăzute de lege și pentru a preveni sau atenua consecințele încălcării. Acțiune: în Codul infracțiunilor administrative trebuie de prevăzut: 1) amenzi administrative care sunt eficiente, proporționale și disuasive; 2) amenzi administrative detaliate, astfel cum sunt prevăzute la articolul 83 alineatul (2) din GDPR și 3) este necesar să se prevadă că Centrul are puterea de a impune amenzi administrative pentru încălcarea Legii în mod direct violatorilor Legii.
Codul penal al Republicii Moldova nu prevede penalități pentru încălcarea legii. Dar, prin folosirea interpretării, aceste sancțiuni pot deriva din articolele 177 și 178 din Codul penal al Republicii Moldova.	Acțiune: în Codul penal al Republicii Moldova trebuie să se prevadă sancțiuni specifice pentru încălcarea legii. (Articolul 84 alineatul (1) din GDPR)



Proiect Twinning UE
Consolidarea Capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal
MD-13ENPI JH0317 (MD/29)

Studiul de impact al GDPR asupra companiilor private din Moldova

INTRODUCERE

Prelucrarea datelor cu caracter personal ajută la atingerea obiectivelor fiecărei organizații și este strâns legată de principalele sale activități. Cu toate acestea, prelucrarea datelor cu caracter personal este obiectul reglementărilor naționale sau internaționale specifice. Cerințele de prelucrare a datelor cu caracter personal în Uniunea Europeană (UE) sunt stabilite în prezent prin Regulamentul general al UE privind protecția datelor (GDPR). GDPR va fi aplicat începând cu data de 25 mai 2018.

Multe companii din Moldova servesc companiilor din UE oferind astfel bunuri și servicii. De exemplu, în anul 2017, exportul total al mărfurilor către UE din Moldova a fost de 1596,6 milioane dolari, reprezentând 65,8% din totalul exporturilor de bunuri în anul respectiv. O mare parte din cetățenii Republicii Moldova au relații de lucru și relații de afaceri cu alte țări ale UE¹. În afară de aceasta, statul a decis să dezvolte integrarea țării în UE și să pună în aplicare normele UE în diferite sectoare, inclusiv cel ce ține de protecția datelor. În acest context, vor exista tot mai multe situații în care companiile din Moldova sunt supuse aplicabilității directe sau aplicabilității indirecte a GDPR-ului atunci când o companie servește ca persoană împuternicită de operator a companiei în UE.

Scopul acestui studiu este, în primul rând, creșterea gradului de sensibilizare privind cazurile de aplicabilitate directă a GDPR-ului pentru companiile din Moldova și oferirea de recomandări pentru implementarea principiilor GDPR și explicații ale principalelor cerințe GDPR.

Acest studiu de impact a fost pregătit pentru a lua în considerare rezultatele ședințelor organizate de Centrul Național pentru Protecția Datelor cu Caracter Personal (Centrul) cu asociații și companii din sectorul privat cât și revizuirea răspunsurilor lor asupra practicilor existente de prelucrare a datelor.

Acest document cuprinde trei părți principale: a) explicarea principalelor condiții ale GDPR b) indicarea tuturor situațiilor tipice în care GDPR se aplică direct și indirect companiei care operează

în Moldova cu câteva exemple b) recomandări privind protecția datelor privind etapele de implementare a GDPR și înțelegerea principală a cerințelor de bază.

1. NOȚIUNI ȘI DEFINIȚII

Acest capitol reflectă numai cele mai importante definiții care sunt incluse în GDPR. Alte noțiuni importante pot fi regăsite în articolul 4 din GDPR.

1.1. CE SUNT DATELE CU CARACTER PERSONAL?

Datele cu caracter personal reprezintă orice informație care se referă la o **persoană fizică vie identificată sau identificabilă**. Diferite informații, care sunt colectate împreună și pot conduce la identificarea unei anumite persoane, de asemenea constituie date cu caracter personal. De exemplu, datele de identificare a persoanei legate de orice alte informații sunt date cu caracter personal. Chiar și adresa de protocol internet (adresa IP) reprezintă date personale în anumite circumstanțe dacă o companie colectează adrese IP împreună cu alte informații.

Datele personale care au fost dezidentificate, criptate sau **pseudonimizate**, dar care pot fi utilizate pentru a re-identifica o persoană rămân date cu caracter personal și intră în domeniul de aplicare al legii.

Datele cu caracter personal care au fost **anonimizate** în așa fel încât persoana nu este sau nu mai poate fi identificată nu mai sunt considerate date cu caracter personal. Pentru ca datele să fie cu adevărat anonimizate, anonimizarea trebuie să fie ireversibilă.

GDPR protejează datele personale **indiferent de tehnologia utilizată pentru prelucrarea acestor date** - este neutru din punct de vedere tehnologic și se aplică prelucrării atât automatizate cât și manuale, cu condiția ca datele să fie organizate în conformitate cu criterii predefinite (de exemplu, în ordine alfabetică). De asemenea, nu contează cum sunt stocate datele - într-un sistem IT, prin supraveghere video sau pe hârtie; în toate cazurile, datele cu caracter personal sunt supuse cerințelor de protecție stabilite în GDPR. De asemenea, locul de stocare a datelor cu caracter personal nu este important dacă criteriile de aplicabilitate indică faptul că se aplică GDPR.

1.2. CE ESTE PRELUCRAREA?

Prelucrarea acoperă o gamă largă de operațiuni efectuate asupra datelor cu caracter personal, inclusiv prin mijloace manuale sau automatizate. Aceasta include **colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alăturarea sau combinarea, restricționarea, ștergerea sau distrugerea** datelor cu caracter personal.

GDPR se aplică prelucrării datelor cu caracter personal integral sau parțial prin mijloace automatizate, precum și prelucrării neautomatizate, dacă face parte dintr-un sistem structurat de evidență a datelor.

¹ - <http://www.statistica.md/newsview.php?l=ro&id=5908&idc=168>

1.3. OPERATOR ȘI PERSOANA ÎMPUTERNICITĂ DE OPERATOR

Operator - înseamnă persoana fizică sau juridică, autoritatea publică, agenția sau un alt organism care, singur sau împreună cu alții, determină scopurile și mijloacele de prelucrare a datelor cu caracter personal.

Operator comun - în care doi sau mai mulți operatori împreună determină obiectivele și mijloacele de prelucrare. Acestea, în mod transparent stabilesc responsabilitățile respective pentru respectarea obligațiilor care decurg din prezentul regulament, în special în ceea ce privește exercitarea drepturilor subiectului datelor și atribuțiilor respective de a furniza informații la art. 13 și 14, prin intermediul unui acord între ele. Acordul poate desemna un punct de contact pentru subiecții datelor.

Persoana împuternicită de operator înseamnă o persoană fizică sau juridică, o autoritate publică, o agenție sau un alt organism care prelucrează date cu caracter personal în numele operatorului (de exemplu, operatorul UE).

2. APLICABILITATEA GDPR

Dacă nu există nici o îndoială cu privire la aplicabilitatea GDPR în cazul în care o companie este stabilită în UE, ar putea exista unele probleme când și cum se aplică GDPR, dacă compania este stabilită în Moldova. GDPR poate fi direct aplicabil oricărei companii stabilite în Republica Moldova dacă au loc anumite criterii ale activităților sale de prelucrare a datelor cu caracter personal. În plus, chiar dacă GDPR se aplică direct unei companii din Moldova din cauza activităților pe care le desfășoară pe piața UE, se poate aplica și legislația națională privind protecția datelor în Moldova. Astfel, compania va trebui să implementeze și cerințele naționale, dacă acestea diferă de regimul GDPR.

Astfel, succesiunea generală a criteriilor privind aplicabilitatea GDPR va fi următoarea: a) activitate economică b) care implică prelucrarea datelor cu caracter personal c) și care are loc în UE prin înființarea companiei moldovenești în UE sau d) de către o companie care este stabilită în Moldova, dacă prelucrarea este direcționată către subiecții datelor în UE. Exemplele următoare descriu toate situațiile posibile privind aplicabilitatea GDPR.

Situația nr. 1 – aplicabilitate directă

Companie din RM - care nu este stabilită în UE

Conform art. 3 alin. (2) lit. a) din GDPR, se aplică direct oricărei companii sau altei persoane juridice din Moldova în care activitățile de prelucrare a datelor cu caracter personal ale companiei (sau entității) relevante din Republica Moldova se referă la:

oferirea de bunuri sau servicii, indiferent dacă este necesară o plată către subiectul datelor, către astfel de subiecți de date din Uniune.

"Oferirea de bunuri sau servicii" este mai mult decât simpla accesare a unui site web sau a unei adrese de e-mail, dar poate fi evidențiată prin folosirea limbii sau monedei utilizate în mod obișnuit în unul sau mai multe state membre, cu posibilitatea de a comanda bunuri/servicii acolo. De exemplu, serviciile bazate pe

web care au vizat subiecții datelor ale unui sau mai multor state membre ale UE, vânzarea de bunuri sau servicii pe piața UE sau oferirea de servicii publice de tip cloud, astfel colectând date cu caracter personal; rețele de socializare sau aplicațiile care prelucrează date cu caracter personal din UE.

Situația nr. 2 – aplicabilitate directă

Companie din RM - care nu este stabilită în UE

Conform articolului 3 (2) litera (b) din GDPR, se aplică direct oricărei companii sau altei persoane juridice din Moldova în care activitățile de prelucrare a datelor cu caracter personal ale companiei (sau entității) relevante din Republica Moldova se referă la:

Activitățile de prelucrare a datelor cu caracter personal sunt legate de monitorizarea comportamentului subiecților de date, în măsura în care comportamentul acestora are loc în cadrul UE.

De exemplu, profilarea utilizatorilor de internet în UE pe baza activităților legate de utilizatori etc.

În situația nr. 1 și situația nr.2. - GDPR cere ca operatorul sau persoana împuternicită de operator (din Moldova) să desemneze un reprezentant prin informarea autorității de supraveghere relevante din statul membru UE (cu excepția cazului în care prelucrarea este ocazională, nu include prelucrarea la scară largă a categoriilor speciale de date cu caracter personal sau prelucrarea datelor cu caracter personal referitoare la condamnările penale și infracțiuni și este puțin probabil să ducă la un risc pentru drepturile și libertățile persoanelor fizice, ținând seama de natura, contextul, domeniul de aplicare și scopurile prelucrării sau dacă operatorul este o autoritate sau organism public).

Situația nr.3- aplicabilitate directă

Compania din Moldova are o unitate locală în UE și/sau este legată de aceasta

În cazul în care compania înregistrată a Republicii Moldova în statul membru al Uniunii Europene are o companie filială, o reprezentanță sau orice alt sediu care prelucrează datele cu caracter personal în cadrul activității sale economice în UE, acest sediu în UE va fi tratat ca o unitate în UE și atunci GDPR se aplică cel puțin acestui sediu în UE (dacă nu la toate celelalte sedii sau companii din Moldova ca un grup de operatori în UE).

Pentru o decizie clară privind aplicabilitatea GDPR la alte sedii din Moldova, ar trebui să evaluați dacă sediile dvs. din UE prelucrează date cu caracter personal numai în ceea ce privește piața UE, datele personale nu sunt transferate în nici un fel în Moldova sau nu sunt folosite în careva scop în Moldova. În caz contrar, se pot impune sancțiuni companiei în UE și cuantumul sancțiunilor va fi calculat în baza cifrei de afaceri a grupului din întreaga lume.

Situația nr.4 – aplicabilitate indirectă

Compania din Moldova operează ca persoană împuternicită de operator pentru o altă companie din UE

Datele personale sunt transferate companiei moldovenești de la o entitate din UE (poate fi propria companie filială sau orice alt partener din UE) (de exemplu, cu scopul de a face procese de valoare adăugată a datelor personale transferate ca un serviciu, pur și simplu stocarea acestor date pentru o altă companie sau livrarea altor servicii de prelucrare a datelor cu caracter personal către companiile din UE în calitate de persoană împuternicită de operator.

În această situație, datele personale sunt prelucrate de entitatea din Moldova ca persoană împuternicită de operator conform GDPR-ului și unele dintre cerințele acestuia se aplică prin articolul 28 din GDPR și criteriile privind caracterul adecvat de protecție a datelor în cazul transferului de date cu caracter personal către țări terțe.

Situația nr. 5 – GDPR nu se aplică

Compania este stabilită în Moldova și prelucrarea se referă numai la activitatea economică realizată în Moldova

Dacă compania din Moldova nu prelucrează și nu planifică să prelucreze date personale în modul reflectat la Situațiile 1-4, în acest caz GDPR nu se aplică.

3. ASPECTE PRINCIPALE PENTRU A SE CONFORMA LA GDPR

Fiecare companie ar trebui să organizeze autoevaluarea pentru a identifica decalajul dintre practica curentă și prelucrarea datelor cu caracter personal în cadrul companiei private din Moldova și cerințele GDPR.

Este important ca operatorii și persoanele împuternicite de operatori să efectueze o revizuire aprofundată a ciclului existent de politici a datelor, astfel încât să identifice în mod clar datele pe care le dețin, pentru ce scop și în ce temei juridic. Ei trebuie, de asemenea, să evalueze contractele existente, în special cele dintre operatori și persoanele împuternicite de operatori, căile de transfer internațional și guvernanta globală (ce măsuri IT și organizaționale trebuie să aibă în vigoare). Un element esențial al acestui proces este asigurarea faptului că cel mai înalt nivel de conducere este implicat în astfel de revizuirii, oferă contribuția sa și este actualizat periodic și consultat cu privire la modificările aduse politicii de date a companiei.

În acest scop, unii operatori recurg la liste de verificare a conformității (interne sau externe), solicită consultanță din partea firmelor de consultanță și a firmelor de avocatură și caută produse care pot îndeplini cerințele privind protecția datelor, începând cu momentul conceperii și cel al protecției implicite a datelor. De asemenea, se recomandă, în practică, să se țină seama de avizele din cadrul grupului de lucru privind protecția datelor aferente Directivei 95/46/CE cu privire la diferitele aspecte ale interpretării GDPR care vor contribui la realizarea nivelului de implementare necesar.

Capitolele următoare ale acestui studiu de impact se vor referi la recomandări care identifică în scurt timp scopul și obiectul cerinței relevante a GDPR.

3.1. Scopul și temeiurile juridice de prelucrare

În primul rând, compania trebuie să definească scopul operațiunii de prelucrare a datelor cu caracter personal. Definirea scopului va ajuta să înțelegeți dacă prelucrarea datelor nu este excesivă în ceea ce privește tipurile de date necesare, cantitatea și perioadele de stocare.

În cazul în care compania dvs. colectează și utilizează date personale, compania trebuie să evalueze dacă există temei juridic pentru fiecare astfel de operațiune de prelucrare. Compania trebuie să identifice temeiul juridic relevant pentru prelucrare și să asigure cerințele necesare. De exemplu, în cazurile de interese legitime, compania trebuie să definească un interes legitim, să evalueze necesitatea și proporționalitatea prelucrării.

Șase temeiuri legale pentru datele cu caracter personal sunt definite în articolul 6 din GDPR, și anume: (a) acordul subiectului datelor; (b) executarea unui contract cu subiectul datelor; (c) respectarea unei obligații legale impuse operatorului; interesele vitale ale subiectului datelor; (e) îndeplinirea unei sarcini realizate în interesul public sau (f) interesele legitime urmărite de operator, sub rezerva unui test suplimentar de echilibrare față de drepturile și interesele subiectului datelor. Cerințele specifice privind prelucrarea categoriilor speciale de date cu caracter personal sunt prevăzute la articolul 9 din GDPR, în măsura în care prelucrarea generală a categoriilor speciale sau a datelor cu caracter personal este interzisă.

Definirea temeiurilor juridice este importantă și în contextul drepturilor subiecților de date. De exemplu, satisfacerea anumitor drepturi ale subiecților de date este mai importantă atunci când datele cu caracter personal sunt prelucrate pe baza consimțământului (dreptul de a fi uitat) și altor, atunci când datele cu caracter personal sunt prelucrate în baza unor interese legitime (dreptul de opoziție). Cunoștințele privind temeiurile juridice oferă operatorului posibilitatea de a furniza subiectului datelor informații exacte în conformitate cu articolele 13 și 15 din GDPR.

Dacă compania realizează decizii bazate exclusiv pe prelucrarea automatizată (inclusiv crearea de profiluri) care produce efecte juridice care o privesc sau o afectează în mod similar, sunt posibile doar trei temeiuri juridice: a) consimțământul explicit al subiectului datelor b) sau

executarea unui contract între subiectul datelor și un operator de date și c) este prevăzut de legislație.

Pentru a înțelege scopurile și temeiurile juridice pentru prelucrarea datelor personale, compania trebuie să auditeze practicile existente, să stabilească categorii de date cu caracter personal sau chiar tipuri de date personale.

3.2. Protecția datelor începând cu momentul proiectării

și protecția implicită a datelor

La articolul 25 din GDPR se definește principiul *vieții private, din momentul conceperii și în mod implicit: luând în considerare tehnologiile moderne, costul implementării și natura, scopul, contextul și scopurile prelucrării, precum și riscurile variabilei probabilității și gravității drepturilor și libertățile persoanelor fizice create de prelucrare, operatorul, atât în momentul determinării mijloacelor de prelucrare, cât și în momentul prelucrării propriu-zise, pune în aplicare măsuri tehnice și organizatorice adecvate, cum ar fi pseudonimizarea, care sunt destinate să pună în aplicare principiile de protecție a datelor, cum ar fi minimizarea datelor, într-o manieră eficientă și integrarea garanțiilor necesare în prelucrare pentru a îndeplini cerințele prezentului regulament și pentru a proteja drepturile subiecților de date.*

Protecția datelor începând cu momentul conceperii este considerată ca fiind un concept cu mai multe fațete, care implică diferite componente tehnologice și organizaționale, care implementează principiile de confidențialitate și protecția datelor în sisteme și servicii.

GDPR abordează protecția datelor începând cu momentul proiectării ca o obligație legală pentru operatori și persoanele împuternicite de operatori, făcând o referire explicită la minimizarea datelor și posibila utilizare a pseudonimizării. În plus, aceasta introduce obligația de protecție a datelor în mod implicit, mergând în continuare în stabilirea protecției datelor cu caracter personal ca proprietate implicită a sistemelor și serviciilor.

Se recomandă ca compania nu numai să evalueze și să implementeze confidențialitatea începând cu momentul proiectării și în mod implicit în noile proiecte de prelucrare a datelor, dar și în sistemele și serviciile de informații existente.

3.3 Securitatea informațională

Organizarea sistemelor informatice ale companiei și gestionarea riscurilor este o problemă foarte importantă în ceea ce privește implementarea GDPR și protecția datelor cu caracter personal. GDPR nu aprobă standarde sau cerințe de securitate, ci conține principiile de organizare a securității informațiilor.

Articolul 32 din GDPR prevede: *ținând seama de tehnologiile moderne, costurile implementării și natura, scopul, contextul și scopurile prelucrării, precum și riscul variabilității și gravității diferitelor drepturi și libertăți ale persoanelor fizice, operatorul și persoana împuternicită de*

operator să pună în aplicare măsuri tehnice și organizatorice adecvate pentru a asigura un nivel de securitate adecvat riscului.

Operatorul sau persoana împuternicită de operator trebuie să asigure confidențialitatea, integritatea, disponibilitatea și reziliența în continuare a sistemelor și serviciilor de prelucrare. Pentru a realiza acest lucru, este necesar să se evalueze organizarea hardware-ului și software-ului sistemului de informații și riscurile care pot apărea. În cazul unei încălcări a datelor cu caracter personal, operatorul trebuie să notifice instituția de supraveghere. Dacă GDPR este direct aplicabil, operatorul din Moldova trebuie să notifice încălcarea la aceeași instituție de supraveghere în care a fost desemnat reprezentantul. Dacă compania dvs. acționează în calitate de persoană împuternicită de operator, încălcarea trebuie notificată direct operatorului.

Întrebări care vă pot ajuta să înțelegeți dacă în cadrul companiei este adresat principiul confidențialității din momentul proiectării și în mod implicit și aspectul securității sistemului informațional

1. Compania dvs. a aplicat principiile de protecție a datelor când au fost introduse sistemele de prelucrare a datelor?

2. Ați efectuat o evaluare scrisă a securității și riscurilor sistemelor informatice (audit) înainte sau după (perioada ultimelor 3 ani) dezvoltarea sistemelor dvs. informaționale?

3. A introdus compania dvs. documente interne privind securitatea sistemelor informatice (bazată pe evaluarea riscurilor)? (De exemplu, politica de securitate a sistemului de informații, metodologia de evaluare a riscurilor, criteriile de clasificare a activelor informaționale, regulile de acordare a drepturilor de acces, drepturile și obligațiile utilizatorilor, dispozitivele mobile și politica internetului etc.).

4. Aveți o persoană pe intern care este responsabilă de implementarea politicii de securitate a sistemului de informații și mijloace sau responsabilă de protecția datelor cu caracter personal?

5. Accesul la datele personale ale angajaților dvs. este controlat prin parole și nume de utilizator?

Dacă răspunsul dvs. la oricare dintre aceste întrebări este "NU", este posibil ca organizația dvs. de prelucrare a datelor personale să nu corespundă cerințelor GDPR.

6. Ce alte instrumente aveți pentru protecția resurselor informaționale fizice?

7. Care sunt perioadele de stocare a datelor dvs. personale? Ați configurat termenii pentru stocarea, reținerea și ștergerea datelor?

8. Ați implementat procedura internă de înregistrare a încălcărilor securității datelor cu caracter personal și procedura de notificare?

9. Cum distrugeți documentele și cititorii de informații?

Dacă aceste probleme nu sunt soluționate prin proceduri scrise, organizația dvs. de prelucrare a datelor personale nu corespunde cerințelor GDPR.

3.4. Evaluarea impactului asupra protecției datelor

Evaluarea impactului asupra protecției datelor (Evaluarea) este un instrument care are rolul de a evalua respectarea de către companii a obligațiilor privind protecția datelor și de a identifica eventualele riscuri și strategii de atenuare. O evaluare ar trebui să fie finalizată, în mod ideal, în faza de proiectare a unui nou sistem sau program și apoi revizuită odată cu schimbarea cerințelor de program și obligațiilor legale.

Articolul 35 din GDPR prevede: în cazul în care un tip de prelucrare, în special, utilizarea noilor tehnologii și ținând seama de natura, domeniul de aplicare, contextul și scopurile prelucrării, este susceptibil de a genera un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înainte de prelucrare, o evaluare a impactului operațiunilor de prelucrare preconizate asupra protecției datelor cu caracter personal. O singură evaluare poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri similare.

3.5 Relația operator-persoana împuternicită de operator

Operatorul are o responsabilitate în ceea ce privește persoanele împuternicite de operator cu care lucrează, dar persoana împuternicită de operator tot poate să poartă răspundere, împreună cu operatorul sau cu alte persoane împuternicite de operator, în caz de încălcări ale GDPR care ar putea conduce la amenzi. Operatorul trebuie să se asigure că relația cu persoana împuternicită de operator este construită pe baza unui contract care corespunde articolului 28 din GDPR.

Câteva exemple de relație operator-persoana împuternicită de operator:

- Echipa dvs. de marketing prelucrează datele personale ale potențialului client. Atunci când lucrează cu o companie sau agenție de marketing prin e-mail, de exemplu, care utilizează aceste date pentru campanii, acestea din urmă sunt persoane împuternicite de operator.
- S-ar putea să fi externalizat activitățile centrului de contact al organizației dvs. sau să folosiți uneori un centru de apel ("call center") atunci când doriți să permiteți utilizatorilor să formeze un număr specific în cadrul unei campanii. Centrul de contact devine în acel caz persoană împuternicită de operator.
- Închiriați spațiu de stocare pentru stocarea datelor cu caracter personal în centrul de date care aparține altei companii.

Întrebări care vă pot ajuta să înțelegeți dacă aveți relații cu persoana împuternicită de operator și dacă atribuțiile sunt adresate în mod corespunzător.

1. Este prelucrarea datelor dvs. subcontractată unei alte companii din Moldova?
2. Aveți un acord scris cu compania subcontractată care conține clauzele prevăzute la articolul 28 din GDPR?
3. Prin ce mijloace datele personale sunt livrate companiei subcontractate?
4. Contractul cu persoana împuternicită de operator conține clauze privind securitatea datelor personale, perioadele de stocare a datelor, cerințele tehnice și organizaționale? Care sunt aceste cerințe?

3.6 Informații de a fi furnizate subiectului datelor

Operatorul trebuie să furnizeze anumite informații privind prelucrarea datelor subiectului datelor în cazul în care datele cu caracter personal sunt obținute direct de la subiectul datelor (articolul 13) sau de la persoane terțe (articolul 14). Operatorul trebuie să fie în măsură să îndeplinească această obligație, indiferent dacă subiectul datelor a inițiat dreptul de acces la datele sale personale. Aplicarea articolului 13 este deosebit de importantă în cazul consimțământului subiectului datelor, în măsura în care consimțământul trebuie informat, adică, subiectul datelor trebuie să poată obține informații de la operator în ceea ce privește scopul datelor cu caracter personal, numele operatorului, temeiurile legale și alte aspecte importante înainte de a fi de acord cu transmiterea datelor cu caracter personal. De exemplu, dacă compania gestionează un site web și colectează date cu caracter personal, compania trebuie să furnizeze informațiile adecvate subiectului datelor înainte de consimțământul acestui.

3.7. Drepturile subiectului datelor

Subiectul datelor are mai multe drepturi în conformitate cu GDPR decât înainte, conform Directivei. Unul dintre cele mai importante drepturi este dreptul de a-și accesa datele personale în orice moment. Prin urmare, compania trebuie să asigure o posibilitate reală ca subiecții de date să depună o cerere relevantă. Compania trebuie să asigure posibilitatea adecvată de a verifica identitatea persoanei sau a utilizatorului care primește date personale de la operator (datele personale nu pot fi eliberate unei persoane care nu este verificată dacă persoana respectivă este subiectul datelor care a solicitat informații). Dacă cererea subiectului datelor este transmisă direct persoanei împuternicite de operator, acesta din urmă trebuie să informeze operatorul care va decide cum să soluționeze cazul. Persoana împuternicită de operator, dacă nu este autorizată în mod corespunzător înainte, nu poate răspunde în mod

direct subiectului datelor sau la orice altă persoană terță privind aspecte legate de prelucrarea datelor cu caracter personal (cu excepția autorităților de supraveghere a protecției datelor).

Subiectul datelor poate să realizeze și alte drepturi: dreptul de acces, dreptul la portabilitatea datelor sale personale, dreptul la opoziție, dreptul la restricționarea prelucrării, dreptul de a fi uitat.

Întrebări care vă pot ajuta să înțelegeți dacă compania dvs. asigură drepturile subiecților de date.

1. Ați făcut o evaluare cu privire la care dintre drepturile subiecților de date (articolul 15-21 din GDPR) sunt relevante pentru prelucrarea dvs.?
2. Ați implementat careva procedură referitoare la dreptul de acces al subiectului datelor?
3. Site-ul companiei conține informații pentru subiecții de date sub forma politicii privind protecția vieții private, a politicii de confidențialitate cu informații pentru subiecții de date?
4. Ați primit compania dvs. vreun drept de acces la cerere înainte? Ați răspuns într-o lună?

Dacă aceste probleme nu sunt adresate prin proceduri scrise, organizația dvs. de prelucrare a datelor personale nu corespunde cerințelor GDPR.

3.8. Responsabilul pentru protecția datelor cu caracter personal

Operatorul și persoana împuternicită de operator trebuie să desemneze un responsabil pentru protecția datelor cu caracter personal 1) în cazul în care compania prelucrează categorii speciale de date cu caracter personal pe scară largă ca activități de bază sau 2) activitățile principale ale companiei respective constau în operațiuni de prelucrare care, prin natura lor, domeniul de aplicare și/sau scopurile acestora necesită o monitorizare periodică și sistematică a subiecților de date la scară largă.

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

ÎNTREBĂRI PRIVIND PRELUCRAREA DATELOR CU CARACTER PERSONAL

Acest tabel cu întrebări Vă va ajuta să evaluați domeniul de aplicare al prelucrării dvs. actuale de date personale.

Cunoașterea cerințelor GDPR	Informații privind autoevaluarea de conformare la GDPR
Activități și scopuri de prelucrare a datelor personale	1. Vă rugăm să enumerați activitățile dvs. tipice de prelucrare a datelor personale? <i>De exemplu, contabilitate, registrul angajaților, camere de supraveghere video, evidența apelurilor de intrare, cookies de pe situri web, profiluri de utilizatori colectate prin siturile web a companiei, monitorizarea angajaților și altele.</i> 1.1. 1.2. 2. Care este scopul real a tuturor celorlalte activități de prelucrare care nu sînt reglementate de legislație sau reglementări publice? Vă rugăm să indicați scopul activității! <i>În gestionarea companiei și ansamblului de activități ar putea fi necesar de a colecta, a stoca și a utiliza alte informații, inclusiv și informații despre clienți. Totuși, fiecare unitate de date personale trebuie evaluată în sensul scopului și temeiului legal.</i> 2.1. 2.2.
Activități de prelucrare a datelor personale	3. Ce tipuri de date personale sunt prelucrate (recepționate, stocate, transmise) de către organizația dvs? Specificați o listă cu tipuri cele mai frecvente de date personale! 4. Prelucrați categorii speciale de date personale? (datele cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, convingerile religioase sau filosofice sau calitatea de membru al sindicatelor și prelucrarea datelor genetice, datele biometrice în scopul identificării unice a unei persoane fizice, datele privind sănătatea sau datele referitoare la viața sexuală a persoanei fizice sau orientarea sexuală a acesteia). Vă rog, indicați!

	5. Prelucrați date aferente condamnărilor penale sau măsurilor de securitate? Specificați temeiul. 6. Utilizați algoritme care prelucrează date personale și care iau o decizie fără intervenție umană? 7. Utilizați algoritme pentru evaluarea unor aspecte aferente persoanei? (de ex. preferințele utilizatorului în rețea, situația financiară, comportament etc.)
Activități de prelucrare a datelor personale și furnizarea de informații subiectului datelor	8. Ați făcut careva analiză privind temeiurile legale pentru prelucrarea datelor personale? (De ex., care date personale sunt colectate în baza consimțământului subiectului datelor, contractului, cerinței legale sau așa-zisului interes legitim al operatorului) 9. Ați făcut vreo evaluare despre necesitatea prelucrării curente? 10. Furnizați careva informații subiecților de date privind scopurile prelucrării sau alte informații înainte de colectarea datelor personale? (de ex., formularele-chestionare, formulare de înregistrare a profilului utilizatorului în rețea, politica de confidențialitate a sitului conține careva informații privind organizația dvs. în calitate de operator și scopul prelucrării?) 11. Ați făcut o evaluare privind care drepturi ale subiecților de date (art. 15-21 din GDPR) sunt relevante prelucrării dvs.? 12. Ați implementat vreo procedură privind dreptul de acces al subiectului datelor?

	13. Situl companiei conține informații pentru subiecții de date sub forma politicii cu privire la viața privată, politicii de confidențialitate cu informarea subiecților de date? 14. Compania dvs. a primit anterior vreun drept privind accesarea cererii? Ați răspuns în termen de 1 lună?
Securitatea informațională	15. Compania dvs. a implementat principiile de protecție a datelor când au fost introduse sistemele de prelucrare a datelor? 16. Ați făcut o evaluare scrisă a securității și riscurilor aferente sistemelor informaționale (audit) înainte sau după (ultimii 3 ani) dezvoltarea sistemelor informaționale? 17. Compania dvs. a introdus documente interne ce țin de securitatea sistemelor informaționale (în baza analizei riscurilor)? (De ex., politica privind securitatea sistemelor informaționale, metodologia de evaluare a riscurilor, criterii de clasificare a activelor informaționale, regulile privind acordarea drepturilor de acces, drepturile și obligațiile utilizatorului, dispozitive mobile, și politica în rețea etc.) 18. Aveți o persoană pe intern responsabilă de implementarea politicii privind securitatea sistemelor și mijloacelor informaționale sau responsabilul privind protecția datelor cu caracter personal? 19. Accesul la datele personale ale angajaților este controlat prin intermediul parolelor și numelor de utilizatori? 20. Ce alte instrumente aveți disponibile pentru protecția resurselor cu informații fizice? 21. Care este perioada de stocare (reținere) a datelor personale în compania dvs.? Ați instituit careva termeni pentru stocarea, reținerea și ștergerea datelor? 22. Ați implementat procedura internă de înregistrare și notificare privind încălcarea securității datelor cu caracter personal? 23. Cum distrugeți documentele și alte suporturi informaționale?

Relația operator – persoana împuternicită de operator	24. La prelucrarea datelor personale subcontractați careva companie din Moldova? 25. Aveți un acord scris cu vreo companie subcontractată ce conține clauze stipulate în art. 28 din GDPR? 26. Prin ce mijloace sunt transmise datele personale către compania subcontractată? 27. Acordul cu persoana împuternicită de operator conține careva clauze privind securitatea datelor personale, perioadele de stocare a datelor, cerințele tehnice și organizatorice? Care sunt acele cerințe?
--	--

Pentru informații suplimentare și actualizări, accesați site-ul Centrului Național pentru Protecția Datelor cu Caracter Personal.

TABELUL
divergențelor rezultate din avizul prezentat de Centrul de Implementare a Reformelor la
proiectul de lege privind Centrul Național pentru Protecția Datelor cu Caracter Personal

Denumirea instituției	Norma juridică la care sînt obiecții sau propuneri	Obiecția/propunerea formulată	Acceptare/argumentare neacceptări
<i>Centrul de Implementare a Reformelor</i>	Art.2 alin.(1)	Art.2 alin.(1), prevede că „Centrul este o autoritate publică autonomă a statului, cu personalitate juridică, independentă față de orice alte autorități publice, persoane fizice și juridice de drept privat, cu atribuții de supraveghere, de prevenire, de decizie, de reglementare, de interdicție, de intervenție, de investigație și de sancționare, în domeniul prelucrării datelor cu caracter personal și al liberei circulații a acestor date”. Astfel, cu referire la spectrul de competente atribuite prin normele de la art. 2 în coroborare atribuțiile Centrului stabilite la art.8, (de la supravegherea respectării legislației în domeniul protecției datelor cu caracter personal; reglementarea operațiunilor de prelucrare a datelor cu caracter personal; efectuarea investigațiilor privind cazurile de încălcare a legislației privind protecția datelor cu caracter personal; elaborarea actelor normative necesare implementării legislației în domeniu; aplicarea sancțiunilor pecuniare pentru încălcarea legislației în domeniu) relevăm că o asemenea reglementare comportă riscuri de abuzuri din partea Centrului, datorită concentrării tuturor pârghiilor de reglementare, control, investigare, sancționare al unui domeniu (prelucrarea datelor cu caracter personal).	- Cu referire la invocarea faptului că concentrarea pîrghiilor de reglementare incluse în proiect comportă riscuri de abuzuri din partea CNPDCP o considerăm eronată. Competențele CNPDCP prevăzute în proiectul de lege nu exced competențele atribuite autorităților europene pentru protecția datelor de către Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (a se vedea art. 55-58), Directiva (UE) 2016/680 referitoare la protecția datelor personale în cadrul activităților specifice desfășurate de autoritățile de aplicare a legii și Directiva (UE) 2016/681 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. Menționăm, că prin Legea nr. 120/2017 cu privire la prevenirea și combaterea terorismului a fost transpusă Directiva (UE) 2016/681, prin care Centrul a fost investit cu noi competențe, spre exemplu în raport cu SIS. În acest sens, remarcăm art. 58 din noul Regulament 2016/679, care statuează competențele de investigație a Autorităților de supraveghere a protecției datelor cu caracter personal prevede, inclusiv următoarele competențe:

	În context, este necesară cel puțin atribuirea funcției de elaborare și promovare a politicii de stat în domeniul protecției datelor cu caracter personal, precum și a funcției de reglementare către un organ central de specialitate care va asigura realizarea politicii în domeniu (eventual - Ministerul Justiției). Totodată, prevederile proiectului de lege nu oferă un mecanism de control și supraveghere a activității Centrului din partea unor instituții ale statului fapt care exclude posibilitatea monitorizării și verificării obiective a activității acestuia, în schimb proiectul abundă de garanții mari de protecție juridică și anume: - sediul Centrului constituie perimetru de securitate cu acces restricționat (art.2 alin.(4); - nici un act normativ nu poate suprima sau diminua competențele Centrului fără a opera modificări în prezenta lege (art.4 alin.(4); - secretul de stat, secretul profesional, secretul bancar, secretul comercial sau a dosarului special, confidențialitatea procesului contravențional sau penal și/sau orice alt tip de restricționare, nu poate constitui temei pentru refuz în solicitarea și obținerea informațiilor, materialelor și documentelor (art.8 alin.(3) lit.e); - personalul Centrului nu poate fi atras la răspunderea penală, contravențională sau civilă pentru actele sau faptele îndeplinite într-o situație de risc profesional justificat, chiar dacă au fost cauzate prejudicii, inclusiv de natură patrimonială, drepturilor și intereselor ocrotite de lege ale unei persoane. Riscul se consideră profesional justificat dacă acțiunile decurg în mod obiectiv din informația, faptele și circumstanțele cunoscute, iar scopul legii nu putea fi atins prin acțiuni ce nu ar fi implicat riscul, luându-se	a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale; e) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale; f) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern. - Remarcăm, că la moment Centrul efectuează investigații asupra prelucrării datelor cu caracter personal și această atribuție nu poate fi considerată drept una excesivă și abuzivă, avînd în vedere că pînă în prezent nu au fost înregistrate careva situații de abuzuri din partea reprezentanților Centrului în cadrul exercitării atribuțiilor sale. Acțiunile Centrului se verifică de instanța de judecată. Mai mult, art. 8 alin. (5) din proiect propunem de a fi completat în final, după cum urmează: <i>...iar activitatea generală a Centrului este supusă controlului parlamentar.</i> De asemenea, activitatea CNPDPC nu este exclusă de controlul din partea altor organe, conform competenței lor în cazul în care se încalca alte prevederi legale. - Se accepta. În partea ce ține de atribuirea funcției de elaborare și promovare a politicii de stat în domeniul protecției datelor de către Centru, aceasta a fost exclusă.
--	---	--

		toate măsurile posibile pentru a preîntâmpina consecințele negative (art.22 alin,(1); - în exercitarea atribuțiilor de serviciu directorul, directorii adjuncți și inspectorii de protecție nu pot fi reținuți, arestați ori trași la răspundere contravențională sau penală decât la cererea Procurorului General (art.22 alin,(2); - personalul Centrului nu poate fi audiat sau interogat referitor la esența informațiilor ce vizează viața intimă, familială și privată a subiectului de date cu caracter personal, de care a făcut cunoștință în cadrul exercitării atribuțiilor de serviciu cu excepția situației când acesta este audiat în cadrul unei ședințe de judecată, iar documentele și materialele în cauză se utilizează doar cu autorizația Centrului. Acțiunile sau procedeele întreprinse cu încălcarea prevederilor prezentului alineat sunt lipsite de forță juridică (art.22 alin.(4)).	- Asigurarea garanțiilor este condiționată de specificul autorității, care este o contrabalanță, aceasta fiind în drept să verifice legalitatea operațiunilor de date cu caracter personal în diferite domenii, inclusiv în domeniul activității organelor de drept. În această situație riscul intimidării angajaților urmează a fi diminuat prin garanții adecvate. Prin normele în cauză se urmărește scopul asigurării unor condiții de siguranță, pentru angajații Centrului în partea ce ține de executarea în deplină independență și fără posibilitate de intimidare sau intervenție, inclusiv din partea organelor de drept a atribuțiilor sale. Garanțiile încorporate în proiect nu pot fi considerate excesive având în vedere noul cadru comunitar în domeniul protecției datelor, prevede ca Autoritatea națională de supraveghere este responsabilă nu doar de consilierea privind aplicarea legislației în domeniu, ci și de monitorizarea respectivei aplicări urmărind protejarea drepturilor fundamentale legate de prelucrarea datelor cu caracter personal. Garanții similare sunt prevăzute în Legea nr. 308/2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, Legea nr. 1104/2002 cu privire la Centrul Național Anticorupție.
	La art. 10	Art. 10, prevede instituirea „Unității de instruire în domeniul protecției datelor cu caracter personal” ca subdiviziune specializată, cu personalitate juridică distinctă, aflată în subordinea Centrului, care are sarcina de instruire și sporire a calificării în domeniul protecției datelor cu caracter personal Astfel, nu este argumentată necesitatea creării unei Unități de instruire în domeniul protecției datelor cu caracter personal din următoarele considerente: - existența mecanismului de dezvoltare profesională continuă a funcționarilor publici, statuat la art.37-38 din Legea nr. 158/2008 cu privire la	Se accepta. Art. 10 din proiect a fost exclus

		funcția publică și statutului funcționarului public, și detaliat în Regulamentul cu privire la dezvoltarea profesională continuă a funcționarilor publici, aprobat prin Hotărârea Guvernului nr.201/2009 (anexanr.10); - ineficiența constituirii unei Unități specializate în asigurarea instruirii și perfecționării pentru un număr redus de personal al Centrului (pornind de la efectivul-limită al Centrului - 45 de unități de personal, potrivit art. 1 din Legea nr. 182/2008).	
	Art. 12	Art.12, conține reglementări privind personalul Centrului, care este constituit din funcționari publici cu statut special - inspectori de protecție a datelor și funcționari publici supuși reglementărilor Legii nr. 158-XVI din 4 iulie 2008 cu privire la funcția publică și statutul funcționarului public, precum și personal auxiliar, supus reglementărilor legislației muncii. Astfel, nu este clar ce presupune statutul „inspectorului de protecție” care potrivit art.25 este funcționar public cu statut special, comparativ cu funcționarii publici din cadrul Centrului, întrucât prevederile capitolului III „Cariera inspectorului de protecție” constituie în mare parte referințe la Legea nr. 158-XVI din 4 iulie 2008 cu privire la funcția publică și statutul funcționarului public.	Statutul inspectorilor de protecție a datelor - funcție publică cu statut special este conferit în dependență de: a) principiile profesionale; c) sistemul de carieră; d) formarea profesională; e) exercitarea funcției publice cu statut special, potrivit atribuțiilor legale date în competența entității din care face parte, cum ar fi: verificarea legalității prelucrării datelor, desfășurarea investigațiilor, inspecțiilor și audituri în conformitate cu legislația națională, fie prin autosesizare, fie pe baza unei plângeri; h) îndeplinirea de atribuții exclusiv în folosul cetățeanului și comunității, ce impun asumarea unei conduite speciale, interdicții și restricții individuale, restrângerea exercițiului unor drepturi fundamentale și instituirea de incompatibilități, etc.; Statutul inspectorului de protecție se deosebește de statutul funcționarului public, acestea fiind categorii diferite de funcționari, competențele cărora sunt reglementate prin norme distincte. Atribuțiile specifice ale inspectorului de protecție se deosebesc esențial de atribuțiile funcționarului public. Astfel, potrivit art. 20 alin. (1) doar inspectorul de protecție este în drept să efectueze investigația legalității prelucrării datelor în cadrul căreia este în drept:

			a) să solicite și să primească informații și materialele ce țin de prelucrarea datelor cu caracter personal necesare îndeplinirii obligațiilor, inclusiv informații oficiale cu accesibilitate limitată și informații ce constituie secret de stat, având autorizația conducătorului subdiviziunii și/sau a conducerii Centrului; b) să prelucreze informații oficiale cu accesibilitate limitată potrivit atribuțiilor funcționale; c) să aibă acces gratuit la sistemele informaționale de stat și private în care sunt prelucrate și stocate date cu caracter personal; d) să supravegheze respectarea legislației privind protecția datelor cu caracter personal și să efectueze activități de prevenire a cazurilor de încălcare a acesteia; e) să efectueze investigații privind cazurile de încălcare a legislației privind protecția datelor cu caracter personal, cu sau fără ieșirea la fața locului, etc; Astfel, inspectorul primește calitatea de statut special prin natura și esența atribuțiilor cu care este înzestrat. Cu referire la obiecțiile aduse în partea ce vizează trimiterile în tot conținutul textului proiectului la normelor generale ce se referă la activitatea funcționarilor publici, menționăm că astfel de practică a fost utilizată, spre exemplu și în Legea nr. 302 din 21 decembrie 2017 cu privire la Serviciul Vamal elaborată de Ministerul Finanțelor, etc.
	La art. 18	Art.18, alin.(1) lit.o), prevede atribuția Directorului Centrului de sesizare a Curții Constituționale în vederea controlului constituționalității legilor și hotărârilor Parlamentului Republicii Moldova, decretelor Președintelui Republicii Moldova, hotărârilor și ordonanțelor Guvernului Republicii Moldova pe probleme ce țin de protecția datelor cu caracter personal, inclusiv prin prisma respectării dreptului la viață intimă, familială și privată.	Se accepta

		În acest sens, art.38 din Codul jurisdicției constituționale și art.25 din Legea cu privire la Curtea Constituțională nr.317/1994, prevede expres subiecții cu drept de sesizare. În acest sens, relevăm că Directorul Centrului nu face parte din lista subiecților cu drept de sesizare a Curții Constituționale.	
	La art. 24	Salarizarea personalului Centrului, urmează a fi revăzut, în contextul noii legi privind sistemul unitar de salarizare în sectorul bugetar, care va interzice includerea în alte acte normative a prevederilor ce țin de salarizare, fiind stabilit un cadru unic și complex, cu acoperire integrală a sectorului bugetar.	La moment nu exista o lege noua cu privire la salarizare, dar se accepta. Normele privind salarizarea personalului Centrului incontestabil vor fi revizuite în cadrul comisiilor parlamentare, ținând cont de noul proiect de Lege privind sistemul unitar de salarizare în sectorul bugetar.
	În concluzie	Totodată, deși din sintezele obiecțiilor și propunerilor atașate la proiectele de lege, se constată consultarea acestora cu mediul de afaceri (Asociația Națională a Companiilor din Domeniul TIC; Camera de Comerț Americană din Moldova; Asociația Businessului European), considerăm că proiectele urmează să fie remise spre expertizare către grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător, întrucât acestea vor avea impact asupra activității de întreprinzător.	Considerăm inoportună remiterea proiectelor spre expertizare către grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător din considerentul că expertul din cadrul proiectului Twinning „Consolidarea capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova” a efectuat Studiul de impact al GDPR asupra companiilor private din Moldova, care a fost prezentat în cadrul ședințelor organizate cu reprezentanții sectorului privat. Remarcăm că, începând cu 25 mai anul 2018, domeniul protecției datelor cu caracter personal în Republica Moldova înregistrează o deficiență majoră de reglementări, care să rezoneze cu reglementările dreptului comunitar european în materie de protecție a datelor cu caracter personal și care să ofere o protecție sigură persoanelor în privința prelucrării datelor cu caracter personal și respectării dreptului la inviolabilitatea vieții intime, familiale și private. Astfel, un număr mare de companii din RM, inclusiv exponenți ai businessului european vor fi nevoiți să aplice direct prevederile normative ale comunității europene, în speță a GDPR, cadru normativ care contravine cu legislația națională.

			Menționăm că peste 60 la sută din companiile ce activează în Moldova au raporturi economice cu cele din UE, iar o mare parte din ele prelucrează date cu caracter personal a cetățenilor europeni. Un exemplu elocvent este cazul unei bănci comerciale străine care a devenit acționar al unei bănci comerciale naționale, în urma căreia cea din urmă și-a manifestat intenția de a transmite datele cu caracter personal ale clienților săi peste hotarele Republicii Moldova, inclusiv în scopul recuperării creanțelor. Remarcăm că potrivit notificării depuse inițial la Centru în cadrul procedurii de notificare a operațiunilor de prelucrare a datelor, banca comercială națională a declarat că datele cu caracter personal pe care le prelucrează sunt stocate pe teritoriul RM, iar un ulterior transfer transfrontalier de date în condițiile actualei Legi privind protecția datelor cu caracter personal, în scopurile declarate nu este posibil și crează impedimente serioase în activitatea economică. Ca rezultat Centrul a identificat o soluție parțială a problemei, însă soluționarea definitivă depinde de implementarea cât mai urgentă a noului pachet de legi. Situații similare sunt reclamate din ce în ce mai des, fapt ce necesită o soluționare urgentă. Dorim să menționăm că proiectele date au fost avizate de asociațiile de business din RM, care participă în Comisia de stat pentru reglementarea activității de întreprinzător. În altă ordine de idei, propunerile și obiecțiile asociațiilor de bussines au fost luate în calcul de către Centru într-o proporție considerabilă. Cu titlu separat remarcăm că Centrul este sesizat cu regularitate de MAEIE cu privire la pașii întreprinși în vederea recunoașterii statului Republica Moldova de către Comisia Europeană, drept stat care asigură un nivel adecvat de protecție a datelor cu caracter personal. Specificăm că o asemenea procedură nu poate avea loc fără o reglementare temeinică și conformă a legislației naționale în domeniul protecției datelor, care urmează să corespundă în totalitate cu aquis-ul comunitar.
--	--	--	--

			În cazul în care RM va fi recunoscută drept stat ce asigură un nivel adecvat de protecție a datelor cu caracter personal echivalent cu cel din UE, aceasta va crea posibilitatea noilor relații economice și dezvoltarea esențială a RM în ansamblu.
--	--	--	---

222

TABELUL
divergențelor rezultate din avizul prezentat de Asociația Națională a Companiilor din Domeniul TIC referitor la
proiectul de lege privind protecția datelor cu caracter personal

Nr. d/o	Denumirea instituției	Norma juridică la care sînt obiecții sau propuneri	Obiecția/propunerea formulată	Acceptare/argumentare neacceptări
	Asociația Națională a Companiilor din Domeniul TIC	La art. 3	<i>operator</i> - 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 aceste date; <i>Propunem sa fie exclus textul " intenționează să prelucreze " deoarece nu este prevăzut de GDPR.</i> Se solicită de exclus fraza” De regulă, persoana împuternicită este o persoană juridică sau fizică, alta decât operatorul;” Nu se regăsește în GDPR (pare a fi inutilă) și ar putea fi și alte situații, ceea ce ar induce în eroare - interpretare multiplă (de ex. Aceeași instituție sa aiba statut de operator pentru activitățile sale de baza și totodată persoana împuternicită pentru alte activități adiționale) <i>servicii ale societății informaționale</i> - înseamnă orice serviciu prestat, la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciului. <i>Modificarea este necesară deoarece aplicațiile gratuite trebuie să intre la fel în sfera acestor servicii.</i>	Se acceptă parțial. - Noțiunea de „operator” nu contravine Regulamentului UE 2016/679. - Fraza” De regulă, persoana împuternicită este o persoană juridică sau fizică, alta decât operatorul;” este o concretizare a noțiunii și nu influențează asupra sensului definiției expuse de Regulamentul UE 2016/679. Noțiunea a fost modificată și expusă în următoarea redacție: <i>servicii ale societății informaționale</i> - înseamnă orice serviciu prestat la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciului. Considerăm că redacția actuală acoperă și aplicațiile gratuite.

		La art. 4	Se propune de exclus lit.g, alin. 1 art. 4, deoarece GDPR-ul nu prevede acest fapt.	Nu se acceptă. Norma nu contravine GDPR, a se vedea considerentul (10) și are drept scop de a atrage atenția că un anumit document conține date cu caracter personal și în privința lui urmează să fie aplicate măsuri de securitate respective.
		La art. 5 alin. (1) lit. b)	De exclus propoziția 'Transmiterea datelor personale, altele decât cele legate de executarea contractului, către un alt operator sau persoană împuternicită de către operator, poate avea loc doar cu condiția existenței consimțământului subiectului de date, în condițiile expres prevăzute de lege; <i>GDPR-ul nu prevede acest aspect.</i>	Se acceptă. Prevederea a fost exclusă.
		La art. 13 alin. (2)	Se solicită de modificat alin. 2 art. 13 (2) în cazul în care legislația nu prevede în mod expres condițiile și termenele pentru stocarea și utilizarea datelor personale, ele sunt stabilite de către operator. <i>Solicităm excluderea notificărea/aprobarea Centrului, deoarece chiar si GDPR-ul precizează ca aceasta măsura generează sarcini administrative si financiare, care nu au contribuit la îmbunătățirea protecției datelor personale, ci doar a transformat într-o procedura birocratică (recital. 89 al GDPR-ului).</i>	Se acceptă parțial. Norma a fost expusă în următoarea redacție: „(2) În cazul în care legislația nu prevede în mod expres condițiile și termenele pentru stocarea și utilizarea datelor personale, ele sunt stabilite de către operator. Operatorii autorități și instituții publice consultă Centrul privind termenele pentru stocarea și utilizarea datelor personale.” Totodată remarcăm că prin prezentul proiect a fost exclusă procedura de notificare a operațiunilor de prelucrare a datelor cu caracter personal.
		La art. 18 alin. (3)	Se solicită de modificat alin. 3 art.18 (3) Informarea subiectului de date de regulă se face în formă scrisă, electronică sau în orice alt format.	Se acceptă. Norma a fost expusă în următoarea redacție: „Informarea subiectului de date se face în formă scrisă, electronică sau în orice alt format cu condiția

			<i>Se propune de modificat cu sintagma "a fost informat ", deoarece publicarea pe site-ul oficial nu poate fi demonstrata receptionarea. Totodată propunem de a fi introdusa posibilitatea de a informa prin intermediul poștei electronice indicate de subiectul de date, fara necesitatea de a proba receptionarea in acest caz de către operator.</i>	că operatorul poate demonstra că subiectul de date a fost informat.
		La art. 35	Se solicită modificarea alin.5 din art. 35. Se propune redactarea ca și în GDPR: "250 de angajați".	Prin prezentul proiect de lege se transpune Regulamentului (UE) 2016/679. În acest sens remarcăm că potrivit prevederilor expuse la art. 35 alin. (5) norma în cauză este conformă dispozițiilor Regulamentului (UE) 2016/679, în conformitate cu care „<i>Obligațiile menționate la alineatele 1 și 2 nu se aplică unei întreprinderi sau organizații cu mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10.</i>” Totuși, avînd în vedere că în Republica Moldova puțini agenți economici dispun de un staff de personal mai mare de 250 angajați s-a mers pe formula mai puțin de 20 de angajați.
		La art. 37	La alin. (1). Avînd în vedere stadiul dezvoltării tehnologice și costurile implementării în raport cu riscurile și cu natura datelor cu caracter personal a căror protecție trebuie asigurată, actual prelucrării, domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, operatorul, operatorul asociat, persoana împuternicită de	Se acceptă parțial - Cu referire la art. 37 (36) alin. (1), sintagma „<i>costurile implementării și natura</i>” a fost inclusă în conținutul art. 36 alin. (1).

		operator, destinatarul, precum și entitățile care nu sunt considerate a fi destinatari (oganele de ocrotire a legii), terțul, indiferent de tipul proprietății și domeniul de activitate, forma juridică de organizare, implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele să asigure cel puțin: Se propune de adăugat conform pct. 83 din preambulul GDPR “costurile implementării și natura”. Este un termen prea mare. Propunem să fie cum este în variant actuală - 2 ani. k) ținerea evidenței ieșirii din sistemele de evidență gestionate a informațiilor ce conțin date personale; Textul ” marcarea informațiilor ” se propune de exclus, deoarece nu este prevăzut în GDPR. 1) înregistrările de audit al prelucrării datelor personale. Evidența evenimentelor și/sau acțiunilor înregistrate de sistemul de audit a securității în sistemele de date personale va fi păstrată pentru o perioadă de 3 ani; Este un termen prea mare. Propunem să fie cum este în variant 3 ani. Se propune de adăugat alin. 6 art. 37 “6) Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la alineatul (1) din prezentul articol.” În conformitate cu pct. 3, articolul 24 GDPR	- Cu referire la art. 37 (36) alin. (1) lit. k), menționăm că norma nu contravine GDPR și are drept scop de a atrage atenția că un anumit document conține date cu caracter personal și în privința lui urmează să fie aplicate măsuri de securitate respective. - Cu referire la art. 37 (36) alin. (1) lit. l) remarcăm că necesitatea prevederii unui asemenea termen este generată de cererile subiecților de date personale care solicită verificarea legalității prelucrării datelor ce îl vizează de anumiți operatori. - Cu referire la completarea art. 37 (36) cu un nou alin. (6) remarcăm că norma propusă de ATIC se regăsește în prezentul proiect de lege la art. 29 alin. (6).
--	--	--	---

		La art. 42	Se solicită modificarea alin.2 din art. 42 ”(2) în termen de cel mult o lună de la primirea cererii, cu privire la orice astfel de prelungire, prezentând motivele întârzierii. Aceste perioade pot fi suspendate până când Centrul a obținut informațiile pe care le-a solicitat în scopul consultării.” <i>In conformitate cu pct. 2, articolul 36 GDPR</i>	Nu se acceptă . Considerăm termenul prevăzut în normă unul rezonabil care reiese din multitudinea și complexitatea solicitărilor de acordare a consultațiilor adresate CNPDCP.
		La art. 43	Se propune de exclus alin. 8, art. 43 Nu este prevăzut de GDPR. Nu este clar în ce context și nu este relevant. La fel, prin crearea subdiviziunilor, se intervine în treburile agentului economic/operator.	Nu se acceptă din considerentul că norma prevede crearea subdiviziunilor în anumite condiții ”<i>în dependență de numărul de angajați</i>” și nu ca o prevedere obligatorie.
		La art. 81	(5) în cazul investigației la fața locului, directorul Centrului, directorul adjunct sau șeful direcției generale care este autorizat în mod corespunzător de director în aceste scopuri, emite o decizie în care se indică scopul și obiectul investigației cu indicarea posbililor încălcări ce rezulta din informația și probele deținute până la inițierea invistigației, persoanele delegate privind efectuarea investigației, perioada de timp, precum și drepturile și obligațiile părților implicate în investigație. <i>Organele de control au tendința de a indica la obiectul controlului termeni foarte generali (ex. verificarea respectării legislației) și astfel, investigația poate căpăta un caracter abuziv.</i>	Nu se acceptă. - Cu referire la propunerile la art. 81 alin. (5), considerăm suficient ca în normă să fie specificat doar scopul și obiectul investigației, care prezumă reflectarea în decizie a aspectelor concrete care au stat la inițierea investigației. Remarcăm că drepturile CNPDCP, inclusiv cel prevăzut prin norma la care se face referire este dictat de prevederile art. 58 din noul Regulament 2016/679, care prevede competențele de investigație a autorităților de supraveghere a protecției datelor cu caracter personal prevede, inclusiv următoarele:

		Accesul Centrului la Secretul comercial, trebuie limitat la maxim, iar orice solicitare în acest sens din partea Centrului trebuie argumentată cu indicarea scopului solicitării accesului la informația ce constiuie secret comercial și cu posibilitatea persoanei de la care se solicită această informație de a ataca solicitarea în instanță, în orice caz, operatorului trebuie să i se ofere opțiunea de a prezenta doar partea din informația clasificată ca secret comercial care prezintă interes pentru investigația Centrului și nu toată informația solicitată (acte în întregime, procedee, tehnologii etc). d) să sigileze încăperile și mijloacele, unde și prin care se efectuează prelucrarea datelor personale, mijloacele, sistemele de evidență și documentele aferente obiectului și scopului investigației, pe perioada și în măsura în care este necesar pentru desfășurarea investigației, fara a bloca activitatea persoanei investigate și ținându- se cont de interesele persoanelor care pot fi lezate prin acțiunile de sigilare și cu respectarea Codului de Procedură Penală”. <i>Art. 58 al REGULAMENTULUI (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI nu prevede ca autoritatea națională de control/ supraveghere a respectării legii privind protecția datelor cu caracter personal sa aiba astfel de drepturi. De aceea se impune respectarea CPP.</i> e) să solicite persoanei, entității supuse investigației sau reprezentantului legal, care poate oferi Centrului informațiile necesare pentru soluționare unei cereri în legătură cu prelucrarea datelor cu caracter personal în cadrul investigației și de a înregistra, inclusiv prin mijloace audio, video sau prin	a) de a da dispoziții operatorului și persoanei împuternicite de operator și, după caz, reprezentantului operatorului sau al persoanei împuternicite de operator să furnizeze orice informații pe care autoritatea de supraveghere le solicită în vederea îndeplinirii sarcinilor sale; e) de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale; f) de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor, în conformitate cu dreptul Uniunii sau cu dreptul procesual intern. - Cu referire la propunerile la art. 81 alin. (9) lit. d) menționăm că acestea nu se acceptă din considerentul că măsura vizată are drept scop de a opri prelucrarea ilegală a datelor cu caracter personal. Totodată remarcăm că, activitatea operatorului poate fi blocată doar în măsura în care este necesar pentru efectuarea investigațiilor. Astfel, norma în cauză specifică: d) să sigileze încăperile și mijloacele, unde și prin care se efectuează prelucrarea datelor personale, mijloacele, sistemele de evidență și documentele aferente obiectului și scopului investigației, <u>pe perioada și în măsura în care este necesar pentru desfășurarea investigației;</u>
--	--	--	--

			alte mijloace, răspunsurile acestora doar cu acordul prealabil al persoanei. g) să fie asistată de avocați, de alți reprezentanți împuterniciți conform legislației. Dacă persoana fizică supusă investigației solicită prezența avocatului, efectuarea investigației se suspendă pînă la prezentarea avocatului, dar nu mai mult de 4 ore. <i>Nici Codul de Procedură Penală nu are termene așa de mici. Minimum este 3 ore!!!</i>	- Cu referire la propunerile la art. 81 alin. (9) lit.d) remarcăm că norma a fost modificată și expusă în următoarea redacție: <i>„e) să audieze și să solicite persoanei, entității supuse investigației sau reprezentantului legal sau altor persoane care pot oferi Centrului informațiile necesare pentru soluționarea unei cereri în legătură cu prelucrarea datelor cu caracter personal în cadrul investigației și de a înregistra, cu informarea prealabilă a persoanei supuse investigației, inclusiv prin mijloace audio, video sau prin alte mijloace, răspunsurile acestora;”</i> Remarcăm că aceste măsuri reies din specificul acțiunilor ce urmează a fi întreprinse urmare a efectuării măsurilor de investigații în scopul verificării legalității operațiunilor de prelucrare a datelor cu caracter personal. - Cu referire la propunerile la art. 81 alin. (11) lit.f) considerăm termenul prevăzut unul rezonabil, avînd în vedere că persoana este informată din timp despre efectuarea investigației, a scopului și obiectului acesteia. <i>Codul de Procedură Penală nu prevede termeni pentru suspendarea acțiunilor în cazul solicitării prezentei avocatului.</i>
		La art. 92	Se propune de modificat alin. 5 și alin.6 art. 92 Sancțiunile sunt prea mari pentru agenții economici naționali Se propune de modificat alin. 5 și alin.6 art. 92	Nu se acceptă. - Cu referire la art. 92 alin. (5) remarcăm: La moment se constată ineficiența măsurilor punitive în vigoare, care se manifestă prin caracterul îndelungat al examinării de către instanțele de judecată a cauzelor contravenționale pornite de

			Este necesar de definit noțiunile de “incalcari minore” si “incalcare grava”, pentru previzibilitatea individualizării sancțiunilor pecuniare.	Centru. Mai mult, soluționarea cauzelor contravenționale prin recunoașterea vinovăției contravenienților și sancționarea acestora în limitele prevăzute la art. 74¹-74³ Cod contravențional, se rezumă la constatarea de către instanța de judecată a faptelor contravenționale comise, fără a dispune obligarea contravenientului în vederea înlăturării cauzelor ce au dus la comiterea încălcărilor vizate. Într-o altă ordine de idei, urmează a menționa că noul Regulament 2016/679, la art. 83 prevede dreptul autorităților naționale de supraveghere de a aplica amenzi administrative. De altfel, în prezent art. 34 din Codul contravențional limitează cuantumul maxim al amenzilor pasibil a fi aplicate. Totodată, ținând cont de realitățile din Republica Moldova, în proiectul vizat se propune un mecanism treptat de aplicare a sancțiunilor pentru a nu împovăra operatorii de date și a le permite să se adapteze noilor rigori europene. Într-o altă ordine de idei, trebuie de menționat că în Republica Moldova există practici când autoritățile de control pot impune prin decizia sa sancțiuni pecuniare cum ar fi spre exemplu Consiliul concurenței, Banca Națională a Moldovei, CNPF. Remarcăm că Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului prevede sancțiuni în mărime de pînă la echivalentul în lei al sumei de 5000000 de euro, calculat la cursul oficial al leului moldovenesc. - Cu referire la art. 92 alin.(6) considerăm că din conținutul normei sunt clare situațiile care definesc
--	--	--	---	---

				încălcările minore (acestea au fost substituite în proiect cu sintagma încălcări ușoare) și încălcările grave.
		La art. 94	Se propune de exclus alin. 1, art. 94 <i>Aceasta reprezintă o motivație de a aplica sancțiuni pecuniare NEFONDATE, mai ales în baza criteriului cifrei de afaceri.</i> <i>Drept aplicarea sancțiunii în mod nefondat servește Dosarul nr. 12-4-45021-04072018, Centrul vs QSystems - articolul 74[1], Prelucrarea datelor cu caracter personal cu încălcarea legislației privind protecția datelor cu caracter personal Astfel, Centru fără careva plingeri și fără a stabili partea vătămată sau prejudiciată a întocmit Procesul Verbal.</i> Se propune de modificat alin. 4, art. 94 (4) în cazul în care persoanele prevăzute în decizia de sancționare au achitat sancțiunea pecuniară în termen de 5 zile de la data notificării, acestea au dreptul la o scutire cu 50% din cuantumul sancțiunii calculate.	Nu se acceptă. - Cu referire la excluderea din art. 94 (91) a alin. (1) menționăm că obiecția nu are un substrat juridic și obiectivitate. În urma acumulării unor resurse financiare suplimentare, Centrul va avea posibilități mai ample în vederea implementării politicii în domeniul protecției datelor cu caracter personal ca exemplu: angajarea experților din domeniul, efectuarea vizitelor cu scopul schimbului de experiență, dotarea tehnico-materială a Centrului, organizarea instruirilor etc. În privința abuzului, Centrul nu este lipsit de controlul din partea Parlamentului precum și jurisdicțional. Suplimentar, remarcăm că asemenea procedură este prevăzută în activitatea mai multor autorități, spre exemplu a MAI. - Cu referire la propunerea de a modifica în art. 94 (91) alin. (4) considerăm că aceasta nu este justificată. Mai mult în dispozițiile tranzitorii ale proiectului autorul a prevăzut un mecanism treptat de aplicare a sancțiunilor de Centru pentru fiecare an de la intrarea în vigoare a prezentei legi.
		La Art. IV	Se propune de modificat art. IV	Nu se acceptă

			Se propune 2 ani, conform GDPR-ului, intrarea în vigoare proiectul de lege din data publicării în Monitorul Oficial. De remarcat că Regulamentul general privind protecția datelor (2016/679 din 27 aprilie 2016) a fost publicat la 04 mai 2016, dar a intrat în vigoare la 25 mai 2018.	Considerăm termenul prevăzut unul rezonabil din considerentul că GDPR deja a intrat în vigoare, iar în anumite situații prevederile acestuia pot fi aplicate și în privința operatorilor naționali și, respectiv, acestora li se pot aplica sancțiuni din partea autorităților de supraveghere europene.
--	--	--	---	---

TABELUL
divergențelor rezultate din avizele prezentate de organizațiile non-guvernamentale referitor la
proiectul de lege privind aprobarea proiectului de lege pentru modificarea și completarea unor acte legislative

Nr. d/o	Denumirea instituției	Norma juridică la care sînt obiecții sau propuneri	Obiecția/propunerea formulată	Acceptare/argumentare neacceptări
1	Asociația Businessului European	art. 2	Propunerea de excludere a sintagmei <i>“intenția/inițierea de a prelucra și/sau”</i> pe motiv că o astfel de sintagmă nu există în Regulamentul General Protecție Datelor (GDPR)	Acceptat. A fost modificată după cum urmează: (1) <i>Prezenta lege se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.</i>
		art. 3	1. La noțiunea de <i>“operator”</i> s-a propus excluderea sintagmei <i>“intenționează să prelucreze”</i>, pe motiv că această sintagmă nu este prevăzută de GDPR. 2. La noțiunea de <i>“persoană împuternicită de operator”</i> s-a propus excluderea ultimei propoziții, or, acesta nu corespunde cu definiția expusă de GDPR. 3. La noțiunea <i>“destinatar”</i> s-a propus excluderea sintagmei <i>“prelucrarea acelor date de către acele autorități publice se va face în baza normelor aplicabile privind protecția datelor personale, conform scopului prelucrării”</i>. Prevederea dată dublează sensul în	1. Nu se acceptă. Nu are un substrat juridic. 2. Nu se acceptă. Ultima propoziție este o concretizare a noțiunii și nu influențează asupra sensului noțiunii expuse de GDPR. 3. Nu se acceptă. Nu este aplicată dublarea ci o concretizarea detaliată cu scopul de a evita interpretarea eronată. Prevederea în cauză nu este o dublare a normei din considerentul că face referire la autoritățile publice ce nu sunt considerate destinatari.

		fraza de mai sus: <i>“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”</i> 4. La noțiunea <i>“servicii ale societății informaționale”</i> s-a propus de a exclude cuvântul <i>“remunerare”</i>, or serviciile gartuite nu s-ar încadra în această definiție	4. Se acceptă. Noțiunea a fost expusă în următoarea redacție: <i>„servicii ale societății informaționale - înseamnă orice serviciu prestat la distanță, prin mijloace electronice și la solicitarea individuală a beneficiarului serviciului.</i>
	Art. 4	Propunerea excluderea lit, g), dat fiind faptul că prevederea dată nu este prevăzută în GDPR	Nu se acceptă. Norma nu contravine GDPR, a se vedea considerntul (10) și are drept scop de a atrage atenția că un anumit document conține date cu caracter personal și în privința lui urmează să fie aplicate măsuri de securitate respective.
	art. 5	Alin (1) lit. b) sintagma <i>“altele decât neexecutarea contractului”</i> se consideră că s-a avut în vedere <i>“altele decât executarea contractului”</i> , or, altele decât neexecutarea contractului presupune cele legate de executarea contractului cere deja sunt reglementate mai sus. Suplimentar s-a propus excluderea ultimei propoziții pe motiv că nu este prevăzută de GDPR.	Acceptat. A fost modificată după cum urmează:<i>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.</i>
	art. 7	S-a propus transferarea art. 7 La Capitolul III al prezentei norme	Nu se acceptă. Norma în cauză face referire la solicitarea de acces la informații ce conțin date cu caracter personal înaintată de alte

			persoane decît subiectul de date personale, pe cînd Capitolul III statuează drepturile subiecţilor de date personale în raport cu datele care îi vizează pe ei.
	art. 8	S-a propus la alin. (3) sintagma <i>“titularul răspunderii părinteşti”</i> urmează substituit cu <i>“reprezentantul legal”</i> în vederea uniformizării terminologiei utilizate în acest sens în Republica Moldova.	Acceptat. A fost modificată după cum urmează: (3) <i>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.</i>
	Art. 13	La alin. (2) s-a propus excluderea sintagmei <i>“cu aprobarea Centrului”</i> , or, ţinînd cont de obligaţia operatorului de a demonstra că prelucrarea datelor cu caracter personal este conformă, considerăm excesivă necesitatea aprobării termenilor de stocare de către Centru. Mai mult ca atît în contextul excluderii obligaţiilor de a notifica şi autoriza sistemele de evidenţă nu este clar care va fi procedura de aprobare din partea Centrului, precum şi această prerogativă a Centrului nu este prevăzută în proiectul legii privind CNPDCP	Acceptat. A fost modificată după cum urmează: (2) <i>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.</i>
	art. 18	1. alin. (1) lit. a), se propune de redactat în următoarea redacţie: <i>“identitatea şi datele de contact ale operatorului şi, după caz, ale reprezentantului acesteia”</i> – care este exact ca în	Nu se acceptă. 1. Subiectul de date urmează să cunoască informaţii depline cu privire la persoanele care îi prelucrează datele, inclusiv şi despre reprezentantul operatorului. Prevederea nu

		GDPR, or, redacția anterioară este excesivă în raport cu norma prevăzută de GDPR. 2. La alin. (2), lit. a) propunem excluderea sintagmei „<i>inclusiv și acțiunile întreprinse asupra acestora la atingerea scopurilor pentru care au fost prelucrate</i>” fiindcă GDPR nu prevede acest fapt. 3. Lit. b) din alin. (2) propunem să fie exclusă fiindcă dublează sensul din lit. c) și nu este prevăzut în GDPR. 4. La alin. (3) propunem substituirea sintagmei „<i>a recepționat această informație</i>” cu sintagma „<i>a fost informat</i>”, deoarece prin publicarea pe site-ul oficial nu poate fi demonstrată recepționarea.	contravine GDPR și are drept scop de a exclude interpretările eronate. 2. Nu se acceptă. Conținutul normei nu contravine GDPR doar aduce claritate pentru a protejarea datelor cu caracter personal. Astfel operatorul va fi obligat de a prezenta informația cu privire la datele cu caracter personal prelucrate la atingerea scopului (ca exemplu: arhivarea, distrugerea, transmiterea unui alt operator de date cu caracter personal). 3. Acceptat. Prevederile din art. 18 alin. (2) lit. b) și c) au fost redactate în corespundere cu GDPR. 4. Nu se acceptă. Conform alin. (1): <i>în cazul în care datele personale sunt colectate direct de la subiectul de date, operatorul sau persoana împuternicită de către operator are obligația să-i furnizeze gratuit următoarele informații.</i> Astfel, corelația directă cu subiectul de date, impune necesitatea informării la momentul colectării a datelor cu caracter personal, cu posibilitatea probării acestui fapt. Din acest considerent, simpla publicare nu garantează aducerea la cunoștință a informației transmise.
	art. 22	La alin. (3) propunem ca primul termen să fie de 30 de zile lucrătoare cu posibilitatea extinderii cu încă 15 zile lucrătoare, or, termenul inclus în proiectul de lege este prea mic, având în vedere că în anumite situații sunt implicați	Acceptat. Termenul a fost modificat fiind prevăzut o lună de zile.

		operatori asociați sau mai multe persoane împuternicite de operator.	
	art. 30	Prevederile alin. (3) și (5) sunt ambigue prin folosirea termenilor diferiți. Etimologia termenului de „coordonare” de la alin. (3), ca și a termenului de „consultare” de la alin. (4) nu implică adoptarea unui document de către Centru, fapt ce generează discordanță cu prevederile alin. (5), astfel, nefiind clare situațiile în care se solicită avizul Centrului. Propunem ca suportul acordat de Centru la crearea unui sistem informațional să fie un drept și nu o obligație a operatorului. În acest context, solicităm excluderea alin. (3) care nu este prevăzut în GDPR, iar în alin. (5) de a fi substituită sintagma „avizul Centrului” cu sintagma „În condițiile alin. (4), Centrul emite un aviz care”.	1. Alin. (4) și alin. (5) din art. 30 au fost reformulate: <i>„4) Autoritățile și instituțiile publice coordonează cu Centrul înainte de momentul conceperii și pe parcurs crearea oricărui sistem/registru de informații în care sunt prelucrate date personale. (5) Avizul Centrului în condițiile prezentului articol relevă conformitatea prelucrării la momentul examinării situației, care se emite în baza evaluării impactului asupra protecției datelor și a informațiilor și materialelor prezentate de către entitatea solicitantă. Atunci când se cere avizul Centrului, solicitantul prezintă:”</i>
	art. 31	1. S-a propus excluderea primei fraze din alin. (1) odată ce definiția de operator asociat care este prevăzută în art. 3 din proiect. 2. La alin. (2) s-a propus substituirea sintagmei ”Acordul” din a 2-a frază cu sintagma „Esența acordului”, deoarece acordul ar putea conține date comerciale confidențiale.	1. Acceptat. Fraza a fost exclusă. 2. Acceptat partial, fraza fiind completată la final cu cuvintele: „în caz contrar se va aduce la cunoștința acestuia doar esența acordului.”
	Art. 35	S-a propus substituirea sintagmei „50 de angajați” din alin. (5) cu sintagma „250 de angajați”, astfel cum este prevăzut în GDPR.	Neacceptată. Prin prezentul proiect de lege se transpune Regulamentului (UE) 2016/679. În acest sens remarcăm că potrivit prevederilor expuse la art. 35 alin. (5) norma în cauză este conformă

			dispozițiilor Regulamentului (UE) 2016/679, în conformitate cu care „<i>Obligațiile menționate la alineatele 1 și 2 nu se aplică unei întreprinderi sau organizații cu mai puțin de 250 de angajați, cu excepția cazului în care prelucrarea pe care o efectuează este susceptibilă să genereze un risc pentru drepturile și libertățile persoanelor vizate, prelucrarea nu este ocazională sau prelucrarea include categorii speciale de date, astfel cum se prevede la articolul 9 alineatul (1), sau date cu caracter personal referitoare la condamnări penale și infracțiuni, astfel cum se menționează la articolul 10.</i>” Totuși, avînd în vedere că în Republica Moldova puțini agenți economici dispun de un staff de personal mai mare de 250 angajați s-a mers pe formula <i>mai puțin de 50 de angajați</i>
	Art. 36	Alin. (2) și (3) urmează a fi exclus, or, conținutul acestora sunt identice cu prevederile art. 33.	Acceptată . Art. 36 a fost exclus, numărul de ordine fiind transmis următorului articol.
	Art. 37 (după modificări 36)	1. La alin. (1) se propune după sintagma „<i>dezvoltării tehnologice actual prelucrării</i>” de introdus sintagma „<i>costurile implementării și natura</i>”, racordând în acest sens prevederea cu GDPR. 2. La alin. (1) lit. I), urmează a fi definit ce înseamnă înregistrările de audit și de stabilit exact termenul de stocare de 12 luni, or extinderea acestui termen pentru o perioadă de până la 5 ani va genera costuri exagerat de mari pentru operatorii de date, mai mult ca atât această prevedere nu se regăsește în GDPR. Termenul de	1. Acceptat 2. Nu se acceptă. În prezent prevederi referitoare la durata stocării rezultatelor auditului securității în sistemele informaționale este prevăzut în Hotărîrea Guvernului nr. 1123 din 14.12.2010. Necesitatea prevederii unui asemenea termen este generată de cererile subiecților de date personale care solicită verificarea legalității prelucrării datelor ce îl vizează de anumiți operatori.

		12 luni urmează a fi stabilit și la art. 72 (69), or, nu este clar care este diferența dintre aceste două norme. 3. După alin. (5) se propune de completat o clauză adițională conform GDPR-ului, care a fost omisă: „<i>Aderarea la un cod de conduită aprobat sau la un mecanism de certificare aprobat, poate fi utilizată ca element prin care să se demonstreze îndeplinirea cerințelor prevăzute la alineatul (1) din prezentul articol.</i>”.	Prevederile art. 72 (69) sunt aplicabile organelor de ocrotire a legii, care nu sunt scutite de obligația de a respecta termenii generali stabiliți prin prezenta lege, în cazul în care nu sunt prevăzute excepții pentru ei. 3. Nu se acceptă. Propunerea înaintată se regăsește în art. 33, 45 și 47 din proiect.
	Art. 42 (41)	1. La alin. (1) cuvântul „<i>consultă</i>” a se înlocui cu sintagma „<i>poate consulta</i>”, or, GDPR nu stabilește o astfel de obligație, mai mult, se va aduce o claritate în raport cu această activitate. 2. La alin. (1) precum și pe tot textul proiectului propunem înlocuirea sintagmei „<i>Autoritatea de supraveghere</i>” cu sintagma „<i>Centru</i>”, pentru a exclude aparența precum că ar mai exista o autoritate responsabilă pe lângă Centru. 3. La alin. (2) este prevăzut un termen de consultare de cel mult opt săptămâni de la primirea cererii de consultare cu posibilitatea de a fi prelungit cu 6 săptămâni, nu este clar ce rămâne cu termenul de executare a unei obligații	1. Nu se acceptă. Nu are un substrat juridic. Norma corespunde art. 36 din GDPR 2. Acceptat 3 Acceptat.

		legale a operatorului ce presupune prelucrarea datelor prevăzută la art. 41 al proiectului de lege, care este unul mai restrâns de 8 săptămâni. Termenul de <i>"cel mult 2 luni"</i> se propune de modificat conform GDPR-ului la 1 luna. 4. Alin. (4) urmează a fi încadrat în alt articol, or, art. 41 se referă la operatorii de date cu caracter personal care intenționează să prelucreze datele cu caracter personal dar nu și la autoritățile publice care intenționează aprobarea unor acte normative.	3. Nu se acceptă Nu are un substrat juridic. Norma este aplicabilă tuturor operatorilor de date atât din sectorul privat, cât și sectorul public.
	Art. 43 (42)	La alin. (7) după cuvântul <i>"oficială"</i> prepoziția <i>"și"</i> urmează a fi completată cu prepoziția <i>"/sau"</i>, pentru că nu în toate cazurile operatorul de date deține în gestiune site web.	Nu se acceptă Paginile-web sunt un mecanism/instrument eficient de a informa subiectul de date, iar operatorul trebuie pe larg să-l valorifice.
	Art. 48-49 (47-48)	Propunem completarea/modificarea acestor articole în așa fel încât să fie clar din norma vizată activitatea ce se referă la certificarea și acreditarea entităților vizate.	Nu se acceptă. Normele sunt expuse explicit fiind conforme GDPR.
	Art. 72 (69)	Urmează a fi stabilit expres perioada de ținere a înregistrărilor de audit, în acest sens solicităm includerea termenului de 3 ani.	Nu se acceptă. Termenile de păstrare a înregistrărilor de audit sunt fixate în art. 36 alin (1) lit l): <i>înregistrările de audit al prelucrării datelor personale. Evidența evenimentelor și/sau acțiunilor înregistrate de sistemul de audit a securității în sistemele de date personale va fi păstrată pentru o perioadă de la 3 - 5 ani;</i>

		Art. 78 (75)	La alin. (5) propunem substituirea sintagmei „în termen în condițiile Codului de procedură civilă” cu sintagma „în termen aplicând prin analogie condițiile Codului de procedură civilă.” Conform art. 1 din Codul de procedură civilă, acesta reglementează raporturile ce derivă din înfăptuirea justiției de către instanțele judecătorești în cadrul unui proces civil. Fapt ce îl face inaplicabil altor relații civile. Propunem concretizarea că Codul de procedură civilă se va aplica prin analogie.	Nu se acceptă. Norma se referă la aprocadura de repunere în termen și nu contravine art. 116 Cod procedură civilă: <i>Repunerea în termen</i> (1) <i>Persoanele care, din motive întemeiate, au omis termenul de îndeplinire a unui act de procedură pot fi repuse în termen de către instanță.</i> (2) <i>Cererea de repunere în termen se depune la instanța judecătorească care efectuează actul de procedură și se examinează în ședință de judecată. Participanților la proces li se comunică locul, data și ora ședinței. Neprezentarea lor însă nu împiedică soluționarea repunerii în termen.</i> (3) <i>La cererea de repunere în termen se anexează probele ce dovedesc imposibilitatea îndeplinirii actului. Totodată, trebuie efectuat actul de procedură care nu a fost îndeplinit în termen (să fie depusă cererea, să fie prezentate documentele respective etc.).</i> (4) <i>Repunerea în termen nu poate fi dispusă decât în cazul în care partea și-a exercitat dreptul la acțiune înainte de împlinirea termenului de 30 de zile, calculat din ziua în care a cunoscut sau trebuia să cunoască încetarea motivelor care justifică depășirea termenului de procedură.</i> (5) <i>Încheierea judecătorească prin care este respinsă cererea de repunere în termen poate fi atacată cu recurs. Încheierea prin care s-a făcut repunerea în termen nu se supune recursului.</i>
		Art. 81 (78)	1. În textul acestui articol urmează a fi stabilit expres că accesul inspectorului precum și desfășurarea controlului se efectuează cu acordul operatorului, dacă nu există mandatul judecătoresc în acest sens.	1. Se acceptă, astfel art. 78 alin. (1) prevede: (18) <i>Accesul reprezentanților Centrului în domiciliu, în sediu sau alte încăperi, terenuri și mijloace de transport, echipamentele de prelucrare, la programele și aplicațiile, precum și la documentele, înregistrările referitoare la prelucrarea de date personale, ce aparțin, sînt în posesie sau în folosința persoanei la care se efectuează investigația, în lipsa acceptului scris, se permite numai în baza mandatului judiciar</i>

			emis în condițiile prezentului articol și prezentat persoanei supuse investigației. Totodată, alin. (6) din același articol statuează că: (6) Decizia privind efectuarea investigației la fața locului se aduce la cunoștință sub semnătură persoanei, entității supuse investigației, sau reprezentantului legal. În cazul refuzului primirii și semnării deciziei se întocmește un act, în prezența unui martor sau în cazul înregistrării video și audio, în care se consemnează acest fapt. 2. La alin. (9) lit. d) propunem completarea cu sintagma „fără a bloca activitatea operatorului”. 2. Nu se acceptă din considerentul că măsura vizată are drept scop de a opri prelucrarea ilegală a datelor cu caracter personal. Totodată, activitatea operatorului poate fi blocată doar în măsura în care este necesar pentru efectuarea investigațiilor. d) să sigileze încăperile și mijloacele, unde și prin care se efectuează prelucrarea datelor personale, mijloacele, sistemele de evidență și documentele aferente obiectului și scopului investigației, <u>pe perioada și în măsura în care este necesar pentru desfășurarea investigației;</u> 3. La alin. (9) lit. e) urmează a fi indicat expres că înregistrarea video/audio se va efectua cu informarea prealabilă a entității supuse investigației. 3. Acceptat 4. Cu privire la alin. (18)-(23) comunicăm că conform art. 428 alin. (2) din Codul contravențional, perchezițiile se efectuează doar în baza autorizației judecătorului de instrucție. În acest sens, proiectul de lege nu aduce modificări 4. Nu se acceptă. În cazul normelor invocate nu se aplică prevederile Codului contravențional.	
--	--	--	--	--

		la Codul contravențional pentru a face aplicabile prevederile alin. (18) – (23) și altele care prevăd termenul de <i>"mandat judecătoresc"</i>. Considerăm oportună ca, efectuarea perchezițiilor în lipsă consimțământului persoanei investigate să se facă cu autorizarea judecătorului de instrucție în cazul în care sub termenul de <i>"mandat judecătoresc"</i> se înțelege <i>"autorizarea judecătorului de instrucție"</i>, astfel, considerăm necesară clarificarea acestui fapt care creează confuzie atât pentru operatori cât și pentru instanțele de judecată care vor fi în imposibilitate să emită un document neprevăzut de legea procesuală. 5. Termenul de 2 ani stabilit la alin. (25) este excesiv. De asemenea, nu sunt prevăzute criteriile care ar determina/justifica durata investigației, ceea ce poate duce la abuzuri din partea autorității și imixtiune în activitatea operatorului. Propunem reducerea acestui termen la 6 luni. 6. Ținând cont de faptul că directorul-adjunct este membru al personalului Centrului, considerăm că lipsește garanția unui control independent. Propunem completarea alin. (26) cu sintagma „și instanța de judecată”.	5. Nu se acceptă. Cazurile investigate de Centru sunt complexe, în cadrul cărora se întreprind măsuri de audieri a persoanelor implicate, de solicitare a informațiilor pentru a acumula probe suficiente, astfel reprezentanții Centrul întreprind măsuri similare organelor de urmărire penală. Reieșind din practica Centrului acesta este un termen rezonabil. 6. Acceptat
--	--	---	--

			7. Alin. (27) propunem expunerea în următoarea redacție: „(27) Dacă la scurgerea termenului de 6 luni, Centrul nu are acumulate probe suficiente pentru a aprecia cu certitudine existența sau lipsa încălcării, efectuarea investigației se suspendă pe termen maxim de 3 luni, cu informarea subiectului de date, care a depus cererea. Reluarea examinării investigației poate avea loc în intervalul acestui termen, cu condiția apariției probelor noi ce sunt pertinente și concludente pentru soluționarea cazului.”.	7. Nu se acceptă. Obiecția a fost expusă la punctul 5.
		Art. 84 (81)	La alin. (8) nu este stipulat timpul de păstrare a materialelor de investigație, în acest sens propunem a stabili termenul de 10 ani.	Acceptat.
		Art. 85 (82)	1. La alin. (2), lit. d) considerăm că este folosit incorect termenul de „a impune lipsa încălcării”. Propunem modificarea acestuia cu sintagma „poate dispune separat sau cumulativ lipsa încălcării”. 2. La alin. (3) urmează a fi stabilite expres situațiile sau criteriile în care inspectorul va fi în drept de a semna decizii.	1. Nu se acceptă. Conform alin (2) lit. d): <i>În funcție de rezultatul și de faptele constatate în cadrul investigației, Centrul prin decizie poate impune separat sau cumulativ următoarele: d) lipsa încălcării.</i> Norma prevede că centru printr-o decizie costată lipsa încălcării. 2. Nu se acceptă. Asemenea situații/prerogative vor fi stabilite prin ordinul directorului, în conformitate cu redacția modificată a alin. (3) din acest articol. (3) Deciziile emise de Centru în rezultatul investigațiilor efectuate se semnează de către directorul Centrului sau de directorul adjunct, șeful/șeful adjunct al direcției generale, șeful/șeful adjunct al direcției sau inspectorul de protecție

				care a efectuat investigația, dacă aceștea dispun de o astfel de prerogativă stabilită prin ordinul directorului.
		Art. 86 (83)	La art. 86 (83) urmează a fi stabilit expres că odată cu contestarea actelor administrative emise de Centru, caracterul executoriu al acestora se suspendă.	Nu se acceptă avînd în vedere că art. 86 alin. (4) statuează deja situațiile de suspendare a deciziilor Centrului: <i>(4) Prin derogare de la prevederile Legii contenciosului administrativ nr. 793-XIV din 10 februarie 2000, pînă la soluționarea definitivă a cauzei, executarea deciziilor Centrului nu poate fi suspendată, cu excepția cazurilor în partea ce vizează aplicarea sancțiunilor pecuniare, dispunerea distrugerii sau ștergerii datelor personale sau în cazul în care prejudiciul ar putea depăși interesul privat sau public urmărit.</i>
		Art. 87 (84)	Propunem a fi completat acest articol, fiind menționat expres că citarea poate avea loc doar în cadrul investigației inițiate.	Neacceptată. Nu are un substrat juridic și relevanță.
		Art. 89 (86)	1. Considerăm necesar de a stabili expres că toate actele administrative emise de Centru pot fi contestate la Curtea de Apel Chișinău. Totodată propunem reformularea alin. (2), ca în cazul emiterii/semnării actelor administrative de către angajații Centrului să fie necesară procedura prealabilă prin contestarea actului la conducătorul ierarhic superior. 2. Conform alin. (4), „ <i>executarea deciziilor Centrului nu poate fi suspendată, cu excepția</i>	Norma a fost reformulată (2) În condițiile alin. (1), contestația în privința actului administrativ poate fi depusă în termen de 10 zile din momentul aducerii la cunoștință a deciziei. Conducătorul ierarhic superior va examina contestația în termen de 30 de zile lucrătoare. În cazul în care actul administrativ se contestă direct în instanța de judecată sau după ce contestația a fost examinată de conducătorul ierarhic superior, cererea urmează a fi depusă la Curtea de Apel Chișinău.

			cazurilor în partea ce vizează aplicarea sancțiunilor pecuniare, dispunerea distrugerii sau ștergerii datelor personale sau în cazul în care prejudiciul ar putea depăși interesul privat sau public urmărit”, în acest context nu este clar cum corelează această normă cu prevederile art. 6 și art. 114 din Constituția Republicii Moldova care prevăd separația și colaborarea puterilor în stat și faptul că justiția se înfăptuiește în numele legii numai de instanțele judecătorești, respectiv verificarea legalității aplicării suspendărilor ține de competența exclusivă a instanțelor judecătorești, iar scoaterea de sub spectrul posibilităților instanței a dreptului de a suspenda deciziile CNPDCP aduce atingere normelor suscitute, în special în cazul când se urmărește prevenirea unei pagube iminente (în cazul în care paguba nu întrunește condițiile de depășire a intereselor private sau publice). Exemplu: un număr nedeterminat de persoane depune o plângere la Centru împotriva unui operator privind încălcarea regimului confidențialității (ceea ce presupune un interes public enorm) CNPDCP dispune suspendarea activităților operatorului care implică un prejudiciu de 300 000 EUR pe zi, în cazul în care instanța nu poate anula decizia de suspendare și în rezultat se constată că nu a fost încălcat regimul de confidențialitate, va repara CNPDCP (persoana responsabilă din cadrul Centrului) operatorului prejudiciul cauzat, în cazul în care nu,	1. Neacceptată. În cazul aplicării sancțiunilor pecuniare este prevăzută suspendarea executării deciziilor Tototodă reliefăm că în conformitate cu art. 21 alin. (1) și (2) al Legii Nr. 793 din 10.02.2000 contenciosului administrativ, suspendarea executării actului administrativ contestat nu este un drept absolut ci urmează a fi demonstrat după cum urmează: (1) <i>Suspendarea executării actului administrativ contestat poate fi solicitată de către reclamant instanței de contencios administrativ concomitent cu înaintarea acțiunii.</i> (2) <i>În cazuri temeinic justificate și în scopul prevenirii unei pagube iminente, instanța poate dispune suspendarea actului administrativ și din oficiu.</i> În aceste împrejurări alin. (4) stabilește expres cazurile prin care se permite aplicarea suspendării executării actelor administrative. Mai mult ca atât CNPDC este unica instituție din RM care efectuează controlul asupra conformității prelucrării datelor cu caracter personal, fapt ce presupune emiterea unor decizii neabuzive, legale, obiective etc. În cazul în care persoana consideră că Centru i-a lizat drepturile, potrivit art. 1 al Legii Nr. 793 din 10.02.2000 contenciosului administrativ: (1) <i>Contenciosul administrativ ca instituție juridică are drept scop contracararea abuzurilor și exceselor de putere ale autorităților publice, apărarea drepturilor persoanei în spiritul legii, ordonarea activității autorităților publice, asigurarea ordinii de drept.</i> (2) <i>Orice persoană care se consideră vătămată într-un drept al său, recunoscut de lege, de către o autoritate publică, printr-un act administrativ sau prin nesoluționarea în termenul legal a unei cereri, se poate adresa instanței de contencios administrativ competente pentru a obține anularea actului, recunoașterea dreptului pretins și repararea pagubei ce i-a fost cauzată.</i>
--	--	--	--	---

			considerăm că această atribuție a instanțelor judecătorești urmează a fi neatinsă.	
		Art. 90 (87)	Alin. (1) <i>„Orice subiect de date are dreptul de a depune o cerere direct în instanța de judecată, dacă pretinsa încălcare s-a desfășurat în Republica Moldova, fără a aduce atingere drepturilor și atribuțiilor Centrului”,</i> alin. (2) al aceluiași articol prevede următoarele: <i>„În cazul în care cererea se referă la exercitarea drepturilor subiecților de date prevăzute în Capitolul III, această cerere va fi inițial înaintată operatorilor de date în condițiile legii. În cazul în care subiectul de date nu primește un răspuns din partea operatorului în timpul stabilit conform Capitolului III sau în cazul în care răspunsul sau acțiunile întreprinse de operator sunt considerate inadecvate sau nu rezolvă cererea, subiectul de date poate, în termen de 30 zile din momentul când a primit răspunsul sau trebuia să primească răspunsul să depună o cerere în instanța de judecată”,</i> totodată conform art. 78 alin. (2) <i>„În cazul în care cererea se referă la exercitarea drepturilor subiecților de date prevăzute în Capitolul III, această cerere va fi inițial înaintată operatorilor de date în condițiile legii. Dacă subiectul de date nu primește un răspuns din partea operatorului în termenii stabiliți conform Capitolului III sau atunci când răspunsul sau acțiunile întreprinse de operator sunt considerate inadecvate sau nu rezolvă cererea, subiectul de date poate, în</i>	Norma este în corespundere cu art. 79 din GDPR.

			<i>termen de 30 zile din momentul când a primit răspunsul sau trebuia să primească răspunsul, depune o cerere la Centru”, reieșind din normele citate supra, reiese o vădită neconcordanță între căile de atac asupra cererii depuse de către persoanele interesate, ceea ce influențează cu certitudine la termenele de prescripție de adresare autorităților competente în vederea apărării drepturilor persoanelor interesate, scurgerea cărora implică imposibilitatea apărării.</i>	
		Art. 92 (89)	1. Articolul conține sintagma „<i>răspunderea administrativă</i>” în această ordine de idei, este necesar de a elucida dacă răspunderea prevăzută de acest articol, survine în aceeași ordine și procedură ca răspunderea contravențională sau nu, în cazul în care nu trebuie descrisă în lege procedura de aplicare examinare și contestare, precum și includerea anumitor garanții față de persoanele atrase la răspundere după cum conține spre exemplu (deși nu pe deplin) în Legea concurenței nr. 183 din 11.07.2012 art. 49 -92. 2. Alin. (2) lit. l) urmează a fi exclusă pe motiv că nu se regăsește în GDPR. 3. La alin. (4), considerăm că sancțiunile prevăzute sunt unele excesive având în vedere puterea de cumpărare a cetățenilor și veniturile persoanelor juridice. Din acest motiv, considerăm necesar ajustarea sancțiunilor realităților pieței Republicii Moldova, inclusiv	1. Nu se acceptă . Sintagma „<i>răspunderea administrativă</i>” este conform cerințelor legale. Răspunderea administrativă este o procedură separată de răspunderea contravențională. De altfel, obiecția invocată nu este clară. 2. Neacceptată Remarcăm faptul că norma este prevăzută în art. 83 din GDPR. 3. Acceptată parțial, mărimea sancțiunii a fost modificată - 250 000 EUR.

		stabilirea acestora în lei, deoarece pe teritoriul Republicii Moldova toate relațiile comerciale se efectuează în moneda națională. Considerăm că echivalentul sancțiunii de 250 000 EUR (5 000 000 lei) este suficient pentru a determina la neîncălcarea legii pe viitor. Propunem excluderea sancțiunii suplimentare cu „4 % din cifra de afaceri mondială totală anuală”. 4. Lipsește definiția <i>”cifra de afaceri mondială totală anuală”</i>. Conținutul alineatului nu prevede clar obligațiile pentru încălcarea cărora survine răspunderea pecuniară. În special, lit. a) face trimitere la un set de articole, din conținutul cărora nu rezultă o obligație de executare. De exemplu, art. 10 alin. (2) prevede că operatorul nu este ținut de obligația de neidentificare. Identificarea subiectului este lăsată la latitudinea operatorului, exact ca și certificarea prevăzută la art. 48 alin. (2) din proiectul legii. Considerăm abuzivă sancționarea operatorului pentru că nu a beneficiat de dreptul de fi certificat; 5. La alin. (7) nu este clar definit termenul de <i>„încălcare minoră”</i>, pentru a asigura previzibilitatea legii, considerăm oportună definirea termenului sau exemplificarea.	4. Neacceptată Definirea sintagmei <i>”cifra de afaceri mondială totală anuală”</i>, este pertinentă. Norma corespunde GDPR, Norma a fost interpretată greșit, remarcăm că potrivit prevederilor proiectului de lege nu survine sancționarea în cazul în care operatorul nu a beneficiat de dreptul de a fi certificate, dar în cazurile în care nu au fost respectate condițiile certificării. 5. Neacceptată În baza explicațiilor expuse de dexonline.ro, <i>minor- lipsit de importanță, neînsemnat, secundar</i>. Interpretare uniformă care nu poate prejudicia conținutul normei.
--	--	--	---

		Art. 94 (91)	1. La alin. (1) obligațiunea de a vărsa 25% în bugetul Centrului ar putea fi interpretat ca o motivație de a aplica sancțiuni pecuniare, mai ales în baza criteriului cifrei de afaceri. 2. La alin. (2) propunem să fie completat cu sintagma „<i>cu excepția cazului în care executarea deciziei a fost suspendată</i>”. 3. La alin. (3) propunem de a stabili expres obligația de a publica toate deciziile emise cu excepția datelor cu caracter personal care urmează a fi anonimizate. Mai mult, considerăm necesar ca datele ce vizează funcționarii publici, persoanele publice sau în cazul unor situații de interes public deciziile să fie publicate integral. 4. Propunem completarea articolului cu un nou alineat după cum urmează - ”(6) În dependență de mărimea amenzii pecuniare aplicate și de situația financiară a persoanelor vizate în decizia de sancționare, Centrul poate dispune/admite eşalonarea amenzii pe un termen	1. Neacceptată Nu are un substrat juridic și obiectivitate. În urma acumulării unor resurse financiare suplimentare, Centrul va avea posibilități mai ample în vederea implementării politicii în domeniul protecției datelor cu caracter personal ca exemplu: angajarea experților din domeniul, efectuarea vizitelor cu scopul schimbului de experiență, dotarea tehnico-materială a Centrului, organizarea instruirilor etc. În privința abuzului, Centrul nu este lipsit de controlul din partea Parlamentului precum și jurisdicțional. Suplimentar, remarcăm că asemenea procedură este prevăzută în activitatea mai multor autorități, spre exemplu a MAI. 2. Completarea nu este necesară din considerentul că excepția este clară și se subînțelege din normele menționate mai sus (art. 86 alin. (4) din proiect). 3. Neacceptată Acțiuni ce vor implica cheltuieli majore, mai mult ca atât această informație la necesitate se poate de obținut în conformitate cu Legea Nr. 982 din 11.05.2000 privind accesul la informație. 4. Nu se acceptă din considerentul că în dispozițiile tranzitorii ale proiectului autorul a prevăzut un mecanism treptat de aplicare a sancțiunilor de Centru pentru fiecare an de la intrarea în vigoare a prezentei legi.
--	--	--------------	--	--

			de pînă la 5 ani cu condiția achitării în prima tranșă a 25% din amendă.”	
		Art. 99 (96)	La alin. (5) propunem a fi modificat ca legea să intre în vigoare în termen de 6 luni din momentul adoptării, iar sancțiunile să fie aplicabile după 2 ani – perioadă în care se vor aplica sancțiunile existente în Codul contravențional. Modificările propuse sunt esențiale pentru mediul de afaceri care conștientizează importanța și necesitatea acestor prevederi, totodată termenul de 2 ani pentru aplicarea sancțiunilor ar fi unul corespunzător inclusiv din perspectiva GDPR care a intrat în vigoare după 2 ani din momentul adoptării.	Nu se acceptă Sancțiunea precaută prevenirea încălcării legislației, lipsa sancțiunii va genera sporirea ilegalității ce este inadmisibil. Pentru amortizarea trecerii de la pedeapsă contravențională la pedeapsa administrativă s-a propus o etapă de tranziție prin care sancțiunile se vor aplica în volum redus. Considerăm că data prevăzută pentru intrarea în vigoare a legii - 01 martie 2019 un termen rezonabil.
		Suplimentar	Suplimentar propunem suplینirea proiectului de lege cu un articol în care să fie prevăzută reprezentarea subiectului de date de către un organism sau asociație fără scop lucrativ în conformitate cu prevederile art. 80 din GDPR. Considerăm că această propunere trebuie să vină din partea societății civile, mai ales că conținutul acestui articol la nivel național poate lua diferite forme și abordări, care în prealabil ar trebui supuse unei analize și discuții publice. Spre exemplu alin. (2) al art. 80 din GDPR prevede posibilitatea inițierii plângerilor fără existența mandatului persoanei vizate: <i>(2) Statele membre pot prevedea că orice organism, organizație sau asociație menționată la alineatul (1) din prezentul articol, independent de mandatul unei persoane vizate, are dreptul de</i>	La momentul actual o astfel de implementare nu este posibilă din motivul că necesită un studiu separat, care în viitor ar putea să se regăsească printr-un articol în proiectul nominalizat. Fapt ce poate fi introdus suplimentar după aprobarea prezentului proiect, mai mult ca atât această propunere nu influențează implementarea dispozițiilor proiectului.

			<i>a depune în statul membru respectiv o plângere la autoritatea de supraveghere care este competentă în temeiul articolului 77 și de a exercita drepturile menționate la articolele 78 și 79, în cazul în care consideră că drepturile unei persoane vizate în temeiul prezentului regulament au fost încălcate ca urmare a prelucrării.</i>	
2	Camera de Comerț Americană din Moldova	Art.1	Considerăm că expunerea de către autor a întregului text a unei legi într-o redacție nouă, în cadrul unei legi de modificare și completare a mai multor acte legislative, reprezintă o încălcare a esenței de modificare a unui act legislativ. Totodată, aceasta încalcă prevederile Legii nr.11 din 22.12.2017 cu privire la actele normative, care stabilesc cum trebuie să fie operate modificările și completările la actele legislative. Prin urmare, autorul: - fie trebuie să formuleze modificările și completările pentru fiecare articol/secțiune/capitol aparte și ulterior să dispună republicarea legii (conform art. 41 alin. (3) din legea sus menționată, republicarea este obligatorie dacă actul legislativ a suferit modificări esențiale (a peste o treime din articole); - fie trebuie să vină cu o lege nouă, separată.	Propunerea se va lua în considerare.
		Art. 2	1. S-a constatat, că art. 2 alin. (1) din proiectul de modificare a Legii nr. 133/2011 deviază semnificativ de la domeniul de aplicare	1. Acceptată parțial. A fost modificată după cum urmează: (1) Prezenta lege se aplică prelucrării datelor cu caracter personal, efectuată total

		material stabilit în art. 2 (1) din Regulamentul 2016/679, prin reglementarea intenției de prelucrare a datelor precum și a mijloacelor de prelucrare utilizate sau intenționate a fi utilizate la prelucrare. Astfel, propunem modificarea art. 2 (1) din Legea nr. 133/2011 și expunerea acestuia în corespundere cu art. 2 alin. (1) și (4) din Regulamentul 2016/679: „(1) <i>Prezenta lege se aplică prelucrării datelor cu caracter personal, efectuată total sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate, a datelor cu caracter personal care fac parte dintr-un sistem de evidență sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor. Prezenta lege nu aduce atingere aplicării Legii nr. 284-XV din 22.07.2004 privind comerțul electronic, în special a normelor privind răspunderea furnizorilor de servicii, prevăzute la art. 14-17 din Legea nr. 284/2004.</i>” 2. S-a propus modificarea art. 2 alin. (2) lit. a) din proiect, conform art. 3 alin. (1) din Regulamentul 2016/679: „a) prelucrării datelor cu caracter personal în cadrul activităților unui sediu al unui operator sau unei persoane împuternicite de operator pe teritoriul Republicii Moldova, indiferent dacă prelucrarea are loc sau nu pe teritoriul Republicii Moldova.” 3. Propunem înlocuirea cuvântului „informațiilor” cu sintagma „datelor cu caracter personal”, dat fiind faptul că prezenta Lege reglementează regimul juridic al datelor cu	<i>sau parțial prin mijloace automatizate, precum și prelucrării prin alte mijloace decât cele automatizate a datelor cu caracter personal care fac parte dintr-un sistem de evidență a datelor sau care sunt destinate să facă parte dintr-un sistem de evidență a datelor.</i> Totodată, remarcăm că furnizorii de servicii electronice nu pot fi exceptați de la prezenta lege avînd în veder că în activitatea lor se prelucrează un volum mare de date cu caracter personal. Mai mult asemenea excepții nu au fost prevăzute nici prin Convenția nr. 108 și ni de către GDPR. Totodată considerăm că Legea privind comerțul electronic este învechită și urmează a fi adaptată noilor rigori. 2. Nu se acceptă, norma nu contravene GDPR. 3. Acceptat.
--	--	---	---

			caracter personal, dar nu al informațiilor în general.	
		Art. 3	1. <i>date cu caracter personal</i> (în continuare <i>date personale</i>) această noțiune urmează a fi adusă în corespundere cu Regulamentul 2016/679. Pentru asigurarea aplicării corecte a normelor transpuse, este imperios necesar ca <u>noțiunile de bază</u> utilizate în Legea nr. 133/2011 să corespundă cât mai exact definițiilor din Regulamentul 2016/679, exceptând doar situațiile justificate de faptul că R. Moldova nu este stat membru al UE. 2. <i>Categoria specială de date personale</i> Această prevedere este în contradicție cu dispozițiile GDPR-ului care nu definește datele personale referitoare la condamnări și infracțiuni în calitate de categorie specială de date cu caracter personal și ar putea crea impedimente în activitatea agențiilor de aplicare a legii. Recomandăm elaborarea unui articol separat pentru a determina condițiile de prelucrare a datelor cu caracter personal referitoare la condamnări penale și infracțiuni.	1. Neacceptată. Noțiunea nu contravine GDPR doar este redată într-o formă mai clară, ulterior definind separat noțiunile de <i>categoria obișnuită de date personale</i> și <i>categoria specială de date personale</i> 2. Nu se acceptă. din considerentul că datele personale referitoare la condamnările penale, măsurile procesuale de constrângere sau sancțiunile contravenționale necesită un nivel mai ridicat de protecție prin aplicarea măsurilor specifice și adecvate pentru a proteja drepturile fundamentale și datele cu caracter personal ale persoanelor fizice. Astfel, se impune necesitatea de a menține sau de a introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea acestor date. Totodată, atât GDPR, cât și Directiva 2016/680 oferă posibilitatea statelor, în anumite situații, de a introduce reglementări speciale în ce privește prelucrarea datelor personale. Norma corespunde cu art.10 din GDPR. Suplimentar remarcăm prevederile art. 9 lit. g) g) prelucrarea este efectuată de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, cu condiția ca aceasta să se efectueze cu respectarea drepturilor subiectului datelor

			3. <i>operator</i> – se propune substituirea noțiunii după cum urmează: <i>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 mijloacele de prelucrare a datelor personale.”</i> Pentru asigurarea aplicării corecte a normelor transpuse, este imperios necesar ca <u>noțiunile de bază</u> utilizate în Legea nr. 133/2011 să corespundă cât mai exact definițiilor din Regulamentul 2016/679, exceptând doar situațiile justificate de faptul că R. Moldova nu este stat membru al UE. 4. <i>servicii ale societății informaționale</i> - Noțiunea ”servicii ale societății informaționale” propunem să fie definită cu referire la art. 4 din Legea nr. 284-XV din 22.07.2004 privind comerțul electronic. Pentru asigurarea aplicării corecte a normelor transpuse, este imperios necesar ca <u>noțiunile de bază</u> utilizate în Legea nr. 133/2011 să corespundă cât mai exact definițiilor	personale și a celorlalte cerințe și garanții prevăzute de prezenta lege. Orice registru care conține date personale în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor se ține doar de către o autoritate de stat investită cu acest drept. 3. Neacceptată Noțiunea corespunde GDPR. 4. Noțiunea a fost redactată.
--	--	--	---	--

			din Regulamentul 2016/679, exceptând doar situațiile justificate de faptul că R. Moldova nu este stat membru al UE. 5. <i>marketing direct (prospectare comercială)</i> intenția autorului proiectului de lege este de a califica ca și sinonime marketingul direct și prospectarea comercială. În practică, de fapt, există diferențe între aceste două noțiuni, în special în partea ce ține de scopurile urmărite. Dacă marketingul direct urmărește generarea unei reacții cuantificabile, atunci prospectarea comercială se poate limita doar la scopul de informare și comunicare cu consumatorul/clientul. Prin urmare, propunem excluderea sintagmei „(prospectare comercială)”, astfel încât definiția din art. 3 a proiectului de lege să se refere doar la marketing direct.	5. Din considerentul că atât marketing-ul direct, precum și prospectarea comercială utilizează în mod inevitabil prelucrarea datelor cu caracter personal a subiecților de date, noțiunea urmează a fi păstrată. Totodată, noțiunea a fost reformulată în „<i>marketing direct și prospectare comercială</i>” Noțiunile <i>marketing direct și prospectare comercială</i> au la bază scopul de a utiliza date. <i>Marketing direct</i> presupune o formă de publicitate care se adresează unui set de ținte bine definit cu scopul de a genera un rezultat măsurabil, folosind instrumente media adresabile, ca poșta sau e- mailul. <i>prospectare comercială</i> - cercetări de piață cu scopul de stabilirea unei baze pentru deciziile de marketing ce trebuie luate conform procedurilor formale constituite pe principiul folosirii metodelor științifice pentru a asigura calitatea acestor informații.
		Art. 4	S-a propus excluderea art. 4 alin. 1 lit. g) din proiectul de lege, deoarece: • este contrară principiilor stabilite exhaustiv în art. 5 al Regulamentului 2016/679, • de fapt nu este un principiu general, ci este o obligație concretă, excesivă și costisitoare impusă în sarcină	Neacceptată. Este o cerință pentru asigurarea securității prelucrării datelor cu caracter personal, mai mult ca atât forma și modalitatea de marcă va fi stabilite de Guvern. Remarcăm faptul că marcarea nu necesită costuri suplimentare din partea operatorului, iar potrivit prevederilor proiectului lipsa marcajului este calificată ca o încălcare minoră.

			operatorilor, pentru neexecutarea căreia fiind stabilite sancțiuni exorbitante.	
		Art. 5	1. Propunem excluderea din art. 5 alin. 1 lit. b) al proiectului a următoarei sintagme: „<i>Transmiterea datelor personale, altele decât cele legate de neexecutarea contractului, către un alt operator sau persoană împuternicită de către operator, poate avea loc doar cu condiția existenței consimțământului subiectului de date, în condițiile expres prevăzute de lege.</i>”, deoarece aceasta instituie o restricție abuzivă și contrară prevederilor art. 6 din Regulamentul 2016/679. De exemplu, în practică această restricție <u>va face imposibilă</u> prelucrarea datelor personale de către operator (în baza temeiului legal prevăzut de art. 5. alin. 1 lit. b) <u>prin intermediul unor persoane împuternicite</u>, cu excepția cazurilor de neexecutare a contractului, fapt care va restricționa în mod abuziv și nejustificat activitățile economice legale ale companiilor din Moldova. Cerințele menționate mai sus modifică prezumția temeiurilor legale de prelucrare a datelor cu caracter personal prevăzute în GDPR și contravin regulilor privind alte temeiuri legale, prelucrări ulterioare în alte scopuri și cerințelor stabilite în articolul 5 alin. (2) din proiectul de lege. 2. S-a propus excluderea art. 5 alin. (3) și (4) din proiect, deoarece aceste prevederi sunt pe	1. Acceptată. S-a modificat: b) <i>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.</i> 2. Neacceptate.

			de o parte vagi, iar pe de altă parte nu sunt necesare, deoarece condițiile de aplicare a legii sunt deja reglementate în art. 2. În plus, vis-a-vis de alin. (4) al art. 5, atenționăm că alte <u>legi speciale</u> (nu doar Legea 133/2011) stabilesc condiții de prelucrare a datelor personale. La fel, condițiile survenirii răspunderii disciplinare, civile, contravenționale și penale sunt reglementate expres de legile speciale respective și nu de Legea nr. 133/2011.	Alin. (3) intervine cu o explicație suplimentară care nu a fost expusă în art. 2 al prezentului proiect. Alin (4) reglementează expres: <i>pentru refuzul de a efectua prelucrarea ilegală a datelor personale nu poate surveni răspundere disciplinară, civilă, contravențională sau penală.</i> Legea nr. 133 este o lege organică care conține norme generale în domeniul protecției datelor cu caracter personal, în cazul conflictului de norme se vor aplica prevederile Legii 780 din 27.12.2001 privind actele legislative.
		Art. 8	S-a solicitat excluderea art. 8 alin. (5) care stabilește faptul că consimțământul nu are efect retroactiv, deoarece această restricție nu este prevăzută de Regulamentul 2016/679, totodată legislația civilă reglementează aspectele privind efectele actelor juridice.	Nu se acceptă. Norma aduce claritate pentru evitarea interpretării eronate și nu contravine legislației civile. Faptul că nu este prevăzut de GDPR nu este un argument plauzibil, GDPR oferă posibilitatea statelor, în anumite situații, de a introduce reglementări speciale în ce privește prelucrarea datelor personale.
		Art. 11	Se solicită excluderea alin. (3) și alin. (4) al art. 11 din proiect deoarece sunt restrictive, nu țin seama de toate tipurile de prelucrări (de ex. on-line) și pot bloca activitatea operatorilor legată de prestarea serviciilor la distanță. De exemplu, art. 11 alin. (3) nu poate fi aplicat în cazul prestării serviciilor societății informaționale, deoarece în asemenea cazuri nu poate fi efectuată identificarea subiectului prin prezentarea unui act original.	Neacceptată. În cazul prestării serviciilor prin intermediul sistemelor electronice se aplică prevederile Legii Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic. Exemplul dat de CCAM nu este relevant. Nu se poate cunoaște cu certitudine că persoana care a transmis on/line documentul de identitate este titularul acestui document.

		Art. 13 1. GDPR-ul prevede că stabilirea unor termene pentru stocarea și utilizarea datelor cu caracter personal constituie obligația operatorului. În cazul în care operatorul este o autoritate publică, termenele trebuie să fie prevăzute într-un act legislativ. GDPR-ul nu prevede obligația autorității pentru protecția datelor de a aproba toate condițiile și termenele pentru stocarea și utilizarea datelor cu caracter personal. Potrivit articolului din proiectul de lege, Centrul va aproba condițiile și termenele pentru stocarea și utilizarea datelor cu caracter personal pentru toți operatorii. Trebuie remarcat faptul că aceasta constituie o povară administrativă pentru operatori, fiind similară cu procedura de înregistrare, care a fost exclusă din GDPR. La art. 13 alin. (2) se propune excluderea sintagmei „..., cu aprobarea Centrului”, deoarece reieșind din cerințele art. 4 alin. (1) lit. e), operatorul urmează să stabilească condițiile și termenele de stocare/utilizare a datelor. 2. Se Propune modificarea normei în următoarea redacție: alin 3 lit. „b) transformate în documente de arhivă și stocate în conformitate cu prevederile legislației în vigoare...”. Se argumentează prin faptul că, nu doar legislația din domeniul arhivelor poate prevedea careva termene specifice de păstrare a informației. De	1. Acceptată. S-a modificat alin. (2): <i>În cazul în care legislația nu prevede în mod expres condițiile și termenele pentru stocarea și utilizarea datelor personale, ele sunt stabilite de către operator. Operatorii autorități și instituții publice consultă Centrul privind termenele pentru stocarea și utilizarea datelor personale.</i> 2. Neacceptată. Nu are un substrat juridic, norma face referire la domeniul de aplicare și nu la legea exactă. Exemplul adus nu este relevant, atragem atenția că norma vizează documentul de arhivă care conține date cu caracter personal care deja și-au atins scopul prelucrării. Totodată, remarcăm faptul că Legea nr. 190 din 26.07.2007 a fost abrogată, iar noua Lege cu privire la prevenirea și
--	--	---	--

			exemplu, potrivit art. 7 din Legea nr. 190 din 26.07.2007 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, instituțiile financiare au obligația de a păstra informații ce conțin date cu caracter personal și ulterior încheierii tranzacțiilor. 3. Se constată că norma alin. (5) al art. 13 nu este conformă cu legislația UE. Companiile private își pot stoca datele oriunde, dar trebuie să asigure un nivel adecvat de protecție a datelor cu caracter personal. Solicităm excluderea acestei prevederi.	combaterea spălării banilor și finanțării terorismului prevede termeni concreți de păstrare a documentele și informațiile obținute pentru executarea prezentei legi. Ulterior la atingerea scopului acestea vor deveni documente de arhivă în privința cărora va putea fi aplicat art. 13 alin. 3) lit. b). 3. Acceptată. Norma a fost exclusă din proiect.
		Art. 17	1. Articolul 12 din GDPR prevede că operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul articolelor 15 - 22, fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar, ținându-se seama de complexitatea și numărul cererilor. Termenul limită pentru a răspunde la solicitarea persoanei vizate este prelungit cu 30 zile lucrătoare (5 săptămâni) și nu este conform cu termenul limită stabilit în GDPR. 2. La art. 17 alin. (3) s-a propus excluderea sintagmei „cu semnătură electronică”, deoarece cerința deținerii semnăturii electronice nu este impusă de Regulamentul 2016/679, iar pe de altă parte această cerință va restricționa semnificativ și nejustificat cercul potențial subiecților de date care ar putea depune cererile în formă	1. Acceptat. 2. Neacceptată. Cerințele sunt impuse de Legea Nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic.

			electronică, doar la deținătorii unei semnături electronice valabile.	
		Art. 18	1. Se solicită completarea la începutul lit. f) alin. (1) al art. 18, cu sintagma „dacă este cazul,” conform art. 13 alin. (1) lit. f) din Regulamentul 2016/679. 2. La art. 18 alin (2) urmează a fi exclusă sintagma „În momentul obținerii datelor personale”, deoarece restricția privind momentul informării subiectului de date este excesivă și contrară Regulamentului 2016/679. 3. Art. 18 alin. 3 din proiect urmează a fi exclus, deoarece impunerea în sarcina operatorului a obligației de a proba (sub sancțiunea unor penalități) faptul că subiectul de date a recepționat această informație este excesivă și nejustificată în raport cu cerințele Regulamentului 2016/679. De exemplu, în cazul furnizării unor servicii ale societății informaționale este suficientă informarea subiecților de date prin postarea informațiilor relevante pe paginile web ale operatorilor, iar obligarea de a proba recepționarea de către subiect a informațiilor fiind excesivă/imposibil de realizat într-un astfel de caz.	1. Neacceptată. Obligația este expresă din motivul excluderii interpretării eronate. 2. Neacceptată. Corespunde art. 13 alin. (2) din GDPR. 3. Neacceptată. Norma nu contravine prevederilor GDPR și asigură realizarea informării subiectului de date.
		Art. 19	Articolul 12 din GDPR prevede că operatorul furnizează persoanei vizate informații privind acțiunile întreprinse în urma unei cereri în temeiul articolelor 15-22, fără întârzieri nejustificate și în orice caz în cel mult o lună de la primirea cererii. Această perioadă poate fi prelungită cu două luni atunci când este necesar,	Acceptat. Termenul se regăsește în art. 17 din proiect.

			ținându-se seama de complexitatea și numărul cererilor. Termenul limită pentru a răspunde la solicitarea persoanelor vizate este prelungit cu 30 zile lucrătoare (5 săptămâni) și nu este conform cu termenul limită stabilit în GDPR.	
		Art. 20	Art. 20 alin. (5) urmează a fi exclus deoarece este absolut abuziv și excesiv în raport cu obligațiile operatorilor prevăzute în Regulamentul 2016/679. Oferirea dreptului subiectului de a obține accesul fizic la datele personale stocate în sistemele de evidență, poate periclita grav activitatea operatorilor sub aspect operațional, financiar (presupunând costuri enorme), precum și sub aspectul asigurării securității informaționale. Totodată, această prevedere va constitui o sursă potențială de plângeri și potențiale acțiuni judiciare abuzive împotriva operatorilor din partea subiecților de date, suplimentar aceștia vor fi supuși riscului impunerii unor penalități exorbitante.	Acceptat parțial. În art. 20 alin. (5) a fost prevăzută excepția când nu poate fi acordat dreptul subiectului de a obține accesul fizic la datele personale. (5) Subiectul de date are dreptul să obțină la cerere, gratuit și fără întârzieri nejustificate, accesul fizic la datele personale stocate care îl privesc și care sunt prelucrate în sistemele de evidență, cu excepția în care acest drept ar putea fi susceptibil de a aduce atingere cerințelor de securitate asigurate sau din punct de vedere tehnic nu este posibil a fi realizat.
		Art. 22	Art. 22 alin. (3) din proiect urmează a fi exclus, deoarece este excesiv în raport cu obligațiile corelative cerute conform Regulamentului 2016/679. Astfel, obligația de ajustare a operațiunilor de prelucrare în termen de maxim 30 zile (sub riscul aplicării sancțiunilor) nu doar contravine prevederilor Regulamentului 2016/679, ci și poate fi imposibil de realizat în practică, de exemplu, în	Acceptat parțial. Norma a fost redactată fiind prevăzut termenul de o lună, cu posibilitatea prelungirii cu 15 zile.

			cazul în care este necesară efectuarea unor modificări la nivelul sistemelor automatizate.	
		Art. 33 și 36	Două articole conțin prevederi similare. Articolul 33 și articolul 36 au același text și prevăd aceleași reglementări. Un articol urmează a fi exclus.	Acceptată. Art. 36 exclus.
		Art. 37 (36)	1. Se solicită modificarea art. 37 alin. (1) prin excluderea literelor a) – o) și înlocuirea acestora cu prevederile lit. a) – d) din art. 33 al Regulamentului 2016/679. Menționăm că art. 33 din Regulament stabilește cerințe generale de securitate, fără a indica exact măsurile tehnice concrete care trebuie implementate de către toți operatorii. Conform Regulamentului, însuși operatorii urmează să determine, pe propria răspundere, măsurile tehnice și organizatorice care sunt <u>adecvate</u>, reieșind din riscurile prelucrării și alte criterii relevante. Practica instituirii prin lege a <u>aceluiași</u> set minim de cerințe tehnice obligatorii pentru toți operatorii (indiferent de riscuri, categorii de date prelucrate etc.) este defectuoasă deoarece: i) măsurile tehnice concrete urmează a fi implementate reieșind din fiecare caz separat, și ii) datorită progresului tehnic continuu, măsurile tehnice stabilite prin lege riscă să devină învechite în termeni restrânși, neasigurând nivelul de protecție adecvat, dar obligând absolut toate companiile private să investească considerabil în tehnologii învechite.	1. Nu se acceptă. În prezent, măsurile tehnice concrete care trebuie implementate de către toți operatorii sunt stabilite prin HG nr. 1123 din 14/12/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal. Prin prevederile statuate la art. 37 autorul nu prezintă o listă de măsuri tehnice și organizatorice care urmează a fi întreprinse de operatorul, dar ce urmează să garanteze operatorul prin asigurarea securității datelor.

			Remarcăm că unele măsuri tehnice, de exemplu prevăzute de lit. h) art. 37 alin. (1), privind <u>obligativitatea</u> utilizării mijloacelor de protecție criptografică și a semnăturii electronice la transmiterea datelor personale, precum și obligația de marcarea și ținere a evidenței (prevăzută lit. e) vor presupune costuri enorme de implementare pentru toți operatorii, și pot bloca dezvoltarea serviciilor on-line și chiar comunicările obișnuite prin mijloace electronice. 2. Reieșind din considerentele expuse mai sus, solicităm expunerea art. 37 alin. (4) după cum urmează: „<i>Descrierea detaliată a măsurilor de securitate a prelucrării datelor personale efectuate de către <u>autoritățile publice</u>, la necesitate se stabilesc prin hotărâre de Parlament.</i>”	2. Nu se acceptă. Aplicarea măsurilor de securitate la prelucrarea datelor personale este obligatorie pentru toți operatorii de date.
		Art. 43 (42)	Se propunemodificarea și expunerea art. 43 alin. (7) și (8) în următoarea redacție: 1. „(7) <i>Operatorul sau persoana împuternicită de operator publică pe pagina web oficială și/sau la sediul său datele de contact ale responsabililor de protecția datelor și le comunică Centrului (numele, prenumele, numărul de telefon, adresa de e-mail).</i> 2.(8) <i>Operatorul sau persoana împuternicită de operator, în dependență de numărul de angajați, de volumul și de categoriile de date personale prelucrate (categoriile obișnuite sau speciale) și riscuri, poate crea</i>	Nu se acceptă Paginile-web sunt un mecanism/instrument eficient de a informa subiectul de date, iar operatorul trebuie pe larg să-l valorifice. 3. Nu se acceptă. Norma stabilește situația crearii subdiviziunii structurale <i>în dependență de numărul de angajați, de volumul și de categoriile de date personale prelucrate (categoriile obișnuite sau speciale) și riscuri...</i>

			<i>subdiviziuni structurale pentru asigurarea protecției datelor”.</i>	
		Art. 50 (49)	1. La art. 50 alin. (4) din proiect urmează a fi exclusă sintagma „și autorizarea”, deoarece transferul de date respectiv nu presupune emiterea unei autorizații de către Centru. 2. La art. 50 urmează a fi excluse integral alin. (5) și (6), deoarece prevederile respective se repetă în art. 56 (55) alin. (1) și (2).	1. Art. este expus într-o nouă redacție 2. Remarcăm faptul că prevederile din Capitolul VII, inclusiv art. 55 sunt aplicabili doar organelor de ocrotire a legii, iar alți operatori nu au tangență cu aceste prevederi.
		Art. 52 (50)	Art. 52 alin. (6) urmează a fi modificat sau exclus, deoarece nu este clar și conține enunțuri incorecte, nefiind conform cu Regulamentul. În particular răspunderea nu poate surveni decât pentru încălcări, și nu pentru simplul transfer.	Se acceptă. Art. 50 alin. (6) din proiect a fost modificat.
		Art. 60 (57)	Se constată că termenul de 1 an pentru revizuirea periodică a termenelor de stocare a datelor este unul excesiv și creează sarcini administrative suplimentare pentru autoritățile de aplicare a legii și ar putea fi considerată ca fiind o suprareglementare. La stabilirea termenelor, este important să se țină cont de activitățile specifice de prelucrare a datelor.	Acceptată. Alin (1) a fost modificat după cum urmează: <i>se vor stabili termene de stocare corespunzătoare și adecvate scopului prelucrării. Dacă asemenea termene nu pot fi stabilite, se va asigura revizuirea periodică a necesității de stocare a datelor.</i>
		Art. 80-90 (77-87)	Prevederile Cap. VIII și Cap. IX (în special art. 80 - 89) din Legea nr. 133 prevăd proceduri speciale și drepturi ale Centrului care sunt excesive atât în raport cu prevederile actuale din Legea nr. 131 privind controlul de stat asupra activității de întreprinzător, cât și cu sarcinile și	Neacceptată. CNPDCP nu urmărește scopul de a interveni în activitatea autorităților publice sau private, ci de a efectua investigația legalității prelucrării datelor cu caracter personal ale subiectului de date de către entități, în calitate de operatori de date cu caracter personal, care au obligația de a asigura confidențialitatea și securitatea datelor cu caracter personal prelucrate.

		competențele autorităților de supraveghere stabilite în cap. VI al Regulamentului 2016/679. <u>Astfel, s-a solicitat:</u> - excluderea art. 80 – 89 din proiectul Cap. VIII și Cap. IX al Legii 133, deoarece acestea instituie proceduri speciale de investigare, acces, emitere decizii, contestare decizii Centrului, prin derogare de la Legea nr. 131 privind controlul de stat asupra activității de întreprinzător, având ca efect anularea reformei cadrului de reglementare a activității de întreprinzător, scopul căreia a fost uniformizarea normelor aplicabile controlului de stat, creșterea previzibilității legii, reducerea costurilor de conformare cu legea, adoptarea unor garanții suficiente împotriva controalelor abuzive și asigurarea dreptului efectiv la apărare. - revizuirea sarcinilor și competențelor Centrului și aducerea lor în corespundere cu prevederile art. 55 – 59 al cap. VI din Regulamentul 2016/679, care stabilesc sarcinile și competențele unei autorități de supraveghere naționale. În sprijinul celor menționate mai sus, cu titlu de exemplu, atragem atenția asupra unor competențe ale Centrului care sunt absolut excesive, trezind îngrijorări:	Actualmente Centrul nu întreprinde măsuri de control în conformitate cu Legea nr. 131 privind controlul de stat asupra activității de întreprinzător. Toate acțiunile Centrului sunt efectuate doar în corespundere cu Legea nr. 133 privind protecția datelor cu caracter personal. Activitățile de investigație a Centrului nu pot fi sub nici o formă aliniate cu măsurile întreprinse de alte organe de control din considerentul că se deosebesc radical de acestea. La moment Centrul dispune de propriul Regulament privind controlul legalității prelucrărilor de date cu caracter personal, aprobat în corespundere cu prevederile legale, prin ordinul directorului. Remarcăm faptul, că de la fondarea Centrului și până în prezent, nu s-a constatat o situație de abuz din partea Centrului în cadrul efectuării controalelor la operatorii de date. Reticențele expuse sunt declarative și nefondate. Reiterăm faptul că reieșind din atribuțiile funcționale Centrul nu efectuează controlul asupra activității de întreprinzător ci veghează legalitatea respectării prevederilor Legii nr. 133/2011, precum și a altor acte normative ce reglementează domeniul și derive din dispozițiile art. 28 din Constituție - Viața intimă, familială și privată. În partea ce ține de insinuarea drepturilor excesive ale Centrului. Atragem atenția că art. 58 din GDPR statuează expres competențe de investigare fiecărei autorități de supraveghere. În special, autoritatea de supraveghere are dreptul de a obține, din partea operatorului și a persoanei împuternicite de operator, accesul la toate datele cu caracter personal și la toate informațiile necesare pentru îndeplinirea sarcinilor sale, de a obține accesul la oricare dintre incintele operatorului și ale persoanei împuternicite de operator, inclusiv la orice echipamente și mijloace de prelucrare a datelor (art. 58 alin. (1) lit. e) și lit. f)).
--	--	---	--

			- art. 81 alin. (2) și alin. (9) lit. d) care acordă <u>dreptul discreționar</u> al Centrului, în cadrul unei investigații, să dispună asupra mijloacelor, precum și să sigileze încăperile și mijloacele, sistemele de evidență etc., este excesiv, nefiind prevăzut de Regulamentul 2016/679 și poate conduce la blocarea abuzivă a activității economice a unor operatori. De exemplu, în practică acest drept poate duce la blocarea utilizării unor mijloace (echipamente costisitoare sau sisteme de evidență etc.) importate, dezvoltate și utilizate în mod legal, care corespund tuturor cerințelor de conformitate, reglementărilor tehnice etc. - art. 81 alin. (9) lit. g) stabilește dreptul Centrului de a accesa sistemele de evidență, inclusiv prin efectuarea unor simulări, măsuri tehnice speciale etc. Aceste drepturi sunt excesive, pot periclita grav operațiunile economice ale operatorului, precum și securitatea și integritatea datelor personale prelucrate. Totodată această atribuție nu este prevăzută de Regulamentul 2016/679. - Termenii de investigare de până la 2 ani cu posibilitate de suspendare pentru 1 an (cu drept de reluare ulterioară), stabiliți la art. 81 alin. (25) și (27) nu sunt deloc rezonabili, fiind excesivi în raport cu termenii stabiliți în Legea nr. 131, creând incertitudini majore operatorilor. Dreptul Centrului, conform art. 81 (29) din proiect, de a-și stabili și aproba propriul	Garanții similare sunt acordate autorităților de supraveghere și de Directiva (UE) 2016/680 privind protecția 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. În partea ce șine de simulare, remarcăm că simularea unor eventuale incidente de securitate la prelucrarea datelor cu caracter personal este o condiție imperioasă în contextul protejării drepturilor și libertăților altuia în contextul preîntâmpinării unor scurgeri de date cu caracter personal. Faptic, aceasta este o penetrare în sistem care este efectuată atât la nivel al securității fizice cât și cel al securității informaționale. Într-o altă ordine de idei, la moment Centrul în conformitate cu prevederile pct. 83 din Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010 dispune de acest drept și anume: În scopul verificării nivelului de protecție a sistemelor informaționale de date cu caracter personal, precum și în scopul preîntâmpinării unor eventuale cazuri de acces ilicit sau întâmplător asupra acestor sisteme informaționale, depistării locurilor slabe în mecanismele de protejare a acestora, Centrul întreprinde periodic controale de securitate, inclusiv cu efectuarea unor măsuri tehnice speciale pentru simularea unui model de accesare a sistemelor informaționale de date cu caracter personal.
--	--	--	--	--

			Regulament privind efectuarea investigației este abuziv, deoarece Centrul este o parte interesată.	
		Art. 92, 94, 99	S-a propus excluderea art. 92, 94 și 99 (1) din Legea nr. 133/2011 care stabilesc sancțiuni administrative pentru încălcarea cerințelor Legii nr. 133, deoarece: - sancțiunile pentru încălcarea prevederilor Legii nr. 133/2011 urmează a fi reglementate în continuare de către Codul contravențional care conține prevederi procedurale necesare, urmând a fi decise de către instanțele de judecată. În acest sens, Codul contravențional ar putea fi revizuit, pentru a ține seama de condițiile de individualizare a sancțiunilor prevăzute în art. 83 din Regulament . - mărirea semnificativă a sumei amenzilor (în unele cazuri chiar până la 500,000 EUR sau 4 % din cifra de afaceri mondială) <u>coroborată cu dreptul Centrului de a trece la venituri 25 % din amenzi</u>, este absolut excesivă și nejustificată reieșind din realitățile economice și de drept ale R. Moldova, depășind cu mult cuantumul sancțiunilor economice aplicabile chiar și în cazul comiterii unor infracțiuni grave. Introducerea bruscă a unor asemenea sancțiuni, coroborată cu stabilirea în	Nu se acceptă. La moment se constată ineficiența măsurilor punitive în vigoare, care se manifestă prin caracterul îndelungat al examinării de către instanțele de judecată a cauzelor contravenționale pornite de Centru. Mai mult, soluționarea cauzelor contravenționale prin recunoașterea vinovăției contravenienților și sancționarea acestora în limitele prevăzute la art. 74¹-74³ Cod contravențional, se rezumă la constatarea de către instanța de judecată a faptelor contravenționale comise, fără a dispune obligarea contravenientului în vederea înlăturării cauzelor ce au dus la comiterea încălcărilor vizate. Într-o altă ordine de idei, urmează a menționa că noul Regulament 2016/679, la art. 83 prevede dreptul autorităților naționale de supraveghere de a aplica amenzi administrative. De altfel, în prezent art. 34 din Codul contravențional limitează cuantumul maxim al amenzilor pasibil a fi aplicate. Totodată, ținând cont de realitățile din Republica Moldova, în proiectul vizat se propune un mecanism treptat de aplicare a sancțiunilor pentru a nu împovăra operatorii de date și a le permite să se adapteze noilor rigori europene. Într-o altă ordine de idei, trebuie de menționat că în Republica Moldova există practici când autoritățile de control pot impune prin decizia sa sancțiuni pecuniare cum ar fi spre exemplu Consiliul concurenței, Banca Națională a Moldovei, CNPF. Remarcăm că Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului prevede sancțiuni în

			sarcina operatorilor prin Legea nr. 133 a unor noi obligații costisitoare, va contribui la creșterea poverii financiare în sarcina operatorilor, va favoriza creșterea fenomenului corupției, în detrimentul obligațiilor de implementare a noilor obligații privind asigurarea protecției datelor personale și poate duce la falimentarea unor agenți economici.	mărime de până la echivalentul în lei al sumei de 5000000 de euro, calculat la cursul oficial al leului moldovenesc. Este neîntemeiată invocarea faptului de introducere bruscă a sancțiunilor din motivul existenței în dispozițiile tranzitorii ale proiectului a unui mecanism treptat de aplicare a sancțiunilor de Centru pentru fiecare an de la intrarea în vigoare a prezentei legi.
		Art. 96 (93)	Art. 96 care reglementează prelucrarea datelor personale în cadrul relațiilor de muncă nu corespunde prevederilor Regulamentului 2016/679, fiind excesiv și trebuie exclus.	Nu se acceptă. Nu are un substrat juridic. Art. 28 al Constituției RM prevede expres: <i>statul respectă și ocrotește viața intimă, familială și privată</i>. Astfel statul indiferent de raporturile sociale, garantează respectarea dreptului la viața intimă, familie și privată.
		Art. IV	Articolul IV din proiectul de modificare a legii prevede că modificările introduse vor intra în vigoare din 01 martie 2019. Considerăm că acest termen este irealizabil din punct de vedere tehnic, deoarece pentru implementarea cerințelor noi impuse prin aceste acte legislative, în special celor din domeniul IT, sunt necesari cel puțin 1-2 ani din data publicării (în cazul Regulamentului 2016/679 au fost oferiți aproximativ 2 ani.	Neacceptată. Nu vedem necesitate. Din considerentul că GDPR deja a intrat în vigoare, iar în anumite situații prevederile acestuia pot fi aplicate și în privința operatorilor naționali și, respectiv, acestora li se pot aplica sancțiuni din partea autorităților de supraveghere europene.