



CENTRUL NAȚIONAL PENTRU PROTECȚIA DATELOR CU CARACTER PERSONAL AL REPUBLICII MOLDOVA

RAPORT DE ACTIVITATE PENTRU ANUL 2020

CUPRINS

INTRODUCERE 3

PREZENTARE GENERALĂ..... 4

CAPITOLUL I

**EXAMINAREA ADRESĂRILOR
ÎNAINȚATE CENTRULUI 5**

CAPITOLUL II

ACTIVITATEA DE CONTROL 9

CAPITOLUL III

**RECOMANDĂRILE ȘI CAZUISTICA
ANULUI 2020 12**

CAPITOLUL IV

**ACTIVITATEA DE REPRESENTARE
ÎN INSTANȚELE DE JUDECATĂ..... 26**



CAPITOLUL V

**ACTIVITATEA DE SUPRAVEGHERE
A PRELUCRĂRILOR DE DATE
CU CARACTER PERSONAL 31**

CAPITOLUL VI

**AVIZAREA ȘI ELABORAREA PROIECTELOR
DE ACTE NORMATIVE..... 38**

CAPITOLUL VII

COOPERAREA INTERNAȚIONALĂ 41

CAPITOLUL VIII

**ACTIVITĂȚI DE INSTRUIRE
ȘI SENSIBILIZARE..... 46**

CAPITOLUL IX

MANAGEMENTUL RESURSELOR UMANE 49

CAPITOLUL X

ACTIVITATEA ECONOMICO-FINANCIARĂ 55

PROBLEME ȘI OBIECTIVE 58

ANEXE 61



INTRODUCERE

În scopul informării societății despre evoluția domeniului protecției datelor cu caracter personal, Centrul Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova (Centrul) prezintă Raportul de activitate pentru anul 2020.

Anul 2020 a fost unul specific în special pentru domeniul protecției datelor cu caracter personal, în această perioadă protecția datelor a necesitat o atenție sporită din partea întregii societăți ca urmare a pandemiei provocate de COVID -19 la nivel global.

Pandemia a impus aplicarea de măsuri rapide și eficiente în diferite domenii de activitate, determinând utilizarea sporită a tehnologiilor digitale. Utilizarea celor mai noi tehnologii informaționale pentru comunicarea la distanță, munca sau studiile la distanță a devenit noul „normal” în viața cotidiană a societății. Or, acest salt în digitalizarea vieții noastre necesită o protecție sporită a datelor cu caracter personal.

Chiar dacă pandemia a avut impact inclusiv asupra activității Centrului, condiționând imposibilitatea desfășurării sau amânării unor activități planificate, precum și diminuând nesemnificativ numărul activităților efectuate, reflectate în prezentul raport, perioada de referință este marcată de multiple realizări, fiind axată pe implementarea continuă a prevederilor legislației ce reglementează domeniul protecției datelor cu caracter personal, exercitarea optimă a atribuțiilor legale de supraveghere și control al conformității prelucrărilor de date cu caracter personal, examinarea și soluționarea plângerilor și sesizărilor primite și verificărilor din oficiu a unor aspecte legate de prelucrarea datelor cu caracter personal, în scopul asigurării respectării principiilor de protecție ale acestor date de către operatorii din domeniul public și privat, elaborarea și avizarea proiectelor de acte normative cu incidență în acest domeniu, consolidarea cooperării interne și externe în domeniul protecției datelor cu caracter personal.

La fel, raportul reflectă problemele și preocupările prioritare, situația din domeniul protecției datelor cu caracter personal, oferă recomandări și opinii ale Centrului, precum și exemplifică un șir de încălcări constatate de Centru în cadrul activității desfășurate iar, pentru asigurarea confidențialității datelor cu caracter personal devenite cunoscute în cadrul exercitării atribuțiilor de control, în conformitate cu prevederile art. 29 și art. 31 din Legea privind protecția datelor cu caracter personal, acestea sunt depersonalizate în scopul neadmiterii ingerinței în viața privată, precum și imposibilității asocierii lor cu o persoană identificată ori identificabilă.

Cu respect,

Eduard RĂDUCAN
Director al Centrului Național pentru
Protecția Datelor cu Caracter Personal



PREZENTARE GENERALĂ

Anul 2020 în cifre

ADRESĂRI/PLÂNGERI

11191 documente de corespondență:
5115 intrate
4564 ieșite
679 interne
833 petiții



ACTIVITATEA DE CONTROL

303 controale inițiate
170 fapte contravenționale constatate
125 procese-verbale întocmite
43 decizii suspendare/încetare/
ștergere



ACTIVITATEA DE SUPRAVEGHERE

1472 notificări examinate
504 operatori înregistrați
710 sisteme de evidență
înregistrate
762 decizii de refuz

ACTIVITATEA DE REPREZENTARE
ÎN INSTANȚELE DE JUDECATĂ

777 ședințe de judecată:
470 în ordinea contravențională
307 în contencios administrativ

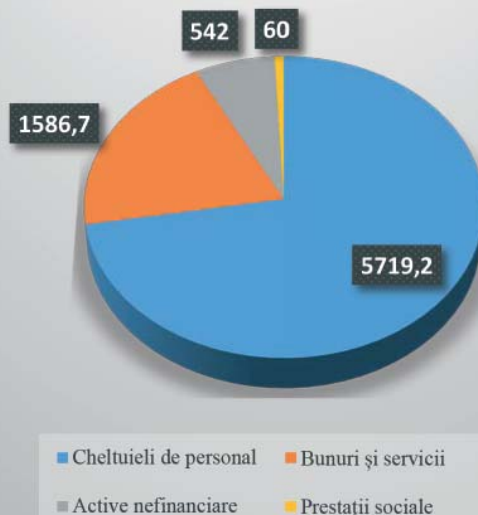


INFORMARE ȘI PROMOVARE

2030 consultații pentru operatorii de date
14712 accesări contul Facebook/ CNPDCP
49034 vizualizări pe site-ul CNPDCP
80 comunicate/articole pe pagina web

RESURSE UMANE

35 angajați, din efectivul de 45
8 concursuri desfășurate
9 persoane angajate/7 debutanți
6 persoane au demisionat
21 cursuri de instruire

Repartizarea Bugetului CNPDCP
pentru anul 2020
(mii, lei)



CAPITOLUL I

EXAMINAREA ADRESĂRILOR
ÎNAINȚATE CENTRULUI

În anul 2020, Centrul a examinat **11191** documente de corespondență. Această cifră denotă creșterea constantă pe parcursul anilor a numărului tot mai impunător de adresări înaintate autorității spre examinare.

Astfel, chiar dacă anul 2020 a fost marcat de pandemia de COVID-19, care a avut impact inclusiv asupra activității Centrului, și în acest an se constată tendința în creștere atât în partea ce vizează subiecții de date cu caracter personal în dorința de a-și exercita drepturile prin înaintarea plângerilor asupra pretinselor neconformități la prelucrarea datelor, cât și a operatorilor de date cu caracter personal în intenția de a se conforma obligațiilor prescrise de Legea privind protecția datelor cu caracter personal și de a cunoaște reglementările din domeniu în vederea asigurării prelucrării conforme a datelor cu caracter personal.

Statistica comparativă a documentelor de corespondență pentru anii 2014-2020

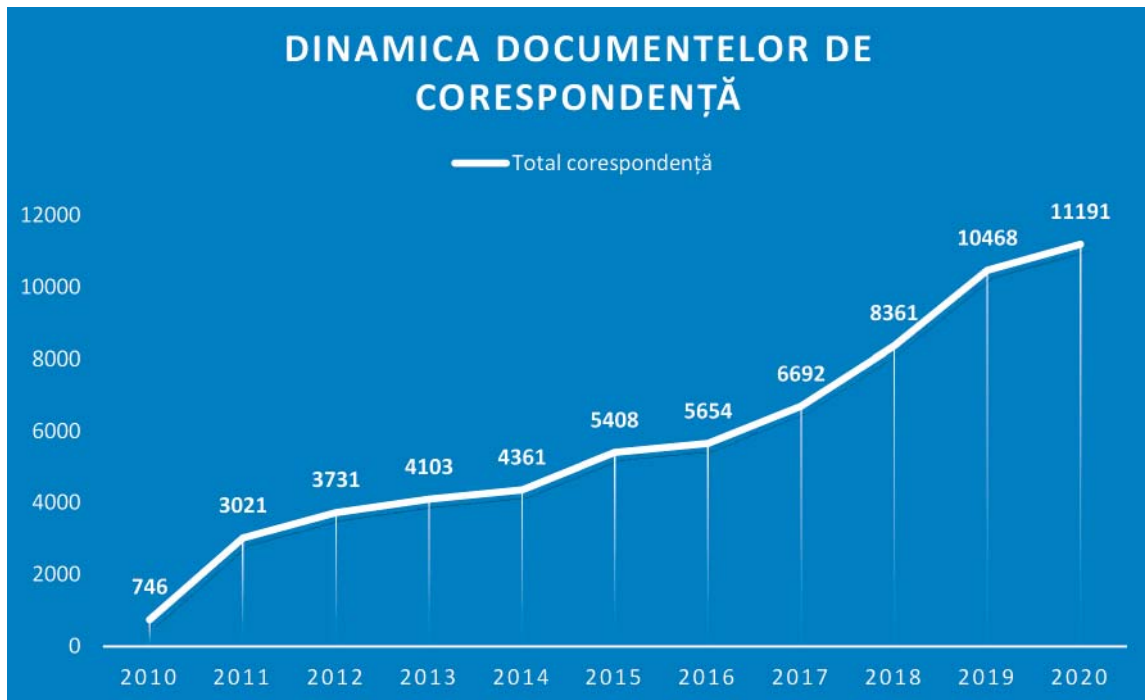
Anul	Total corespondență	Documente intrate	Documente ieșite	Petiții	Documente interne
2014	4361	1738	1836	302	485
2015	5408	2425	2098	420	465
2016	5654	2811	2055	410	374
2017	6692	3605	2455	554	316
2018	8361	4180	3113	637	431
2019	10468	4982	4217	743	526
2020	11191	5115	4564	833	679

Majorarea semnificativă, de la an la an, a numărului documentelor de corespondență examinate de Centru, demonstrează faptul creșterii nivelului de cunoaștere a importanței domeniului protecției datelor cu caracter personal în societate. Totodată, acest fapt determină indubitabil creșterea constantă și esențială a volumului de muncă pus în sarcina angajaților Centrului.

**Informația în dinamică privind corespondența Centrului, pentru anii 2014-2020**

Perioada de referință	Total corespondență	Dinamica
2014-2015	4361-5408	↑24%
2015-2016	5408-5654	↑5%
2016-2017	5654-6692	↑18%
2017-2018	6692- 8361	↑25%
2018-2019	8361-10468	↑25%
2019-2020	10468-11191	↑7%
Dinamica între anul 2014 și anul 2020	4361-11191	↑157%

Informația mai reprezentativă a dinamicii în permanentă ascensiune a numărului documentelor de corespondență, pe un termen mai extins, care cuprinde practic întreaga perioadă de activitate efectivă a Autorității naționale de protecție a datelor cu caracter personal, este reflectată în continuare:

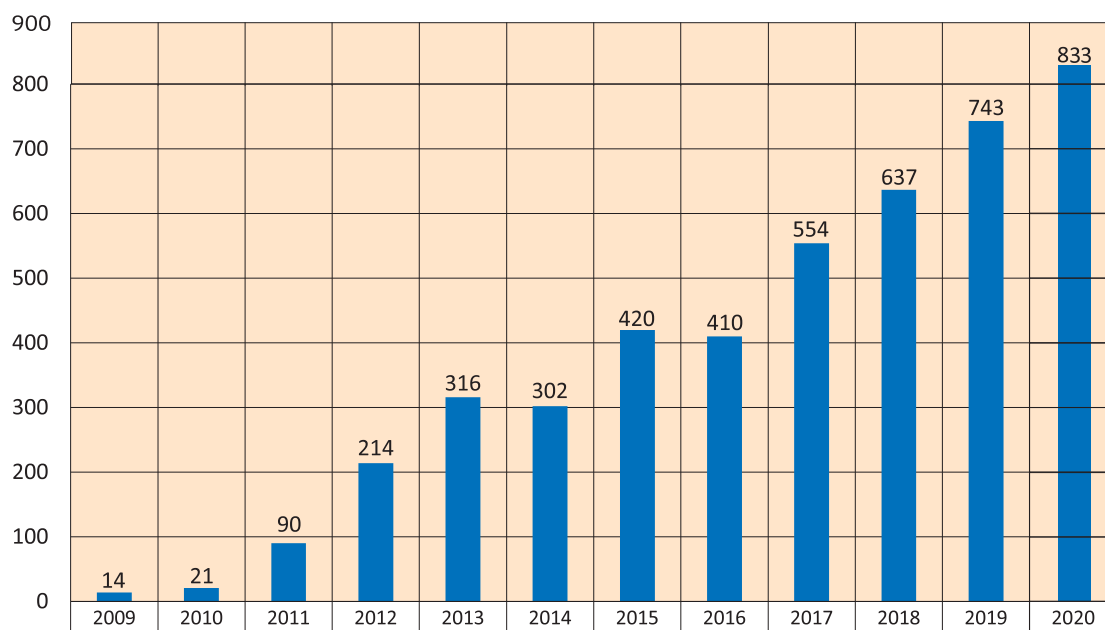
**Activitatea de examinare a adresărilor subiecților de date cu caracter personal**

În perioada de referință propusă, Centrul a examinat **833** de petiții parvenite din partea persoanelor fizice – subiecți ai datelor cu caracter personal. Comparativ cu anul precedent (743 petiții înregistrate în anul 2019), numărul plângerilor a înregistrat o creștere de 12%.

Din numărul total de petiții înregistrate în anul 2020, **303** cazuri au fost examinate complex, în ordine de control privind legalitatea operațiunilor de prelucrare a datelor cu caracter personal.



Numărul de petiții, 2009-2020

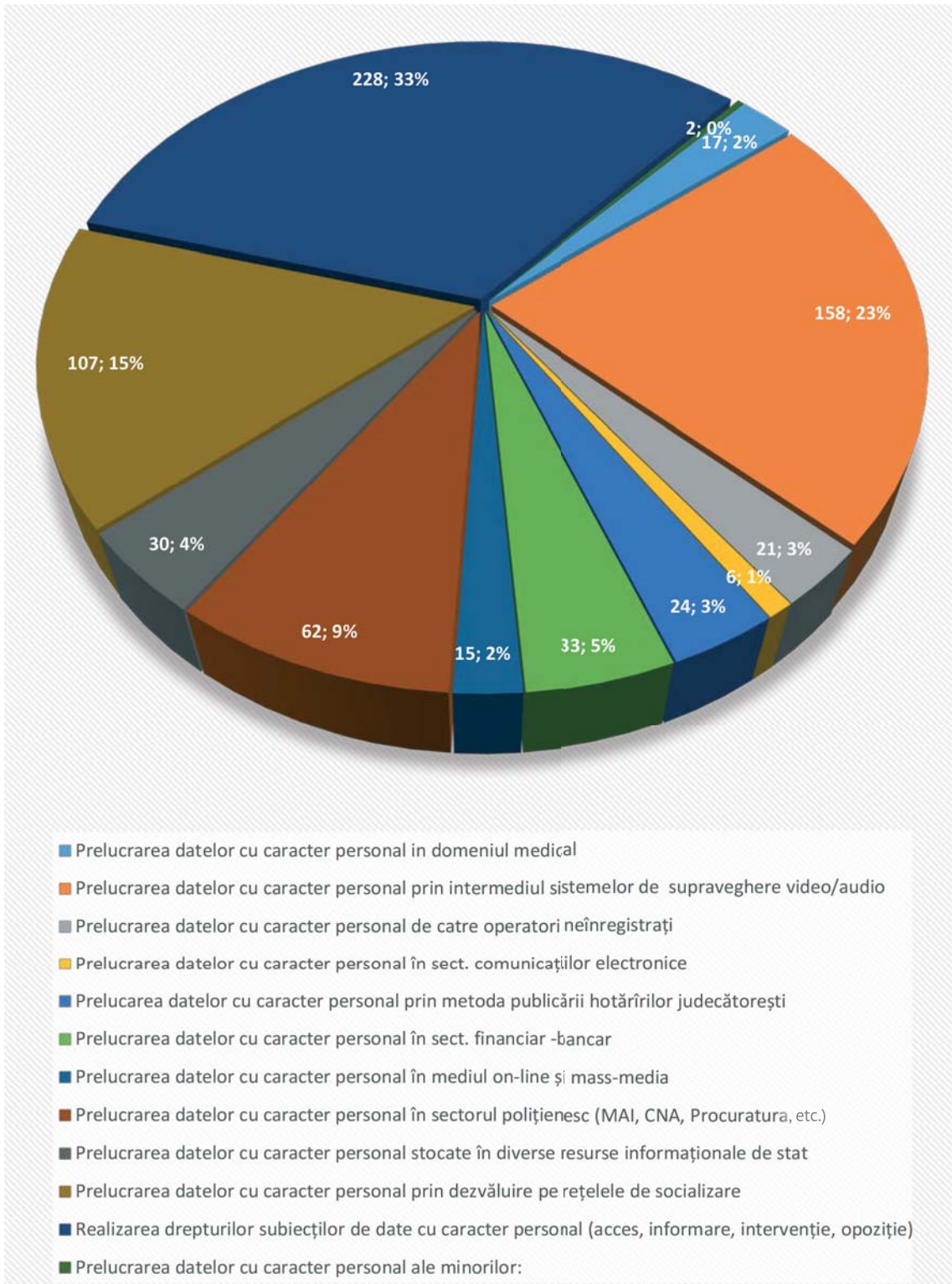


Din specificul plângerilor abordate, Centrul a relevat următoarele linii directorii ale tematicilor semnalate:

- ✓ Prelucrarea datelor cu caracter personal prin intermediul sistemelor de supraveghere video/ audio: **158** cazuri;
- ✓ Prelucrarea datelor cu caracter personal fără notificarea și/sau autorizarea organului de control în domeniul prelucrării datelor cu caracter personal, precum și prelucrarea datelor cu caracter personal de un operator neînregistrat în modul stabilit: **21** cazuri;
- ✓ Prelucrarea datelor cu caracter personal în sectorul comunicațiilor electronice: **6** cazuri;
- ✓ Prelucrarea datelor cu caracter personal ale minorilor: **2** cazuri;
- ✓ Publicarea hotărârilor judecătorești fără depersonalizarea acestora: **24** cazuri;
- ✓ Prelucrarea datelor cu caracter personal în sectorul financiar-bancar, a companiilor de asigurări: **33** cazuri;
- ✓ Prelucrarea datelor cu caracter personal în mediul on-line și mass-media: **15** cazuri;
- ✓ Prelucrarea datelor cu caracter personal stocate în diverse resurse informaționale de stat: **30** cazuri;
- ✓ Prelucrarea datelor cu caracter personal prin dezvăluire pe rețelele de socializare: **107** cazuri;
- ✓ Prelucrarea datelor cu caracter personal în lipsa consimțământului subiectului de date și/sau a temeiului legal: **130** cazuri;
- ✓ Realizarea drepturilor subiecților de date cu caracter personal (acces, informare, intervenție, opoziție): **228** de adresări;
- ✓ Prelucrarea datelor cu caracter personal în domeniul medical: **17** cazuri;
- ✓ Prelucrarea datelor cu caracter personal în sectorul polițienesc (MAI, CNA, Procuratura etc.): **62** cazuri.



Situația generală privind plângerile aflate în examinare în anul 2020





CAPITOLUL II

ACTIVITATEA DE CONTROL

Informația comparativă a activității de control, pentru perioada 2018-2020

Perioada pentru comparație	Numărul controalelor inițiate în baza: plângerilor/ sesizărilor, solicitărilor de autorizare a transmiterii transfrontaliere	Acte de reacționare emise ca rezultat al efectuării controalelor			
		Decizii privind suspendarea operațiunilor de prelucrare a datelor cu caracter personal	Decizii privind încetarea operațiunilor de prelucrare a datelor cu caracter personal	Decizii privind distrugerea/ștergerea datelor prelucrate cu încălcarea legii	Fapte contravenționale constatate/ Procese-verbale contravenționale întocmite
Anul 2018	326	16	4	27	191/92
Anul 2019	376	26	8	24	186/105
Anul 2020	303	20	6	17	170/125

Controlul conformității prelucrării datelor cu caracter personal cu cerințele Legii privind protecția datelor cu caracter personal se efectuează în exclusivitate de către Centrul Național pentru Protecția Datelor cu Caracter Personal și poate fi inițiat: în temeiul plângerii subiectului de date cu caracter personal; sesizării/autosesizării; solicitării autorizării transmiterii transfrontaliere de date cu caracter personal.

În perioada de referință au fost inițiate și examinate **303** materiale de control, dintre care:

- **275** în baza plângerilor subiecților de date cu caracter personal, sesizărilor/autosesizărilor,
- **28** în baza solicitărilor de autorizare a transmiterii transfrontaliere de date cu caracter personal.

Analiza comparativă în raport cu statistica anului precedent relevă că, în perioada anului 2020, s-a constatat o scădere nesemnificativă a numărului verificărilor inițiate în baza plângerilor înaintate de subiecții de date cu caracter personal. În opinia Centrului, factorul important care a cauzat diferența relevată se constată a fi situația pandemică generată de virusul COVID-19, or, pe parcursul perioadei de referință, în Republica Moldova a fost declarată stare de urgență, fiind sistată periodic activitatea tuturor instituțiilor, inclusiv activitatea Centrului de două ori, iar populația aflându-se în izolare.

Suplimentar se notează că, în special ținând cont de modificările operate prin Legea nr. 124 din 09 iulie 2020 (în vigoare din 24 august 2020) asupra prevederilor art. 27 din Legea privind protecția datelor cu caracter personal, verificarea conformității operațiunilor de prelucrare a datelor cu caracter personal în baza plângerilor subiecților de date se inițiază/demara doar urmare a realizării în prealabil, de către subiecții de date, a drepturilor lor consfințite la art. 12-14, 16-17 ale Legii privind protecția datelor cu caracter personal, direct față de operatorii de date cu caracter personal, aspect care la fel a influențat asupra numărului de controale inițiate în anul 2020.



De menționat că, modificările efectuate în anul 2020 asupra prevederilor art. 27 al Legii 133/2011 au un rol foarte important pentru activitatea aferentă controlului legalității prelucrării datelor cu caracter personal. Or, modificările survenite au adus îmbunătățiri esențiale de ordin conceptual și procedural, pe de o parte oferind claritate acțiunilor necesare a fi întreprinse de către subiecții de date ce înaintează plângeri în adresa Centrului precum și de către operatorii de date, iar pe de altă parte stabilind expres aspecte organizatorice precum: proceduri, termene, criterii și chiar competențe, care au venit să eficientizeze și să optimizeze capacitățile instituționale aferente efectuării controlului legalității prelucrării datelor cu caracter personal.

Este de remarcat tendința continuă de creștere a complexității cazurilor și tematicilor reclamate în plângeri, precum și numărul actorilor implicați la caz, aspecte care generează iminent o diversitate de măsuri de control necesare a fi întreprinse întru verificarea legalității prelucrării datelor cu caracter personal, acestea fiind tot mai vaste și mai complicate.

Și în anul 2020, inclusiv având în vedere situația pandemică la nivel de țară, controalele legalității prelucrării datelor cu caracter personal au fost desfășurate, în marea majoritate a cazurilor, din oficiu, fiind aplicată procedura scrisă de obținere a informațiilor necesare examinării neconformităților invocate și soluționării cazurilor sesizate.

În rezultatul materialelor de control examinate de Centru și finalizate cu constatarea încălcării prevederilor legale din domeniul protecției datelor cu caracter personal, în funcție de consecințele survenite în urma încălcărilor admise și gravitatea încălcării constatate, au fost dispuse măsuri de constrângere manifestate prin:

- suspendarea operațiunilor de prelucrare a datelor cu caracter personal – 20 cazuri,
- distrugerea/ștergerea datelor cu caracter personal prelucrate cu încălcarea prevederilor legale – 17 cazuri,
- încetarea operațiunilor de prelucrare a datelor cu caracter personal – 6 cazuri.

Concomitent, prin prisma calității de agent constator în raport cu faptele statuate la art. 74¹ – 74³ Cod contravențional, pe parcursul anului 2020 au fost întocmite **125** procese-verbale cu privire la contravenții, fiind constatate **170** fapte contravenționale, cauzele contravenționale fiind expediate spre examinare în instanța de judecată competentă, în temeiul prevederilor Codului contravențional.

Spectrul faptelor contravenționale constatate denotă caracterul frecvent al unor încălcări comise la prelucrarea datelor cu caracter personal, după cum urmează:

- art. 74¹ alin. (1): nerespectarea cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea lor în cadrul sistemelor informaționale de date cu caracter personal – 20 fapte;
- art. 74¹ alin. (2): prelucrarea datelor cu caracter personal fără notificarea și/sau autorizarea organului de control în domeniul prelucrării datelor cu caracter personal, precum și prelucrarea datelor cu caracter personal de un operator neînregistrat în modul stabilit – 48 fapte;
- art. 74¹ alin. (3): încălcarea drepturilor subiectului datelor cu caracter personal de a fi informat – 9 fapte;
- art. 74¹ alin. (4): încălcarea regulilor de prelucrare, stocare și utilizare a datelor cu caracter personal – 69 fapte;
- art. 74¹ alin. (5): transmiterea transfrontalieră a datelor cu caracter personal cu încălcarea legislației privind protecția datelor cu caracter personal-1 faptă;
- art. 74² alin. (1): refuzul de a furniza informațiile sau documentele solicitate de Centrul Național pentru Protecția Datelor cu Caracter Personal în procesul exercitării atribuțiilor de control, prezentarea unor informații neautentice sau incomplete, precum și neprezentarea în termenul stabilit de lege a informațiilor și a documentelor solicitate – 22 fapte;



– art. 74³: neîndeplinirea în termenul stabilit a deciziei Centrului privind repunerea în drepturi a subiectului datelor cu caracter personal, inclusiv privind suspendarea sau încetarea prelucrării datelor cu caracter personal, privind blocarea, distrugerea parțială ori integrală a datelor cu caracter personal prelucrate cu încălcarea legislației în domeniul protecției datelor cu caracter personal- 1 faptă.

Activitatea legată de autorizarea operațiunilor de transmitere transfrontalieră a datelor cu caracter personal

La capitolul activității legate de autorizarea operațiunilor de transmitere transfrontalieră a datelor cu caracter personal, prin prisma prevederilor art. 32 al Legii privind protecția datelor cu caracter personal, se relevă că transmiterea transfrontalieră a datelor cu caracter personal care fac obiectul unei prelucrări sau care urmează să fie prelucrate după transmitere poate avea loc doar cu autorizarea Centrului, în modul stabilit de lege și doar în cazul în care statul de destinație asigură un nivel adecvat de protecție a drepturilor subiecților datelor cu caracter personal și a datelor destinate transmiterii.

În anul 2020, Centrul a autorizat transmiterea transfrontalieră a datelor cu caracter personal doar în cazurile în care solicitările corespunzătoare au fost documentate adecvat de către actorii implicați, continuând a fi centrat pe asigurarea respectării principiilor de protecție a datelor cu caracter personal și drepturilor subiecților de date, precum și pe asigurarea nivelului optim de protecție a datelor transmise și/sau colectate în scopul prelucrării ulterioare în afara Republicii Moldova.

Totodată, în contextul activității relevante supra, se menționează că, demersurile și notificările examinate de Centru au vizat entități publice și private cu sediul în țări precum: Germania, România, Letonia, Ucraina, Olanda, Italia, Irlanda, Finlanda, Federația Rusă etc.

Prin urmare, în anul 2020 Centrul a recepționat **70** de solicitări ce vizează domeniul prelucrării transfrontaliere de date cu caracter personal, dintre care **28** – în bază de demersuri, iar **42** prin notificări depuse la „Ghișeul unic” al Centrului. Astfel, din cele 28 demersuri înaintate Centrului, în 14 cazuri a fost autorizată transmiterea transfrontalieră a datelor cu caracter personal iar în celelalte 14 cazuri demersurile au fost soluționate prin emiterea deciziei de refuz în autorizarea transmiterii transfrontaliere. În ceea ce privește numărul de notificări depuse de operatorii de date la „Ghișeul unic” al Centrului care aveau ca obiect inclusiv transferul transfrontalier de date cu caracter personal, au fost emise 13 decizii de autorizare și 29 decizii de refuz.

Ca și în perioadele precedente de raportare, motivele care au dus la emiterea deciziilor de refuz a autorizării transmiterii transfrontaliere de date cu caracter personal, au constituit: nerespectarea condițiilor de fond a demersului și/sau a înscrisurilor care vin să confirme circumstanțele și instrumentele legale pe care se întemeia solicitarea asistenței juridice. În context, în partea ce ține de nerespectarea condițiilor de fond a demersurilor și documentelor aferente, se evidențiază aspecte precum: lipsa consimțământului subiectului de date vizat; consimțământul nevalabil pentru anumite operațiuni indicate în solicitare; lipsa unui scop determinat, legitim și neexcesiv; numărul nejustificat al subiecților vizați sau volumul excesiv de date pe care operatorul intenționa să le prelucreze, atât în cadrul operațiunii de transmitere, cât și în cadrul unor eventuale transferuri transfrontaliere de date cu caracter personal în afara frontierei Republicii Moldova; neprezentarea documentelor necesare stabilirii legalității transmiterii transfrontaliere a datelor cu caracter personal sau prezentarea înscrisurilor neautentificate în modul corespunzător etc.

În ceea ce privește cazurile de refuz al autorizării transmiterii transfrontaliere a datelor cu caracter personal în baza notificărilor depuse la „Ghișeul unic” al Centrului, în majoritatea situațiilor au fost constatate: lipsa descrierii operațiunilor de prelucrare a datelor cu caracter personal; neindicarea măsurilor de protecție a datelor cu caracter personal în cadrul sistemelor de evidență; absența instrucțiunilor operatorului destinate persoanelor împuternicite să acționeze în numele acestuia etc.

III
CAPITOLUL III**RECOMANDĂRILE ȘI CAZUISTICA
ANULUI 2020**

Periodic, Centrul informează societatea despre problemele și preocupările prioritare în domeniul protecției datelor cu caracter personal, în special despre situația din domeniul protecției drepturilor subiecților datelor personale.

Totodată, în scopul asigurării prevenirii încălcărilor similare celor constatate deja, comise la prelucrarea datelor cu caracter personal, anual, inclusiv prin intermediul rapoartelor de activitate, Autoritatea de protecție a datelor cu caracter personal prezintă spețe/problematici aferente domeniului de referință.

Recomandări și opinii emise de Centru în anul 2020:

Astfel, pe parcursul anului 2020, Centrul a emis recomandări și opinii vizând unele situații de aplicabilitate generală sau de interes major pentru societate, având drept scop a oferi claritate în aplicabilitatea conformă și fără echivoc a prevederilor legale de domeniul protecției datelor cu caracter personal la prelucrarea acestor date. Printre opiniile/recomandările oferite de către Centru pe parcursul anului 2020 au fost următoarele:

Prelucrarea datelor cu caracter personal în contextul pandemiei de coronavirus (COVID-19) în Republica Moldova

Centrul a accentuat asupra riscurilor și provocărilor privind protecția persoanelor în partea ce vizează prelucrarea datelor cu caracter personal în contextul combaterii Coronavirusului (COVID-19), în special, a datelor privind starea de sănătate a pacienților.

Lupta împotriva COVID-19 este un obiectiv valoros împărtășit de toate națiunile, inclusiv de Republica Moldova și, prin urmare, trebuie susținut în cel mai bun mod posibil pentru a diminua și lichida răspândirea acestui virus. Din momentul declanșării COVID-19, se asistă zilnic la diverse operațiuni de prelucrare a datelor cu caracter personal privind starea de sănătate în contextul combaterii COVID-19. Toate aceste operațiuni de prelucrare a datelor cu caracter personal privind starea de sănătate trebuie să reprezinte o parte componentă a eforturilor concertate întru menținerea sănătății publice iar protecția datelor nu poate fi în niciun caz și nu este sub nici o formă un obstacol în calea salvării de vieți, respectiv, principiile aplicabile de legislația națională în domeniul protecției datelor cu caracter personal permit întotdeauna o echilibrare a intereselor puse în joc.

Întrucât nu orice operațiune de prelucrare a datelor cu caracter personal privind starea de sănătate poate fi justificată prin necesitatea statală de menținere a sănătății publice, devine stringentă păstrarea și implementarea unui mecanism fundamentat pe conceptul de echilibru între sănătatea/securitatea publică și dreptul la protecția datelor cu caracter personal.

Urmează a fi luat în considerație faptul că, datele cu caracter personal privind starea de sănătate, reprezintă o categorie specială de date, recunoscută ca atare în toate jurisdicțiile statale existente care dispun de un cadru juridic solid în materie de protecție a datelor cu caracter personal și care au aderat la Convenția 108 din 28.01.1981 pentru protecția persoanelor referitor la prelucrarea



automatizată a datelor cu caracter personal, nu doar în Republica Moldova. Caracterul special al datelor cu caracter personal privind starea de sănătate antrenează o conduită mult mai riguroasă la prelucrarea acestora, dar și norme de securitate care să asigure confidențialitatea datelor din partea autorităților în domeniul sănătății, alte autorități statale, persoane juridice de drept privat, persoane fizice etc. (operatorul, persoana împuternicită de operator și terț). Or, anume această operațiune de prelucrare a datelor cu caracter personal poate genera efecte extrem de negative în raport cu drepturile subiectului de date vizat.

Este evident că principiile de protecție a datelor cu caracter personal rămân în vigoare inclusiv pe perioada combaterii pandemiei de COVID-19 pentru toți actorii implicați în această luptă. Potrivit art. 4 al Legii 133/2011 privind protecția datelor cu caracter personal, pentru atingerea obiectivelor urmărite, datele cu caracter personal trebuie prelucrate în mod corect și conform prevederilor legii, colectate în scopuri determinate, explicite și legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri, să fie exacte și, dacă este necesar actualizate, respectiv, să fie stocate într-o formă care să permită identificarea subiecților datelor cu caracter personal pe o perioadă care nu va depăși durata necesară atingerii scopurilor pentru care sunt colectate și ulterior prelucrate. În același context, prelucrarea datelor cu caracter personal privind starea de sănătate de către operator, persoana împuternicită de operator sau terț care au nevoie de a prelucra întemeiat date personale, se pot încadra la temeiul legal reglementat la art. 5 alin. (5) lit. b), c), d), e) și art. 7 alin. (1) lit. a) și b) ale Legii 133/2011 privind protecția datelor cu caracter personal – prelucrarea este necesară pentru protecția sănătății publice sau prelucrarea este necesară în scopuri de medicină preventivă, de stabilire a diagnosticelor medicale, de administrare a unor îngrijiri sau tratamente pentru subiectul datelor cu caracter personal sau de gestionare a serviciilor de sănătate care acționează în interesul subiectului datelor cu caracter personal.

În plus, subiecții datelor cu caracter personal ar trebui să primească informații transparente cu privire la activitățile de prelucrare a datelor sale cu caracter personal și categoriile acestor date, inclusiv perioada de păstrare a datelor colectate, scopurile prelucrării etc. Informațiile furnizate ar trebui să fie ușor accesibile și furnizate într-un limbaj clar și simplu. În această ordine, drepturile subiectului datelor cu caracter personal sunt reglementate de Legea 133/2011 privind protecția datelor cu caracter personal, care la fel rămân în vigoare și acestea urmează a fi respectate de către toți operatorii și persoanele împuternicite de către operatori, vorbim despre: dreptul la informare a subiectului – art. 12; dreptul de acces la datele cu caracter personal – art. 13; dreptul de intervenție asupra datelor cu caracter personal – art. 14; dreptul de opoziție al subiectului datelor cu caracter personal – art. 16.

În cazul instituirii excepțiilor și restricțiilor în legătură cu existența unor circumstanțe statuate la alin. (1) art. 15 al Legii 133/2011 privind protecția datelor cu caracter personal, care justifică restrângerea drepturilor subiecților de date cu caracter personal, după încetarea situației care a justificat aplicarea excepțiilor și restricțiilor reglementate de alin. (1) și (2) al art. 15, operatorii vor lua măsurile necesare pentru a asigura respectarea drepturilor subiecților datelor cu caracter personal prevăzute la art. 12–14.

În acord cu art. 11 al Convenției 108 din 28.01.1981 pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, orice excepție și restricție pe dimensiunea prelucrării datelor cu caracter personal, trebuie să fie reglementate de lege, să respecte drepturile și libertățile fundamentale ale omului și să reprezinte o măsură necesară într-o societate democratică.

Prezintă relevanță Declarația comună a Președintelui Comitetului Convenției 108 și a Comisarului pentru protecția datelor al Consiliului Europei privind dreptul la protecția datelor în contextul pandemiei COVID-19, adoptată la Strasbourg în 30.03.2020, prin care s-a notat că, comunicarea



către public de către autoritățile competente ar trebui să rămână o prioritate de a avea capacitatea de a proteja, informa și consilia publicul. Cu toate acestea, în timpul acestor comunicări, publicarea de date sensibile (cum ar fi datele referitoare la sănătate) ale anumitor persoane ar trebui să fie evitată și se recomandă ca prelucrarea acestor date să fie făcută numai dacă se vor lua măsuri tehnice și organizatorice suplimentare [...].

Este de remarcat și Declarația Comitetului European pentru Protecția Datelor (EDPB-The European Data Protection Board) privind prelucrarea datelor cu caracter personal în contextul pandemiei COVID-19 (conținutul căreia poate fi vizualizat accesând link-ul: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonald ataandcovid-19_en.pdf).

O atenție deosebită urmează a fi acordată principiilor de protecție a datelor cu caracter personal și de către instituțiile mass-media care informează populația vizavi de pandemia de coronavirus. Efortul acestora urmează a fi îndreptat spre păstrarea confidențialității victimelor COVID-19 și neadmiterea divulgării identității acestora.

Pe perioada desfășurării activității profesionale de la domiciliu, ca măsură de combatere a COVID-19, pentru transmiterea în scop de serviciu a informațiilor care integrează date cu caracter personal vor fi utilizate adresele de e-mail securizate, metode de criptare și mijloace tehnice de comunicare destinate strict realizării atribuțiilor de serviciu, întru evitarea declanșării breșelor de securitate.

Prelucrarea datelor cu caracter personal privind localizarea subiecților de date în scopul monitorizării dacă aceștia respectă regimul de izolare, poate fi încadrată în temeiul legal al protecției sănătății publice. Totuși, această operațiune de prelucrare a datelor cu caracter personal care este extrem de intruzivă, urmează a fi implementată cu o deosebită prudență, proporționalitate și cu implementarea absolută a tuturor măsurilor de securitate, întrucât asemenea operațiune antrenează după sine implicații grave în adresa drepturilor și libertăților fundamentale ale subiecților. Dezvoltarea acestor soluții de supraveghere sau alte aplicații electronice (sisteme informaționale) menite să combată pandemia de COVID-19 trebuie să se bazeze pe o evaluare prealabilă a impactului prelucrării datelor asupra drepturilor și libertăților fundamentale ale persoanelor vizate și trebuie să proiecteze prelucrarea datelor astfel încât să prevină sau să reducă la minimum riscul de interferență negativă cu drepturile și libertățile fundamentale. Cu titlu informativ, operațiunea de prelucrare a datelor cu caracter personal prin metoda de monitorizare a locației persoanelor fizice (subiecți de date), în scopul determinării respectării regimului de izolare de către acestea, urmează a fi încetată imediat, odată cu atingerea scopurilor pentru care sunt colectate și prelucrate datele cu caracter personal ale subiectului de date.

Aspecte privind înregistrarea și transmiterea on-line a ședințelor consiliilor locale

Pe parcursul anului 2020, în adresa Centrului au parvenit multiple adresări prin care se solicita opinia autorității în legătură cu înregistrarea și transmiterea în direct prin intermediul internetului a ședințelor consiliilor locale. În acest sens, Centrul a venit cu următoarele reperi:

Analizând subiectul abordat, urmează a se nota, că prin publicarea în internet a ședințelor consiliilor locale, se va oferi acces la anumite informații care sunt puse în discuție în cadrul ședințelor, nu doar părților interesate din localitatea respectivă, dar unui număr nelimitat de persoane.

Atragem atenția că problematica discutată în cadrul ședințelor nu se referă doar la activități privind organizarea administrativă a localității, dar și cazuri/spețe individuale care vizează persoane fizice concrete, care pot dezvălui anumite aspecte ale vieții private, cum ar fi situația materială sau categorii speciale de date, spre exemplu privind starea de sănătate.



În acest sens, aducem în vizor următoarele noțiuni și prevederi ale Legii nr. 133 din 08 iulie 2011 privind protecția datelor cu caracter personal și anume:

operator – persoana fizică sau persoana juridică de drept public sau de drept privat, inclusiv autoritatea publică, orice altă instituție ori organizație care, în mod individual sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal prevăzute în mod expres de legislația în vigoare;

prelucrarea datelor cu caracter personal – orice operațiune sau serie de operațiuni care se efectuează asupra datelor cu caracter personal prin mijloace automatizate sau neautomatizate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, păstrarea, restabilirea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea prin transmitere, diseminare sau în orice alt mod, alăturarea ori combinarea, blocarea, ștergerea sau distrugerea;

sistem de evidență a datelor cu caracter personal – orice serie structurată de date cu caracter personal accesibile conform unor criterii specifice, fie că este centralizată, descentralizată ori repartizată după criterii funcționale sau geografice;

date cu caracter personal – orice informație referitoare la o persoană fizică identificată sau identificabilă (subiect al datelor cu caracter personal). Persoana identificabilă este persoana care poate fi identificată, direct sau indirect, prin referire la un număr de identificare sau la unul ori mai multe elemente specifice identității sale fizice, fiziologice, psihice, economice, culturale sau sociale.

Potrivit prevederilor art. 4 al Legii privind protecția datelor cu caracter personal, datele cu caracter personal care fac obiectul prelucrării trebuie să fie: prelucrate în mod corect și conform prevederilor legii; colectate în scopuri determinate, explicite și legitime, iar ulterior să nu fie prelucrate într-un mod incompatibil cu aceste scopuri; adecvate, pertinente și neexcesive în ceea ce privește scopul pentru care sunt colectate și/sau prelucrate ulterior.

În conformitate cu prevederile art. 5 alin. (1) al Legii privind protecția datelor cu caracter personal, operațiunile de prelucrare a datelor cu caracter personal se efectuează cu consimțământul subiectului datelor cu caracter personal. Totodată, consimțământul subiectului datelor cu caracter personal nu este cerut în cazurile prevăzute exhaustiv de art. 5 alin. (5) al aceluiași act legislativ, spre exemplu, pentru îndeplinirea unei obligații care îi revine operatorului conform legii ori executarea sarcinilor de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este investit operatorul sau terțul căruia îi sunt dezvăluite datele cu caracter personal.

Nu în ultimul rând, urmează a menționa că deciziile cu caracter individual, ar putea să conțină categorii speciale de date cu caracter personal care dezvăluie apartenența socială a persoanelor, datele privind starea de sănătate etc. Prelucrarea acestor categorii de date urmează a fi efectuată în strictă conformitate cu prevederile art. 6-8 ale Legii nr. 133/2011, având la bază cerința asigurării nivelului sporit de protecție din motivul prezenței unor riscuri speciale pentru inviolabilitatea dreptului la viață intimă, familială și privată.

În continuare, remarcăm prevederile art. 17 alin. (1) al Legii nr. 436-XVI din 28 decembrie 2006 privind administrația publică locală, potrivit cărora ședințele consiliului local sunt publice. Alin. (2) al aceluiași articol, menționează că orice persoană interesată poate asista la ședințele consiliului local.

Suplimentar, alin. (3) al aceluiași act normativ, prevede că cetățenii, asociațiile constituite în corespundere cu legea și alte părți interesate au dreptul: a) de a participa, în condițiile legii, la orice etapă a procesului decizional; b) de a avea acces la informațiile privind bugetul localității și modul de utilizare a resurselor bugetare, la proiectele de decizii și la ordinea de zi a ședințelor consiliului local și ale primăriei; c) de a propune inițierea elaborării și adoptării unor decizii; d) de a prezenta autorităților publice locale recomandări, în nume propriu sau în numele unor grupuri de locuitori ai colectivităților respective, privind diverse proiecte de decizie supuse dezbaterilor.



În acest sens, remarcăm că actul normativ prenotat nu instituie dreptul cetățenilor, asociațiilor și altor părți interesate de a înregistra și plasa ședințele consiliilor locale în spațiul on-line, ci oferă oportunitatea persoanelor interesate de a participa în procesul decizional.

Totodată, potrivit alin. (1), art. 3 din Legea privind statutul alesului local nr. 768-XIV din 02 februarie 2000, în unitatea administrativ-teritorială respectivă, alesul local este persoană oficială, el fiind reprezentantul autorității deliberative sau executive din administrația publică locală.

Subliniem că, în contextul art. 11 al Legii cu privire la libertatea de exprimare, informația despre viața privată și de familie a persoanei publice sau celei ce exercită o funcție publică, poate fi dezvăluită doar dacă prezintă un interes public (interes al societății și nu simpla curiozitate a indivizilor față de evenimentele ce țin de exercitarea puterii publice într-un stat democratic sau față de alte probleme care, în mod normal, nu trezesc interesul societății sau al unei părți a ei).

Chiar și potrivit raționamentelor CEDO, persoanele publice trebuie să accepte anumite ingerințe în viața lor privată în mai mare măsură decât persoanele obișnuite și gradul accesibil de cercetare mai atentă urmează să fie cu atât mai mare cu cât figura publică în cauză și informația ce se dezvăluie sunt mai importante. Elementul care trezește interesul public poate fi statutul persoanei (mandatul consilierului local) sau orice alte circumstanțe legate de exercitarea mandatului alesului local.

Astfel, anumite informații, inclusiv datele cu caracter personal ce vizează un ales local ar putea deveni informații de interes public în măsură în care nu afectează capacitatea de exercitare a funcției publice de persoana dată, ținându-se cont de existența dreptului la respectarea vieții sale private și de familie.

Pornind de la raționamentele menționate supra, ținând cont de sarcinile de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este investit operatorul (Consiliul local, Primăria), ultimul urmează să analizeze prin prisma normelor menționate supra și să reglementeze clar, printr-un act normativ, ce subiecte urmează a fi plasate public, ce categorii de date cu caracter personal vor fi dezvăluite în acest sens, modalitatea de informare a subiecților de date cu caracter personal despre plasarea în spațiul internet a ședințelor, oferirea posibilității realizării dreptului de opoziție, asigurarea măsurilor de securitate și confidențialitate a datelor cu caracter personal, stabilirea unui termen concret pentru care informațiile vor fi lăsate publice, mecanismul de ștergere a acestor înregistrări etc. Respectiv, acesta trebuie să stabilească clar care ședințe urmează a fi înregistrate și ulterior plasate în spațiul public, cine sunt persoanele desemnate/autorizate pentru înregistrarea ședințelor și difuzarea acestora în spațiul public, în condițiile legale.

Totodată, având în vedere că operatorul de date cu caracter personal (Consiliul local/Primăria) stabilește scopul și mijloacele prelucrării datelor cu caracter personal, de asemenea este responsabil și răspunde pentru orice prelucrare a datelor cu caracter personal efectuată, doar acestuia îi revine dreptul de a decide asupra posibilității furnizării datelor cu caracter personal spre acces public.

Precizări privind înregistrarea și transmiterea în direct prin intermediul internetului a ședințelor consiliilor locale

În contextul reacției societății civile, precum și a unor autorități publice locale, care au tratat greșit opinia expusă anterior în legătură cu înregistrarea și transmiterea în direct prin intermediul internetului a ședințelor consiliilor locale, Centrul ține să precizeze că nu intenționează să restricționeze înregistrarea și transmiterea în direct prin intermediul internetului a ședințelor consiliilor locale, iar anumite raționamente expuse anterior asupra subiectului dat au fost rupte din context și interpretate într-o manieră eronată.



În aceste circumstanțe este necesar a pune în evidență următoarele:

– *Transparența și accesul la informații reprezintă una dintre componentele esențiale ale oricărui sistem democratic. Pentru ca cetățenii să se poată implica în treburile publice, să participe în procesele de luare a deciziilor, să monitorizeze felul în care autoritățile își respectă atribuțiile iar persoanele alese promisiunile, aceștia trebuie să aibă acces la informațiile veridice despre faptele celor din urmă, iar autoritățile să asigure transparența în procesul decizional.*

– *Pe același palier de idei urmează a fi notat că potrivit alin. (1) art. 3 din Legea privind statutul alesului local nr. 768-XIV din 02 februarie 2000, în unitatea administrativ-teritorială respectivă, alesul local este persoană oficială/publică, el fiind reprezentantul autorității deliberative sau executive din administrația publică locală. Persoanele publice trebuie să accepte anumite ingerințe în viața lor privată în mai mare măsură decât persoanele obișnuite. Astfel, anumite informații, inclusiv datele cu caracter personal ce vizează un ales local ar putea deveni informații de interes public în măsură în care acestea sunt legate de exercitarea funcției publice de către persoana dată, ținându-se cont de existența dreptului la respectarea vieții sale private și de familie.*

– *În acord prevederile art. 17 alin. (1) al Legii nr. 436-XVI din 28 decembrie 2006 privind administrația publică locală, ședințele consiliului local sunt publice. Alin. (2) al aceluiași articol, menționează că orice persoană interesată poate asista la ședințele consiliului local. Totuși, remarcăm că actul normativ prenotat nu instituie dreptul/obligația acestora de a înregistra și plasa ședințele consiliilor locale în spațiul on-line. Chiar dacă prevederile art. 17 alin. (3) al legii prenotate, prescriu obligativitatea asigurării transparenței ședințelor consiliului local, aceasta urmează a fi realizată, inclusiv în conformitate cu prevederile legislației privind protecția datelor cu caracter personal, care reclamă respectarea anumitor cerințe/principii în acest sens.*

– *Subliniem că, caracterul deschis al anumitor date cu caracter personal trebuie să fie prevăzut de actele normative care reglementează anumite raporturi juridice. Precizăm că, chiar și potrivit prevederilor pct. 30 al Regulamentului cu privire la modul de ținere a Registrului de stat al actelor locale, aprobat prin Hotărârea Guvernului nr. 672 din 28 august 2017, deciziile cu caracter individual emise/adoptate de autoritățile administrației publice locale pot fi vizualizate public doar în formă depersonalizată. Aceiași abordare este necesar a fi pusă și la baza asigurării transparenței ședințelor consiliilor locale, urmare a înregistrării și transmiterii în direct prin intermediul internetului a subiectelor puse în discuție în cadrul acestora, în special în partea ce vizează adoptarea deciziilor cu caracter individual.*

– *Nu în ultimul rând, urmează a menționa că adesea, ținând cont de sarcinile de interes public sau care rezultă din exercitarea prerogativelor de autoritate publică cu care este investit consiliul local, în cadrul ședințelor sunt puse în discuție nu doar aspecte ce țin de comunitatea locală sau activitatea administrativă a autorității, dar și aspecte ce țin de viața privată a unor persoane concrete, care ar putea să dezvăluie, spre exemplu, informații/date despre apartenența socială a persoanelor (familii, copii, persoane în vârstă aflate în dificultate), datele privind starea de sănătate etc.*

În aceste circumstanțe, precum și în scopul asigurării unui echilibru între dreptul la libertatea de exprimare și dreptul de acces la informații, pe de o parte și dreptul la protecția datelor cu caracter personal, pe de altă parte, Centru a intervenit cu anumite recomandări în legătură cu înregistrarea și transmiterea în direct prin intermediul internetului a ședințelor consiliilor locale.

Respectiv, s-a recomandat ca consiliile locale să vină cu reglementări clare, prin acte normative, ce subiecte urmează a fi plasate public, ce categorii de date cu caracter personal vor fi dezvăluite în acest sens, modalitatea de informare a persoanelor despre plasarea în spațiul internet a ședințelor, oferirea posibilității realizării drepturilor în calitate de subiecți de date cu caracter personal, asigurarea măsurilor de securitate și confidențialitate a datelor cu caracter personal, stabilirea unui



termen concret pentru care informațiile vor fi lăsate publice, mecanismul de ștergere a acestor înregistrări etc. Actul normativ trebuie să stabilească clar care ședințe/parte a ședințelor urmează a fi înregistrate și plasate în spațiul public, cine sunt persoanele desemnate/autorizate pentru înregistrarea ședințelor și difuzarea acestora în spațiul public, în condițiile legale.

Unele aspecte privind cazuistica specifică anului 2020

Dezvăluirea neconformă a datelor cu caracter personal privind starea de sănătate

În baza plângerii unui subiect de date, Centrul a inițiat examinarea legalității operațiunii de prelucrare a datelor cu caracter personal, efectuate prin colectarea și dezvăluirea informației privind starea de sănătate a petentului, de către directorul unei companii în care activa petentul și directorul unei instituții medico-sanitare.

În fapt, s-a invocat că angajatorul petentului, a solicitat de la instituția medico-sanitară, informația din certificatele medicale eliberate ultimului, cum ar fi tratamentul staționar administrat nemijlocit și perioada de tratament, fără a avea consimțământul acestuia.

Analizând conținutul interpelării companiei, expediată către instituția medico-sanitară, Centrul a stabilit faptul că, compania în cauză a solicitat informația cu privire la concediile medicale acordate petentului în perioada 2015-2020 de către medicul neuropatolog, precum și diagnoza în temeiul căreia au fost acordate aceste concedii medicale.

Potrivit materialelor prezentate s-a reținut că angajatorul a solicitat informația care viza starea de sănătate a petentului în scop de a fi prezentată în instanța de judecată.

Ulterior, IMSP a expediat în adresa solicitantului răspunsul prin care a dezvăluit informații cu privire la perioada de timp a tratamentului și natura afecțiunilor ce viza petentul, în conformitate cu certificatele concediilor medicale eliberate, și anume:

1. „din 29.01.2016 până la 07.02.2016, tratament ambulatoriu ginecologic. Medic”;
2. „din 01.07.2019 până la 11.07.2019, tratament ambulatoriu ginecologic. Medic”;
3. „din 27.01.2020 până la 07.02.2020, tratament ambulatoriu neurologic. Medic”

Noțiunea de viață privată înglobează atât aspecte „tradiționale”, precum dreptul la imagine, starea civilă a persoanei, identitatea, starea de sănătate, apartenența religioasă, integritatea fizică și morală, viață sentimentală, dar și aspecte „moderne”, legate de percepții noi în viața socială referitoare la avort, homosexualitate, transsexualitate etc.

În acest context, informațiile privind starea de sănătate a pacientului, rezultatele investigațiilor, diagnosticul, pronosticul, tratamentul, înscrise în documentația medicală, contrapuse unui pacient, constituie categorii speciale de date cu caracter personal, acestea având un nivel sporit de protecție, prezentând riscuri ridicate pentru dreptul la viață intimă, familială și privată și urmând a fi necesară asigurarea confidențialității acestor date, în ordinea prevăzută de Legea privind protecția datelor cu caracter personal.

Corespunzător speței au fost scoase în evidență prevederile Legii nr. 263/2005 cu privire la drepturile și responsabilitățile pacientului, care conține norme juridice speciale care au drept scop consolidarea drepturilor fundamentale ale omului în sistemul serviciilor de sănătate, asigurarea respectării demnității și integrității pacientului și, reieșind din natura datelor sensibile privind starea de sănătate, stabilește condiții stricte de dezvăluire a acestora. Urmează a remarcă că datele privind starea de sănătate a pacientului, prin natura lor, pot prezenta risc pentru persoanele vizate



atunci când sunt prelucrate și, prin urmare, necesită o protecție sporită. Aceste date fac obiectul unui principiu de interdicție și trebuie să existe un număr limitat de circumstanțe în care o astfel de prelucrare este legitimă. Totodată, confidențialitatea datelor medicale reprezintă secret profesional, care este o formă a dreptului la respectarea vieții private. Interzicerea divulgării informațiilor medicale, calificate drept confidențiale este necesară pentru a garanta că instituțiile medico-sanitare asigură dreptul pacientului la respectarea vieții private.

Astfel, inclusiv art. 12 din Legea cu privire la drepturile și responsabilitățile pacientului, subliniază obligația lucrătorului medical de a proteja datele privind sănătatea. În consecință, confidențialitatea informațiilor cu privire la solicitarea de asistență medicală, examinare și tratament, inclusiv a altor informații ce constituie secret medical, este asigurată de medicul curant și specialiștii implicați în acordarea serviciilor de sănătate sau în cercetarea biomedicală (studiul clinic), precum și de alte persoane cărora aceste informații le-au devenit cunoscute datorită exercitării obligațiilor profesionale și de serviciu (alin. (2));

Totodată, informațiile ce se consideră confidențiale pot fi furnizate numai în cazul în care pacientul consimte acest lucru în mod explicit sau la solicitarea reprezentantului său legal (a rudei apropiate), în condițiile consimțite de pacient, în măsură adecvată capacității lui de înțelegere, în cazul în care în privința pacientului a fost instituită o măsură de ocrotire judiciară ori dacă legea o cere în mod expres (alin. (3)). În situații aparte, prezentarea informației confidențiale fără consimțământul pacientului sau al reprezentantului său legal (al rudei apropiate) se admite: c) la solicitarea motivată a organului de urmărire penală, a instanței judecătorești în legătură cu efectuarea urmăririi penale sau a procesului judiciar, în conformitate cu legislația (alin. (4)).

Prin urmare, Centrul a reținut că dezvăluirea informației cu privire la perioada de timp a tratamentului și natura afecțiunilor în speța examinată a avut loc contrar prevederilor legale menționate supra și principiilor de prelucrare a datelor cu caracter personal prevăzute la art. 4 alin. (1) lit. a) și b) din Legea privind protecția datelor cu caracter personal.

Încălcarea drepturilor subiecților de date cu caracter personal

Art. 12-14, 16-17 ale Legii nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal consacră drepturi personale și inviolabile (dreptul la informare, dreptul de acces, dreptul de intervenție, de opoziție), pe care subiectul datelor cu caracter personal le poate realiza în raport cu operatorul de date care a efectuat operațiunea de prelucrare a datelor cu caracter personal a acestuia.

În continuitatea considerentului expus, se arată că pe parcursul anului 2020, Centrul a înregistrat și examinat plângeri ale subiecților de date, care au reclamat nerespectarea de către operatorii de date a drepturilor acestora, în special a dreptului de acces la datele cu caracter personal prelucrate de către operatori, fiind constatat, cu regret, faptul că unii operatori de date nu reacționează la solicitările subiecților de date, neoferindu-le răspunsuri în termenul prevăzut de legislație, precum și neasigurând realizarea efectivă a drepturilor acestora prin prisma legislației din domeniul protecției datelor cu caracter personal.

La începutul anului 2020, în adresa Centrului a parvenit plângerea unui subiect de date cu caracter personal, solicitând examinarea pretinsei încălcări a dreptului de acces la datele cu caracter personal ce-l vizează, de către o companie de creditare.

În context, subiectul de date a invocat faptul că a depus o cerere în adresa companiei de creditare, indicând datele cu caracter personal ce îl vizează, nefiind informat de către reprezentanții companiei despre rezultatul examinării cererii menționate.



În acest sens, subiectul de date cu caracter personal a depus altă cerere în adresa companiei de creditare solicitând informații privind modul de prelucrare a datelor cu caracter personal ce îl vizează, context în care, nici până la data depunerii plângerii către Centru, compania de creditare nu i-a oferit nici un răspuns.

Astfel, în urma examinării plângerii menționate, Centrul a constatat încălcarea prevederilor art. 13 alin. (1) al Legii privind protecția datelor cu caracter personal de către compania de creditare, în partea ce ține de nerealizarea dreptului de acces la prelucrarea datelor cu caracter personal ce vizează subiectul de date.

Drept rezultat, companiei de creditare i-a fost întocmit proces-verbal cu privire la contravenție în baza art. 74¹ alin. (3) Cod Contravențional.

Prelucrarea prin dezvăluire/publicare a IDNP-ului subiecților de date cu caracter personal

În adresa Centrului au parvenit plângerile unor subiecți de date cu caracter personal, care au solicitat verificarea legalității prelucrării datelor cu caracter personal care îi vizează, de către un executor judecătoresc, manifestată prin publicarea în Monitorul Oficial al Republicii Moldova a unui anunț privind desfășurarea licitației, în care sunt indicate IDNP-urile subiecților de date cu caracter personal.

Examinând cadrul legal ce reglementează activitatea executorilor judecătorești, Centrul a constatat că prevederile legale aplicabile speței de referință, nu prevăd publicarea IDNP-ului persoanei fizice (debitor/creditor) în anunțurile publicate în Monitorul Oficial al Republicii Moldova, iar art. 9 al Legii privind protecția datelor cu caracter personal stabilește expres cazurile/temeiurile când poate fi prelucrat IDNP-ul.

În acest sens, este de menționat că numărul de identificare de stat (IDNP) se supune unui regim juridic special, statuat la art. 9 al Legii privind protecția datelor cu caracter personal, potrivit căruia, prelucrarea IDNP-ului persoanei fizice, a amprentelor digitale sau a altor date cu caracter personal având o funcție de identificare de aplicabilitate generală poate fi efectuată în următoarele condiții:

- a) subiectul datelor cu caracter personal și-a dat consimțământul;
- b) prelucrarea este prevăzută în mod expres de legislație.

Este important de menționat că Centrul nu a pus la îndoială și nu a negat drepturile executorului judecătoresc, prevăzute de Codul de executare, privind întreprinderea anumitor acțiuni care sunt strict necesare îndeplinirii atribuțiilor dictate de lege. Totuși, toate potențialele operațiuni care presupun prelucrarea datelor cu caracter personal întru realizarea atribuțiilor legale, urmează a fi efectuate cu respectarea principiilor statuate de Legea privind protecția datelor cu caracter personal.

Astfel, în rezultatul examinării cazului s-a constatat că prelucrarea prin dezvăluire/publicare a IDNP-ului subiecților de date cu caracter personal, de către executorul judecătoresc, în Monitorul Oficial al Republicii Moldova, la care au acces un număr nelimitat de persoane, a avut loc în mod contrar prevederilor art. 4 alin. (1) lit. a), art. 5 alin. (1), art. 9 și art. 29 ale Legii privind protecția datelor cu caracter personal.

Respectiv, executorului judecătoresc i-a fost întocmit proces-verbal cu privire la contravenție în baza art. 74¹ alin. (4) Cod Contravențional.



Protecția datelor cu caracter personal vs libertatea de exprimare și dreptul la informare

În linii generale, urmează a reliefa că dreptul la respectarea vieții private, intime și de familie, precum și dreptul la libertatea de exprimare sunt două drepturi fundamentale care se regăsesc atât în actele internaționale în materia ocrotirii drepturilor și libertăților omului cât și în Constituția Republicii Moldova

Se notează că, Constituția Republicii Moldova conferă oricărui cetățean și îi garantează libertatea gândirii, a opiniei, precum și libertatea exprimării în public prin cuvânt, imagine sau prin alt mijloc posibil, atât timp cât nu se prejudiciază onoarea, demnitatea sau dreptul altei persoane la viziune proprie. Totodată, la art. 55 din actul suprem se regăsește acea limitare, potrivit căreia, orice persoană își exercită drepturile și libertățile constituționale cu bună-credință, fără să încalce drepturile și libertățile altora.

Executarea acestor libertăți ce comportă îndatoriri și responsabilități poate fi supusă unor formalități, condiții, restrângeri sau sancțiuni prevăzute de lege, care constituie măsuri necesare, într-o societate democratică, pentru securitatea națională, integritatea teritorială sau siguranța publică, apărarea ordinii și prevenirea infracțiunilor, protecția sănătății sau a moralei, protecția reputației sau a drepturilor altora, pentru a împiedica divulgarea de informații confidențiale sau pentru a garanta autoritatea și imparțialitatea puterii judecătorești.

Astfel, putem să constatăm că situațiile examinate generează o problemă extinsă și complexă, datorită drepturilor și valorilor care constituie obiectul raportului juridic creat, astfel, fiind necesară o conciliere între unele dintre drepturile fundamentale care guvernează un stat de drept și o societate democratică: dreptul la informare, libertatea de exprimare și dreptul la inviolabilitatea vieții private.

*Centrul a fost sesizat prin plângerile unor subiecți de date, care au reclamat acțiunile pretins ilegale ale unui activist civic privind publicarea pe profilul personal de pe rețeaua de socializare "Facebook", în lipsa consimțământului acestora, a înregistrărilor video ce conțin categoria obișnuită de date cu caracter personal ale acestora – nume, prenume, funcția deținută și instituția publică în care activează subiectul de date cu caracter personal și, cel mai important – **adresa de domiciliu**.*

În cadrul examinării cauzelor s-a determinat că, contul de profil al persoanei ce a publicat înregistrările video pe rețeaua de socializare "Facebook", sunt accesibile oricărui utilizator al rețelei în cauză, fie că vorbim despre prietenii acesteia sau urmăritorii rețelei de socializare, care pot vizualiza postarea/publicarea în fluxul de știri de la alți utilizatori și care au link-ul direct la postările respective prin motoare de căutare.

De asemenea, pentru fiecare caz în parte, s-a stabilit că înregistrările video captează imagini cu adresa de domiciliu ale subiecților de date – strada și numărul casei de locuit, care au fost diseminate în spațiul public, pe rețeaua de socializare "Facebook", fără consimțământul acestora, informațiile în cauză fiind vizualizate și distribuite de un număr impunător de persoane/utilizatori.

Totodată, în latura publicării/dezvăluirii pe rețeaua de socializare "Facebook" a datelor cu caracter personal – adresa de domiciliu/viza de reședință a subiecților de date, Centrul a analizat separat 1) scopul prelucrării datelor cu caracter personal – publicarea/diseminarea adresei de domiciliu a subiectului de date cu caracter personal, informație referitoare la persoana fizică, care, în sensul art. 3 al Legii privind protecția datelor cu caracter personal, constituie date cu caracter personal, precum și 2) mijloacele prelucrării datelor cu caracter personal, care au fost utilizate de către operator la publicarea/diseminarea acestora, îndeosebi – adresa de domiciliu, pe pagina personală de profil pe rețeaua de socializare „Facebook”.



Raportat la cauzele examinate, Centrul a constatat că prin publicarea înregistrării video pe profilul personal din rețeaua de socializare „Facebook” de către activistul civic a fost dezvăluită categoria obișnuită de date cu caracter personal – nume, prenume, funcția deținută și instituția publică în care activează subiectul de date cu caracter personal, date ce sunt strâns legate de calitatea de persoană publică, de caracterul public al faptelor în care este implicat subiectul de date, care deține o funcție publică, de demnitate publică, ordine în care, prelucrarea acestor date a fost efectuată în condițiile art. 10 al Legii privind protecția datelor cu caracter personal.

Este lesne de specificat, în limite generale, când abordăm subiectul privind persoanele care exercită anumite funcții publice, gradul de ingerință în inviolabilitatea vieții private este mult mai mare, comparativ cu persoanele care nu dispun de un asemenea statut. Cu atât mai mult, acest grad de ingerință se extinde în ipoteza unor circumstanțe publice/fapte publice și în cazul existenței unor subiecte care pot prezenta interes public. Totuși, trebuie de avut în vedere faptul că, statul are obligația pozitivă de a legifera mecanisme legale de protecție a inviolabilității vieții private chiar și în cazul persoanelor publice care exercită funcții, care sunt implicate în circumstanțe/fapte publice și/sau sunt vizate în subiecte de ordin public. Or, este inadmisibil faptul ca această categorie de subiecți de date cu caracter personal să fie lipsiți de garanții juridice și mecanisme care să le asigure protecția dreptului lor constituțional – inviolabilitatea vieții private.

Distinct de cele expuse supra, în partea ce ține de dezvăluirea/diseminarea înregistrării video în spațiu public pe rețeaua de socializare „Facebook”, fără consimțământul subiectului de date a categoriei obișnuite de date cu caracter personal – adresa de domiciliu se accentuează că prelucrarea acestor date prezintă un risc sporit pentru viața privată și de familie a subiectului de date, întrucât aceasta nu intră în categoria informației publice, spre deosebire de celelalte date cu caracter personal – nume, prenume, funcția deținută și instituția publică în care activează subiectul de date, ce ar putea fi considerate informații publice odată ce subiectul de date este funcționar public/persoană cu funcție de demnitate publică/persoană publică.

În contextul cazurilor examinate a fost reținut că activistul civic – operator de date în sensul art. 3 al Legii privind protecția datelor cu caracter personal, **avea obligația să asigure confidențialitatea datelor cu caracter personal, și anume a adresei de domiciliu, prin prisma obligativității prevăzute la art. 29 al Legii privind protecția datelor cu caracter personal.**

Prin urmare, în fiecare caz în parte, Centrul a constatat că publicarea/dezvăluirea pe profilul de pe rețeaua de socializare „Facebook”, a datelor cu caracter personal ale subiecților de date, și anume a adresei de domiciliu, în lipsa consimțământului acestora, este contrară prevederilor art. 4 alin. (1) lit. a), art. 5 alin. (1) și art. 29 alin. (1) ale Legii privind protecția datelor cu caracter personal.

Astfel, în privința activistului civic au fost întocmite procese-verbale cu privire la contravenție în temeiul art. 74¹ alin. (4) Cod contravențional.

Nerespectarea confidențialității și securității datelor cu caracter personal

Centrul a recepționat notificarea unui operator de date – agent economic, prin care ultimul a raportat producerea incidentului de securitate materializat prin depistarea de către terțe persoane, într-o pădurice, a unui număr impunător de carduri de pontaj ale salariaților din cadrul agentului economic (vizând 394 de persoane), în care se conțin date cu caracter personal precum: nume, prenume, IDNP, cod de identificare în cadrul unității, fotografie.

Astfel, în urma examinării materialelor aferente incidentului de securitate produs, s-a determinat, că persoanele care se fac responsabile de încălcarea instrucțiunilor interne ale operatorului, sunt: specialistul resurse umane și un agent din cadrul entității, fiind încălcate prevederile Regulamentului privind protecția datelor cu caracter personal ale salariaților companiei, care stabilește că:



– în cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau suport electronic care conține date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie;

– scoaterea și introducerea mijloacelor de prelucrare a datelor cu caracter personal din/în perimetrul de securitate se înregistrează în registru.

Prin urmare, s-a constatat încălcarea prevederilor art. 29 alin. (2) și art. 30 alin. (2) ale Legii privind protecția datelor cu caracter personal, deoarece, acțiunile/inacțiunile persoanelor responsabile, manifestate prin neîndeplinirea corespunzătoare a instrucțiunilor interne ale operatorului, în latura asigurării confidențialității și securității datelor cu caracter personal la care au avut acces, au cauzat producerea incidentului de securitate sub formă de dezvăluire prin diseminare a datelor cu caracter personal ale 394 de subiecți de date, inclusiv acces neautorizat la aceste date, or, potrivit informațiilor prezentate de către operator, cardurile de pontare ale subiecților de date au fost depistate de niște trecători, deci terți.

Ca urmare, dat fiind prezența semnelor constitutive ale componenței de contravenții prevăzute de art. 74¹ alin. (1) și alin. (4) Cod Contravențional, în privința persoanelor responsabile din cadrul operatorului de date au fost întocmite procese-verbale cu privire la contravenție.

Totodată, în pofida circumstanțelor indicate supra, având în vedere incidentul de securitate produs, în cazul în care operatorul nu are o necesitate legitimă și explicită, bazată strict pe un scop bine determinat, Centrul a dispus reevaluarea de către operator a necesității utilizării numărului de identificare de stat în cardurile de pontare emise de către operator, dacă acest fapt nu presupune cheltuieli disproporționate de timp, mijloace și forță de muncă.

Ca rezultat, în contextul executării măsurilor legale dispuse de Centru, agentul economic a informat despre înlocuirea numărului de identificare de stat de pe cardurile de pontare cu numărul tabelar al salariatului, această din urmă identificare suplimentară fiind indispensabilă inclusiv prin prisma faptului că la întreprindere există multe cazuri când angajații au același nume și prenume.

Accesarea datelor cu caracter personal stocate în resurse informaționale de stat de către colaboratorii organelor de poliție

Centrul a recepționat mai multe demersuri ale Inspectoratului General al Poliției (IGP), în baza cărora au fost inițiate proceduri de verificare a conformității prelucrării datelor cu caracter personal efectuate de către angajații unei subdiviziuni a Inspectoratului Național de Investigații din cadrul IGP.

Din conținutul demersurilor s-a stabilit că examinarea aspectelor sesizate vizează aproximativ **12 000 de operațiuni de accesare a datelor cu caracter personal**, stocate în sisteme informaționale de stat, efectuate de către angajații respectivei entități.

Circumstanțele examinate de Centru în cazurile date au demonstrat cu certitudine numărul exorbitant al operațiunilor de accesări de date cu caracter personal efectuate de către colaboratorii organelor de poliție, vizând un număr impunător de subiecți de date, precum și faptul că o mare parte a acestor operațiuni, nu au avut la bază un scop bine determinat, un temei legal expres și o legătură causală dintre un material/dosar aflat în examinare și persoana fizică ale cărei date cu caracter personal au fost supuse prelucrării prin accesare/vizualizare/imprimare etc.

În special, au fost stabilite o multitudine de încălcări, atât ale prevederilor Legii privind protecția datelor cu caracter personal, cât și ale Regulamentului privind reglementarea prelucrării datelor cu caracter personal de către subdiviziunile Ministerului Afacerilor Interne aprobat prin Ordinul Ministrului Afacerilor Interne al Republicii Moldova nr. 444 din 28.12.2012 și ajustat prin Ordinul Ministrului Afacerilor Interne al Republicii Moldova nr. 260 din 04.09.2017, cum ar fi:



– număr foarte mare de operațiuni de accesare/consultare a datelor cu caracter personal care nu au fost consemnate în Registrele de evidență a accesărilor/prelucrărilor datelor cu caracter personal de către utilizatorii autorizați;

– necompletarea în modul corespunzător a rubricii “justificarea, scopul, temeiul și necesitatea accesării/prelucrării datelor cu caracter personal” din Registrul de evidență a accesărilor/prelucrărilor datelor cu caracter personal. Or, cu titlu de precizare se va menționa că, temeiul legal care poate sta la baza prelucrării datelor cu caracter personal în cadrul diverselor sisteme informaționale, în special în cadrul registrelor de stat și, care ar acorda operatorului de date cu caracter personal/utilizatorului dreptul de a efectua asemenea operațiuni, este condiționat de situația în care operatorul de date cu caracter personal/utilizatorul are în examinare un material, în care este vizat subiectul de date cu caracter personal, demonstrând astfel o legătură de cauzalitate dintre datele cu caracter personal prelucrate și materialul examinat, cu condiția prelucrării unui volum de date neexcesiv, strict necesar scopului. Astfel, că **nu este suficientă indicarea** ca fiind temei legal doar a informației precum **“necesitate de serviciu”/“cauză penală”/“dosar penal”** etc.;

– refuzul prezentării informațiilor solicitate de Centru în vederea exercitării activității de control sub pretextul că acestea ar face parte din categoria documentelor atribuite la secret de stat. Or, analizând categoriile de informații atribuite la secret de stat, indicate în Nomenclatorul informațiilor atribuite la secret de stat, aprobat prin Hotărârea Guvernului nr. 411 din 25.05.2010 și prevederile Hotărârii Guvernului nr. 1176 din 22.12.2010 pentru aprobarea Regulamentului cu privire la asigurarea regimului secret în cadrul autorităților publice și al altor persoane juridice, s-a constatat că informațiile ce urmau a fi puse la dispoziția Centrului nu aparțin la categoria informației ce poate fi atribuită la secret de stat. Astfel, afirmațiile invocate la caz de utilizatori și operatorul vizat au fost apreciate ca fiind critice, deoarece pretinsa atribuire la secret de stat a unor informații și materiale necesar a fi ținute/gestionate de utilizatorii autorizați cu dreptul de a accesa resurse informaționale de stat a constituit doar paravan în a prezenta anumite probe.

În consecință, în toate cazurile vizând totalul celor 12 000 de operațiuni de accesare a datelor cu caracter personal, Centru a constatat încălcarea prevederilor Legii privind protecția datelor cu caracter personal prin acțiunile/inacțiunile angajaților IGP/INI.

Totodată, **au fost dispuse măsuri necesar a fi întreprinse de către IGP/INI și MAI, cum ar fi următoarele:**

Entitățile vizate **vor dispune implementarea măsurilor adiționale pentru protecția datelor cu caracter personal, în partea ce ține de evidența accesărilor/consultărilor datelor cu caracter personal stocate în registrele de stat la care au acces, prin:**

– înăsprirea controlului intern (trimestrial sau semestrial) privind obligativitatea ținerii de către efectivul IGP și INI a Registrului de evidență manual și/sau electronic a accesărilor/prelucrărilor efectuate, în scopul neadmiterii pe viitor a accesării/consultării datelor cu caracter personal de către efectivul IGP și INI, în cazul inexistenței **legăturii de cauzalitate între: (1) dosarul special/dosarul analitic/dosarul operativ/dosarul de căutare/cauza penală/cauza contravențională și (2) persoana vizată;**

– înăsprirea controlului intern privind obligativitatea păstrării la Registrul de evidență a accesărilor/prelucrărilor efectuate a cererilor (rapoartelor/notelor) prezentate utilizatorului în vederea accesării/consultării resurselor informaționale și dezvăluirii datelor cu caracter personal de către efectivul IGP și INI;

– înregistrarea (în cancelarie/altă subdiviziune responsabilă) în ordinea stabilită a Registrelor de evidență manuală și/sau electronică a accesărilor/prelucrărilor efectuate;



- crearea unui mecanism intern, care ar stabili ca, la eliberarea sau transferul în altă subdiviziune a angajatului MAI, Registrul de evidență manual și/sau electronic a accesărilor/prelucrărilor efectuate să fie transmis spre arhivare;
- transmiterea Registrului de evidență manual și/sau electronic a accesărilor/prelucrărilor, urmează a fi inclusă în lista de lichidare, pe care angajatul MAI urmează să o prezinte la eliberarea din funcție;
- ținerea Registrului de evidență manual și/sau electronic a accesărilor/prelucrărilor efectuate în strictă conformitate cu cerințele legale, cu consemnarea tuturor rubricilor indicate;
- aducerea la cunoștință fiecărui angajat MAI/IGP, contra semnătură, a conținutului Ordinului MAI nr. 444 din 28.12.2012 cu privire la aprobarea Regulamentului privind reglementarea prelucrării datelor cu caracter personal de către subdiviziunile Ministerului Afacerilor Interne etc.



CAPITOLUL IV

ACTIVITATEA DE REPREZENTARE ÎN INSTANȚELE DE JUDECATĂ

În ordine de contencios administrativ

Pe parcursul anului 2020, interesele Centrului au fost reprezentate în cadrul instanțelor de contencios administrativ în **126** de procese de judecată, dintre care: 121 în calitate de pârât; 5 în calitate de autoritate publică ce depune concluzii.

Astfel, se atestă o creștere a numărului acțiunilor înaintate spre examinare în instanțele de judecată prin care au fost contestate actele emise de Autoritatea națională de protecție a datelor cu caracter personal, care, în perioada de raportare au ajuns la 121, spre deosebire de anul 2019 când au fost înaintate 105 cereri de chemare în judecată.

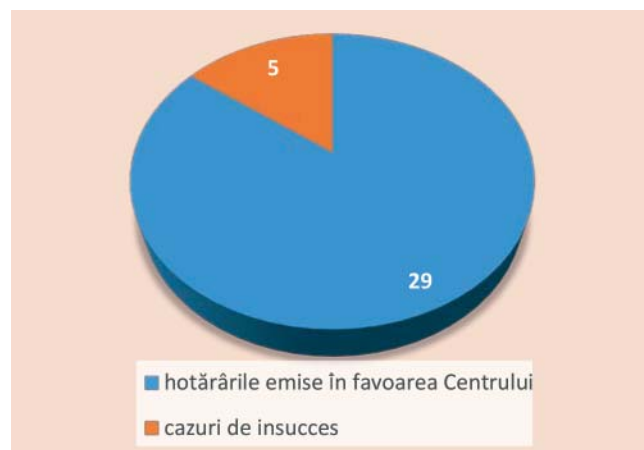
Acest fapt se datorează inclusiv numărului tot mai mare de acte administrative emise de Centru, precum și de conștientizarea tot mai înaltă a complexității consecințelor și a însemnătății caracterului constatărilor consemnate în deciziile emise de Centru.

Prin urmare, pe parcursul anului 2020, reprezentanții Centrului au asigurat participarea în cadrul a **307** ședințe de judecată în ordine de contencios administrativ, întocmind **200** de acte procedurale necesare pentru examinarea cât mai eficientă a cauzelor judiciare.

Totodată, remarcăm că în 5 procese de judecată Centrul a fost atras ca autoritate publică ce a depus concluzii, în conformitate cu prevederile art. 74 alin. (1) Cod de Procedură Civilă.

La fel, menționăm că pe parcursul anului 2020 a fost finalizată examinarea a **34** dosare judecătorești în care hotărârile/deciziile instanțelor judecătorești au rămas definitive și irevocabile, dintre care:

- 29 hotărâri/decizii judecătorești au fost emise în favoarea Centrului;
- 5 cazuri s-au soldat cu insucces pentru Centru.

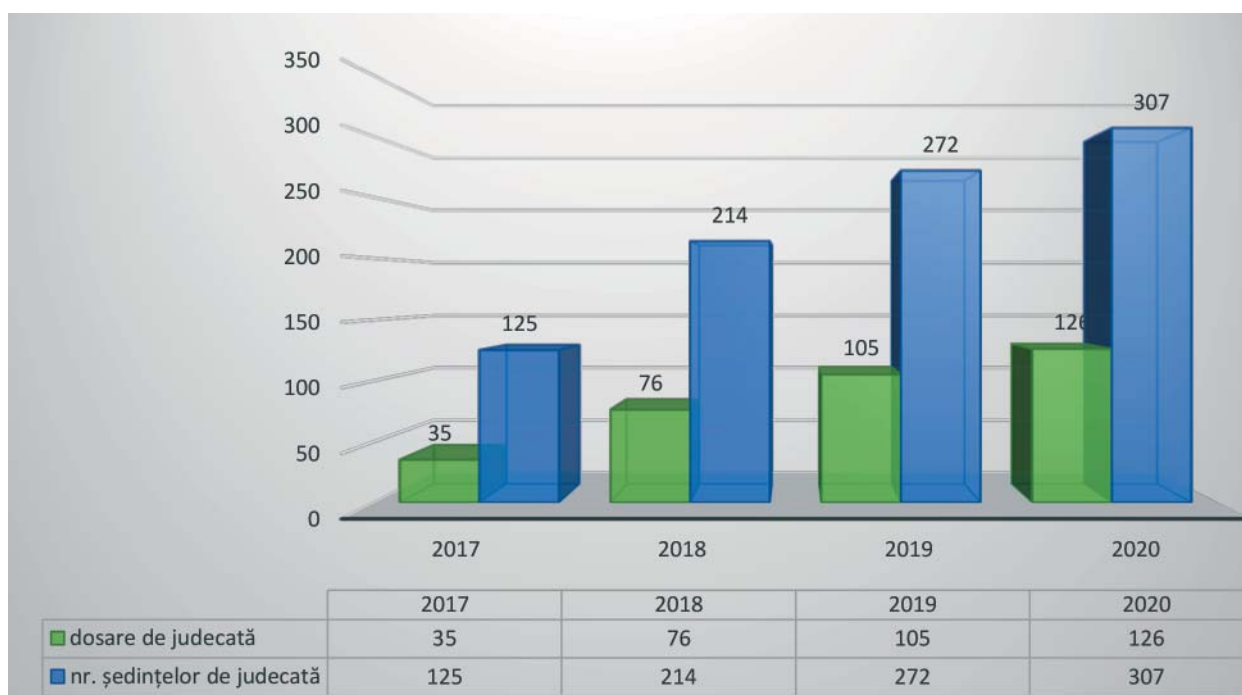
Dinamica hotărârilor judecătorești 2020



Astfel, constatăm că în **85%** din numărul de dosare judiciare examinate, acțiunile întreprinse de Centru au fost considerate legale și întemeiate de către instanțele de judecată.

De menționat că, reieșind din specificul aspectelor abordate în cererile de chemare în judecată, în 90% obiect al examinării acțiunilor în contencios administrativ îl constituie anularea deciziilor emise în urma investigațiilor efectuate de Centru cu privire la constatarea/lipsa încălcării principiilor de protecție a datelor cu caracter personal, 9% constituie anularea deciziilor cu privire la refuzul înregistrării în Registrul de evidență al operatorilor de date cu caracter personal, 1% reprezintă cauzarea pretinselor prejudicii.

Dinamica comparativă a numărului de dosare și ședințe de judecată în ordine de contencios administrativ, în perioada 2017-2020



La capitolul reprezentării intereselor Centrului în instanța de contencios administrativ, este important **a exemplifica un dosar judiciar de rezonanță**, examinarea judecătorească al căruia s-a finalizat în perioada de referință, soldându-se cu succes pentru Autoritatea de protecție a datelor cu caracter personal și având impact asupra realizării drepturilor unui număr impunător de subiecți de date cu caracter personal:

La 20 mai 2020, Curtea Supremă de Justiție a Republicii Moldova a decis în mod irevocabil menținerea în vigoare a deciziei Centrului din 16 noiembrie 2018, prin care a fost constatăată prelucrarea neconformă a datelor cu caracter personal cu cerințele legislației în domeniul protecției datelor cu caracter personal de către Ministerul Afacerilor Interne, prin intermediul Sistemului Informațional Automatizat „Registrul informației criminalistice și criminologice”, ultimul fiind obligat să distrugă informațiile ce conțin date cu caracter personal referitoare la subiectul de date vizat de această prelucrare, care au fost colectate/obținute de la autoritățile/instituțiile nerecunoscute din regiunea transnistreană.

La caz, în cadrul examinării celor invocate în plângere de către subiectul de date cu caracter personal, Centrul a scos în evidență practica vicioasă de recepționare și stocare de către autoritățile constituționale ale Republicii Moldova a informațiilor parvenite de la structurile neconstituționale din stânga Nistrului.



Urmează a sublinia că, **prelucrarea în mod automatizat a datelor cu caracter personal ale cetățenilor statului Republicii Moldova în baza unor informații parvenite de la structurile neconstituționale, care de fapt nu pot fi considerate autentice/veridice, precum și utilizarea acestora în detrimentul subiectului de date cu caracter personal vizat, reprezintă o încălcare gravă a drepturilor și libertăților omului.**

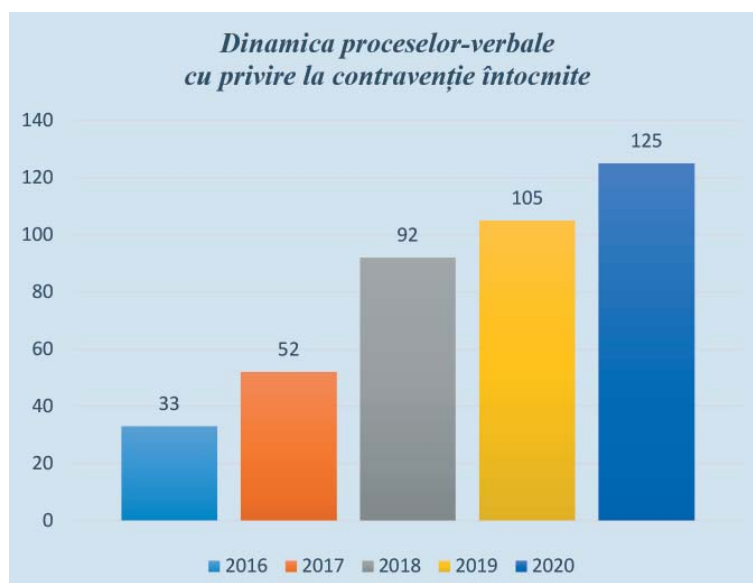
În acest sens, urmează a remarca Hotărârea Consiliului Superior al Magistraturii (CSM) nr. 209/14 din 10 aprilie 2012 *“cu privire la demersul domnului Oleg Efrim, ministru al Justiției, referitor la opinia asupra adresării domnului Eugen Carпов, viceprim-ministru, pe marginea abordării unor probleme de natură juridică”, prin care CSM a constatat: “că orice act emis de autoritățile autoproclamate din această parte a Republicii Moldova contravin din capul locului Constituției, faptul referindu-se în egală măsură și asupra oricăror hotărâri, decizii, sentințe pronunțate de judecătorii instituite în regiunea dată ilegal. Astfel, Consiliul consideră ca fiind inacceptabile orice colaborări, conlucrări în aspect juridic și propuneri de soluții juridice cu structurile din regiunea transnistreană.”*

În consecință, în jurisprudența ce vizează Republica Moldova, Curtea Europeană a Drepturilor Omului în numeroase cazuri (Ilașcu și alții vs. Moldova și Rusia; Eriomenco c. Republicii Moldova și Federației Ruse; Mozer c. Republicii Moldova și Federației Ruse; Catan alții c. Republicii Moldova și Rusiei) a constatat ilegalitatea actelor adoptate de entități nerecunoscute și neconstituționale din stânga Nistrului.

De specificat că, potrivit Declarațiilor depuse odată cu instrumentul de ratificare al Convenției nr. 108 pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, Republica Moldova nu a declarat rezerve asupra dispozițiilor convenției, în ceea ce privește aplicarea acesteia asupra teritoriului din regiunea transnistreană. Astfel, Republica Moldova are obligația de a asigura protecția drepturilor și libertăților fundamentale ale cetățenilor săi în ceea ce privește prelucrarea datelor cu caracter personal, în special a dreptului la inviolabilitatea vieții intime, familiale și private, pe întreg teritoriul său.

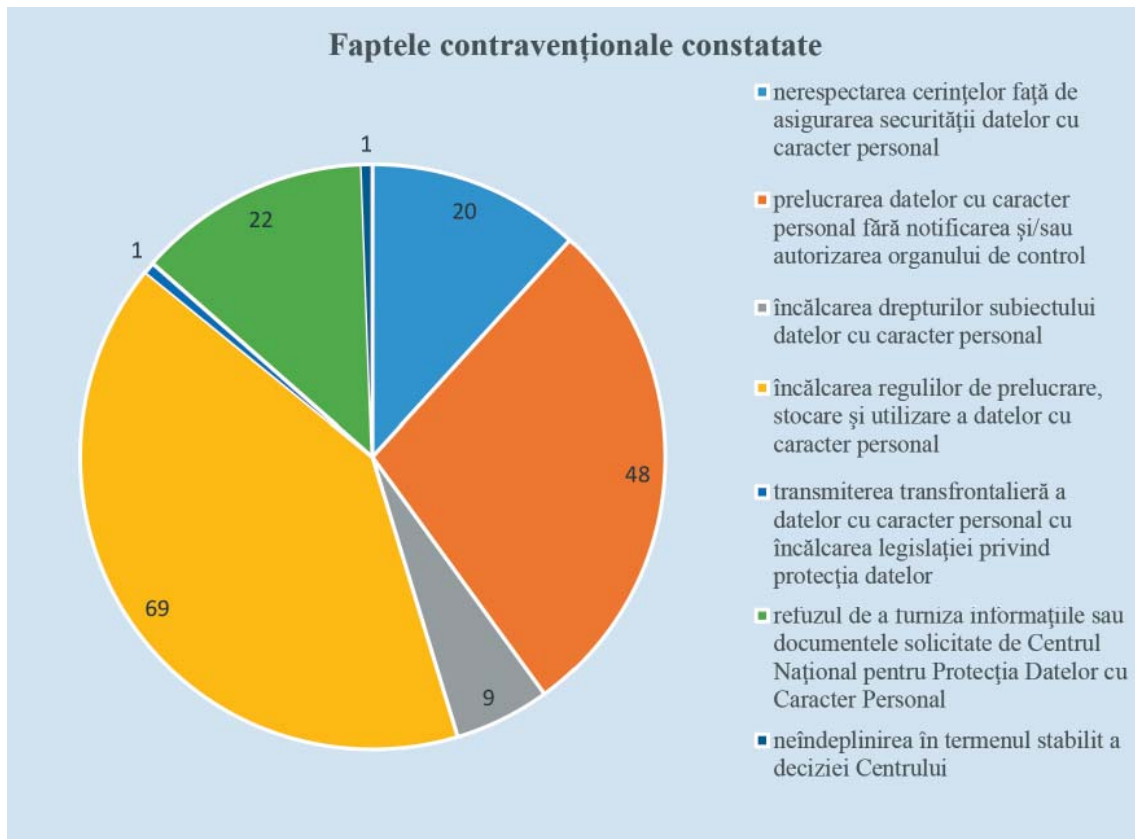
În ordinea procedurii contravenționale

Pe parcursul anului 2020, au fost întocmite **125** procese-verbale cu privire la contravenții, fiind constatate **170** fapte contravenționale aferente încălcării prevederilor legale din domeniul protecției datelor cu caracter personal, prin prisma prevederilor art. 74¹ – 74³ Cod contravențional, cauzele contravenționale fiind expediate spre examinare în instanța de judecată competentă.





Spectrul faptelor contravenționale constatate prin prisma articolelor vizate de Codul contravențional în baza încălcărilor comise la prelucrarea datelor cu caracter personal sunt reflectate în diagrama ce urmează:



În context, se relevă că, în pofida faptului că pe parcursul anului 2020 o perioadă de timp a fost restricționat accesul în instanțele de judecată din motivul pandemiei COVID-19, agenții constatori ai Centrului au participat la peste **470** ședințe de judecată pe cauzele contravenționale aflate în examinare, atât în instanța de fond cât și la Curtea de Apel Chișinău.

Urmează a fi precizat că, odată cu intrarea în vigoare la 01.01.2020 a noilor prevederi a Codului Contravențional, instanțele de judecată recurg la aplicarea procedurii scrise în examinarea cauzelor contravenționale, în conformitate cu prevederile art. 464¹ și 464² ale Codului Contravențional, practică considerată de către Centru aplicabilă la soluționarea cauzelor contravenționale de o complexitate redusă, nefiind necesară prezența fizică a agentului constator în cadrul ședințelor de judecată.

De menționat că din totalul celor **125** de cauze contravenționale expediate spre examinare în instanța de judecată pe parcursul perioadei de referință, în **30** de proceduri examinate Centrul a obținut câștig de cauză, instanța de judecată recunoscând vinovăția persoanelor în privința cărora au fost întocmite procese-verbale cu privire la contravenție, cu stabilirea sancțiunilor în formă de amendă. Suplimentar, urmează a fi menționat că alte **124** de proceduri se află în prezent în examinare pe rol în instanțele de judecată, inclusiv pe marginea unora din cauzele contravenționale inițiate în 2019.

Cu titlu informativ, numărul și dinamica proceselor-verbale cu privire la contravenții întocmite în perioada de când Centrul a dobândit calitatea de agent constator este reflectată în tabelul ce urmează:



Perioada de referință	Numărul proceselor-verbale cu privire la contravenție	Dinamica
2012-2013	4-26	↑550%
2013-2014	26-34	↑31%
2014-2015	34-24	↓29%
2015-2016	24-33	↑38%
2016-2017	33-52	↑57%
2017-2018	52-92	↑77%
2018-2019	92-105	↑14%
2019-2020	105-125	↑19%
2016-2020	33-125	↑279%



CAPITOLUL V

ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

V

ACTIVITATEA DE SUPRAVEGHERE A PRELUCRĂRILOR DE DATE CU CARACTER PERSONAL

Activitatea de înregistrare a operatorilor și sistemelor de evidență a datelor cu caracter personal

În perioada anului 2020, Direcția prevenire, supraveghere și evidență din cadrul Direcției generale supraveghere și conformitate a examinat **1472** de notificări depuse în vederea înregistrării în Registrul de evidență a operatorilor de date cu caracter personal, atât a operatorilor de date cu caracter personal cât și a sistemelor de evidență ținute în formă automatizată și/sau manuală în care sunt prelucrate date cu caracter personal.

Amintim că prevederile cadrului normativ național din domeniul protecției datelor cu caracter personal, în special art. 23 al Legii privind protecția datelor cu caracter personal, impun obligația operatorilor de date cu caracter personal să notifice Centrul (personal sau prin intermediul persoanelor împuternicite de către operatori) anterior operațiunilor de prelucrare a datelor cu caracter personal într-un sistem de evidență automatizat sau manual, cu prezentarea informațiilor care justifică prelucrarea datelor cu caracter personal, precum și asigurarea implementării măsurilor organizatorice și tehnice necesare pentru protecția datelor cu caracter personal.

În cadrul examinării notificărilor depuse la Centru spre autorizare și înregistrare, au fost efectuate **995 verificări prealabile**.

Ca rezultat al examinării notificărilor depuse în perioada de raportare au fost înregistrați **504 operatori** de date cu caracter personal și **710 sisteme** de evidență a datelor cu caracter personal.

Informația privind înregistrarea operatorilor și a sistemelor de evidență în care sunt prelucrate date cu caracter personal în Registrul de evidență al operatorilor de date cu caracter personal, în dinamică pentru anii 2016-2020, este reflectată în tabelul care urmează:

Anul	Numărul total de notificări examinate	Numărul operatorilor înregistrați	Numărul sistemelor de evidență a datelor cu caracter personal înregistrate	Numărul sistemelor de evidență refuzate a fi înregistrate	Numărul deciziilor de refuz contestate în ordine de contencios administrativ
2016	850	386	761	89	1
2017	1046	500	843	203	0
2018	1388	639	938	451	1
2019	1652	654	944	708	1
2020	1472	504	710	762	2

Din informația menționată, numărul notificărilor depuse spre examinare la „Ghișeu unic” al Centrului pe parcursul anului 2020 a fost în ușoară scădere. Astfel, și la acest capitol se observă că, din motivul situației pandemice provocate de COVID-19, care a impus restricții în activitatea tuturor entităților de drept public și privat, operatorii de date cu caracter personal au fost mai puțin activi în vederea notificării sistemelor de evidență gestionate, comparativ cu anii precedenți.



Principalele aspecte examinate în mod cert și primordial la evaluarea/analiza notificărilor și actelor aferente acestora, depuse în vederea înregistrării în Registrul de evidență a operatorilor de date cu caracter personal, ca și în anii precedenți, au fost următoarele:

- Corectitudinea determinării calității de operator de date cu caracter personal sau persoană împuternicită de către operator, în raport cu sistemele de evidență notificate;
- Existența temeiului legal de prelucrare a datelor cu caracter personal;
- Conformitatea măsurilor organizatorice și tehnice necesare pentru protecția datelor cu caracter personal declarate de către operatorul de date cu caracter personal cu prevederile cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;
- Existența instrucțiunilor oferite de către operator pentru persoanele împuternicite printr-un contract sau alt act juridic care va avea caracter obligatoriu pentru părți și care va stabili obiectul și durata prelucrării, natura și scopul prelucrării, statul în care vor fi prelucrate datele cu caracter personal, tipul de date cu caracter personal, categoriile subiecților de date, obligațiile și drepturile operatorului și ale persoanei împuternicite etc.;
- Condițiile în care se realizează transmiterea transfrontalieră a datelor cu caracter personal ținând cont de natura acestora, scopul și durata prelucrării propuse, de statul de destinație, de legislația acestuia, precum și de normele profesionale și măsurile de securitate respectate în statul de destinație etc.

Totodată, în anul 2020 se observă creșterea numărului notificărilor refuzate a fi înregistrate/autorizate, cele mai frecvente motive de refuz fiind:

- 1) indicarea în formularul de notificare a unor informații neveridice referitor la: categoriile de date cu caracter personal, scopurile de prelucrare, modul de colectare, precum și termenul de prelucrare a datelor cu caracter personal, care nu corespund cu cele stabilite în actele anexate la notificare;
- 2) neindicarea în formularul notificării a informațiilor referitor la persoanele împuternicite de către operator în cazul prelucrării datelor cu caracter personal în numele și pe seama operatorului de date cu caracter personal;
- 3) stabilirea în politica de securitate și în documentația referitoare la aceasta a unor măsuri organizatorice și tehnice necesare pentru protecția datelor cu caracter personal care nu corespund prevederilor cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;
- 4) supravegherea prin mijloace video a unor spații/bunuri care nu aparțin operatorului de date cu caracter personal sau supravegherea neconformă a spațiilor de lucru, în special a tehnicii de calcul ale salariaților, inclusiv al mijloacelor de introducere a datelor de către aceștia (tastaturi), fapt care duce la eventuale cazuri de încălcare de către angajator a prevederilor art. 91 alin. (1) lit. f) al Codului muncii, precum și a securității și confidențialității datelor cu caracter personal, în cazul în care prin imaginile video este posibilă vizualizarea introducerii credențialelor de autentificare de către utilizatorii interni în sistemele de evidență gestionate de către operator.

Ca și în anii precedenți, cel mai des au fost notificate și înregistrate sisteme de evidență auxiliare, care nu constituie/reflectă activitatea de bază a operatorilor de date cu caracter personal, cum ar fi: evidența contabilă, resursele umane, supravegherea video, corespondența, etc., sisteme care cu certitudine conțin date cu caracter personal și, la fel, urmează a fi notificate Centrului.



Mai mult, în vederea oferirii suportului metodologic și consultativ operatorilor de date cu caracter personal și/sau persoanelor împuternicite, privind procedura de notificare a sistemelor de evidență și înregistrare în calitate de operator în Registrul de evidență al operatorilor de date cu caracter personal, pe parcursul anului 2020, doar angajații subdiviziunii responsabile pentru înregistrarea operatorilor/sistemelor de date cu caracter personal, au oferit telefonic sau prin e-mail, **2030 de consultații și instrucțiuni**. Din nou, reieșind din situația specifică determinată de pandemia COVID-19, pe parcursul perioadei de referință au predominat consultațiile oferite la telefon sau prin poșta electronică, fără prezența fizică a solicitanților de consultații la sediul Centrului, fapt care a avut impact semnificativ atât asupra calității notificărilor înaintate și actelor întocmite de operatori în vederea înregistrării în Registrul de evidență a operatorilor de date cu caracter personal, cât și asupra numărului de notificări depuse la „Ghișeul unic” spre examinare.

Activitatea de prevenire a neconformității prelucrării datelor cu caracter personal

În perioada anului 2020, în scopul prevenirii practicilor neconforme de prelucrare a datelor cu caracter personal, Centrul a informat, inclusiv prin intermediul paginii web oficiale, operatorii de date cu caracter personal din diferite domenii asupra multiplelor cazuri de compromitere a securității și confidențialității datelor în diferite state, care s-au soldat cu aplicarea unor amenzi semnificative aplicate operatorilor care au admis prelucrarea neconformă a datelor cu caracter personal.

La fel în contextul asigurării prevenirii neconformităților la prelucrarea datelor cu caracter personal, reieșind din creșterea constantă a numărului sesizărilor legate de prelucrarea datelor cu caracter personal prin intermediul camerelor de supraveghere video, Centrul a elaborat și publicat pe pagina web oficială **opinia autorității asupra aspectelor practice și legale în legătură cu instalarea și gestionarea mijloacelor de supraveghere video**, de care urmează să țină cont persoanele fizice și juridice care intenționează să prelucreze date cu caracter personal prin intermediul sistemelor de evidență a supravegherii video.

În scop preventiv, informativ și aplicativ, în perioada de referință Autoritatea națională de protecție a datelor cu caracter personal a emis recomandări/opinii în vederea asigurării conformității prelucrării datelor cu caracter personal, vizând următoarele aspecte:

- **Prelucrarea datelor cu caracter personal în contextul pandemiei de coronavirus (COVID-19) în Republica Moldova:** Centrul a accentuat asupra riscurilor și provocărilor privind protecția persoanelor în partea ce vizează prelucrarea datelor cu caracter personal în contextul combaterii Coronavirusului (COVID-19), în special, a datelor privind starea de sănătate a pacienților.
- **Aspecte privind înregistrarea și transmiterea on-line a ședințelor consiliilor locale:** opinia autorității în legătură cu înregistrarea și transmiterea în direct prin intermediul internetului a ședințelor consiliilor locale.
- **Precizări privind înregistrarea și transmiterea în direct prin intermediul internetului a ședințelor consiliilor locale:** în contextul reacției societății civile, precum și a unor autorități publice locale, care au tratat greșit opinia expusă anterior în legătură cu înregistrarea și transmiterea în direct prin intermediul internetului a ședințelor consiliilor locale, Centrul a venit cu precizări clare că nu intenționează să restricționeze înregistrarea și transmiterea în direct prin intermediul internetului a ședințelor consiliilor locale, precum și cu repere exacte cu caracter aplicativ pentru a asigura prelucrarea conformă a datelor cu caracter personal în contextul abordat.

Informațiile menționate supra pot fi vizualizate integral pe pagina web a Centrului www.datepersonale.md la rubrica Legislație/Recomandările CNPDCP, (accesând link-ul: <https://www.datepersonale.md/legislation/ncpdp-guidelines/>).



Totodată, în contextul realizării atribuției Centrului de monitorizare a respectării legislației cu privire la protecția informației și verificarea aplicării acesteia, în special a dreptului la informare, de acces la date, de intervenție asupra datelor și de opoziție, precum și având ca scop neadmiterea/prevenirea încălcării drepturilor subiecților ale căror date cu caracter personal au fost/sunt prelucrate de către organele de drept din Republica Moldova, entități care, în exercitarea competențelor, prelucrează un volum impunător de date cu caracter personal, Centrul a intervenit în raport cu ultimii asupra următoarelor aspecte:

• Executarea prevederilor art. 15 al Legii privind protecția datelor cu caracter personal și măsurile întreprinse în vederea asigurării respectării drepturilor subiecților de date cu caracter personal:

Este notabil că libera circulație a datelor cu caracter personal între 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 în cadrul jurisdicției Republicii Moldova, trebuie facilitată asigurând, totodată, un nivel ridicat de protecție a datelor cu caracter personal.

Centrul pledează cu fermitate pentru asigurarea unei concilierii între dezideratul juridic protecția datelor cu caracter personal și prelucrarea 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.

Potrivit art. 12-14 al Legii nr. 133/2011 privind protecția datelor cu caracter personal, subiectul de date dispune de dreptul la informare, dreptul de acces la datele cu caracter personal și dreptul de intervenție asupra datelor cu caracter personal, în virtutea cărora subiectul poate solicita de la operatorul de date, informație cu privire la: scopurile prelucrării, categoriile de date avute în vedere și destinatarii sau categoriile de destinatari cărora le sunt dezvăluite datele; datele cu caracter personal care fac obiectul prelucrării, precum și originea acestor date; principiile de funcționare a mecanismului prin care se efectuează prelucrarea automatizată a datelor care vizează subiectul datelor cu caracter personal; informații cu privire la consecințele juridice generate de prelucrarea datelor cu caracter personal pentru subiectul acestor date; informații privind modul de exercitare a dreptului de intervenție asupra datelor cu caracter personal, etc.

În lumina prevederilor Legii nr. 133/2011, operatorii au obligația de a răspunde cererilor subiecților de date, fără întârzieri nejustificate, cu excepția cazului în care operatorul aplică limitări statuate de lege în raport cu drepturile subiecților de date.

Astfel, potrivit art. 15 al Legii nr. 133/2011 (întitulat „Excepții și restricții”), prevederile art. 4 alin. (1), art. 12 alin. (1) și (2), art. 13, 14 și 28 nu se aplică în cazul în care prelucrarea datelor cu caracter personal este efectuată în cadrul acțiunilor prevăzute la art. 2 alin. (2) lit. d) și la art. 5 alin. (5) lit. g), în scopul apărării naționale, al securității statului și menținerii ordinii publice, al protecției drepturilor și libertăților subiectului datelor cu caracter personal sau ale altor persoane, dacă prin aplicarea acestora este prejudiciată eficiența acțiunii sau obiectivul urmărit în exercitarea competențelor legale ale autorității publice. Prelucrarea datelor cu caracter personal în scopurile stabilite la alin. (1) nu poate depăși perioada necesară atingerii obiectivului urmărit.

În acord cu art. 15 alin. (3) al Legii nr. 133/2011, **după încetarea situației care justifică aplicarea alin. (1) și (2) din articolul 15, operatorii vor lua măsurile necesare pentru a asigura respectarea drepturilor subiecților datelor cu caracter personal prevăzute la art. 12–14** (informarea subiectului datelor cu caracter personal, dreptul de acces la datele cu caracter personal, dreptul de intervenție asupra datelor cu caracter personal).

În același context, potrivit art. 15 alin. (4) al Legii nr. 133/2011, **autoritățile publice țin evidența aplicării excepțiilor stabilite la alin. (1) și informează Centrul, în termen de 10 zile, despre datele cu caracter personal prelucrate în condițiile prezentului articol.**



În optica celor prezentate, Centrul a solicitat: Procuraturii Generale, Ministerului Afacerilor Interne, Ministerului Apărării, Serviciului de Informații și Securitate, Centrului Național Anticorupție, Serviciului Vamal furnizarea, în termen de 30 de zile, a informației cu privire la următoarele aspecte:

- Numărul total de cazuri în care au fost aplicate excepțiile și restricțiile în temeiul art. 15 alin. (1) al Legii nr. 133/2011;
- Numărul de cazuri în care a fost realizată informarea subiectului de date cu caracter personal după încetarea situațiilor care au condiționat aplicarea excepțiilor și restricțiilor reglementate de art. 15 alin. (1) al Legii nr. 133/2011 și modalitatea de realizare a informării subiectului;
- Numărul de cazuri în care a fost omisă informarea subiectului de date cu caracter personal după încetarea situațiilor care au condiționat aplicarea excepțiilor și restricțiilor reglementate de art. 15 alin. (1) Legii nr. 133/2011, cu nuanțarea motivelor care au condiționat o atare omisiune;
- Existența unor verificări pe plan intern vizavi de asigurarea respectării dreptului la informare a subiectului de date, ulterior decăderii situațiilor care au condiționat instituirea excepțiilor și restricțiilor statuate la art. 15 alin. (1) al Legii nr. 133/2011.

Urmează a remarca că marea majoritate a entităților menționate au prezentat informații evazive, neoferind răspunsuri clare la întrebările înaintate, atât în ceea ce privește careva date statistice, cât și din punct de vedere a eventualei existențe a unor mecanisme și măsuri organizatorice și tehnice certe implimentate în vederea asigurării evidenței eficiente a persoanelor în privința cărora au fost instituite restricții la realizarea drepturilor, cât și a persoanelor în raport cu care au fost/urmează a fi realizate drepturile urmare a epuizării scopului pentru care aceste restricții au fost anterior instituite. Or, **circumstanțele constatate denotă necesitatea stringentă de instituire a mecanismelor și pârgھیilor corespunzătoare legislative, inclusiv întreprinderea de către entitățile vizate a măsurilor necesare întru asigurarea și eficientizarea realizării drepturilor subiecților de date cu caracter personal, fapt care, cu părere de rău, nu a fost realizat.**

• ***Legalitatea prelucrării datelor cu caracter personal stocate în resursele informaționale automatizate de stat***

Urmare a activității analitice efectuate în raport cu informația acumulată de la Agenția Servicii Publice, a fost sistematizată, per instituție, statistica operațiunilor de accesare a datelor cu caracter personal stocate în diverse sisteme informaționale de stat: Registrul de stat al populației, Registrul bunurilor imobile, Registrul de stat al conducătorilor de vehicule, Registrul de stat al transporturilor, Registrul unităților de drept, dezagregate pe ani, efectuate de către utilizatorii: Ministerului Afacerilor Interne, Centrului Național Anticorupție, Procuraturii Generale, Autorității Naționale de Integritate, Ministerului Apărării, Serviciului Vamal, Serviciului fiscal de Stat, entități care s-au identificat cu cel mai mare număr de accesări a datelor cu caracter personal efectuate.

În context, reliefăm în tabelul ce urmează informația privind numărul operațiunilor de accesare a datelor cu caracter personal în resursele informaționale de stat menționate, efectuate de către utilizatorii autorizați ai autorităților indicate supra:



Instituția vizată	Numărul de accesări efectuate în sistemele informaționale de stat: RSP, RBI, RST, RSCV, RUD prin intermediul SIA „Acces-Web” și COI		
	2018	2019	2020
Ministerul Afacerilor Interne	3541231	20887797	11213170
Serviciul de Informații și Securitate	93897	78939	65180
Centrul Național Anticorupție	96017	112235	86891
Procuratura Generală	20109	24611	19985
Serviciul Vamal	28509	25551	12381
Ministerul Apărării	347	2050	1002
Autoritatea Națională de Integritate	nu a fost solicitată informația pentru anul 2018	20740	17217
Serviciul Fiscal de Stat		3541231	3535927

Astfel, în vederea asigurării monitorizării respectării legislației cu privire la protecția datelor cu caracter personal, Centrul a solicitat entităților menționate prezentarea, în termen de 60 de zile, a informației cu privire la unele aspecte tangențiale operațiunilor de accesare a datelor cu caracter personal stocate în sistemele informaționale indicate în demersurile de referință, și anume:

- Categoria subiecților a căror date cu caracter personal stocate în sistemele informaționale indicate în demersuri, sunt susceptibile de a fi accesate și tipologia datelor cu caracter personal care sunt accesate *per* fiecare categorie de subiecți;
- Temeiurile de fapt, de drept și scopurile care de regulă întemeiază operațiunile de accesare a datelor cu caracter personal stocate în sistemele informaționale indicate;
- Operațiunile care sunt efectuate în raport cu datele cu caracter personal stocate în sistemele informaționale indicate (consultare, imprimare și stocare ulterioară, copiere, divulgare, combinare, transmitere, inclusiv transmiterea transfrontalieră, etc.);
 - a) În cazul efectuării operațiunilor de imprimare, copiere și stocare ulterioară, urmează a fi precizate detaliile cu privire la măsurile implementate și orientate spre prevenirea acțiunilor neintenționate, care pot genera distrugerea, copierea neautorizată, pierderea sau defectarea suportului material pe care sunt stocate datele cu caracter personal, extrase din sistemele informaționale indicate;
 - b) Termenele de stocare a datelor cu caracter personal care au fost extrase din sistemele informaționale indicate;
 - c) În ce scopuri este efectuată operațiunea de extragere a datelor cu caracter personal din sistemele informaționale indicate;
 - d) Confirmarea/infirmarea informației cu privire la depistarea/identificarea unor breșe de securitate declanșate urmare a efectuării operațiunilor de accesare, imprimare, copiere și stocare ulterioară, a datelor cu caracter personal stocate în sistemele informaționale indicate;
 - e) Măsurile implementate în scopul prevenirii, depășirii, combaterii și escaladării incidentelor de securitate și remedierii vulnerabilităților de securitate;



- Existența unei înregistrări și evidențe a persoanelor care efectuează operațiuni de accesare a datelor cu caracter personal, stocate în sistemele informaționale indicate;
- Lista persoanelor autorizate care dispun de dreptul de acces la sisteme informaționale;
- Dacă accesarea prin intermediul COI oferă posibilitatea de a identifica persoanele care efectuează accesările;
- Motivul evitării efectuării accesării prin intermediul aplicației SIC „Acces-WEB” și utilizarea masivă a COI.

De menționat că, și în acest caz, entitățile vizate fie au oferit răspunsuri evazive și neconcludente, fie nu au răspuns la demersul Centrului, ultimul fiind nevoit a interveni repetat în vederea acumulării informațiilor necesare, **fapt care demonstrează, spre regret, ineficiența/insuficiența măsurilor întreprinse de operatorii vizați întru asigurarea ținerii evidenței eficiente a operațiunilor de accesare a datelor cu caracter personal, stocate în diferite resurse informaționale de stat, efectuate de către utilizatorii autorizați ai acestora.**

Suplimentar, în contextul asigurării prevenirii prelucrărilor neconforme de date cu caracter personal, Centrul reiterează că, **lipsa/insuficiența implementării măsurilor de asigurare a securității și confidențialității datelor cu caracter personal, la modul practic, precum și inexistența unui control riguros asupra corectitudinii operațiunilor de prelucrare a datelor cu caracter personal efectuate, poate duce, iminent, la prelucrări neconforme a datelor cu caracter personal ale subiecților de date vizați**, generând în final, eventuale litigii civile cu repararea prejudiciilor materiale și morale, impunerea emiterii de către Centru a deciziilor de suspendare și/sau încetare a operațiunilor de prelucrare a datelor cu caracter personal.

Totodată, este de menționat necesitatea realizării obligației operatorilor de date cu caracter personal vizând revizuirea politicii de securitate a datelor cu caracter personal și documentației referitoare la aceasta, cel puțin o dată în an, ca rezultat al modificărilor sau reevaluării componentelor acesteia, ținând cont de evoluția tehnologiilor informaționale utilizate pentru prelucrarea datelor cu caracter personal, de regimul juridic al protecției datelor cu caracter personal, precum și necesitatea asigurării implementării principiilor de protecție a datelor cu caracter personal, în mod implicit, până la elaborarea și punerea în funcțiune a sistemelor informaționale automatizate.

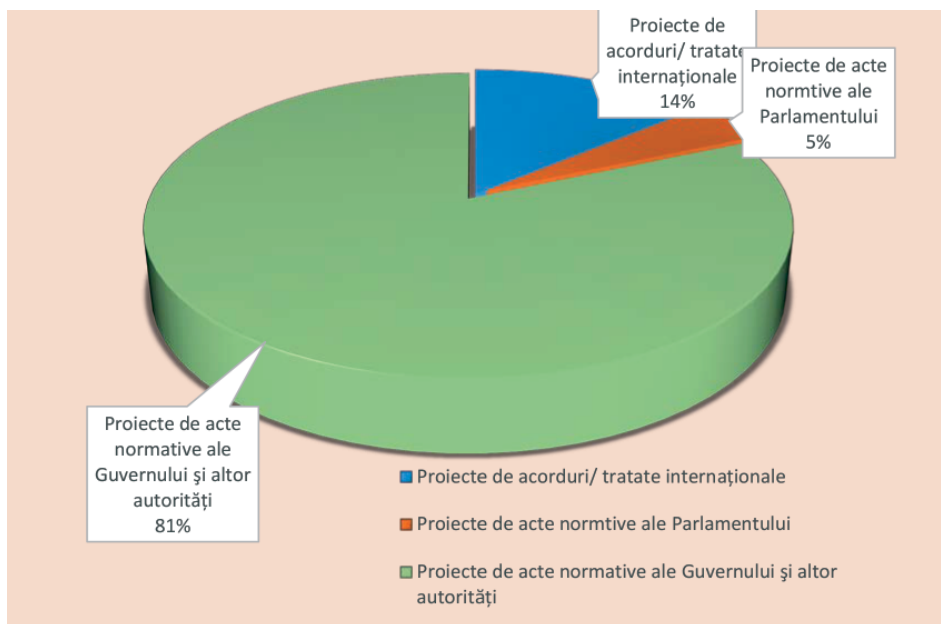
AVIZAREA ȘI ELABORAREA PROIECTELOR DE ACTE NORMATIVE

Avizarea actelor normative

În temeiul prevederilor art. 32 alin. (2) al Legii nr. 100/2017 cu privire la actele normative, proiectele actelor normative care țin de domeniul protecției datelor cu caracter personal se transmit spre avizare Centrului Național pentru Protecția Datelor cu Caracter Personal.

Drept urmare, pe parcursul anului 2020, către Centru au parvenit spre avizare **65** de proiecte de acte normative naționale/internaționale, care au fost examinate prin prisma respectării principiilor de protecție a datelor cu caracter personal, precum și a asigurării drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, dintre care:

- **9** proiecte de acorduri/tratate internaționale;
- **3** proiecte de acte normative de modificarea legilor, codurilor;
- **53** proiecte de acte normative ale Guvernului și altor autorități.

Procentajul avizelor oferite de către Centru pe parcursul anului 2020

De menționat că, aspectele reglementate prin actele normative transmise în vederea avizării au fost diverse, fiecare act vizând domenii și proceduri distincte care necesitau studiere minuțioasă în vederea asigurării obiectivității și legalității avizelor oferite. Chiar și în aceste condiții, în cele mai multe cazuri, la avizarea proiectelor de acte normative s-a determinat că este necesară completarea și revizuirea textelor actelor respective, fiind înaintate obiecții și propuneri de rigoare prin prisma necesității respectării reglementărilor legale referitoare la protecția datelor cu caracter personal.



Prin urmare, asupra majorității proiectelor de acte normative analizate s-au efectuat recomandări pentru ajustarea acestora și armonizarea lor cu dispozițiile legale privind protecția datelor cu caracter personal.

De menționat că, comparativ cu anii precedenți, în perioada de referință se atestă o creștere de circa 15% a avizelor înaintate Autorității naționale de protecție a datelor cu caracter personal vizând aprobarea actelor corespunzătoare implementării sistemelor informaționale automatizate în care urmează a fi prelucrate date cu caracter personal.

În continuare prezentăm, pentru exemplificare, unele dintre cele mai relevante proiecte de acte normative avizate:

– Proiectul hotărârii de Guvern pentru aprobarea Conceptului Platformei Guvernamentale de instruire de la distanță (e-Learning) și a Regulamentului privind utilizarea și administrarea acestuia, unde s-a propus racordarea conceptului vizat la cadrul normativ în domeniul protecției datelor cu caracter personal, precum și includerea în textul proiectului prescris a noilor prevederi care vor asigura respectarea drepturilor subiectului de date cu caracter personal.

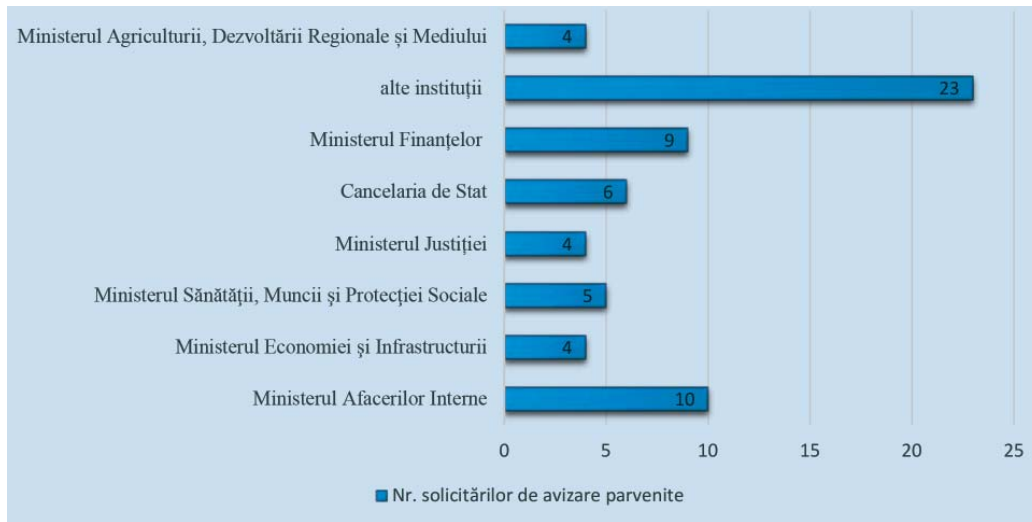
– Proiectul Regulamentului privind utilizarea, administrarea și dezvoltarea portalului guvernamental al cetățeanului, unde a fost propusă revizuirea pct. 5, 7, 9, 11, 13, 19, 20 și 24 ale proiectului Regulamentului prescris, reieșind din necesitatea de asigurare a securității și confidențialității datelor cu caracter personal pentru toți participanții la schimbul de date pe platforma de interoperabilitate.

– Proiectul hotărârii de Guvern privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental.

– Proiectul hotărârii Guvernului cu privire la aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică, unde a fost propusă revizuirea termenelor de păstrare a datelor cu caracter personal și modalitatea automatizată de ștergere a acestora în SI MNotify.

– Proiectul hotărârii Guvernului cu privire la aprobarea Regulamentului cu privire la organizarea și funcționarea Sistemului informațional automatizat „E-Integritate”, unde s-a propus racordarea măsurilor tehnice și organizatorice necesare pentru protejarea datelor cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite în conformitate cu Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal.

– Proiectul de hotărâre de Guvern cu privire la aprobarea proiectului de lege pentru modificarea unor acte normative, prin care s-a propus, inclusiv, modificarea Legii privind protecția datelor cu caracter personal, în speță a art. 23, 24 și 25, prin care se intenționează substituirea obligativității notificării operațiunilor de prelucrare a datelor cu caracter personal cu alte proceduri, cum ar fi: evaluarea impactului asupra protecției datelor cu caracter personal, consultarea prealabilă, desemnarea responsabilului de protecția datelor. Astfel, analizând prin prisma considerentelor expuse în 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 (GDPR), care consemnează raționamentele privind necesitatea abrogării obligației de notificare privind prelucrarea datelor cu caracter personal și înlocuirea acesteia cu anumite proceduri și mecanisme eficiente, Centrul a apreciat propunerea înaintată ca fiind oportună. Totodată, având în vedere că modificările propuse de autorul proiectului nu acopereau toate procedurile care urmează a fi implementate de operator și persoana împuternicită, urmare a excluderii notificării, Centrul a venit cu un șir de propuneri de îmbunătățire a proiectului.

**Numărul de solicitări de avizare, parvenite în anul 2020, per entităţi****Elaborarea proiectelor de acte normative**

Modificarea
art. 27 al Legii
133/2011

Pe parcursul anului 2020, activitatea Centrului pe segmentul creației legislative a fost canalizată pe elaborarea proiectului de lege privind modificarea și completarea art. 27 al Legii 133/2011 privind protecția datelor cu caracter personal, care a fost aprobat de Parlamentul Republicii Moldova la 09 iulie 2020, intrat în vigoare la 24 august 2020.

Condiția esențială care a fundamentat inițierea prezentului proiect de lege, a constat inclusiv în necesitatea stringentă de optimizare și eficientizare a procedurii de efectuare de către Centru a investigațiilor/controlului privind conformitatea prelucrării datelor cu caracter personal, sub aspect de reglementare a unui termen care să fie proporțional complexității procedurii de verificare a conformității prelucrării datelor cu caracter personal.

Astfel, prin proiectul de lege s-a propus ca termenul de examinare și soluționare a plângerii înaintate Centrului să fie de 3 luni, cu posibilitatea prelungirii justificate a acestuia la fiecare 30 de zile, în funcție de complexitatea cauzei, volumul de informații ce urmează a fi obținute și analizate, comportamentul participanților vizați, conduita autorităților relevante și importanța procedurii administrative pentru partea interesată, dar nu mai mult de 6 luni.

Pe de altă parte, acest proiect de lege a înglobat amendamente în partea ce vizează informarea subiectului de date cu caracter personal despre cursul examinării plângerii sale, la solicitarea ultimului sau la fiecare prelungire, cu indicarea motivelor obiective ce determină prelungirea termenului de examinare. Respectiv, subiectul de date cu caracter personal, în situația în care nu va fi satisfăcut de modul de examinare a petiției sale, va avea posibilitatea de a contesta acțiunile controlorului de stat care are în examinare petiția sa, în instanța de judecată sau la Centru.

O altă condiție care s-a aflat la premisa elaborării proiectului de lege menționat, a constat în necesitatea la fel de stringentă de dispersare și organizare clară a responsabilităților angajaților Centrului în procesul de examinare a plângerilor și desfășurare a procedurii de verificare a conformității prelucrării datelor cu caracter personal, întru eficientizarea procesului de lucru și evitarea blocajelor interne instituționale, cât și reglementării posibilității de delegare a responsabilității de emitere/semnare a deciziilor Centrului, pe lângă directorul și directorul adjunct al autorității, și personalului abilitat cu funcții de control al Centrului, în conformitate cu competențele atribuite prin ordinul directorului.



CAPITOLUL VII

COOPERAREA INTERNAȚIONALĂ

VII



Stabilirea și dezvoltarea cooperării internaționale în domeniul protecției datelor cu caracter personal a continuat a fi unul din elementele de bază în fortificarea capacităților funcționale ale Centrului în anul 2020.

Chiar dacă anul de referință a fost un an al provocărilor, reieșind din situația pandemică la nivel global, Centrul a încercat să își concentreze activitatea pe întărirea relațiilor bilaterale și multilaterale cu partenerii externi, atât în cadrul organizațiilor internaționale cât și individual. Pentru atingerea acestui scop angajații Centrului au participat la ședințele de lucru ale Comitetelor europene și internaționale. Trebuie de menționat că din cauza situației pandemice globale, anul 2020 a fost unul limitat în ceea ce privește întâlnirile și ședințele internaționale în formatul în care aveau loc anterior. Cu toate acestea unele progrese totuși au fost înregistrate. Pe parcursul anului 2020 reprezentanții Centrului au participat la diverse conferințe, reuniuni și grupuri de lucru.



European Data Protection Board

• Ședințele plenare ale Comitetului European pentru Protecția Datelor

Pe parcursul anului 2020, reprezentanții Centrului au participat la reuniuni plenare organizate de Comitetul European pentru Protecția Datelor (CEPD), care au avut loc la Bruxelles, Belgia. Printre cele mai importante ședințe se numără: Ședința plenară din 28-29 ianuarie 2020 și ședința plenară din 18-19 februarie 2020.

Importanța ședințelor menționate se conturează prin încercarea de a elabora mecanisme de cooperare internațională pentru a facilita asigurarea aplicării efective a legislației privind protecția datelor cu caracter personal, acordarea de asistență internațională reciprocă în

asigurarea aplicării legislației din domeniul protecției datelor cu caracter personal, inclusiv prin notificare, asistență în investigații și schimb de informații, sub rezerva unor garanții adecvate pentru protecția datelor cu caracter personal și a altor drepturi și libertăți fundamentale. Acestea oferă posibilitatea de implicare a părților interesate în discuțiile și activitățile care au ca scop intensificarea cooperării internaționale în domeniul aplicării legislației privind protecția datelor cu caracter personal, precum și dă posibilitatea promovării schimbului reciproc și a documentației cu privire la legislația și practicile în materie de protecție a datelor, inclusiv în ceea ce privește conflictele jurisdicționale cu țările terțe.

Globalizarea fluxurilor de date necesită consolidarea la nivel internațional a drepturilor persoanelor la protecția datelor. Pentru aceasta, trebuie adoptate principii solide privind protecția datelor personale, menite să faciliteze circulația transfrontalieră a datelor cu caracter personal, asigurând în același timp un nivel ridicat și coerent de protecție, fără lacune și lipsite de complexitate inutilă. Astfel, una din funcțiile ședințelor plenare ale CEPD este o colaborare structurată între autoritățile de protecție a datelor cu caracter personal, lucru pe care reprezentanții Centrului îl realizează în permanență.



• Ședințele plenare în cadrul Consiliului Europei

Comitetul Consultativ al Convenției pentru protecția persoanelor cu privire la prelucrarea automatizată a datelor cu caracter personal (Convenția 108)

Protecția datelor este un drept protejat încă din anii 80 prin tratate internaționale, prima convenție internațională care a intrat în vigoare a fost elaborată de Consiliul Europei. Protecția datelor este supusă unui proces de regândire nu numai în Uniunea Europeană, ci și în cadrul Consiliului Europei. Aici reformele se caracterizează prin protecția cetățenilor statelor membre în funcție de dezvoltarea tehnologiei. Încă din octombrie 2011 au început discuțiile privind modernizarea Convenției 108, Comitetul Consultativ (T-PD) ajungând la adoptarea, în 2012, a unui text de protocol de revizuire. Comitetul miniștrilor a decis înființarea unui comitet ad-hoc privind protecția datelor format din reprezentanți ai statelor membre ale Consiliului Europei cu misiunea de a finaliza modernizarea Convenției 108 prin negocierea formală a textului protocolului de amendare.

Procesul de modernizare a Convenției 108 are ca finalitate transformarea sa într-un instrument juridic internațional cu valoare universală, aplicabil și statelor din afara Consiliului Europei. Menționăm că, potrivit situației de la finele anului 2020, din cele 47 state membre ale Consiliului Europei și 8 non membre (total 55 state), Protocolul amendat la Convenția 108 pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, a fost semnat de 33 state din numărul total și ratificat de 10.

În perioada de raportare, Centrul a participat la două ședințe plenare ale Comitetului Consultativ al Convenției 108, care au avut loc la distanță (on-line). Aceste întruniri au pus accent în primul rând pe prezentarea făcută de secretariat cu privire la activitățile și evoluțiile majore din domeniul protecției datelor în 2020, în special la publicarea textului compilat, care conține



actualizările furnizate de delegații, dar și cu privire la cele trei declarații comune emise de președintele Comitetului Convenției 108 și a Comisarului pentru protecția datelor al Consiliului Europei:

- a) cu privire la dreptul la protecția datelor în contextul pandemiei COVID-19 (publicat la 30 martie 2020),
- b) privind urmărirea digitală a contactelor (publicat la 28 aprilie 2020) și
- c) referitor la “O mai bună protecție a persoanelor în contextul fluxurilor internaționale de date: necesitatea de supraveghere democratică și eficientă a serviciilor de informații (publicat la 7 septembrie 2020)”.

Aceste prezentări/declarații vin să explice unele aspecte din domeniul protecției datelor cu caracter personal dificil a fi gestionate și care nu pot fi soluționate decât prin cooperare internațională eficientă. Or, ținând cont de dezvoltarea tehnologică rapidă, de prelucrare a informațiilor și de intensificarea fluxului internațional de date, sunt necesare a fi stabilite mecanisme la nivel internațional, care ar permite statelor de a se informa și consulta cu privire la protecția datelor. În acest sens, ședințele plenare ale Comitetului Consultativ al Convenției 108 vin ca instrumente internaționale cu caracter regional care contribuie la dezvoltarea și evoluția domeniului protecției datelor.

Tot în perioada de raportare, reprezentantul Centrului a participat la Reuniunea internațională de cooperare cu furnizorii de servicii electronice, care a avut loc în perioada 26-28 februarie 2020 la Tbilisi (Georgia). Reuniunea menționată a fost organizată în cadrul proiectului CyberEast, ca o continuare a proiectelor Cybercrime @ EAP, prin care se propune de a sprijini țările din Parteneriatul Estic în construirea și menținerea parteneriatelor cu entitățile din sectorul privat, în principal furnizori de servicii Internet, pentru consolidarea mecanismelor de cooperare și încredere între sectorul privat, cetățeni și autoritățile de justiție penală.



• Implementarea prevederilor Acordului de Asociere RM-UE

La acest aspect este de menționat că în perioada de raportare Centrul a elaborat și prezentat Ministerului Afacerilor Externe și Integrării Europene cât și Ministerului Economiei și Infrastructurii raportul final general privind implementarea acțiunilor din Planul Național de Acțiuni privind Implementarea Acordului de Asociere 2017- 2019. Tot în limitele acestui capitol a fost făcută avizarea la noua Agendă de Asociere 2021-2027.

• Cooperarea cu agențiile Uniunii Europene

În conformitate cu prevederile stipulate la articolul 19 alin. (2) din Acordul de cooperare dintre Republica Moldova și Eurojust, potrivit căruia ofițerul de protecție a datelor Eurojust și Autoritatea de protecție a datelor din Republica Moldova își vor raporta reciproc, minim o dată în an, asupra implementării prevederilor acordului menționat supra, Centrul a prezentat către



Eurojust informația privind activitatea sa, privind implementarea prevederilor legale în materie de protecție a datelor cu caracter personal, cât și privind colaborarea interinstituțională cu Procuratura Generală.

Menționăm că cooperarea cu Eurojust reprezintă un punct-cheie în dezvoltarea raporturilor de asistență juridică internațională în materie penală în concordanță cu standardele europene și în sensul vectorului de integrare europeană a Republicii Moldova.

Aceasta permite ca Eurojust să sprijine, prin diverse mecanisme moderne de care dispune, eforturile de prevenire, contracarare și urmărire penală a unui șir de încălcări grave, precum și sprijinirea organelor de drept din Republica Moldova.

• Cooperarea cu Autoritățile de Protecție a Datelor din țările membre ale Uniunii Europene

Pe parcursul anului 2020, Centrul a solicitat opinia și experiența mai multor Autorități de Protecție a Datelor din țările membre ale Uniunii Europene cum ar fi: România, Austria, Belgia, Bulgaria, Italia, Franța, Germania, Grecia, Spania, Portugalia, Olanda, etc., cu privire la utilizarea camerelor de supraveghere video în celulele deținuților. Această solicitare a survenit urmare multiplelor adresări referitor la legalitatea utilizării camerelor de supraveghere video (CCTV) instalate în celulele deținuților în penitenciare și/sau în izolatoare de detenție provizorie aflate sub egida organelor de poliție. Scopul acestui demers a fost preluarea bunelor practici europene, precum și aplicarea adecvată a cadrului normativ în soluționarea problemelor aferente camerelor de supraveghere video în celulele deținuților. În acest scop, APD-urile au fost îndemnate să comunice Centrului experiența statelor lor referitor la următoarele subiecte:

- Este permisă utilizarea camerelor de supraveghere video (CCTV) în celulele deținuților în penitenciare și/sau în izolatoare de detenție provizorie?
- Care acte normative/legislative reglementează temeiul legal al utilizării acestora?
- Care sunt scopurile declarate de utilizare a CCTV în aceste cazuri?
- Care este perioada permisă de stocare a informațiilor deținute?
- În ce condiții imaginile obținute prin CCTV pot fi dezvăluite terților?
- Pot fi restricționate drepturile subiectului de date vizat, în cazul dat, drepturile prevăzute de Convenția 108, GDPR sau Directiva UE 680/2016, în special dacă subiecții de date pot să se opună prelucrării datelor cu caracter personal prin intermediul CCTV?, etc.

Informația deja recepționată de la APD-uri la tematica expusă, precum și cea în curs de a fi recepționată de Centru, este/urmează a fi sistematizată în vederea studierii bunelor practici și deciderii în continuare asupra aplicabilității acestora la nivel național.

Proiecte internaționale

Pe parcursul anului 2020, Centrul a aplicat și a beneficiat de suport în cadrul mai multor proiecte internaționale, după cum urmează:

Programul Erasmus+

Centrul, a participat în cadrul Programul Erasmus+ la *Apelul 2020 – EAC/A02/2019 „Acțiune Cheie 2 (KA2) – Cooperarea pentru inovare și schimbul de bune practici; Consolidarea capacităților în domeniul învățământului superior”*. În cadrul apelului menționat supra se propunea realizarea următorului Proiect: *Oportunități UE de carieră digitală prin intermediul organizării cursurilor de instruire în domeniul protecției datelor cu caracter personal pentru persoanele din medii defavorizate*. Obiectivul general al proiectului propus a fost promovarea antreprenoriatului



persoanelor din medii defavorizate printr-o abordare adaptată, bazată pe cele mai bune practici pentru demonstrarea conformității cu cadrul legal UE în domeniul protecției datelor. În cadrul Programului Erasmus+, Centrul a participat în calitate de membru al unui consorțiu împreună cu parteneri din Bulgaria, Italia, Grecia și Polonia.

Proiectul TAIEX – Instrumentul de asistență tehnică și schimb de informații

Domeniul Mass-media

- **„Dreptul la libertatea de exprimare și protecția datelor cu caracter personal în contextul unor eventuale provocări la nivel global! (pandemia COVID – 19)”**

Domeniul Sănătății Publice

- **„Prelucrarea și protecția datelor cu caracter personal în domeniul sănătății publice în contextul unor eventuale provocări la nivel global! (pandemia COVID – 19)”**

În contextul pandemiei la nivel global provocată de COVID-19, apar tot mai multe întrebări cu privire la legalitatea utilizării și divulgării datelor cu caracter personal referitoare la starea de sănătate de către reprezentanții mass – media în conformitate cu prevederile GDPR. În acest scop, Centrul și-a planificat organizarea unei conferințe internaționale **„Dreptul la libertatea de exprimare și protecția datelor cu caracter personal în contextul unor eventuale provocări la nivel global! (pandemia COVID – 19)”** pentru reprezentanții mass-media, scopul conferinței fiind de a prezenta informații, exemple de bune practici și soluții inovatoare în scopul stabilirii unui echilibru corect dintre libertatea de exprimare și dreptul la viața privată, precum și faptul de a face un schimb de experiență între părți. Aplicarea la proiectul menționat, s-a efectuat prin intermediul platformei on-line TAIEX, dar în final proiectul nu a fost acceptat.

Proiect
TAIEX
obținut

În domeniul sănătății publice, Centrul a aplicat în anul 2020 și a obținut suport din partea proiectului TAIEX în organizarea atelierului de lucru **„Prelucrarea și protecția datelor cu caracter personal în domeniul sănătății publice în contextul unor eventuale provocări la nivel global! (pandemia COVID – 19)”**. Scopul atelierului de lucru este de a consolida și a spori abilitățile reprezentanților din domeniul sănătății publice cu privire la eventualele provocări care pot apărea la nivel global în contextul pandemiei de COVID – 19, care necesită totodată respectarea drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește protecția datelor cu caracter personal atunci când prelucrarea este necesară din motive de interes public în domeniul sănătății publice, precum și adoptarea bunelor practici pe baza jurisprudenței relevante; de a stabili echilibru între prelucrarea, păstrarea și divulgarea datelor cu caracter personal referitoare la sănătate dreptul la confidențialitatea vieții private; de a promova suport în analiza specializată, orientată spre prevederile Legii privind protecția datelor cu caracter personal în domeniul specific de aplicare – cel al sănătății; de a familiariza reprezentanții din domeniul medical cu noile provocări ce țin de prelucrarea datelor cu caracter personal etc. Evenimentul va fi organizat pentru reprezentanți ai Ministerului Sănătății, Muncii și Protecției Sociale și instituțiilor medicale, ai Ministerului Justiției, Ministerului Afacerilor Interne și Inspectoratului General al Poliției. Evenimentul va fi moderat de experți în protecția datelor cu caracter personal din Croația, Slovacia și reprezentanți din cadrul Centrului. Reieșind din situația la nivel global a pandemiei SARS- COV – 2, evenimentul va avea loc on-line la sfârșitul lunii ianuarie 2021, pentru aproximativ 300 de persoane, separat pe 3 regiuni ale țării: centru, nord și sud.

În anul 2020, Centrul a continuat desfășurarea activităților de instruire și sensibilizare. Perioada de referință a fost marcată de pandemia COVID-19, fapt care a influențat asupra numărului activităților de instruire. Din aceleași considerente, în anul 2020 cea mai mare parte din activitățile de instruire și sensibilizare au fost desfășurate on-line.

În anul 2020 instruirile au fost organizate atât pentru sectorul public cât și cel privat, cu precădere în municipiul Chișinău. Chiar dacă aceste activități au avut loc on-line, participanții au manifestat un interes sporit în dorința de a-și consolida cunoștințele în domeniul aferent protecției datelor cu caracter personal și de a conforma activitatea legată de prelucrarea datelor cu caracter personal la prevederile legale din domeniu.

Ațiuni de sensibilizare

Principalele activități de informare și sensibilizare a societății asupra importanței domeniului protecției datelor cu caracter personal desfășurate de Centru pe parcursul perioadei de raportare:

– 17 ianuarie 2020 – formator acreditat de către Proiectul Uniunii Europene Twinning, reprezentant al Centrului a promovat un dialog de discuții libere cu studenții Facultății de Drept, anul III a Universității Libere Internaționale din Republica Moldova, cu genericul „*Protecția datelor cu caracter personal pentru audiența tânără*”. La discuții au participat circa 50 de studenți.



– 28 ianuarie 2020 – de Ziua protecției datelor, Centrul a desfășurat, în premieră, un eveniment public pentru părinți și copii cu genericul „*Protejează-ți copilul în mediul online*”. Evenimentul a fost organizat în parteneriat cu Inspectoratul General al Poliției, Compania „Moldcell”, Asociația Obștească „Părinți Solidari” și Direcția generală educație, tineret și sport din municipiul Chișinău. Evenimentul a adunat circa 60 de părinți, inclusiv copii, din cadrul comitetelor părintești și de elevi din instituțiile de învățământ primar, secundar și general din sectorul Botanica, mun. Chișinău.



– 29 ianuarie 2020 – Centrul a continuat runda de evenimente dedicate Zilei protecției datelor, prin organizarea evenimentului de informare pentru studenți – „*Dreptul de acces la informație și dreptul la viața privată*” cu participarea studenților ultimului an de studii de la Facultatea de



Drept, ULM și Facultatea de Jurnalism, USM, inclusiv, cu participarea reprezentanților societății civile – Promo-Lex, Centrul de Resurse Juridice, Centrul de Investigații Jurnalistice etc. La eveniment au fost prezenți 14 participanți.



În contextul activităților de sensibilizare a importanței domeniului protecției datelor cu caracter personal, în cadrul proiectului UE Twinning „Consolidarea capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal” finanțat de Uniunea Europeană, **au fost elaborate diverse materiale informative destinate diferitor categorii de subiecți de date (inclusiv minorilor, părinților), precum și operatorilor de date cu caracter personal.** Materialele informative au fost utilizate pe parcursul anului 2020 în cadrul multiplelor activități organizate de Centru, acestea **având drept scop atât informarea despre drepturile subiecților de date și responsabilizarea acestora la prelucrarea conformă a datelor cu caracter personal, cât și asigurarea legalității prelucrării datelor cu caracter personal de către operatori.** Unele modele de materiale informative pot fi vizualizate la compartimentul anexe ale prezentului raport.

Activități de instruire

În perioada ianuarie-decembrie 2020, Centrului a desfășurat 7 ședințe de lucru cu reprezentanții instituțiilor publice și private pe aspectele ce vizau: asistență la elaborarea codurilor de conduită în diverse sfere de activitate, examinarea legilor sectoriale, ghidare și consultanță etc.

Totodată, reprezentanții Centrului au organizat 4 instruirii la care au fost prezenți circa 500 de participanți din municipiul Chișinău și din raioanele Republicii Moldova.

– la 27 februarie 2020, la invitația Centrului de Cooperare Polițienească Internațională, angajații Direcției Conformitate a Centrului au desfășurat o ședință de instruire a colaboratorilor Centrului Cooperare Polițienească Internațională.

– la 4 iunie 2020, la invitația conducerii Congresului Autorităților Locale din Moldova (CALM), reprezentanții Centrului au avut o alocuțiune în cadrul webinarului, pentru secretarii consiliilor locale, membri ai Rețelei Secretarilor din cadrul CALM, cu tema: „Elaborarea politicii de securitate și a Regulamentului de prelucrare a datelor cu caracter personal în cadrul APL”. La webinar au participat circa 85 de secretari ai consiliilor locale.





- la 27 iulie 2020, la solicitarea Centrului de Instruire în Domeniul Relațiilor de Muncă, reprezentantul Centrului a participat în calitate de formator, moderând un seminar privind protecția datelor cu caracter personal.
- la 17 noiembrie 2020, Centrul a desfășurat un training despre protecția datelor cu caracter personal la solicitarea Centrului de Instruire în Domeniul Relațiilor de Muncă. La eveniment au participat circa 150 de persoane – directori de școli, grădinițe, gimnazii, dar și angajați din domeniul medical. Instruirea a avut loc on-line.

Activitatea de mediatizare a Centrului

La începutul anului 2020, a fost lansată noua pagină web a Centrului www.datepersonale.md, fapt care constituie o realizare importantă atât pentru instituție cât și pentru societate per general, or, aceasta este o sursă de informare indispensabilă, care facilitează accesul utilizatorilor la totalitatea informațiilor vizând activitatea Autorității naționale de control a prelucrărilor de date cu caracter personal, precum și actualitățile aferente domeniului protecției datelor la nivel național și internațional.

Actuala pagină web a Centrului este inovativă și corespunde tuturor cerințelor și necesităților actuale din punct de vedere tehnic și organizatoric. De menționat că această realizare a fost posibilă datorită suportului acordat de Proiectul UE Twinning „Consolidarea capacităților CNPDCP” finanțat de Uniunea Europeană.

49034
vizualizări
pe pagina web a
CNPDCP
în 2020

Pe parcursul anului 2020, au fost elaborate și publicate pe pagina web a Centrului www.datepersonale.md – 80 de comunicate, articole și anunțuri. Totodată, în perioada de referință Centrul a elaborat și publicat 4 buletine informative trimestriale, vizând inclusiv informații statistice despre activitatea Centrului, precum și informații utile și actuale la nivel național și internațional la capitolul protecției datelor cu caracter personal.

În perioada de referință, despre activitatea Centrului s-a menționat în circa 70 articole de presă. Cifra s-a redus la jumătate față de cea din anul precedent pe fundalul crizei pandemice, care a dus la suspendarea mai multor evenimente ale Centrului. Printre sursele media care au mediatizat activitatea instituției au fost: Agora, Moldpres, TVR Moldova, Moldova1, Bizlaw, Sputnik Moldova, privesc.eu, Agenția de știri – Info Prim Neo, Curentul.md, Noi.md, tribuna.md, Radio Chișinău, democracy.md, Ziarul Moldova Suverană, publika.md, TV8.md, jurnal.md.

14712
vizualizări
pe Facebook/
CNPDCP în
2020

Interesul tot mai mare a cetățenilor față de activitatea Autorității naționale de protecție a datelor cu caracter personal se deduce inclusiv din mediul rețelelor de socializare. În context, pagina oficială de Facebook a Centrului – www.facebook.com/CNPDCP, potrivit postărilor înregistrează circa 1500 de vizitatori, lunar. Numărul urmăritorilor este și el în ascensiune – 2338 cu 37% mai mult în 2020 comparativ cu anul 2019.



CAPITOLUL IX

MANAGEMENTUL RESURSELOR UMANE

IX

MANAGEMENTUL RESURSELOR UMANE

Personalul constituie resursa cea mai valoroasă care contribuie la creșterea eficienței și eficacității instituției. Susținerea, stimularea și aprecierea la justa valoare a personalului angajat sunt factorii esențiali pentru menținerea unui climat organizațional și psihologic pozitiv la locul de muncă.

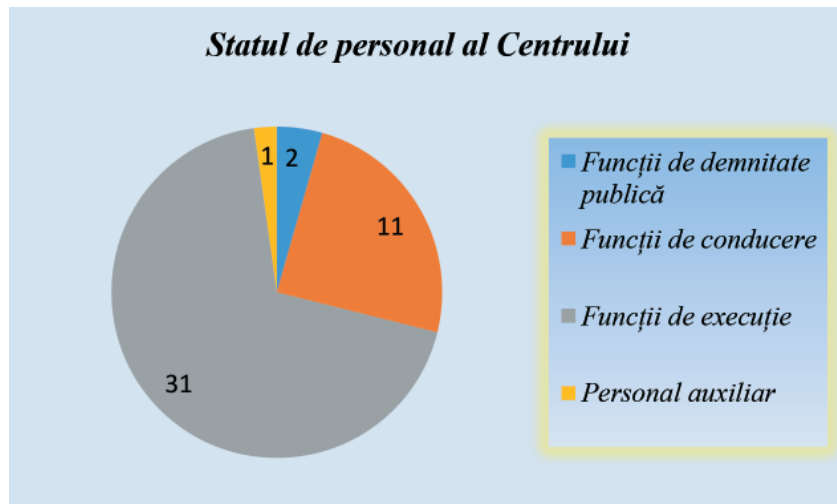
Autoritatea națională de protecție a datelor cu caracter personal își desfășoară activitatea prin personalul care asigură realizarea interesului public în domeniul de competență, și anume, funcționari de demnitate publică, funcționari publici și personal auxiliar.

Directorul și directorul adjunct exercită funcții de demnitate publică care cad sub incidența Legii nr. 199/2010, iar activitatea funcționarilor publici este reglementată de Legea nr. 158/2008 cu privire la funcția publică și statutul funcționarului public. Drepturile și responsabilitățile personalului auxiliar sunt stipulate în legislația muncii.

La îndeplinirea sarcinilor, personalul Centrului ține cont de interesul public în domeniul protecției datelor cu caracter personal, în conformitate cu prevederile Legii privind protecția datelor cu caracter personal nr. 133/2011.

Conform Legii nr. 182/2008, structura Centrului este alcătuită din 8 subdiviziuni structurale, iar efectivul-limită constituie 45 de unități care sunt distribuite în felul următor:

- 2 funcții de demnitate publică (director și director adjunct);
- 42 funcții publice, inclusiv 11 funcții publice de conducere și 31 funcții de execuție;
- 1 funcție auxiliară (conducător auto).



Astfel, la 31 decembrie 2020, gradul de ocupare al funcțiilor din cadrul Centrului a constituit 35 unități de personal, cu un raport de încadrare de doar 77,8 %, dintre care:

- 2 funcții de demnitate publică;
- 32 funcții publice, dintre care: 11 funcții de conducere; 21 funcții de execuție, dintre care 16 sunt controlori (controlori de stat principali – 4, controlori de stat superiori – 4, controlori de stat – 8), 3 consultanți (principal – 1, superior – 1, consultant – 1) și 2 specialiști principali;
- 1 funcție auxiliară (conducător auto).



*Funcții ocupate în cadrul Centrului
potrivit situației din 31 decembrie 2020*



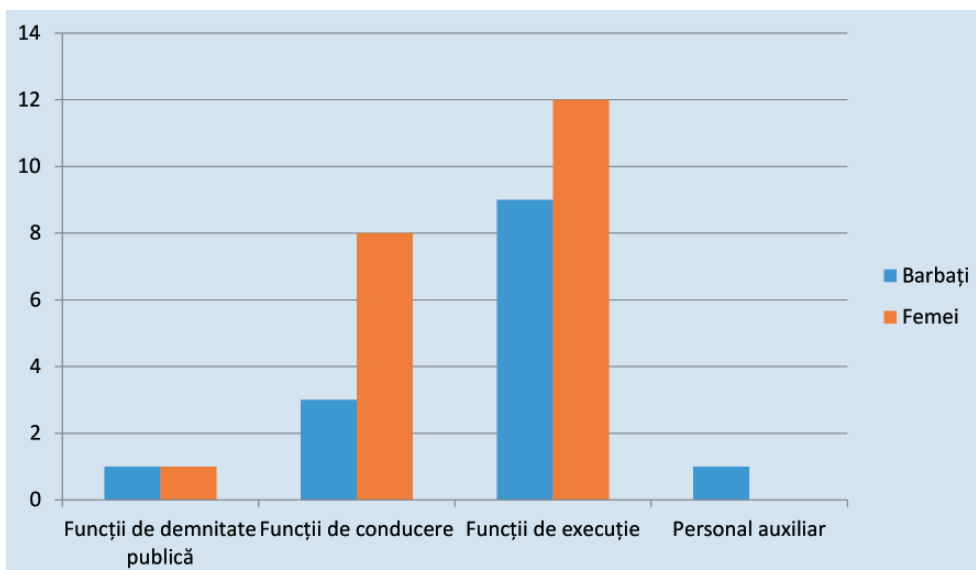
Astfel, comparativ cu anul precedent de raportare, gradul de ocupare a funcțiilor/posturilor a fost în creștere cu aproximativ 3,8 puncte procentuale.

Gradul de ocupare cu personal în perioada 2018-2020

Anul	Unități aprobate	Efectiv, angajați	Pondere, %
2018	45	32	71
2019	45	33	73
2020	45	35	77,8

Centrul a pledat și pledează permanent pentru o politică de egalitate de gen și de tratament egal între bărbați și femei în procesul de recrutare și de gestionare a resurselor umane. Așa dar, din numărul total de angajați, la sfârșitul perioadei de referință, ponderea bărbaților a fost de 40 %, iar cea a femeilor, respectiv, de 60 %.

În context, diagrama de mai jos demonstrează că ponderea femeilor este mai mare decât cea a bărbaților, atât la ocuparea funcțiilor de execuție, cât și a celor de conducere.





Colectivul Centrului este unul relativ tânăr, iar vârsta medie a angajaților în anul 2020 a fost de 36 ani. Ca și în anul precedent, în structura pe categorii de vârste, se menține cea mai mare pondere a persoanelor cu vârsta cuprinsă între 35-45 ani (40 % din total) și cele cu vârsta de 25-35 ani (31,4 % din total).

Angajarea tinerilor specialiști în cadrul Centrului este un fenomen continuu, influențând pozitiv structura profilului de vârstă a personalului, și doar atât, or, acest fapt, spre regret, nu aduce după sine o influență pozitivă și asupra activității autorității. Astfel, se observă o creștere a ponderii angajaților cu vârsta mai mică de 25 ani, ceea ce constituie 5,7 % din numărul total de angajați, fiind de două ori mai mare comparativ cu anul 2019.

Celelalte categorii de vârstă au avut ponderi mai reduse.

Personalul Centrului pe categorii de vârstă

Anul 2020	Total efectiv persoane	Funcțiile de demnitate publică	Funcție publică de conducere	Funcție publică de execuție	Personal auxiliar
Numărul de persoane	35	2	11	21	1
• < 25 ani	4	–	–	4	–
• 25-35 ani	11	–	1	10	–
• 35-45 ani	14	1	7	6	–
• 45-55 ani	4	1	2	1	–
• 55-63 ani	1	–	1	–	–
• 63 ani <	1	–	–	–	1

Cel mai tânăr angajat în anul 2020 avea 24 de ani, iar cel mai vârstnic – 65 de ani.

Politica de recrutare a Centrului are drept scop asigurarea necesarului optim de personal în baza principiilor de competiție deschisă, transparență, șanse egale, precum și merit profesional. Aceste principii sunt necesare pentru recrutarea unui personal care va realiza pe viitor obiectivele propuse de către autoritate.

În perioada de referință au fost organizate și desfășurate 8 concursuri pentru ocuparea funcțiilor publice vacante, dintre care 2 concursuri prelungite.

Aici trebuie de accentuat faptul că, 4 concursuri au fost suspendate pe o perioadă de mai mult de 2 luni, în legătură cu instituirea în Republica Moldova a stării de urgență în sănătate publică, reieșind din situația epidemiologică atât din țară, cât și la nivel mondial, precum și în scopul implementării măsurilor de prevenire și control al infecției cu Coronavirus de tip nou (COVID-19), ulterior fiind reluate.

În 2020 la concurs au fost scoase 11 funcții publice vacante și temporar vacante, dintre care 1 funcție de conducere și 10 de execuție, cum ar fi: 1 funcție de Șef Serviciu de informare, comunicare cu mass-media și e-Transformare, 4 funcții de controlori de stat în Direcția conformitate, 2 funcții de controlori în Direcția prevenire, supraveghere și evidență, 1 funcție de consultant în Direcția relații externe și integrare europeană, 1 funcție de consultant în Serviciul resurse umane, 1 funcție de specialist principal în Serviciul documentare și arhive și 1 funcție de auditor intern în Serviciul audit intern.



Pentru participare la concursuri au fost depuse 68 de dosare ale candidaților. În scopul asigurării transparenței procesului de organizare a concursului, pe pagina web a instituției (www.datepersonale.md) și pe cea guvernamentală (www.cariere.gov.md) au fost plasate informațiile cu privire la organizarea și desfășurarea concursurilor.

Ca urmare, în rezultatul concursurilor petrecute, au fost angajate 9 persoane, dintre care 7 fiind funcționari publici debutanți. Pe parcursul anului de raportare 3 funcționari publici debutanți au fost confirmați în funcțiile publice, obținând calificativul „bine” la evaluarea activității petrecute la finalizarea perioadei de probă, totodată fiind-le conferit și gradul de calificare „consilier de clasa a III-a”. De menționat, că ceilalți 4 funcționari publici debutanți urmează a fi evaluați și, după caz, confirmați în funcțiile publice deținute, în primul semestru al anului 2021.

Ca și în anii precedenți, Centrul se confruntă cu problema lipsei auditorului intern. Deja pe parcursul mai multor ani, începând cu anul 2017, funcția de audit intern a fost în permanență expusă la concurs, dar fără rezultate, din motivul lipsei candidaților, ca urmare a coraportului disproporționat dintre nivelul de salarizare, raportat la volumul de lucru și responsabilitățile solicitate în fișa postului.

Totodată, trebuie de menționat că, concursul pentru ocuparea funcției publice vacante de consultant în Serviciul resurse umane a fost anulat, deoarece învingătorul concursului a refuzat încadrarea în funcția publică, motivul fiind salariul neatractiv. În anul 2021 acest concurs urmează a fi reluat.

În același timp, trebuie de specificat că, în bază de merit, au fost promovați în funcții superioare 4 angajați, 2 funcționari publici au fost transferați în alte subdiviziuni ale Centrului, în scopuri de serviciu iar 2 funcționari publici au asigurat și continuă să asigure până în prezent interimatul a 2 funcții de conducere, pe perioada suspendării raporturilor de serviciu ale titularilor funcțiilor.

În anul 2020, se observă o **fluctuație de personal** mai scăzută în comparație cu anul 2019, numărul de persoane ale căror raporturi de muncă au încetat fiind de 6, față de cele 8 din anul precedent, dintre care 2 persoane s-au transferat în alte autorități publice, iar ceilalți 4 au demisionat la cerere.

De menționat că fluctuația personalului cu sarcini și atribuții de control din cadrul Centrului se menține și în acest an, astfel înregistrând o pondere de 50 % din numărul total de demisionați. Această creștere a fost cauzată de nivelul de salarizare irelevant în raport cu complexitatea activității de verificare a legalității privind prelucrarea datelor cu caracter personal.

Fenomenul fluctuației la un nivel foarte înalt, care sporește riscul de pierdere a memoriei instituționale și de distorsionare a activității instituției, este determinat de carențele din legislația privind salarizarea. Astfel, salariul de referință al angajaților Centrului este cu aproximativ 50% mai mic comparativ cu salariul acordat în cadrul altor entități din sectorul bugetar cu activități și competențe similare.

Mai mult ca atât, după investirea considerabilă în buna pregătire profesională a angajaților, în ridicarea nivelului cunoștințelor, priceperilor și deprinderilor de muncă necesare, în special în domeniul de competență, angajații decid să plece în alte autorități publice pentru un pachet salarial mai atractiv. Drept exemplu, în prezent, 3 dintre foștii angajați ai Centrului activează în cadrul Autorității Naționale de Integritate, entitate mult mai atractivă din punct de vedere a salariilor oferite angajaților săi.

Un element important în cadrul politicii de management a resurselor umane este tendința de dezvoltare profesională continuă a angajaților. În acest sens, a fost elaborat planul anual de dezvoltare profesională, conform căruia, angajații Autorității naționale de protecție a datelor cu



caracter personal au urmat 5 cursuri de instruire internă și 17 cursuri de instruire externă. Astfel, numărul de ore de instruire al participanților a constituit 474 de ore astronomice.

Dezvoltarea profesională continuă a funcționarilor publici din cadrul Centrului în anul de referință s-a realizat preponderent la Academia de Administrare Publică, prin activități de instruire desfășurate în mod mai puțin obișnuit decât în anii precedenți, în legătură cu situația determinată de pandemia COVID-19.

Astfel, cursurile de dezvoltare profesională s-au desfășurat în diferite formate:

- în sala de curs (of-line);



- la distanță (on-line);



- mixt: la distanță prin intermediul „Platformei LearnIn”, precum și cu prezența fizică în ultima zi a cursului la Academia de Administrare Publică.



La Academia de Administrare Publică, care este prestatorul de servicii de instruire și centrul de promovare a politicii de stat în domeniul dezvoltării profesionale a funcționarilor publici de toate nivelurile, 18 angajați ai Centrului au participat la 16 cursuri de dezvoltare profesională,



obținând certificate de dezvoltare profesională în următoarele competențe: *Integrarea profesională în funcția publică, Etica și integritatea profesională, Eficientizarea activității profesionale în administrația publică, Elaborarea și coordonarea proiectelor de acte normative, Managementul conflictelor, Managementul serviciilor publice, Planificarea strategică și operațională în administrația publică, Gestionarea eficientă a stresului la locul de muncă.*

Totodată 2 angajați ai Centrului au participat la Atelierul de lucru cu genericul „Gestionarea incidentelor cibernetice”, organizat de I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” în parteneriat cu I.P. „Agenția de Guvernare Electronică” și Academia de e-Guvernare din Estonia.

Un accent forte în anul 2020 s-a pus pe instruirea internă a angajaților. Astfel, în contextul pandemiei globale, conducerea Centrului, periodic, a realizat instruirea personalului referitor la măsurile-cheie în partea ce ține de prevenirea și atenuarea infecției COVID-19 la locul de muncă. În acest sens, a fost elaborat și un ghid cu reguli concrete, pentru a ajuta angajații să își păstreze sănătatea și siguranța la locul de muncă.

În aceeași ordine de idei, este necesar de menționat că, a fost asigurată și instruirea introductivă generală în domeniul securității și sănătății în muncă, inclusiv a noilor angajați.

La fel, în perioada de referință au fost efectuate și alte cursuri de dezvoltare profesională internă cu diverse tematici, cum ar fi cu privire la: „utilizarea semnăturii electronice”, „utilizarea paginii web a Centrului (www.datepersonale.md)” etc.

Pe parcursul anului de raportare, pentru exercitarea eficientă a atribuțiilor de serviciu, merite deosebite în activitate, manifestare a spiritului de inițiativă și contribuție deosebită în realizarea unor sarcini specifice, pentru activitate îndelungată și ireproșabilă în cadrul instituției, precum și cu prilejul Zilei funcționarului public, unui angajat al Centrului i-a fost conferită Diploma Guvernului.

În scopul asigurării unui management eficient al resurselor umane în anul 2020 au fost elaborate 391 acte administrative interne, ce țin de raporturile de muncă ale salariaților, precum și un șir de documente interne ce reglementează activitatea diferitor comisii, cum ar fi: Comisia de concurs, Comisia de evaluare și evidență a cadourilor, Comisia de disciplină etc.



CAPITOLUL X

ACTIVITATEA ECONOMICO-FINANCIARĂ

X

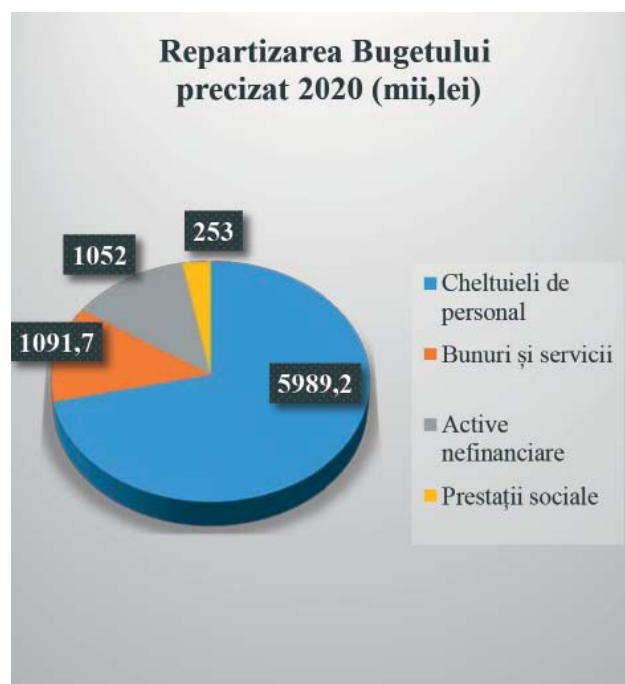
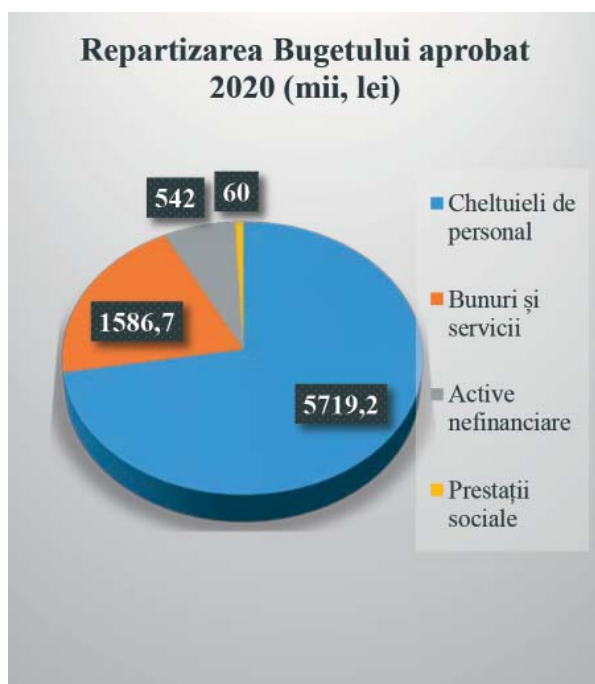
ACTIVITATEA ECONOMICO-FINANCIARĂ

Bugetul Centrului a fost elaborat conform prevederilor Legii finanțelor publice și responsabilitățile bugetar-fiscale nr.181/2014 și regulile stabilite de Ministerul Finanțelor. Astfel, prin Legea bugetului de stat pentru anul 2020 nr.172/2019, pentru Autoritatea de protecție a datelor cu caracter personal au fost aprobate alocații în sumă de **7 907,9 mii lei** la componenta resurse generale.

Totodată, prin Hotărârile Guvernului nr. 854/2020 și nr. 896/2020 privind modificarea Legii bugetului de stat pentru anul 2020, alocațiile Centrului au fost majorate cu 70,0 mii lei și, respectiv, cu 200,0 mii lei, în scopul acoperirii parțiale a cheltuielilor pentru implementarea prevederilor Legii nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar, la capitolul „remunerarea muncii”, precum și pentru achitarea premiului anual personalului din unitățile bugetare pentru rezultatele activității în anul 2019, stabilit prin Hotărârea Guvernului nr. 811/2020.

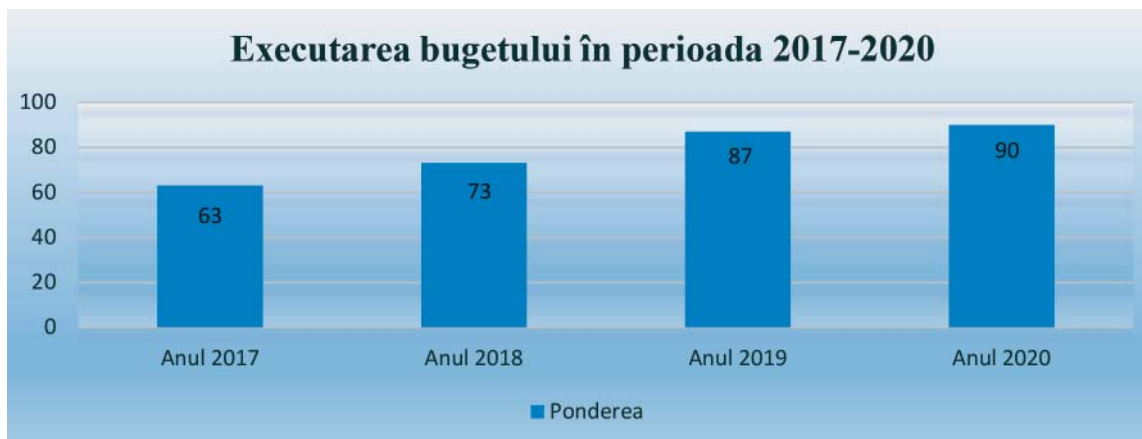
Suplimentar, Centrului i-au fost alocate mijloace financiare în sumă de 208,0 mii lei pentru acordarea indemnizației unice angajaților infectați cu COVID-19 în timpul exercitării atribuțiilor de serviciu, în conformitate cu Legea nr.69/2020 cu privire la instituirea unor măsuri pe perioada de urgență în sănătate publică, conform Hotărârii Guvernului nr. 895/2020.

Astfel, **bugetul precizat** al Centrului pentru anul 2020 a constituit **8 385,9 mii lei**.

Analiza alocațiilor bugetare pentru anul 2020



Potrivit situației la data de 31 decembrie 2020, bugetul Centrului a fost executat în mărime de 7 583,3 mii lei, ceea ce constituie 90,4% din bugetul precizat, fiind în creștere în comparație cu perioada anilor 2017-2020.



Mijloacele financiare alocate din bugetul de stat au fost îndreptate spre acoperirea cheltuielilor necesare pentru întreținerea activității Autorității naționale de protecție a datelor cu caracter personal pe următoarele direcții:

Executarea cheltuielilor în anul 2020 (mii lei)

Indicatori	Aprobat	Precizat	Executat	Executat față de precizat (%)
Cheltuieli de personal	5719,2	5989,2	5946,3	99,3
Bunuri și servicii	1586,7	1091,7	775,6	71,1
Prestații sociale	60,0	253,0	249,1	98,5
Active nefinanciare, inclusiv:	542,0	1052,0	612,3	59,0
<i>mijloace fixe</i>	217,0	807,0	413,1	51,2
<i>stocuri de materiale circulante</i>	325,0	245,0	199,2	81,3
TOTAL	7907,9	8385,9	7583,3	90,4

În structura cheltuielilor, cea mai mare pondere o dețin „**cheltuielile de personal**”, dar urmează a fi specificat că, mijloacele financiare alocate în sumă de 5 719,2 mii lei au fost insuficiente în vederea remunerării muncii angajaților, precum și pentru achitarea premiului anual pentru rezultatele activității din anul 2019. Astfel, în rezultatul înaintării demersului corespunzător către Ministerul Finanțelor, alocațiile precizate au constituit 5989,2 mii lei.

Bugetul precizat la capitolul „**bunuri și servicii**” a constituit 1 091,7 mii lei. Cheltuielile executate la această categorie au fost de 775,7 mii lei, formând un sold neutilizat în mărime de 316,0 mii lei. Astfel s-au format economii la servicii de locațiune, deplasări de serviciu și alte servicii.

La capitolul „**prestații sociale**” au fost aprobate inițial alocații în mărime de 60,00 mii lei. Dar, în urma alocării mijloacelor financiare din fondul de rezervă al Guvernului în sumă de 208,0 mii lei (achitarea indemnizației unice angajaților care s-au infectat cu COVID-19 în timpul exercitării atribuțiilor de serviciu), alocațiile precizate au crescut până la 253,0 mii lei.

Odată cu modificarea structurii Centrului și majorarea, în anul 2017, a efectivului-limită de personal, a intervenit necesitatea extinderii spațiului de muncă, fapt realizat abia la mijlocul



anului 2020. În acest sens, Centrul a primit în folosință spațiu suplimentar situat la etajul IV al sediului în care își desfășoară activitatea, în vederea asigurării condițiilor optime pentru buna desfășurare a activității și realizarea atribuțiilor de bază. Astfel, au fost procurate bunuri (mobilier, tehnică de calcul, etc.), cheltuieli reflectate la capitolul „**active nefinanciare**”.

În conformitate cu Hotărârea Guvernului nr. 1419/2016, **Planul de achiziții publice** pentru anul 2020 al instituției a fost elaborat și publicat pe pagina web a Centrului: <https://datepersonale.md/wp-content/uploads/2020/02/Planul-de-achizitie-2020.pdf>.

În vederea realizării planului menționat, pe parcursul perioadei de referință, au fost încheiate 35 contracte de achiziții publice, dintre care:

- 34 contracte de valoare mică privind achiziționarea de bunuri și servicii;
- 1 contract prin procedura de negociere fără publicare prealabilă a unui anunț de participare, aferent serviciilor de administrare tehnică a SIA „Registrul de evidență a operatorilor de date cu caracter personal”. De menționat că, pct. 11 lit. f) din Hotărârea Guvernului nr. 883 din 25.11.2011 cu privire la aprobarea Conceptului tehnic al sistemului informațional automatizat „Registrul de stat al operatorilor de date cu caracter personal”, stipulează că Î.S. „Centrul de Telecomunicații Speciale”, în prezent I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” are calitatea de entitate care va asigura asistența și mijloacele tehnice necesare implementării și funcționării Registrului, va reprezenta entitatea care va prelua soluția informatică și va asista implementarea și administrarea acestui sistem informatic.

Toate contractele au fost înregistrate la Trezoreria de Stat.

Trebuie de precizat că, la încheierea contractelor de valoare mică, s-au luat în calcul factorii precum: oportunitatea cheltuielilor și criteriul celui mai scăzut preț, alăturat unor cerințe tehnice atent stabilite, ceea ce a condus la utilizarea eficientă a mijloacelor financiare alocate Centrului.

Aplicarea procedurilor de achiziție publică a asigurat contractarea operatorilor economici calificați și cu experiență în domeniul executării contractelor de achiziție publică.

Toate contractele de achiziții încheiate întru asigurarea necesităților Centrului au fost executate integral și în termen.



PROBLEME ȘI OBIECTIVE

Probleme cu care se confruntă Centrul

Este regretabil faptul că, pe parcursul mai multor perioade de raportare deja, se constată același spectru al preocupărilor/problemelor cu care se confruntă Autoritatea națională de protecție a datelor cu caracter personal. De menționat că preocupările majore reflectate de la an la an, inclusiv în rapoartele de activitate ale Centrului, generează impedimente tot mai accentuate atât în activitatea instituțională și organizatorică, cât și în dezvoltarea domeniului protecției datelor cu caracter personal la nivel național. Or, ținând cont de faptul că soluționarea problemelor stringente cu care se confruntă Centrul, în mare parte, depășește competența acestei autorități, devine și mai dificilă asigurarea dezvoltării domeniului de competență.

În acest sens, **problemele de ordin legal, instituțional, de precepție și aplicabilitate**, care necesită soluționare stringentă întru depășirea stagnării domeniului protecției datelor cu caracter personal la nivel național, sunt următoarele:

- **neconcordanța între cadrul legal național din domeniul protecției datelor cu caracter personal și reglementările existente la nivel european**, și anume, 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 și 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;
- **nivelul discriminatoriu al salarizării funcționarilor din cadrul Centrului** în raport cu cel prevăzut pentru alte organe de control cu statut similar și care, ținând cont de specificul activității desfășurate ce prezumă indubitabil prelucrarea datelor cu caracter personal, sunt supuse verificării legalității prelucrării datelor de către Centru. În acest sens, pot fi indicate spre exemplu următoarele entități: Serviciul de Informații și Securitate, Ministerul Afacerilor Interne, organele procuraturii, Centrul Național Anticorupție, Autoritatea Națională de Integritate, Serviciul prevenirea și combaterea spălării banilor etc.;
- **numărul mic de angajați ai Centrului conform statului de personal de 45 unități, în raport cu volumul tot mai mare de lucru**, în special în subdiviziunile de bază ale autorității: Direcția generală supraveghere și conformitate, Direcția juridică, mai ales în contextul investiției autorității pe parcursul ultimilor ani cu multiple atribuții suplimentare (de exemplu prin: Legea comunicațiilor electronice, Legea cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, Legea cu privire la prevenirea și combaterea terorismului etc.), fără fi create/asigurate și mecanisme instituționale fiabile întru realizarea sarcinilor prescrise;
- **fluctuația cadrelor** și insuficiența/lipsa la nivel național a specialiștilor calificați în domeniul protecției datelor cu caracter personal;



- **inexistența garanțiilor corespunzătoare pentru colaboratorii Centrului** în ceea ce privește riscurile generate de activitatea de control și acțiunile de imixtiune a unor organe, în speță Centrul Național Anticorupție, cu scopul de a intimida angajații Centrului prin fabricarea de dosare;
- **ineficiența și insuficiența pârghiilor coercitive pentru prelucrarea ilegală a datelor cu caracter personal**, motivul fiind caracterul dublu, contradictoriu și susceptibil a procedurilor de examinare a constatărilor rezultate în urma verificării legalității prelucrării datelor cu caracter personal, manifestat prin dublarea examinării în instanțele de judecată, în aceeași perioadă, a acelorași acte și constatări emise de Centru, atât în ordine de contencios administrativ cât și în procedură contravențională. Or, deciziile emise de Centru în ordinea statuată de art. 27 al Legii privind protecția datelor cu caracter personal, prin care se constată încălcarea prevederilor legale de domeniul protecției datelor cu caracter personal, pe de o parte sunt pasibile contestării în ordine de contencios administrativ, iar pe de altă parte, servesc drept bază la constatarea faptelor contravenționale și întocmirea proceselor-verbale cu privire la contravenție, care se expediază spre examinare în instanța de judecată. Astfel, pe lângă faptul că pentru comiterea aceleiași fapte/încălcări, operatorul de date cu caracter personal este supus răspunderii/sanționării de 2 ori – circumstanțe ce contravin principiilor de individualizare și atragere la răspundere a persoanei, se evidențiază și situații în care, același operator, pentru aceeași faptă, în ordine contravențională este recunoscut vinovat de către instanța de judecată iar în ordine de contencios administrativ, este declarat ca fiind nevinovat, sau viceversa. Or, este cu atât mai bizară situația descrisă ținând cont de faptul că în cazul ambelor spețe (procedura contravențională și procedura de contencios administrativ) la bază există una și aceeași decizie de constatare a încălcării comise la prelucrarea datelor cu caracter personal. În acest context, existența unor astfel de proceduri contradictorii au dus, în unele cazuri, la determinarea ineficienței acțiunilor întreprinse de Centru pentru a contracara prelucrările neconforme de date și a preveni săvârșirea altor încălcări ce vizează dreptul la inviolabilitatea vieții intime, familiale și private a subiecților de date cu caracter personal. Or, circumstanțele descrise sunt și mai dezolante și dezarmante pentru Autoritatea națională de control a prelucrărilor de date cu caracter personal, ținând cont de numărul angajaților subdiviziunilor de resort ale Centrului care este absolut infim în raport cu volumul excesiv de muncă pus pe umerii acestora;
- **utilizarea abuzivă a prevederilor legale din domeniul protecției datelor cu caracter personal**, în special de către reprezentanții autorităților publice, la pretinsa argumentare a refuzului în prezentarea informațiilor solicitate prin prisma realizării dreptului de acces la informație;
- **lipsa mecanismelor, garanțiilor procedurale și de control efectiv în cazul organelor de drept** la efectuarea măsurilor speciale de investigații, **care ar asigura un just echilibru între interesul organului de urmărire penală de a acumula anumite probe și drepturile subiecților de date cu caracter personal vizați**. Spre exemplu, nu există o evidență a faptului dacă subiecților de date cu caracter personal care au fost supuși măsurilor speciale de investigații le-a fost realizat dreptul de a fi informați în acest sens sau dacă a fost restricționată informarea acestora și motivele care au dus la amânarea informării etc. Or, la moment nu există un mecanism de informare post factum a subiecților de date cu caracter personal privind interceptarea telefonică a acestora sau privind desfășurarea în privința lor a altor măsuri speciale de investigații, or, obligatia realizării drepturilor subiecților de date cu caracter personal, odată cu epuizarea scopului pentru care aceste drepturi au fost restricționate (dreptul de informare, de acces la date etc.) este prevăzută atât de art. 15 al Legii privind protecția datelor cu caracter personal cât și de prevederile legale specifice domeniului de activitate (Codul de procedură penală, Legea privind activitatea specială de investigații etc.). În context, este de menționat **inexistența unui registru electronic** al interceptărilor telefonice, comunicațiilor electronice sau a altor măsuri speciale de investigație, cum ar fi filajul etc., **instituirea căruia ar constitui o soluție eficientă de depășire**



a deficiențelor indicate supra. Informația mai detaliată la tematica dată este reliefată supra, la compartimentul Activitatea de prevenire a neconformității prelucrării datelor cu caracter personal;

- **numărul mare a operațiunilor de accesare a datelor cu caracter personal stocate în resursele informaționale automatizate de stat, efectuate în lipsa unui scop și temei legal**, în special de către angajații organelor de drept, precum și **lipsa sau insuficiența măsurilor necesar a fi implementate în vederea ținerii evidenței eficiente a operațiunilor de prelucrare a datelor cu caracter personal**. Informația mai detaliată vizând aspectul dat este reflectată supra, la compartimentul Activitatea de prevenire a neconformității prelucrării datelor cu caracter personal.

Obiective pentru anul 2021

Obiectivele de bază ale Centrului pentru anul 2021, dar fără a se limita la cele descrise în continuare, se vor centra în vederea:

- asigurării **conformării cadrului legal național din domeniul protecției datelor cu caracter personal la reglementările noi existente la nivel european**, prin aprobarea de către Parlamentul Republicii Moldova în lectură finală a proiectelor de legi: privind protecția datelor cu caracter personal și privind Centrul Național pentru Protecția Datelor cu Caracter Personal. Totodată, urmare a realizării obiectivului dat, se perindă obligativitatea elaborării și implementării cadrului normativ precum și intern aferent punerii în aplicare a noilor prevederi legale;
- asigurării **ridicării nivelului de salarizare a funcționarilor din cadrul Centrului**, racordat celui prevăzut pentru alte organe de control și de drept cu statut similar, care, ținând cont de specificul activității desfășurate ce prezumă indubitabil prelucrarea datelor cu caracter personal, sunt supuse verificării legalității prelucrării datelor de către Centru;
- **majorării efectivului limită de personal** a Autorității naționale de control a prelucrărilor de date cu caracter personal, **în raport cu volumul de lucru și competențele atribuite Centrului**, or, reieșind din actualul specific al activității, pentru o bună desfășurare a competențelor legale este necesară majorarea statelor de personal până la 150 de unități;
- realizării în continuare a Planului de acțiuni pentru implementarea Acordului de Asociere Republica Moldova – Uniunea Europeană;
- continuării și amplificării acțiunilor de **sensibilizare a societății privind importanța domeniului protecției datelor cu caracter personal**, atât din perspectiva respectării/cunoașterii drepturilor subiecților de date, cât și prin prisma asigurării implementării obligațiilor aferente operatorilor de date cu caracter personal;
- contribuiri la **ridicarea nivelului de interpretare corectă și aplicare conformă a prevederilor legale din domeniul protecției datelor cu caracter personal** de către actorii implicați în prelucrarea datelor cu caracter personal, inclusiv prin asigurarea echilibrului între prevederile legale aferente drepturilor de acces la informație, libertății de exprimare și protecției datelor cu caracter personal;
- contribuiri la **crearea practicii judiciare uniforme** la aplicarea prevederilor legislației privind protecția datelor cu caracter personal;
- sensibilizării partenerilor de dezvoltare în realizarea proiectelor comune, în vederea asigurării nivelului adecvat de protecție a datelor cu caracter personal în Republica Moldova.



ANEXE

Materiale informative elaborate și utilizate în activitatea Centrului

Proiect finanțat de Uniunea Europeană

Legalitatea prelucrării datelor cu caracter personal

Centrul Național pentru Protecția Datelor cu Caracter Personal
 www.datepersonale.md
 centru@datepersonale.md
 www.facebook.com/CNPDCP

Consimțământul

Acordul unui subiect de date pentru prelucrarea datelor sale cu caracter personal

Necesitatea contractuală

Prelucrarea este necesară pentru a încheia sau executa un contract

Obligații legale

Operatorul este obligat să prelucreze datele cu caracter personal în virtutea unei obligații legale

Interese vitale

Este de importanță vitală ca anumite date să fie prelucrate în chestiuni de viață și moarte

Interese publice

Autoritățile și organizațiile publice, în contextul sarcinilor și intereselor publice

Interese legitime

Există un interes legitim când prelucrarea este necesară și acest interes nu poate fi suspendat de alte interese.

Acet material a fost pregătit în cadrul Proiectului UE Twinning "Consolidarea Capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova" finanțat de Uniunea Europeană

Informația prezentată se bazează pe conținutul Regulamentului 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor)

Contactează-ne la Linia specializată a Centrului Național pentru Protecția Datelor cu Caracter Personal (CNPD) **022 820 804**

Proiect finanțat de Uniunea Europeană

Ciclul de viață al prelucrării datelor cu caracter personal

Centrul Național pentru Protecția Datelor cu Caracter Personal
 www.datepersonale.md
 centru@datepersonale.md
 www.facebook.com/CNPDCP

Ștergerea

Când și cum ștergem datele cu caracter personal

Identificarea

Ce date cu caracter personal, în ce scop, ce categorii de subiecți de date, cum de obținut datele cu caracter personal, unde vor fi prelucrate, pentru cât timp

Definirea

Cine le va accesa, cum vor fi prelucrate, când vor fi accesate, de ce vor fi prelucrate?

Arhivarea

Când și de ce arhivăm datele cu caracter personal

Colectarea

Cât de sigură este resursa IT

Stocarea

Cât timp, în ce scopuri stocăm datele cu caracter personal

Prelucrarea

Cum prelucram datelor cu caracter personal

Acet material a fost pregătit în cadrul Proiectului UE Twinning "Consolidarea Capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova" finanțat de Uniunea Europeană

Informația prezentată se bazează pe conținutul Regulamentului 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor)

Contactează-ne la Linia specializată a Centrului Național pentru Protecția Datelor cu Caracter Personal (CNPD) **022 820 804**



Proiect finanțat de Uniunea Europeană

Verificați modalitatea de prelucrare a datelor cu caracter personal în companie!

Întrebări esențiale pe care trebuie să vi le puneți, dacă prelucrați date cu caracter personal



Centrul Național pentru Protecția Datelor cu Caracter Personal

- www.datepersonale.md
- centru@datepersonale.md
- www.facebook.com/CNPDCP



Ce date aveți?
Explicați ce date cu caracter personal sunt prelucrate.



De ce date aveți nevoie?
Evaluati de ce date aveți nevoie.



Ce date trebuie să prelucrați și ce date veți șterge?
Asigurați legitimitatea datelor prelucrate.



Cine stabilește de ce trebuie prelucrate datele cu caracter personal?
Evaluati dacă sunteți un operator de date sau o persoană împuternicită de operator.



Cât timp trebuie să păstrați datele?
Definiți termenii de stocare a datelor.



Cine are acces la date?
Monitorizați persoanele care au acces la datele cu caracter personal.



Cu cine le împărtășiți?
Aflați cui transferați datele.



Unde sunt stocate datele dvs.?
Evaluati locațiile din punct de vedere al securității.



Vă testați securitatea?
Evaluati securitatea prelucrării datelor.



Angajații dvs. sunt informați despre prelucrarea datelor și aspectele legate de securitate?
Desfășurați instruirii periodice pentru personal.



Aveți nevoie să desemnați un responsabil de protecția datelor cu caracter personal?
Efectuați o evaluare a impactului asupra protecției datelor cu caracter personal.



Acest material a fost pregătit în cadrul Proiectului UE Twinning "Consolidarea Capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova" finanțat de Uniunea Europeană

Informația prezentată se bazează pe cerințele Regulamentului 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor)

Contactează-ne la Linia specializată a Centrului Național pentru Protecția Datelor cu Caracter Personal (CNPDCP)

022 820 804



Proiect finanțat de Uniunea Europeană

Procesul de respectare a cerințelor față de protecția datelor cu caracter personal



Centrul Național pentru Protecția Datelor cu Caracter Personal

- www.datepersonale.md
- centru@datepersonale.md
- www.facebook.com/CNPDCP

Ce aveți?

Care sunt riscurile?

Ce trebuie să faceți?

Faceți aceasta!

Ați reușit?

Inventariere

Evaluare

Analiză

Implementare

Evaluare



Angajați

Cunoștințe

Nivelul de conștientizare din partea angajaților

Instruiți

Ateliere de lucru / instruirii
Campanii de conștientizare

Ameliorări



Proces

Operator de date/Operator asociat/Persoană împuternicită de operator
Responsabilitate Acorduri cu persoana împuternicită de operator
Bază juridică
Principii

Auditul organizației, proceselor și procedurilor

Elaborați planul de implementare a soluțiilor pentru problemele de prelucrare a datelor cu caracter personal

Implementați documentația. Desemnați un responsabil de protecția datelor

Managementul prelucrării datelor



Tehnologie

Ce rețea, aplicații, baze de date, sisteme sunt implicate?

Vulnerabilitățile: rețea, sisteme, aplicații

Controale de securitate: criptare, protecția la faza de concepere, protecție implicită, controlul accesului, managementul rolului

Implementați documentația și procedurile de securitate

Monitorizarea securității



Acest material a fost pregătit în cadrul Proiectului UE Twinning "Consolidarea Capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova" finanțat de Uniunea Europeană

Informația prezentată se bazează pe cerințele Regulamentului 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor)

Contactează-ne la Linia specializată a Centrului Național pentru Protecția Datelor cu Caracter Personal (CNPDCP)

022 820 804



Proiect finanțat de Uniunea Europeană

Sfaturi. Cum să ne comportăm pe Internet!



Centrul Național pentru Protecția Datelor cu Caracter Personal

- www.datepersonale.md
- centru@datepersonale.md
- www.facebook.com/CNPDCP

Au trecut timpurile parolelor bizare și complexe. Aceste parole sunt greu de reținut, dificil de scris, dar pot fi ușor de spart de către un atacator cibernetic, având în vedere computerele super-rapide de astăzi. Cheia pentru parolele bune este să fie lungi; cu cât mai multe caractere, cu atât mai bine. Acestea se numesc fraze de acces: un tip de parolă puternică care este formată dintr-o propoziție scurtă sau cuvinte aleatorii. Iată două exemple:

Îmi place să beau cafea dimineața!

pierdut-melo-târât-plajă

Ambele sunt puternice, conțin peste douăzeci de caractere, sunt ușor de reținut și simple de scris, dar greu de spart. Rețineți totuși că lungimea parolei este cea mai importantă.

Aveți nevoie de o parolă unică pentru fiecare cont. Dacă reutilizați aceeași parolă pentru mai multe conturi, vă supuneți unui pericol mare. Tot ce trebuie să facă un atacator cibernetic este să spargă un site web pe care îl folosiți, să fure toate parolele, inclusiv ale dvs., apoi să folosească parola dvs. pentru a se conecta la toate celelalte conturi, la fel ca și dvs.

Aflați ce date au colectat, postat sau distribuit despre dvs. online alte persoane sau organizații (școli, cluburi sportive sau alte site-uri ale comunității locale).



Accesați portalul www.havebeenpwned.com pentru a vedea care dintre site-urile utilizate de dvs. au fost sparte, parolele dvs. fiind potențial compromise.

Analizați ce distribuți public și impactul pe care informațiile îl pot avea asupra dvs., familiei sau angajatorului dvs.

Conștientizați că aceste resurse sunt disponibile pentru oricine altcineva, inclusiv infractorii cibernetici, care pot utiliza informațiile respective pentru a vă ținti. Fiți suspicioși. De exemplu, dacă primiți un apel telefonic urgent de la cineva care pretinde că este banca dvs., doar simplul fapt că persoana respectivă cunoaște câteva informații de bază despre dvs. nu dovedește că este cineva de la bancă. Închideți apelul în mod politicos, apoi sunați banca la un număr cunoscut, de încredere, pentru a confirma că apelul a venit din partea lor. La fel este și cu e-mailul, doar pentru că un e-mail conține niște date cunoscute despre dvs. nu înseamnă că este legitim.



Acest material a fost pregătit în cadrul Proiectului UE Twinning "Consolidarea Capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova" finanțat de Uniunea Europeană

Informația prezentată se bazează pe cerințele Regulamentului 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor)

Contactați-ne la Linia specializată a Centrului Național pentru Protecția Datelor cu Caracter Personal (CNPDPCP)

022 820 804



Proiect finanțat de Uniunea Europeană

Aflați dacă datele dvs. sunt prelucrate în mod legal



Centrul Național pentru Protecția Datelor cu Caracter Personal

- www.datepersonale.md
- centru@datepersonale.md
- www.facebook.com/CNPDCP



CINE?

Determinați cine, independent sau în comun, stabilește scopurile și mijloacele prelucrării datelor dvs. – identificați cine poartă răspundere.



CE?

Ce date sunt solicitate? Aflați exact ce a fost solicitat pentru a evalua dacă este adecvat, relevant și limitat la ceea ce este necesar.



DE CE?

De ce au nevoie de date? Aflați scopul prelucrării datelor dvs. și care este baza legală.



PENTRU CÂT TIMP?

Cât timp vor fi păstrate datele? Aflați perioada de timp stabilită pentru stocarea datelor dvs. sau criteriile pentru stabilirea acestei perioade.



CUM?

Cum vor fi prelucrate datele? Aflați despre prelucrarea automatizată: temeiul legal/baza și logica; toți destinatarii datelor dvs. și modul în care datele dvs. sunt salvate și protejate.



Acest material a fost pregătit în cadrul Proiectului UE Twinning "Consolidarea Capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova" finanțat de Uniunea Europeană

Informația prezentată se bazează pe cerințele Regulamentului 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor)

Contactați-ne la Linia specializată a Centrului Național pentru Protecția Datelor cu Caracter Personal (CNPDPCP)

022 820 804



Înainte de a publica fotografiile, recenzii și comentarii pe rețelele de socializare, gândește-te cum te va putea afecta acest lucru peste câțiva ani, când vei fi celebru! **Internetul Nu Uită Niciodată!**



Dacă primești scrisori în lanț, cu sarcini pe care trebuie să le îndeplinești, de exemplu, să transferi bani pe un anumit cont bancar sau să arunci cu ceva în sora ta mai mică, ignoră scrisoarea și nu o trimite prietenilor. Dacă vei continua să primești astfel de scrisori, informează-ți părinții.



Dacă găsești documentele unei persoane, du-le la poliție și nu le publica pe rețelele de socializare. Obligația de a căuta deținătorul documentului este a poliției, nu a ta.



Gândește-te de cel puțin trei ori înainte de a publica un comentariu insultător despre cineva, deoarece acesta poate afecta negativ viața persoanei și poate oferi informații despre tine, ca persoană.



Dacă crezi că identitatea ta este folosită de o altă persoană, informează-ți părinții, care se vor adresa poliției sau la CNPDCP.


 Acest material a fost pregătit în cadrul Proiectului UE Training "Cooperarea Capacităților Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova" finanțat de Uniunea Europeană.


 Proiect finanțat de Uniunea Europeană

Acționează inteligent și protejează-ți datele!




Centrul Național pentru Protecția Datelor cu Caracter Personal

www.datepersonale.md
centru@datepersonale.md
www.facebook.com/CNPDCP

Informația prezentată se bazează pe cerințele Regulamentului 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date (Regulamentul general privind protecția datelor)

022 820 804 Contactează-ne la Linia specializată a Centrului Național pentru Protecția Datelor cu Caracter Personal (CNPDCP)



Datele tale cu caracter personal sunt numele, prenumele, numărul de telefon, adresa, notele școlare și comportamentul.



Datele tale cu caracter personal pot fi folosite de autorități doar dacă au fost informați părinții tăi și dacă există o situație de urgență, cum ar fi un accident, iar tu ai nevoie de ajutor.



Dacă dorești să utilizezi rețelele sociale, dar încă nu ai 16 ani, roagă părinții să te ajute la înregistrarea pe rețeaua de socializare.



Datele tale cu caracter personal sunt utilizate la școală, deoarece acest lucru este necesar pentru a beneficia de studii. Nu dezvăluie datele tale cu caracter personal altor persoane fără permisiunea părinților.



Dacă un străin îți întreabă numele, prenumele sau numărul de telefon, nu reacționa. Spune-le părinților despre aceasta!



Dacă cineva te sună și dorește să afle ceva despre tine sau părinții tăi, nu reacționa și spune-le părinților despre asta.



Datele tale cu caracter personal sunt utilizate de către medicul tău pentru a avea grijă de sănătatea ta.



Părinții tăi știu cum și cine folosește datele tale cu caracter personal. Dacă bănuiești că cineva dorește să „fure” datele tale cu caracter personal pentru a le folosi în scopuri meschine, informează-ți părinții.



Dacă un străin îți scrie pe rețelele de socializare și îți cere să-i trimiți fotografia ta unde ești dezbrăcat, nu face acest lucru, pentru că nu știi ce va face acea persoană cu fotografia ta și cum va fi folosită pentru a te umili.



Proiect finanțat de
Uniunea Europeană

Centrul Național
pentru Protecția Datelor
cu Caracter Personal



www.datepersonale.md
centru@datepersonale.md
www.facebook.com/CNPDCP



Ești un expert în ale Internetului?

Folosește parole sigure!
Folosește o parolă diferită
pentru fiecare site.
Creează parole destul de
complicate pentru a nu fi
ghicite chiar și de oameni
care te cunosc bine!

Nu dezvălui informații despre tine -străinilor!
Nu toți cei pe care îi întâlnești pe Internet sunt
ceea ce spun. Adesea, răufăcătorii își ascund
adevărata față pentru a avea acces mai ușor la
tine, rudele și prietenii tăi. Cu cât mai multe
dezvăluiri despre tine, cu atât mai ușor îți vor
putea face rău în viața reală. Nu-ți dezvălui
numele, locul unde locuiești, cine sunt părinții
tăi sau ce lucruri ai acasă.

Nu organiza întâlniri cu persoane
pe care le-ai întâlnit pe rețelele de
socializare! Reține că oamenii de pe
rețelele sociale nu sunt întotdeauna
cine par a fi! Protejează-te, astfel
încât nimeni să nu-ți poată face rău!
Nu accepta să te întâlnești cu
persoane străine în zone îndepărtate,
unde nu există nimeni care să te
poată ajuta, în caz de necesitate.

Activitățile tale pe
Internet nu sunt
anonime! Dacă este
necesar, acestea pot fi
urmărite de profesori,
părinți și organele de
drept.

Nu publica pe rețelele
de socializare
documente găsite!
Documentul găsit
trebuie dus la poliție,
care va identifica
proprietarul
documentului și îl
va returna.

Nu cumpăra nimic
online fără a informa
părinții! Nu înregistra
online datele de pe
cardul tău de credit sau
al părinților, fără a te
consulta mai întâi cu
părinții. Reține - utilizând
datele cardului de credit,
toți banii disponibili
pe acest card pot fi
furați.

Spamul nu este o scrisoare! Ignoră spamul primit
de la străini. Nu răspunde. De cele mai multe ori,
acestea sunt încercări de a storce bani.

Gândește-te înainte de a publica
fotografiile online! Gândește-te
dacă aceste fotografii nu te
afectează și nu-ți fac rău ție,
prietenilor, colegilor, părinților
sau altor persoane din fotografie.
Nu uita că ceea ce „postezi” pe
internet nu mai poate fi șters
sau uitat. Internetul
ține minte totul!

Nu scrie comentarii
jignitoare! Oamenii care îi
jignesc pe alții se simt
nefericiți. Nimeni nu devine
mai fericit, ofensând pe alții.
Nu răni pe nimeni!

AI grijă de sănătatea
computerului! Nu instalează
programe de origine
necunoscută pe computerul
pe care îl utilizezi. Un
program poate foarte ușor
„să se prefacă” a fi un joc,
dar de fapt poate fi un virus
cărui îi deschizi calea
către calculatorul tău.
Dacă:
- primești online scrisori
neplăcute și jignitoare,
- ai întâlnit materiale
neplăcute pe Internet,
- ai observat activități
suspecte pe Internet,
- te îngrijorează siguranța
ta pe Internet, vorbește
despre aceasta cu părinții
sau cu altcineva în care
ai încredere!



Acest material a fost pregătit în cadrul
Proiectului UE Twinning "Consolidarea
Capacităților Centrului Național pentru
Protecția Datelor cu Caracter Personal
al Republicii Moldova" finanțat de
Uniunea Europeană

Informația prezentată se bazează pe cerințele
Regulamentului 2016/679 privind protecția
persoanelor fizice în ceea ce privește prelucrarea
datelor cu caracter personal și privind libera
circulație a acestor date (Regulamentul general
privind protecția datelor)

022 820 804

Contactează-ne la Linia specializată a Centrului Național
pentru Protecția Datelor cu Caracter Personal (CNPDCP)



NATIONAL CENTER FOR PERSONAL DATA PROTECTION
OF THE REPUBLIC OF MOLDOVA

ACTIVITY REPORT FOR THE YEAR 2020

CONTENTS

INTRODUCTION 69

GENERAL PRESENTATION 70

CHAPTER I

EXAMINATION OF REQUESTS
ADDRESSED TO THE CENTER 71

CHAPTER II

ACTIVITY OF CONTROL 75

CHAPTER III

RECOMMENDATIONS AND CASE
STUDIES OF 2020 78

CHAPTER IV

ACTIVITY OF REPRESENTATION
IN THE COURTS 91



CHAPTER V

**ACTIVITY OF SURVEILLANCE
OF PERSONAL DATA PROCESSINGS 96**

CHAPTER VI

**APPROVAL AND ELABORATION
OF DRAFT NORMATIVE ACTS.....102**

CHAPTER VII

INTERNATIONAL COOPERATION.....105

CHAPTER VIII

**TRAINING AND AWARENESS
ACTIVITIES110**

CHAPTER IX

HUMAN RESOURCES MANAGEMENT.....113

CHAPTER X

ECONOMIC-FINANCIAL ACTIVITY119

PROBLEMS AND OBJECTIVES122



INTRODUCTION

In order to inform the society about the evolution of the field of personal data protection, the National Center for Personal Data Protection of the Republic of Moldova (Center) presents the Activity Report for 2020.

The year 2020 was a specific one especially for the field of personal data protection, during this period the data protection required an increased attention from the whole society as a result of the global pandemic COVID -19.

The pandemic has required the application of rapid and efficient measures in various areas of activity, determining to increased use of digital technologies. The use of the latest information technologies for remote communication, work or distance learning has become the new “normal” in the daily life of the society. However, this leap in the digitization of our lives requires increased personal data protection.

Even if the pandemic had an impact on the Centre’s activity, making it impossible to carry out or postpone planned activities, as well as insignificantly reducing the number of activities performed, reflected in this report, the reference period is marked by multiple achievements, being focused on continuous implementation of legislation in the field of personal data protection, the optimal exercise of the legal attributions of supervision and control of the conformity of personal data processing, examination and settlement of complaints and notifications received and ex officio verifications of aspects related to personal data processing, in the purpose of ensuring the observance of the principles of protection of these data by the controllers in the public and private sectors, the elaboration and endorsement of the draft normative acts with incidence in this field, the strengthening of internal and external cooperation in the field of personal data protection.

Similarly, the report reflects the priority issues and concerns, the situation in the field of personal data protection, offers recommendations and opinions of the Center, as well as exemplifies a series of violations found by the Center in its work and to ensure the confidentiality of personal data known within the exercise of control attributions, in accordance with the provisions of art. 29 and art. 31 of the Law on personal data protection, they are depersonalized in order not to allow interference in private life, such as the impossibility of associating them with an identified or identifiable person.

Respectfully,

Eduard RĂDUCAN
Director of the National Center
for Personal Data Protection



GENERAL PRESENTATION

Year 2020 in numbers

REQUESTS / COMPLAINTS

11191 correspondence documents:
 5115 inbox
 4564 outbox
 679 internal
 833 complaints



ACTIVITY OF CONTROL

303 initiated controls
 170 contravention cases
 125 drawn up minutes
 43 suspension /cessation/
 destruction decisions



SURVEILLANCE ACTIVITY

1472 examined notifications
 504 registered controllers
 710 registered personal
 data filing systems
 762 refused decisions



ACTIVITY OF REPRESENTATION IN THE COURTS

777 court proceedings:
 470 in contravention proceeding
 307 in administrative litigation



INFORMATION AND AWARENESS-RAISING ACTIVITY

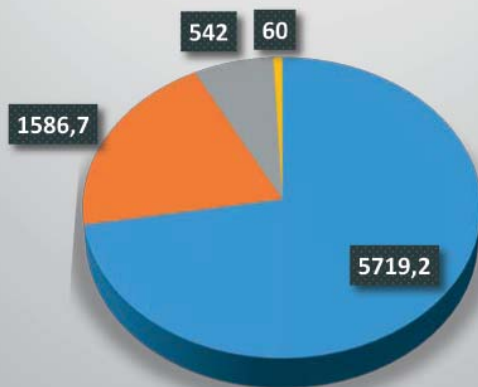
2030 consultations for controllers
 14712 views on Facebook/ NCPDP account
 49034 views on NCPDP web page
 80 press releases/articles on the web page

HUMAN RESOURCES

35 out of 45 staff-limit
 8 competitions held
 9 persons employed / 7 debutants
 6 persons resigned
 21 training courses



BUDGET ALLOCATIONS 2020 (thousand, MDL)



■ Staff expenditures ■ Goods and services
 ■ Non-financial assets ■ Social benefits



CHAPTER I

EXAMINATION OF REQUESTS
ADDRESSED TO THE CENTER

During 2020, the Center examined **11191** correspondence documents. This figure shows a steady increase over the years in the number of correspondence documents submitted to the authority for examination.

Thus, even if the year 2020 was marked by the pandemic COVID-19, which also had an impact on the activity of the Center, this year there is a consistent trend both in the part concerning the rights of personal data subjects by submitting complaints about alleged non-compliance with data processing, as well as personal data controllers in order to comply with the obligations prescribed by the Law on personal data protection and to know the relevant regulations in order to ensure the conformity with personal data processing.

Comparative statistics of the Center's correspondence documents, for the years 2014-2020

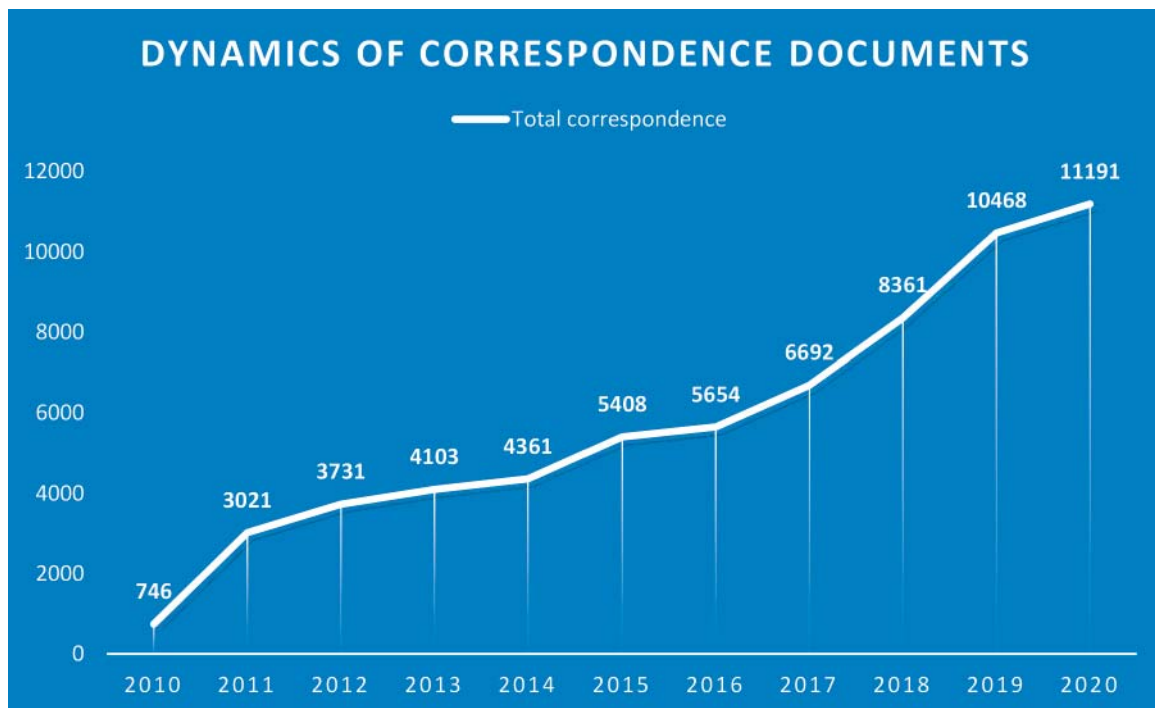
Year	Total correspondence	Inbox documents	Outbox documents	Complaints	Internal documents
2014	4361	1738	1836	302	485
2015	5408	2425	2098	420	465
2016	5654	2811	2055	410	374
2017	6692	3605	2455	554	316
2018	8361	4180	3113	637	431
2019	10468	4982	4217	743	526
2020	11191	5115	4564	833	679

The significant increase, from year to year, in the number of correspondence documents examined by the Center, demonstrates the increased degree of importance of the field of personal data protection in the society. Furthermore, this fact undoubtedly determines the steady and substantial increase of the Center employees' workload.

**Information in dynamics on the correspondence of the Center, for the years 2014-2020**

Reference period	Total correspondence	Dynamics
2014-2015	4361-5408	↑24%
2015-2016	5408-5654	↑5%
2016-2017	5654-6692	↑18%
2017-2018	6692- 8361	↑25%
2018-2019	8361-10468	↑25%
2019-2020	10468-11191	↑7%
Dynamics between the years 2014-2020	4361-11191	↑157%

More representative information on the ever-increasing dynamics of the number of correspondence documents, over a longer period, covering practically the entire period of effective activity of the National Authority for Personal Data Protection, is further reflected:

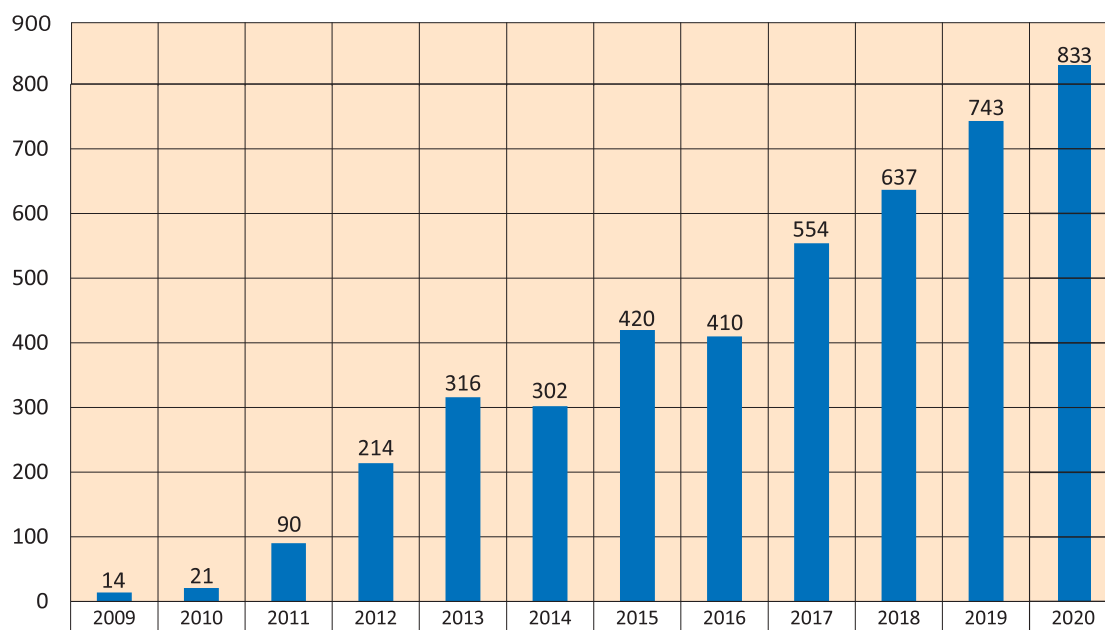
**Activity of examination of personal data subject's complaints**

During the reference period, the Center examined **833** complaints received from natural persons – personal data subjects. Compared to the previous reporting year (743 complaints registered in 2019), the number of complaints increased by 12%.

From the total number of complaints registered in 2020, **303** cases were examined in a complex way, regarding the control over the lawfulness of the processing of personal data.



Dynamics of the number of complaints 2009-2020

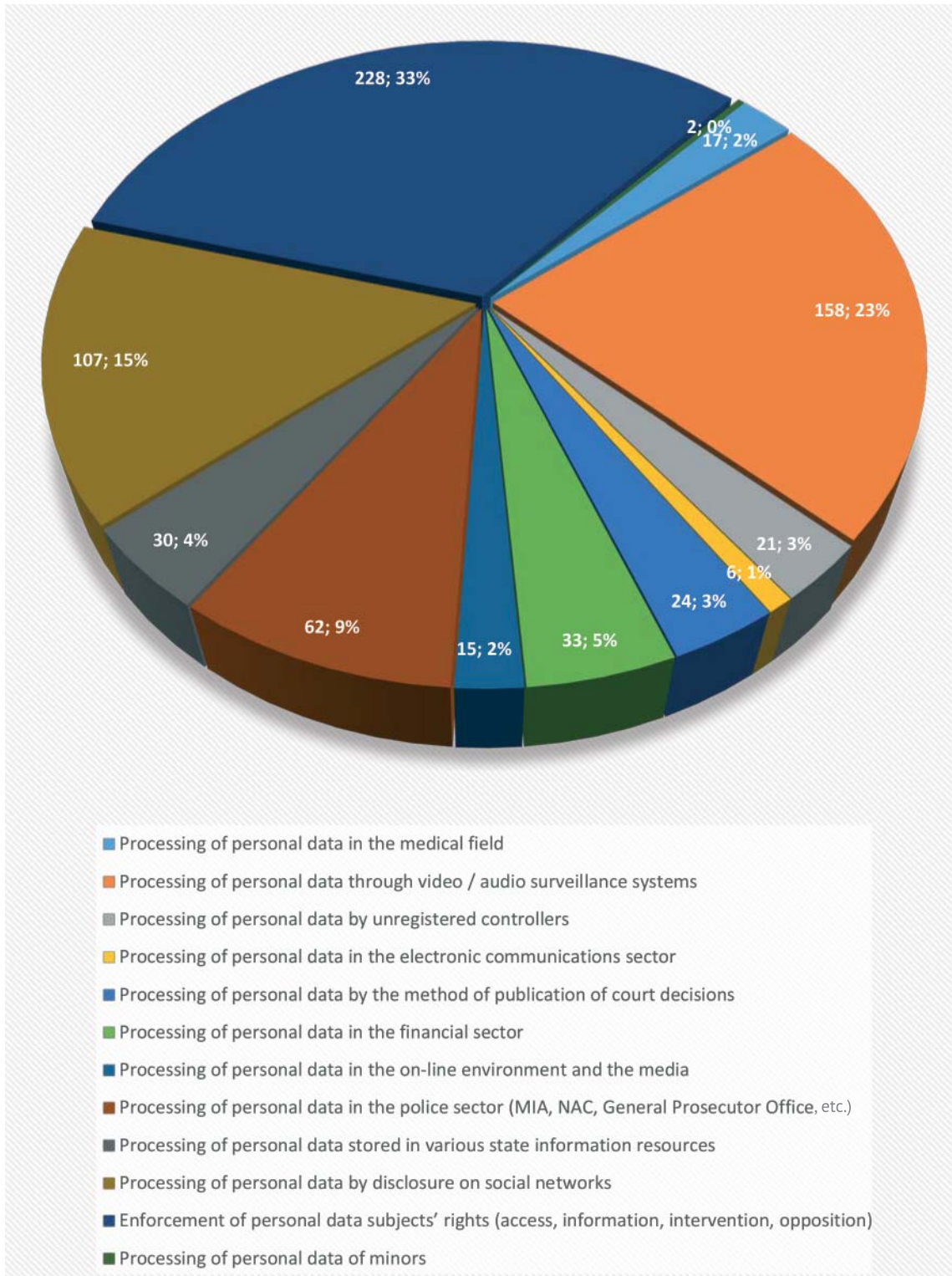


From the specifics of the complaints addressed, the Center emphasized the following guidelines of the mentioned topics:

- ✓ Processing of personal data through video / audio surveillance systems: **158** cases;
- ✓ Processing of personal data without notification and / or authorization of the control body in the field personal data processing, as well as processing of personal data by an unregistered controller: **21** cases;
- ✓ Processing of personal data in the electronic communications sector: **6** cases;
- ✓ Processing of personal data of minors: **2** cases;
- ✓ Publication of court decisions without their depersonalization: **24** cases;
- ✓ Processing of personal data in the financial sector, insurance companies: **33** cases;
- ✓ Processing of personal data in the on-line environment and the media: **15** cases;
- ✓ Processing of personal data stored in various state information resources: **30** cases;
- ✓ Processing of personal data by disclosure on social networks: **107** cases;
- ✓ Processing of personal data in the absence of the consent of the personal data subject, as well as in the absence of any other legal basis: **130** cases;
- ✓ Enforcement of personal data subjects' rights (access, information, intervention, opposition): **228** cases;
- ✓ Processing of personal data in the medical field: **17** cases;
- ✓ Processing of personal data in the police sector (MIA, NAC, General Prosecutor Office, etc.): **62** cases.



General situation regarding complaints examined in 2020





CHAPTER II

ACTIVITY OF CONTROL

Comparative information on the control activity, for the years 2018-020

Period for comparison	Number of controls initiated based on: complaints / notification, requests for cross-border transfer	Acts issued as a reaction to controls			
		Decisions on suspension of personal data processing	Decisions on cessation of personal data processing	Decisions on destruction / erasure of data processed in the breach of law	Cases of contraventions found / minutes issued
Year 2018	326	16	4	27	191/92
Year 2019	376	26	8	24	186/105
Year 2020	303	20	6	17	170/125

The conformity control of personal data processing with the requirements of the Law on personal data protection is performed exclusively by the National Center for Personal Data Protection and may be initiated: on the basis of the complaint of the data subject; complaints / self-notification; request of cross-border transmission of personal data.

During the reference period, **303** control materials were initiated and examined, of which:

- **275** based on the complaints of personal data subject, complaints /self-notification,
- **28** based on the cross – border transmission of personal data authorization requests.

The comparative analysis in relation to the previous year reveals that during 2020 it was noticed an insignificant decrease in the number of controls initiated on the basis of the complaints submitted by personal data subjects. In the opinion of the Center, the important factor that caused the revealed difference is the pandemic situation generated by COVID-19 virus, or, during the reference period, a state of emergency was declared in the Republic of Moldova, periodically ceasing the activity of all institutions, including the activity of the Center, and the population being in isolation.

In addition, it is noted that, especially taking into account the amendments of the Law no. 124 of July 9, 2020 (in force since August 24, 2020) on the provisions of art. 27 of the Law on personal data protection, the verification of the conformity of personal data processing operations based on the data subjects' complaints is initiated / started only following the prior realization, by the data subjects of their rights stipulated in art. 12-14, 16-17 of the Law on personal data protection, directly to personal data controllers, an aspect that also influenced the number of controls initiated in 2020.

It should be mentioned that the amendments made in 2020 on the provisions of art. 27 of the Law 133/2011 have an important role for the activity related to the control of the legality of



personal data processing. However, the changes brought essential conceptual and procedural improvements, on the one hand providing clarity to the actions needed to be taken by data subjects submitting complaints to the Center as well as by data controllers, and on the other hand by establishing expressly organizational aspects such as: procedures, deadlines, criteria and even competencies, which have come to streamline and optimize the institutional capacities related to the control of the legality of personal data processing.

It is relevant to mention, the tendency of increasing the complexity of the issues addressed in the complaints and the number of parties involved in the case, thus generating a variety of control actions to be taken in order to verify the lawfulness of personal data processing, which become more voluminous and complicated.

In 2020, considering the pandemic situation in the country, controls on the lawfulness of the processing of personal data were carried out, in most cases ex officio being applied the written procedure for obtaining the necessary information to examine the non-compliance invoked and the settlement of the cases notified.

As a result of the control materials examined by the Center and finalized with the finding of a violation of the legal provisions in the field of personal data protection, depending on the consequences resulting from the admitted violations and the seriousness of the violations found, the constraint measures were ordered manifested by:

- Suspension of personal data processing – 20 cases,
- Destruction / erasure of personal data processed regarding the infringement of legal provisions – 17 cases,
- Cessation of personal data processing – 6 cases.

At the same time, according to the control activity carried out as an ascertaining body, according to the facts stated in Articles 74¹ – 74³ of the Contravention Code, during the year 2020, **125** minutes on offense were drawn, **170** contravention facts being established and sent for examination in the Court, according to the provisions of the Contravention Code.

The spectrum of contravention facts found indicates the frequent nature of violations committed in the processing of personal data, as follows:

- art. 74¹ para. (1): failure to comply with the requirements for ensuring the security of personal data when processing them within the personal data filing systems – 20 cases;
- art. 74¹ para. (2): processing of personal data without notification and / or authorization of the control body in the field personal data processing, as well as processing of personal data by an unregistered controller – 48 cases;
- art. 74¹ para. (3): violation of the personal data subjects' rights, the right to be informed – 9 cases;
- art. 74¹ para. (4): infringement of personal data processing, storage and usage rules – 69 cases;
- art. 74¹ para. (5): cross-border transfer of personal data with violation of personal data protection legislation -1 case;
- art. 74² para. (1): refusal to provide the information or documents requested by the National Center for Personal Data Protection in the process of exercising control powers, presentation of inauthentic or incomplete information, as well as failure to submit the required information and documents within the deadline established by law – 22 cases;
- art. 74³: failure to comply, within the deadline, with the decision of the Center on the restoration



of the personal data subject's rights, including on the suspension or cessation of personal data processing, on blocking, partial or complete destruction of personal data processed in breach of the legislation on personal data protection – 1 case.

Activity related to the authorization of cross-border transmission of personal data

Regarding the activity related to the authorization of personal data cross-border transfer, in the light of the provisions of Art. 32 of the Law on personal data protection, it is important to reiterate that the cross-border transfer of personal data which are object to processing or to be processed after transmission can only take place with the authorization of the Center, in the manner established by law and only in the case in which the state of destination ensures an adequate level of protection of data subjects' rights and data intended for transfer.

In 2020, the Center authorized the cross-border transfer of personal data only in cases of suitably documented requests made by the actors involved, focusing on respecting the principles of personal data protection and the rights of data subjects concerned, as well as on the proof of ensuring the optimal level of protection of the data transmitted and / or collected for the purpose of further processing outside the Republic of Moldova.

At the same time, in the context of the activity revealed above, it should be mentioned that the demarches and notifications examined by the Center were related to public and private entities from countries such as: Germany, Romania, Latvia, Ukraine, Holland, Italy, Ireland, Finland, Russia Federation etc.

Therefore, in 2020 the Center received **70** requests concerning the cross-border transfer of personal data, of which **28** – based on requests and **42** through notifications submitted at the Center's "One-Stop-Shop". Thus, from 28 demarches submitted to the Center, in 14 cases, the cross-border transfer of personal data was authorized and in other 14 cases, the requests were resolved by issuing refusal decision in authorizing the cross-border transfer. Regarding the number of notifications submitted by data controllers at the Center's "One-Stop-Shop" on the intension of personal data cross-border transfer, 13 cases were authorized and 29 were refused.

As in the previous reporting period, the refusal to authorize the cross-border transfer of personal data was determined by: the non-compliance with the basic conditions of the requests submitted for examination and / or lack of authenticated copies of the documents confirming the circumstances and legal instruments on which the request for legal assistance is based. In this context, in the part regarding the non-compliance with the basic conditions of the demarches / requests, aspects such as: lack of consent of the data subject concerned; invalid consent for certain operations indicated in the request; the lack of a determined, legitimate and non-excessive purpose; the unjustified large number of targeted subjects or the excessive volume of data that the controller intended to process and transmit in the context of cross-border transfers of personal data outside the border of the Republic of Moldova; failure to present the documents necessary to establish the legality of the cross-border transfer of personal data or presentation of unauthenticated documents, are highlighted.

Regarding the cases of refusal to authorize the cross-border transfer of personal data based on a notification submitted to the Center's "One-Stop-Shop", in the majority of cases it was noted: the description of the operations of personal data processing was not described; the data protection measures were not indicated within the filing systems; lack of controller's instructions designed to processor to act on its behalf, etc.

III
CHAPTER III**RECOMMENDATIONS AND CASE STUDIES OF 2020**

The Center, periodically informs the society about priority issues and concerns in the field of personal data protection, in particular about the situation in the field of the protection of personal data subjects rights.

At the same time, in order to ensure the prevention of violations similar to those already found, committed to personal data processing, annually, including through activity reports, the Personal Data Protection Authority presents cases / issues related to the field of reference.

Recommendations and opinions issued by the Center in 2020:

Thus, during 2020, the Center issued recommendations and opinions regarding some situations of general applicability or major interest for the society, with the aim of providing clarity in the compliant and unequivocal applicability of the legal provisions in the field of personal data protection when processing these data. Among the opinions / recommendations offered by the Center during 2020 were the following:

Personal data processing in the context of the COVID – 19 pandemic in the Republic of Moldova

The Center emphasized the risks and challenges of the protection of individuals with regard to personal data processing in the context of the fight against Coronavirus (COVID-19), in particular patient's health data.

The fight against COVID-19 is a valuable goal shared by all nations, including the Republic of Moldova, and must therefore be supported in the best possible way to reduce and eliminate the spread of this virus. Since the launch of COVID-19, various health data processing operations have been witnessed on a daily basis in the context of combating COVID-19. All such processing of personal health data must be an integral part of concentrated efforts to maintain public health, and data protection can in no way be and is in no way an obstacle to safeguarding lives, respectively, the principles applicable by national legislation in the field of personal data protection always allow a balance of the interests at stake.

As not every operation of health data processing can be justified by the state need to maintain public health, it becomes urgent to maintain and implement a mechanism based on the concept of balance between public health / public security and the right to personal data protection.

It should be taken into account that health data is a special category of data, recognized as such, in all existing state jurisdictions that have a strong legal framework for personal data protection and which acceded to Convention 108 of 28.01.1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, not only in the Republic of Moldova. The special nature of health data leads to a much more rigorous conduct in their processing, but also security rules to ensure the confidentiality of data from health authorities, other state authorities, legal entities under private law, individuals and so on (controller, processor, third party). However, namely this operation of processing personal data can generate extremely negative effects in relation to the rights of the data subject concerned.



Obviously, the principles of personal data protection remain in force even during the fight against the COVID-19 pandemic for all actors involved in this fight. According to art. 4 of Law 133/2011 on personal data protection, in order to achieve the objectives pursued, personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, be accurate and, if necessary, updated or stored in a form that allows identification of personal data subjects for no longer than is necessary for the purposes for which the data were collected and further processed. In the same context, the processing of health data by the controller, the processor or a third party who need to substantially process personal data may fall within the legal basis regulated in art. 5 para. (5) let. b), c), d), e) and art. 7 para. (1) let. a) and b) of Law 133/2011 on personal data protection – processing is necessary for protection of public health or processing is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment to the personal data subject, or the management of health-care services, acting in the interest of the personal data subject.

Furthermore, the personal data subjects should receive transparent information on the activities of their personal data processing and the categories of such data, including the retention period of the data collected, the purposes of the processing, etc. The information provided should be easily accessible and provided in clear and simple language. In this order, the rights of personal data subject are regulated by Law 133/2011 on personal data protection, which also remain in force and they are to be respected by all controllers and processors, we are talking about: the right to information of personal data subject – art. 12; the right of access to personal data – art. 13; the right of intervention upon personal data – art. 14; the right of the personal data subject to object – art. 16.

In the case of the establishment of exceptions and restrictions in connection with the existence of circumstances established in para. (1) art. 15 of Law 133/2011 on personal data protection that justifies the restriction of the personal data subjects rights, after the termination of the situation that justified the application of exceptions and restrictions regulated by para. (1) and (2) of art. 15, the controllers will take the necessary measures to ensure the compliance of the personal data subjects rights provided in art. 12–14.

In accordance with art. 11 of Convention 108 of 28.01.1981 on the Protection of Individuals with regard to Automatic Processing of Personal Data, any exceptions and restrictions on the size of the processing of personal data must be governed by law, to respect the fundamental human rights and freedoms and is a necessary measure in a democratic society.

Relevant is the Joint Statement by Chair of the Committee of Convention 108 and Data Protection Commissioner of the Council of Europe on the right to data protection in the context of the COVID-19 pandemic, adopted on 30.03.2020, Strasbourg, noting that the communication to the public by health and government authorities should remain a priority to be in a capacity to protect, inform and advise the public. Nonetheless, during such communications, the publication of sensitive data (such as the health related data) of specific individuals should be avoided and it is recommended that the processing of such data is only done, if additional technical and organizational measures [...].

It should be mentioned the Statement of the European Data Protection Board (EDPB) on the processing of personal data in the context of the COVID-19 outbreak (the content of which can be viewed by accessing the link:

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf).



Particular attention should be paid to the principles of personal data protection and by the media institutions that inform the population about the coronavirus pandemic. Their effort should be aimed at maintaining the confidentiality of COVID-19 victims and not allowing their identity to be disclosed.

During the professional activity from home, as a measure to combat COVID-19, secure e-mail addresses will be used for the transmission of information containing personal data, encryption methods and technical measures of communication intended strictly for the performance of professional duties, in order to avoid triggering security breaches.

The processing of personal data on the location of data subjects for the purpose of monitoring whether they comply with the isolation regime, may be included in the legal basis of public health protection. However, this operation of processing personal data, which is extremely intrusive, must be implemented with particular caution, proportionality and the absolute implementation of all security measures, as such an operation entails serious implications for the fundamental rights and freedoms of the personal data subjects. The development of these surveillance solutions or other electronic applications (information systems) designed to combat the COVID-19 pandemic must be based on a prior impact assessment of data processing on the fundamental rights and freedoms of personal data subjects and must design data processing to prevent or minimize the risk of negative interference with fundamental rights and freedoms. For information purposes, the operation of processing personal data by the method of monitoring the location of individuals (data subjects), in order to determine compliance with the isolation regime, it is to be ceased immediately, once the purposes for which the personal data of the data subject are collected and processed have been achieved.

Aspects regarding the recording and live streaming of local council meetings

During the year 2020, the Center received multiple addresses requesting the opinion of the authority regarding the recording and live streaming of local council meetings via the Internet. In this regard, the Center came up with the following benchmarks:

Analyzing the approached topic, it should be noted that by publishing via Internet the meetings of local councils, will be provided access to certain information that is discussed during the meetings, not only for stakeholders in the locality, but for an unlimited number of people.

We draw attention to the fact that the issue discussed during the meetings does not refer only to activities regarding the administrative organization of the locality, but also individual cases / cases involving specific individuals, which may reveal certain aspects of privacy, such as material situation or special categories of data, for example health data.

In this respect, we would like to inform about the following notions and provisions of Law no. 133 of July 8, 2011 on personal data protection namely:

controller – a natural or legal person governed by public law, or by private law, including public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data expressly provided by applicable law;

processing of personal data – any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, keeping, restoring, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;



personal data filing system – any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

personal data – any information relating to an identified or identifiable natural person (personal data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

According to the provisions of art. 4 of the Law on personal data protection, the personal data that are subject to processing must be: processed correctly and in accordance with the provisions of the law; collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; appropriate, relevant and not excessive in relation to the purposes for which they are collected and /or further processed.

In accordance with art. 5 para. (1) of the Law on personal data protection, the operations of personal data processing are carried out with the consent of the personal data subject. At the same time, the consent of the personal data subject is not required in the cases provided exhaustively by art. 5 para. (5) of the same legislative act, for example, for carrying out an obligation of the controller according to the law or the performance of tasks carried out in the public interest or in the exercise of public authority prerogatives vested in the controller or in a third party to whom the personal data are disclosed.

Finally, it should be mentioned that individual decisions could contain special categories of personal data that reveal the social affiliation of individuals, health data, etc. The processing of these categories of data is to be carried out in strict accordance with the provisions of art. 6-8 of Law no. 133/2011, based on the requirement to ensure the increased level of protection due to the presence of special risks for the right to inviolability of intimate, family and private life.

Next, we note the provisions of art. 17 para. (1) of Law no. 436-XVI of December 28, 2006 on local public authority, according to which the meetings of the local council are public. Para. (2) of the same article, mentions that any interested person may attend the meetings of the local council.

In addition, para. (3) of the same normative act, stipulates that citizens, associations established in accordance with the law and other interested parties have the right: a) to participate, in accordance with the law, in any stage of the decision-making process; b) to have access to the information regarding the locality budget and the way of using the budgetary resources, to the draft decisions and to the agenda of the meetings of the local council and of the city hall; c) to propose the initiation of the elaboration and adoption of some decisions; d) to present to the local public authorities recommendations, in their own name or on behalf of groups of inhabitants of the respective communities, regarding various draft decisions to be debated.

In this regard, we note that the mentioned normative act does not establish the right of citizens, associations and other stakeholders to record and upload local council meetings in the online space, but offers the opportunity for interested parties to participate in the decision-making process.

At the same time, according to par. (1), art. 3 of the Law about the status of the local elected person no. 768-XIV of February 2, 2000, in the corresponding administrative and territorial unit the local elected person is official – the representative of authorized or executive body of local public authority.

We emphasize that, in the context of art. 11 of the Law on freedom of expression, information on the private and family life of the public person or the person exercising a public function, can be disclosed only if it has a public interest (interest of society and not the simple curiosity of individuals about events relating to the exercise of public power in a democratic state or to other matters which, normally, do not arouse the interest of society or any part of it).



Even according to the ECHR's reasoning, public persons must accept certain interferences in their private lives more than ordinary persons must, and the accessible degree of research is to be all the greater the more important the public person in question and the information that is revealed. The element that arouses the public interest can be the status of the person (the mandate of the local elected person) or any other circumstances related to the exercise of the mandate of the local elected person.

Thus, certain information, including personal data concerning a local elected person could become information of public interest in the measure that it does not affect the capacity to exercise the public function of the given person, taking into account the existence of the right to respect for his private and family life.

Based on the above reasoning, taking into account the tasks of public interest or resulting from the exercise of public authority with which the controller is invested (Local Council, City Hall), the latter should analyze in the light of the above rules and clearly regulate, by a normative act, what topics are to be placed publicly, what categories of personal data will be disclosed in this regard, how to inform the personal data subjects about the placement of meetings on the Internet, offering the possibility to exercise the right to opposition, ensuring the measures of security and confidentiality of personal data, establishing a concrete deadline for which the information will be made public, the mechanism for deleting these records, etc. Respectively, it must clearly establish which meetings are to be recorded and subsequently placed in the public space, who are the persons designated / authorized to record the meetings and broadcast them in the public space, under the legal conditions.

At the same time, considering that the data controller (Local Council / City Hall) establishes the purpose and means of personal data processing and it is responsible for any processing of personal data carried out, only he has the right to decide on the possibility of providing personal data for public access.

Specifications regarding the recording and live streaming of local council meetings

In the context of the reaction of civil society, as well as some local public authorities, who have wrongfully interpreted the previous opinion on recording and live streaming of local council meetings via the Internet, the Center emphasizes that it does not intend to restrict the recording and live streaming through the internet of local council meetings, while certain reasoning previously set out on the given topic was taken out of context and misinterpreted.

In these circumstances, it is necessary to highlight the following:

– Transparency and access to information is one of the essential components of any democratic system. In order for citizens to be able to get involved in public affairs, to participate in decision-making processes, to monitor the way in which the authorities respect their responsibilities and the elected person's promises, they must have access to truthful information about done actions, and the authorities to ensure transparency in the decision-making process.

– In the same context it should be noted that according to para. (1) art. 3 of the Law about the status of the local elected person no. 768-XIV of February 2, 2000, in the corresponding administrative and territorial unit the local elected person is official – the representative of authorized or executive body of local public authority. Public persons must accept certain interferences in their private lives more than ordinary persons must. Thus, certain information, including personal data concerning a local elected person could become information of public interest in the measure that it does not affect the capacity to exercise the public function of the given person, taking into account the existence of the right to respect for his private and family life.



– In accordance with art. 17 para. (1) of the Law no. 436-XVI of December 28, 2006 on local public authority, the meetings of the local council are public. Para. (2) of the same article, mentions that any interested person may attend the meetings of the local council. However, we note that the mentioned normative act does not establish their right / obligation to record and place the meetings of the local councils in the online space. Even if the provisions of art. 17 para. (3) of the mentioned law prescribe the obligation to ensure the transparency of the meetings of the local council, this is to be done, inclusive in accordance with the provisions of the legislation on personal data protection, which requires compliance with certain requirements / principles in this regard.

– We emphasize that the openness of certain personal data must be provided by the normative acts that regulate certain legal relations. We specify that even according to the provisions of point 30 of Regulations on procedure for maintaining the State register of local acts, approved by Government Decision no. 672 of August 28, 2017, the individual decisions issued / adopted by the local public administration authorities can be viewed publicly only in depersonalized form. The same approach needs to be taken to ensure the transparency of local council meetings, following the recording and live streaming via internet of the topics discussed, especially in the part aimed at making individual decisions.

– Finally it should be noted that often, taking into account tasks of public interest or resulting from the exercise of the prerogatives of public authority with which the local councils are invested, at meetings are discussed not only issues related to the local community or the administrative activity of the authority, but also aspects related to the private life of some concrete persons, which could reveal, for example, information / data about the social affiliation of persons (families, children, elderly people in difficulty), health data etc.

In these circumstances, as well as in order to ensure a balance between the right to freedom of expression and the right of access to information, on the one hand, and the right to personal data protection, on the other hand, the Center intervened with certain recommendations regarding the recording and live streaming of local council meetings via the Internet.

Respectively, it was recommended that local councils come up with clear regulations, through normative acts, what topics are to be placed publicly, what categories of personal data will be disclosed in this regard, how to inform people about the placement on the Internet of meetings, offering the possibility to exercise the rights as personal data subjects, ensuring security and confidentiality measures of personal data, establishing a concrete deadline for which the information will be made public, the mechanism for deleting these records, etc. The normative act must clearly establish which meetings / part of the meetings are to be recorded and placed in the public space, who are the persons designated / authorized for the recording of the meetings and their dissemination in the public space, under the legal conditions.

Some aspects regarding the specific cases of 2020

Non – compliant disclosure of health personal data

Based on the complaint of a data subject, the Center initiated the examination of the legality of personal data processing, carried out by collecting and disclosing information regarding the health data of the complainant, by the director of the company in which the complainant worked and the director of a medical institution.

In fact, it was invoked that the complainant's employer requested from the medical institution information from medical certificates, such as the administered stationary treatment and the treatment period, without his consent.



Analyzing the content of the company's interpellation, sent to the medical institution, the Center established that the company in question requested information on medical leave provided to complainant in the period 2015-2020 by the neuropathologist, as well as the diagnosis under which these medical leave was provided.

According to the presented materials, it was noted that the employer requested the information regarding the health data of the complainant in order to be presented in the court.

Subsequently, the IMSP sent at the requester's address a reply in which it disclosed information on the treatment period and the nature of the disease of the complainant, in accordance with the sick leaves issued, namely:

1. „29.01.2016 – 07.02.2016, **gynecological outpatient treatment. Doctor ...**”;
2. „01.07.2019 – 11.07.2019, **gynecological outpatient treatment. Doctor ...**”;
3. „27.01.2020 – 07.02.2020, **gynecological outpatient treatment. Doctor ...**”;

The notion of private life integrates both “traditional” aspects, such as the right to image, the marital status of the person, identity, health, religious affiliation, physical and moral integrity, sentimental life, but also “modern” aspects related to new perceptions in social life regarding abortion, homosexuality, transsexuality, etc.

In this context, the information on the patient's health, the results of investigations, diagnosis, prognosis, treatment, written in the medical documentation of the patient, represent special categories of personal data, presenting a high level risks for the right to intimate, family and private life and it will be necessary to ensure the confidentiality of these data, in compliance with the Law on personal data protection.

Corresponding to the case, were highlighted the provisions of the Law No 263/2005 on the rights and responsibilities of the patient, which contains special legal rules aimed at strengthening fundamental human rights in the health care system, ensuring respect for the dignity and integrity of the patient and, based on sensitive health data, establishes strict conditions for their disclosure. It should be noted that patient health data, by their nature, might present a risk for data subjects when processed and therefore require increased protection. These data are subject to a prohibition principle and there must be a limited number of circumstances in which such processing is lawful. At the same time, the confidentiality of medical data is a professional secret, which is a form of the right to respect for privacy. Prohibition of the disclosure of medical information, classified as confidential, is necessary to guarantee that medical institutions ensure the patient's right to privacy.

Thus, including art. 12 of the Law on Patient Rights and Responsibilities, emphasizes the obligation of the medical worker to protect health data. Consequently, the confidentiality of information on the request for medical assistance, examination and treatment, including other information which constitutes medical secrecy, is ensured by the attending physician and the specialists involved in the providing of health services or in biomedical research (clinical study), **and by other persons to whom this information has become known due to the exercise of professional and service obligations** (paragraph (2));

At the same time, the information that is considered confidential **can be provided only if the patient explicitly consents** or at the request of his legal representative (close relative), under the conditions agreed by the patient, to the extent appropriate to his ability to understand, if a measure of legal protection has been instituted in respect of the patient or if the law expressly requires it (paragraph (3)). In special situations, **the presentation of confidential information** without the consent of the patient or his legal representative (close relative) **is allowed: c) at the reasoned request** of the criminal investigation body, **the court** in connection with the criminal investigation or judicial process, in accordance with the legislation (paragraph (4)).



Therefore, the Center noted that the disclosure of information on the treatment period and the nature of the diseases in the case examined took place contrary to the above-mentioned legal provisions and the principles of personal data processing provided in art. 4 para. (1) let. a) and b) of the Law on personal data protection.

Violation of the rights of personal data subjects

Art. 12-14, 16-17 of the Law no. 133 of July 8, 2011 on personal data protection establishes personal and inviolable rights (right to information, right of access, right of intervention, opposition), which the personal data subject may perform them in relation to the data controller who has carried out the processing of his personal data.

Continuing the above recital, it is shown that during 2020, the Center registered and examined complaints from data subjects, who reported about the non-compliance by data controllers of their rights, in particular the right of access to personal data processed by controllers, noting that some data controllers do not respond to data subjects' requests, do not respond within the deadline provided by law, and do not ensure the effective exercise of their rights in the field of personal data protection.

At the beginning of 2020, the Center received a complaint from a personal data subject, requesting the examination of the alleged violation of the right of access to personal data concerning him, by a lending company.

In this context, the data subject invoked the fact that he submitted a request to the lending company, indicating the personal data concerning him, but was not informed by the company's representatives about the result of the examination of his request.

In this regard, the personal data subject submitted another request to the lending company requesting information on the processing of his personal data, context in which, even until the date of submission of the complaint to the Center, the lending company did not offer him any answer.

Thus, following the examination of the mentioned complaint, the Center found the violation of the provisions of art. 13 para. (1) of the Law on personal data protection by the lending company, in the part related to the non-compliance with the right of access to the processing of personal data concerning the data subject.

As a result, to the lending company was drawn up minutes on the contravention based on art. 74¹ para. (3) of the Contravention Code.

Processing by disclosure / publication of state's identification number (IDNP) of personal data subjects

The Center received complaints from some personal data subjects, who requested the verification of the legality of their personal data processing, by a bailiff, manifested by the publication in the Official Gazette of the Republic of Moldova of an announcement on the tender, in which the IDNPs of the personal data subjects are indicated.

Examining the legal framework governing the activity of bailiffs, the Center found that the legal provisions applicable to the reference case do not include the publication of the IDNP of the natural person (debtor / creditor) in the announcements published in the Official Gazette of the Republic of Moldova, and art. 9 of the Law on personal data protection expressly establishes the cases / grounds when the IDNP may be processed.



In this regard, it should be mentioned that the state identification number (IDNP) is subject to a special legal regime, established in art. 9 of the Law on personal data protection, according to which, processing of personal data of individual's state identification number (IDNP), fingerprints or any other identifier of general application may be performed if:

- a) the personal data subject has given his consent;
- b) processing is expressly stipulated by law.

It is important to mention that the Center did not doubt or deny the rights of the bailiff, provided by the Enforcement Code, regarding the undertaking of certain actions that are strictly necessary to fulfill the attributions dictated by law. However, all potential operations that involve the processing of personal data in order to perform legal duties must be carried out in compliance with the principles established by the Law on personal data protection.

Thus, as a result of the examination of the case, it was found that the processing by disclosure / publication of the IDNP of personal data subjects, by the bailiff, in the Official Gazette of the Republic of Moldova, to which an unlimited number of persons have access, took place contrary to the provisions of art. 4 para. (1) let. a), art. 5 para. (1) and art. 9 and art. 29 of the Law on personal data protection.

Respectively, to the bailiff was drawn up minutes on the contravention based on art. 74¹ para. (4) of the Contravention Code.

Personal data protection vs. freedom of expression and the right to information

As a whole, it should be noted that the right to respect for private, intimate and family life, as well as the right to freedom of expression are two fundamental rights found in both international acts on the protection of human rights and freedoms and the Constitution of the Republic of Moldova.

It should be noted that the Constitution of the Republic of Moldova grants and guarantees to every citizen the freedom of thought, opinion and expression in public by word, image or other possible means, as long as it does not harm the honor, dignity or right of another person to its own opinion. At the same time, in art. 55 of the supreme act can be found the limitation, according to which, any person exercises its constitutional rights and freedoms in good faith, without violating the rights and freedoms of others.

The exercise of these freedoms, as long as it carries duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as it is prescribed by law and necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary power.

Thus, we can see that the situations examined generate an extensive and complex issue, due to the rights and values that are the subject of the created legal relationship, thus necessitating a conciliation between some of the fundamental rights governing a rule of law and a democratic society: the right to information, freedom of expression and the right to the inviolability of privacy.



The Center was notified through the complaints of some data subjects, who complained about the allegedly illegal actions of a civic activist regarding the publication on the personal profile of the social network “Facebook”, without their consent, of videos containing the usual category of their personal data – name, surname, position held and the public institution where the personal data subject works in, and most importantly – **home address**.

When examining the cases, it was determined that the profile account of the person who posted the videos on the social network “Facebook”, are accessible to any user of the network, whether we are talking about his friends or followers of the social network, who can view posts/ publications in the news feed from other users and which have a direct link to those posts through search engines.

Also, for each case, it was established that video recording images capture the home address of the data subjects – street and house number, which were disseminated in the public, through the social network “Facebook”. Without having their consent, the information in question was viewed and distributed by an impressive number of people / users.

At the same time, regarding the publication / disclosure on the social network “Facebook” of personal data – home address / residence visa of data subjects, the Center analyzed separately 1) the purpose of personal data processing – publication / dissemination of home address of personal data subject, information regarding the natural person, which according to art. 3 of the Law on personal data protection represent personal data, as well as 2) the means of personal data processing, which were used by the controller when publishing / disseminating them, in particular – home address, on personal profile page of the social network “Facebook”.

Regarding the examined cases, the Center found that by publishing the video on the personal profile of the social network “Facebook” by the civic activist was revealed the usual category of personal data – name, surname, position held and public institution where the personal data subject works in, data that are closely related to the status of public person. The public nature of the facts in which the data subject is involved, holding a public function, public dignity, represents a situation in which the processing of such data is carried out under the conditions of art. 10 of the Law on personal data protection.

It is easy to specify, in general terms that, when we speak about the persons exercising certain public functions, the degree of interference in the inviolability of privacy is much higher, compared to persons who do not have such a status. Moreover, this degree of interference extends to the hypothesis of public circumstances / public facts and in the case of the existence of topics that may be of public interest. However, it should be kept in mind that the state has a positive obligation to legislate legal mechanisms to protect the inviolability of privacy even in the case of public officials, who are involved in public circumstances / facts and / or targeted in matters of public order. It is inadmissible that this category of personal data subjects be deprived of legal guarantees and mechanisms to ensure the protection of their constitutional right – inviolability of privacy.

Contrary to the above, it should be pointed out that in the part related to the disclosure / dissemination of the video recording in public on the social network “Facebook”, without the consent of the data subject of the usual category of personal data – the home address emphasizes that the processing of such data poses an increased risk to the privacy and family life of the data subject, as it does not fall into the category of public information, unlike other personal data – name, surname, position held and the public institution where the data subject works in, things that could be considered public information once the data subject is a civil servant / person with a position of public dignity / public person.



In the context of the examined cases, it was noted that the civic activist – data controller according to the art. 3 of the Law on personal data protection, **has had the obligation to ensure the confidentiality of personal data, namely the home address, in view of the obligation provided in art. 29 of the Law on personal data protection.**

Therefore, for each case, the Center found that the publication / disclosure on the profile of social network “Facebook” of **the personal data of the data subjects, namely the home address**, in the absence of their consent, is contrary to the provisions of art. 4 para. (1) let. a), art. 5 para. (1) and art. 29 para. (1) of the Law on personal data protection.

Thus, in both cases, regarding the civic activist, was drawn up minutes on the contravention based on art. 74¹ para. (4) of the Contravention Code.

Non-compliance with confidentiality and security of personal data

The Center received the notification of a data controller – economic agent, through which the latter reported the occurrence of a security incident materialized by the detection by third parties, in a forest, of an impressive number of time cards of employees of the mentioned economic agent (394 persons), which contain personal data such as: name, surname, personal code, identification code within the unit, photo.

Thus, following the examination of the materials related to the security incident, it was determined that the persons responsible for violating the internal instructions of the controller are: human resources specialist and an employee within the entity, violating the provisions of the Regulation on personal data protection of the company’s employees, which states that:

- in the case of temporary non-use of paper or electronic information carriers containing personal data, they shall be kept in secure metal locks or lockers;
- the removal and introduction of the means of personal data processing from / in the security perimeter shall be registered in the register.

Therefore, it was found the violation of the provisions of art. 29 para. (2) and art. 30 para. (2) of the Law on personal data protection, because the actions / inactions of the responsible persons, manifested by non-compliance with the internal instructions of the controller, in ensuring the confidentiality and security of personal data to which they had access, caused the security incident in the form of disclosure by dissemination of the personal data of 394 data subjects, including unauthorized access to such data, or, according to the information provided by the controller, the data cards of the data subjects have been detected by passers-by, so third parties.

As a result, given the presence of the constitutive signs of the complex of contraventions provided by art. 74¹ para. (1) and para. (4) Contravention Code, in respect of the responsible persons within the data controller, minutes were drawn up regarding the contravention.

At the same time, despite the circumstances indicated above, given the security incident, if the controller does not have a legitimate and explicit need, based strictly on a well-defined purpose, the Center ordered the controller to reassess the need of using the state identification number in the timing cards issued by the controller, if this does not involve disproportionate costs of time, means and labour.

As a result, in the context of the execution of the legal measures ordered by the Center, the economic agent informed about the replacement of the state identification number on the time cards with the tabular number of the employee, the latter additional identification being necessary also in view of the fact that there are many cases when employees have the same name and surname.



Accessing personal data stored in the state information resources by police officers

The Center received several requests from the General Police Inspectorate (IGP), based on which procedures were initiated to verify the compliance of personal data processing performed by employees of a subdivision of the National Inspectorate of Investigations within IGP.

It was established from the content of the proceedings that the examination of the notified issues concerned approximately **12,000 operations of personal data accessing**. Data that have been stored in the state information systems and carried out by the employees of that entity.

The circumstances examined by the Center in these cases have shown with certainty the huge number of personal data access operations carried out by police officers, targeting an impressive number of data subjects, and the fact that a large part of these operations have not been based on a well-defined purpose, an express legal basis and a causal link between a material / file under examination and the natural person whose personal data were subject to processing by accessing / viewing / printing, etc.

In particular, a multitude of violations were established, both of the provisions of the Law on personal data protection and of the Regulation on the regulation of personal data processing by the subdivisions of the Ministry of Internal Affairs approved by Order of the Minister of Internal Affairs of the Republic of Moldova no. 444 of 28.12.2012 and updated by the Order of the Minister of Internal Affairs of the Republic of Moldova no. 260 of 04.09.2017, such as:

- a very large number of operations for accessing / consulting personal data that have not been recorded in the registers of records of accesses / processing of personal data by authorized users;

- failure to duly complete the column “justification, purpose, basis and necessity of accessing / processing personal data” from the Register of records of accessing / processing of personal data. However, it should be clarified that the legal basis which may be the basis for the processing of personal data in various information systems, in particular in the state registers and which would grant the personal data controller / user the right to carry out such operations, is conditioned by the situation in which the personal data controller / user examines a material, in which the personal data subject is concerned, thus demonstrating a causal link between the personal data processed and the material examined, provided that a non-excessive volume of data is processed, strictly necessary for the purpose. Thus, it **is not enough to indicate** as having a legal basis only the information such as **“need for work” / “criminal case” / “criminal file” etc .;**

- refusal to provide the information requested by the Center in order to carry out the control activity under the claim that it falls under the category of documents attributed to State Secret. Analysing the categories of information attributed to state secret, indicated in the Nomenclature of information attributed to State Secret, approved by Government Decision no. 411 of 25.05.2010 and the provisions of the Government Decision no. 1176 of 22.12.2010 for the approval of the Regulation on ensuring the secret regime within public authorities and other legal entities, it was found that the information to be made available to the Center does not belong to the category of information that can be attributed to State Secret. Thus, the allegations made regarding this case by concerned users and controller were considered critical, because the assignment alleged to state secrecy of information and materials necessary to be kept / managed by authorized users with the right to access state information resources represented just a shield in presenting certain evidence.

Consequently, in all cases concerning the total of 12,000 operations for personal data accessing, the Center found a violation of the provisions of the Law on personal data protection through the actions / inactions of IGP / INI employees.



At the same time, **necessary measures were ordered to be taken by the IGP / INI and the Ministry of Internal Affairs**, such as the following:

The entities concerned **shall dispose the implementation of additional measures for personal data protection, in the part related to the record of accesses / consultations of personal data** stored in the state registers to which it has access, by:

- strengthening the internal control (quarterly or half-yearly) regarding the obligation for the IGP and INI staff to keep the Register of manual and / or electronic records of accesses / processing performed, in order not to admit in the future the access / consultation of personal data by the IGP and INI staff, in case of non-existence of the causal link between: (1) the special file / analytical file / operative file / search file / criminal case / contravention case and (2) the person concerned;
- strengthening the internal control regarding the obligation to keep in the Register of records of accesses / processing the requests (reports / notes) submitted to the user in order to access / consult information resources and disclosure of personal data by the IGP and INI;
- registration (in the chancellery / other responsible subdivision) in the established order of the Registers of manual and / or electronic records of the accesses / processing performed;
- the creation of an internal mechanism, which would establish that upon the dismissal or transfer of the Ministry of Internal Affairs' employee to another subdivision, the Register of the manual and / or electronic records of the accesses / processing performed shall be sent for archiving;
- the transmission of the Register of manual and / or electronic records of the accesses / processing is to be included in the liquidation list, which the MIA/IGP employee is to present upon dismissal;
- keeping the Register of manual and / or electronic records of the accesses / processing carried out in strict accordance with the legal requirements, filling in all the indicated fields;
- informing each MIA employee, by signature, of the content of the MIA Order no. 444 of 28.12.2012 on the approval of the Regulation on the regulation of personal data processing by the subdivisions of the Ministry of Internal Affairs, etc.



CHAPTER IV

ACTIVITY OF REPRESENTATION
IN THE COURTS

IV

In administrative contentious

During the year 2020, the Center's interests were represented in the contentious administrative courts in **126** court hearings, amongst which: 121 as a defendant; 5 as a public authority concluding conclusions.

Thus, there is an increase in the number of actions submitted for examination in the courts in which the documents issued by the National Authority for Personal Data Protection were challenged, which in the reporting period reached 121, in comparison to 2019 when 105 lawsuits were filed.

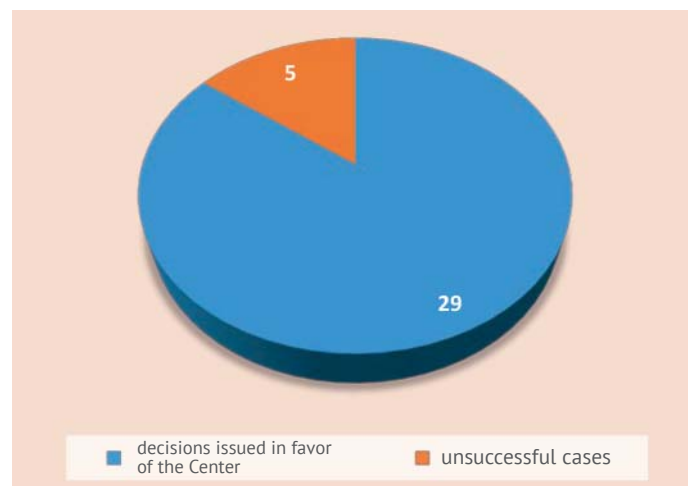
This is also due to the growing number of administrative acts issued by the Center, as well as the growing awareness of the complexity of the consequences and the significance of the nature of the findings recorded in the decisions issued by the Center.

Therefore, during 2020, the representatives of the Center participated in **307** court hearings of administrative litigation, drafting **200** procedural documents necessary for an efficient examination of court cases.

At the same time, we note that in 5 court hearings the Center was called as a public authority that submitted conclusions, in accordance with the provisions of art. 74 para. (1) Code of Civil Procedure.

Likewise, we mention that during 2020 the examination of **34** court files was completed, where the judgements / decisions of the courts remained final and irrevocable, of which:

- 29 judgements/decisions of the court were issued in favour of the Center;
- 5 cases were unsuccessful for the Center.

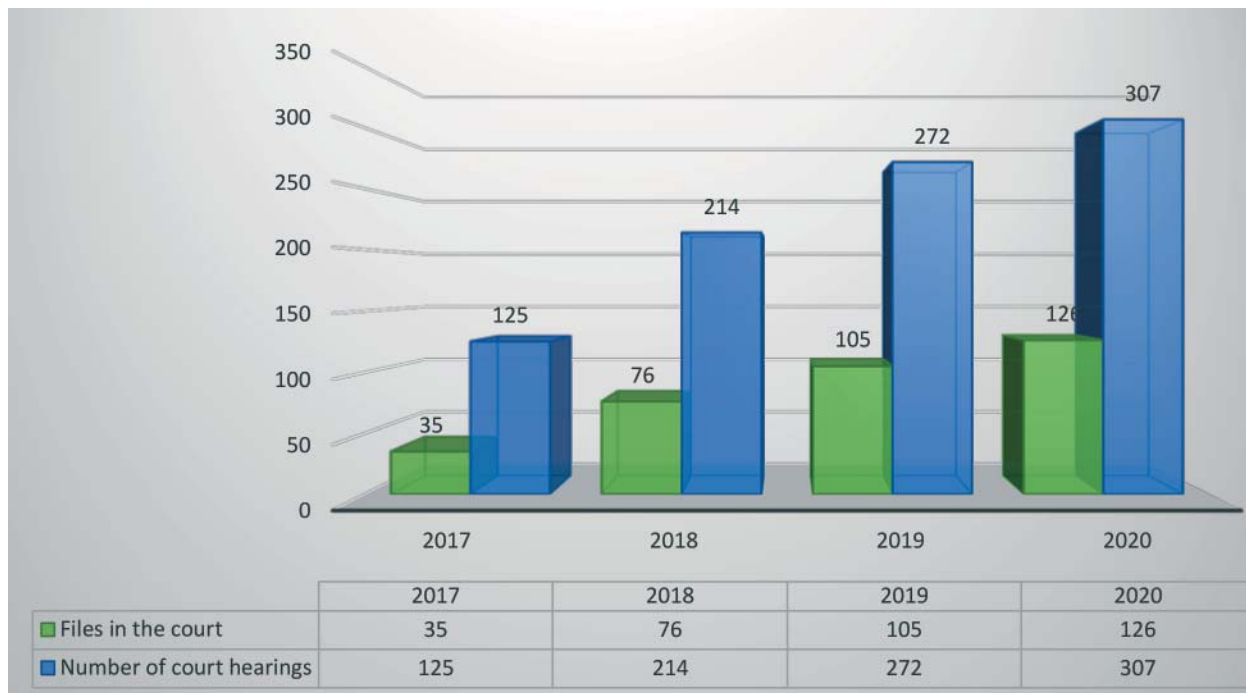
Dynamics of court decisions 2020



Thus, we find that in **85%** of the number of court cases examined, the actions taken by the Center were considered legal and substantiated by the courts.

It should be noted that, based on the specifics of the issues addressed in the lawsuits, in 90% the object of the examination of actions in administrative litigation was the annulment of decisions issued following investigations conducted by the Center on the finding / non-violation of personal data protection principles, 9% was the annulment of decisions regarding the refusal to register in the Register of evidence of personal data controllers, 1% is the cause of the alleged damage.

Comparative dynamics of the number of cases and court hearings in administrative litigation, for the period 2017-2020



Regarding the representation of the interests of the Center in the administrative contentious court, it is important **to exemplify a judicial file**, the judicial examination of which was completed during the reference period, being a success for the Personal Data Protection Authority and having a great impact on realization of the rights of an impressive number of personal data subjects:

On May 20, 2020, the Supreme Court of Justice of the Republic of Moldova irrevocably decided to maintain in force the decision of the Center of November 16, 2018, which found the processing of personal data through the Automated Information System “Register of forensic and criminological information”, made by the Ministry of Internal Affairs inconsistent with the requirements of legislation in the field of personal data protection, the latter being obliged to destroy information containing personal data on data subject targeted by this processing, which were collected / obtained from the unrecognized authorities / institutions from the Transnistrian Region.

In this case, during the examination of facts invoked in the complaint by the personal data subject, the Center highlighted the vicious practice of receiving and storing the information received from unconstitutional structures from the left bank of the Dniester by the constitutional authorities of the Republic of Moldova.



It should be emphasized that the **automatic processing of personal data of the Republic of Moldova's citizens based on information received from unconstitutional structures, which in fact cannot be considered authentic / truthful, as well as its use to the detriment of the data subject concerned, is a serious violation of human rights and freedoms.**

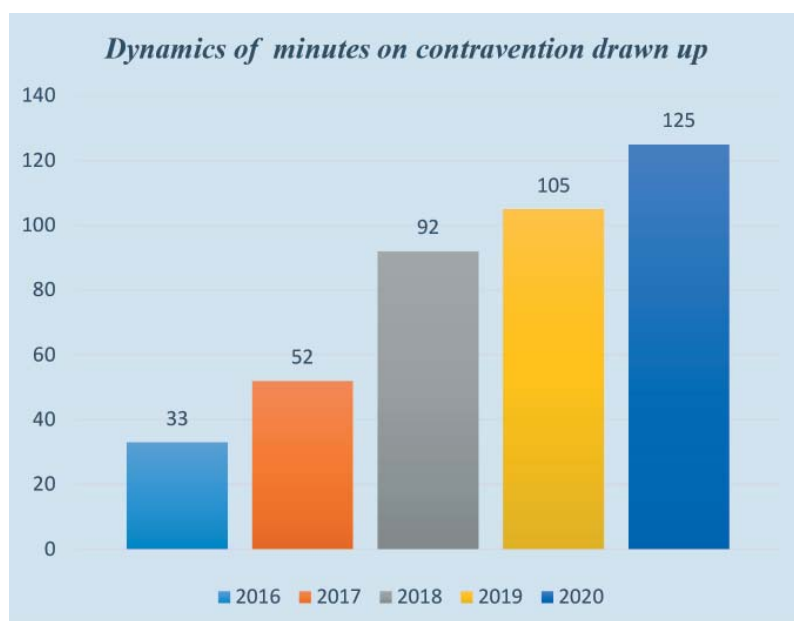
In this sense, the Decision of the Superior Council of Magistracy (SCM) no. 209/14 of April 10, 2012 *“on the approach of Mr. Oleg Efrim, Minister of Justice, regarding the opinion on the address of Mr. Eugen Carpov, Deputy Prime Minister, on approaching some legal issues”, by which the SCM found: “that any act issued by the self-proclaimed authorities of the Republic of Moldova contravenes the Constitution and are considered illegal. This fact refers equally to any decisions, sentences handed down by the courts established in the region. Thus, the Council considers as unacceptable any collaborations, legal cooperation and proposals for legal solutions with the structures from the Transnistrian region.”*

Consequently, in the jurisprudence concerning the Republic of Moldova, the European Court of Human Rights in numerous cases (Ilascu and others vs. Moldova and Russia; Eriomenco against Republic of Moldova and the Russian Federation; Mozer against Republic of Moldova and Russian Federation; Catan and others against Republic of Moldova and Russia) found acts adopted by unrecognized and unconstitutional entities on the left bank of the Dniester as illegal.

It should be specified that, according to the Declarations submitted together with the instrument of ratification of Convention no. 108 for the protection of individuals with regard to the automated processing of personal data, the Republic of Moldova has not declared reservations on the provisions of the Convention, regarding its application on the territory of the Transnistrian region. Thus, the Republic of Moldova has the obligation to ensure the protection of the fundamental rights and freedoms of its citizens with regard to the processing of personal data, especially the right to inviolability of privacy, family and private life, throughout its territory.

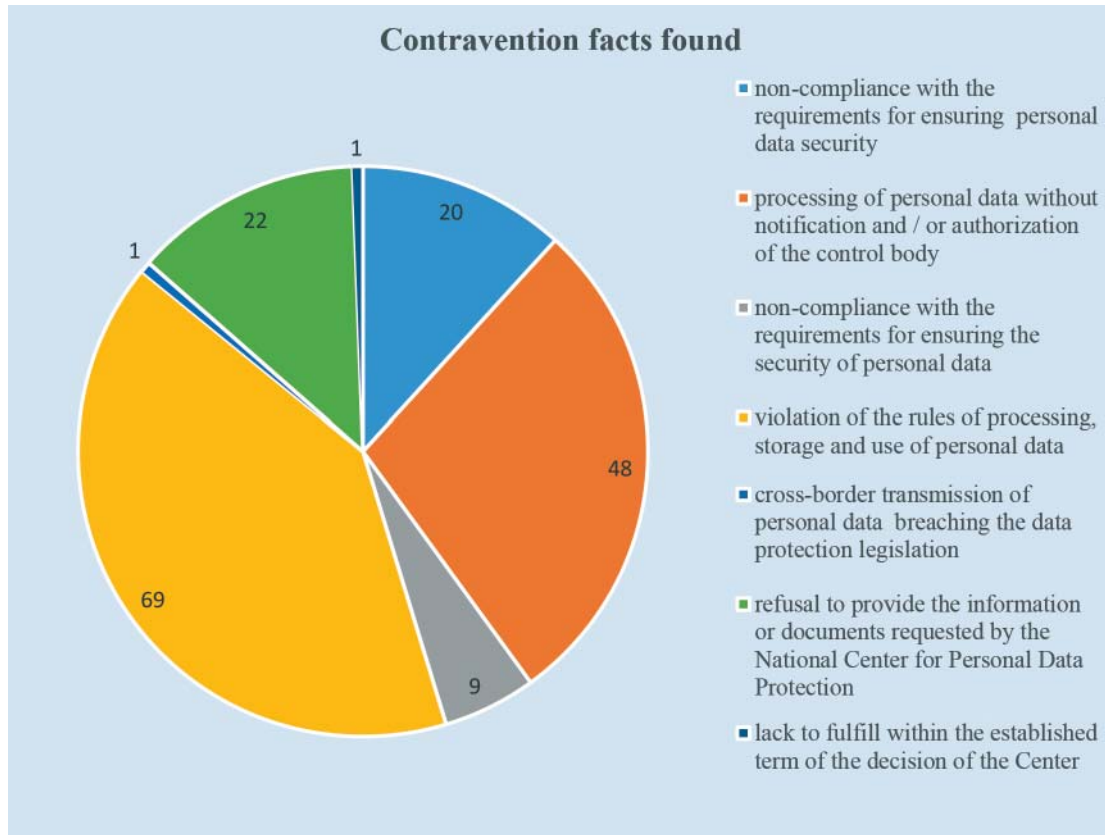
In contravention procedure

During 2020, **125** minutes on contravention were drawn up, being ascertained **170** contravention facts related to the violation of the legal provisions in the field of personal data protection, in view of the provisions of art. 74¹ – 74³ of Contravention Code, the contravention cases being sent for examination in the competent court.





In the diagram below we present the range of contraventions found in the light of the articles of the Contravention Code based on the violations committed in the processing of personal data:



In this context, it should be noted that, despite the fact that during 2020, the access to the courts was restricted for a period of time due to the COVID-19 pandemic, the Centre's employees participated in more than **470** court hearings on contraventions under examination, both in the court of first instance and at the Court of Appeal.

It should be specified that, with the entry into force on 01.01.2020 of the new provisions of the Contravention Code, the courts resort to the application of the written procedure in examining the contravention cases, in accordance with the provisions of art. 464¹ and 464² of the Contravention Code, a practice considered by the Center applicable to the settlement of contravention cases of reduced complexity, not requiring the physical presence of the ascertaining agent during court hearings.

It should be noted that out of the total of **125** contravention cases sent for examination in court during the reference period, in **30** proceedings examined the Center won the case, the court acknowledging the guilt of the persons in respect of whom minutes on contravention were drawn up, establishing sanctions in the form of a fine. In addition, it should be noted that another **124** proceedings are currently pending before the courts, including on some of the infringement cases initiated in 2019.

For information, the number and dynamics of the minutes on contraventions drawn up during the period when the Center acquired the quality of ascertaining agent is reflected in the following table:



Period of reference	Number of minutes on contravention	Dynamics
2012-2013	4-26	↑550%
2013-2014	26-34	↑31%
2014-2015	34-24	↓29%
2015-2016	24-33	↑38%
2016-2017	33-52	↑57%
2017-2018	52-92	↑77%
2018-2019	92-105	↑14%
2019-2020	105-125	↑19%
2016-2020	33-125	↑279%



CHAPTER V

ACTIVITY OF SURVEILLANCE OF PERSONAL DATA PROCESSINGS

The activity of registration of controllers and personal data filing systems

During 2020, the Prevention, Surveillance and Evidence Department of the General Department for Surveillance and Conformity examined **1472** notifications submitted for registration in the Register of evidence of personal data controllers, both personal data controllers and filing systems kept in automated and / or manual form in which personal data are processed.

We remind that the provisions of the national normative framework in the field of personal data protection, especially art. 23 of the Law on personal data protection imposes the obligation of personal data controllers to notify the Center (personally or through processors) prior to the processing of personal data in an automated or manual filing system, with the presentation of the information that justifies the processing of personal data, as well as ensuring the implementation of the organizational and technical measures necessary for personal data protection.

During the examination of the notifications submitted to the Center for authorization and registration, **995 preliminary verifications** were performed.

As a result of the examination the notifications submitted during the reporting period, **504 personal data controllers** and **710 personal data filing systems** were registered.

The information regarding the registration in the Register of evidence of personal data controllers of controllers and filling systems where personal data are processed is shown, in dynamics for the years 2016-2020 in the following table:

Year	Total number of notifications examined	Number of registered controllers	Number of registered personal data filing systems	Number of filing systems refused to be registered	Number of contested refusal decisions in administrative contentious
2016	850	386	761	89	1
2017	1046	500	843	203	0
2018	1388	639	938	451	1
2019	1652	654	944	708	1
2020	1472	504	710	762	2

Out of the mentioned information, the number of notifications submitted for examination at the “One-Stop Shop” of the Center during 2020 was in a slight decrease. Thus, also in this chapter it is observed that, due to the pandemic situation caused by COVID-19, which imposed restrictions on the activity of all public and private entities, personal data controllers were less active in notifying the filing systems managed compared to previous years.

The main aspects examined thoroughly and primarily in the evaluation / analysis of notifications and the related documents, submitted for registration in the Register of personal data controllers, as in previous years, were the following:



- Correctness of determining the status of personal data controller or processor, in relation to the notified filing systems;
- Existence of the legal basis for personal data processing;
- Compliance of the organizational and technical measures necessary for personal data protection declared by the personal data controller with the provisions of the requirements for ensuring the security of personal data when processing them within the personal data information systems;
- Existence of instructions provided by the controller for processors by a contract or other legal act which will be binding on the parties and which will establish the object and duration of processing, the nature and purpose of processing, the state in which personal data will be processed, the type of personal data, the categories of data subjects, the obligations and rights of the controller and processor, etc .;
- Conditions under which personal data cross-border transmission is carried out taking into account their nature, purpose and duration of the proposed processing, the state of destination, its legislation, as well as the professional norms and security measures in the state of destination etc.

At the same time, in 2020 there is an increase in the number of notifications refused to be registered / authorized, the most common reasons for refusal being:

- 1) indication in the notification form of fake information regarding: the categories of personal data, the purposes of processing, the method of collection, as well as the term of personal data processing, that do not correspond to those established in the acts annexed to notification;
- 2) failure to indicate in the notification form the information regarding the processors in case of personal data processing in the name and on behalf of the personal data controller;
- 3) establishing in the security policy and in the documentation related to it some organizational and technical measures necessary for the protection of personal data that do not correspond to the provisions of the requirements for ensuring the security of personal data when processing them within the personal data information systems;
- 4) video surveillance of spaces / goods that do not belong to the personal data controller or non-compliant surveillance of workplaces, especially of employees' computing techniques, including their means of data entry (keyboards), which leads to possible cases of violation by the employer of the provisions of art. 91 para. (1) let. f) of the Labor Code, as well as the security and confidentiality of personal data, when through video images is possible to view the introduction of authentication credentials by internal users in the filing systems managed by the controller.

As in previous years, the auxiliary filing systems most often were notified and registered, which do not constitute / reflect the basic activity of personal data controller, such as: accounting, human resources, video surveillance, correspondence, etc., systems which certainly contain personal data and are also to be notified to the Center.

Furthermore, in order to provide methodological and advisory support to personal data controllers and / or processors, regarding the procedure of notifying the filing and registration systems as a controller in the Register of evidence of personal data controllers, during 2020, the employees of the subdivision responsible for the registration of controllers / personal data filing systems, offered **2030 consultations and instructions** by phone or e-mail. Based on the specific situation caused by the COVID-19 pandemic, consultations provided by telephone or



e-mail predominated during the reference period, without the physical presence of applicants for consultations at the Centre's headquarters, which had a significant impact on both the quality of the notifications submitted and the documents drawn up by the controllers in order to register in the Register of evidence of personal data controllers, as well as on the number of notifications submitted to the "One-Stop Shop" for examination.

The activity of preventing the non-compliance of personal data processing

During 2020, in order to prevent non-compliant practices of personal data processing, the Center informed, including through the official website, personal data controllers in various fields on the multiple cases of data security and confidentiality discreditation from different states, which have resulted in the application of significant fines imposed to controllers who have admitted the non-compliant processing of personal data.

Also in the context of ensuring the prevention of non-conformities in the personal data processing, resulting from the constant increase in the number of complaints related to the personal data processing through video surveillance cameras, the Center developed and published on the official website **the authority's opinion on practical issues in connection with the installation and management of video surveillance means**, to be taken into account by natural and legal persons intending to process personal data through video surveillance systems.

For preventive, informative and applicative purposes, during the reference period, the National Personal Data Protection Authority issued recommendations / opinions in order to ensure the conformity of personal data processing, regarding the following aspects:

- **Personal data processing in the context of COVID-19 pandemic in the Republic of Moldova:** The Center emphasized the risks and challenges regarding the protection of individuals when processing personal data in the context of combating coronavirus (COVID-19), in particular, health data of the patients.
- **Aspects regarding the recording and live streaming of local council meetings:** the opinion of the authority regarding the registration and live streaming of local council meetings via Internet.
- **Specification on the recording and live streaming of local councils meetings:** in the context of the reaction of civil society, as well as some local public authorities, who have misunderstood the previous opinion on the recording and live streaming of local councils meetings, the Center has made some clarifications that it does not intend to restrict the recording and live streaming of local councils meetings via internet, as well as giving precise guidelines of applicative nature to ensure the proper processing of personal data in the context addressed.

The information mentioned above can be viewed in full on the Centre's website www.datepersonale.md under the heading Legislation / NCPDP Recommendations, (by accessing the link: <https://datepersonale.md/legislation/ncpdp-guidelines/>).

At the same time, in the context of the realization the Center's attribution on monitoring the compliance with legislation on information protection and verification of its application, in particular the right to information, access to data, data intervention and opposition, as well as not admitting / preventing violation of the subjects' rights whose personal data have been / are processed by the law enforcement bodies of the Republic of Moldova, entities that, in exercising their powers, process a huge volume of personal data, the Center intervened in relation to the latter on the following issues:

- **Fulfilment of the provisions of art. 15 of the Law on personal data protection and the measures taken to ensure compliance with the rights of personal data subjects:**



It is noteworthy that the free movement of personal data between competent authorities for the purpose of preventing, detecting, investigating or prosecuting crimes or the execution of punishments, including protection against threats to public security and their prevention within the jurisdiction of the Republic of Moldova, must be facilitated while ensuring a high level of personal data protection.

The Center strongly advocates for conciliation between the legal aspiration of the personal data protection and personal data processing in the crime prevention and investigation actions, the execution of convictions and other actions in criminal or misdemeanor proceedings according to the law.

According to art. 12-14 of Law no. 133/2011 on personal data protection, the data subject has the right to information, the right of access to personal data and the right to intervene on personal data, based on which the subject may request from the data controller, information regarding: the purposes of the processing, the categories of data considered and the recipients or categories of recipients to whom the data are disclosed; personal data subject to processing, as well as the origin of such data; the principles and mechanisms through which the automated processing of data concerning the personal data subject is performed; information on the legal consequences generated by the processing of personal data for the subject of these data; information on how to exercise the right to intervene on personal data, etc.

In the light of the provisions of Law no. 133/2011, the controllers have the obligation to respond to the requests of the data subjects, without unjustified delays, unless the controller applies limitations established by law in relation to the rights of the data subject.

Thus, according to art. 15 of Law no. 133/2011 (entitled “Exceptions and restrictions”), the provisions of art. 4 para. (1), art. 12 para. (1) and (2), art. 13, 14 and 28 shall not apply if the processing of personal data is carried out within the actions provided in art. 2 par. (2) let. d) and to art. 5 par. (5) let. g), for the purpose of national defense, state security and maintaining public order, protection of rights and freedoms of personal data subject or other persons, or if the application can harm the efficiency of the action or the objective pursued by public authority when exercising the legal powers. The processing of personal data for the purposes established in par. (1) may not exceed the period necessary to achieve the objective pursued.

In accordance with article 15 par. (3) of Law no. 133/2011, **after the cessation of the situation that justifies the application of par. (1) and (2) of article 15, the controllers will take the necessary measures to ensure respect for the personal data subject’s rights provided in art. 12–14** (informing the subject of personal data, the right of access to personal data, the right to intervene on personal data).

In the same context, according to article 15 par. (4) of Law no. 133/2011, **the public authorities keep record of the application of the exceptions established in par. (1) and informs the Center, within 10 days, about the personal data processed under the conditions of this article.**

In view of the above, the Center requested the General Prosecutor’s Office, the Ministry of Internal Affairs, the Ministry of Defence, the Intelligence and Security Service, the National Anticorruption Center, the Customs Service to provide, within 30 days, information on the following issues:

- The total number of cases in which exceptions and restrictions were applied pursuant to art. 15 par. (1) of Law no. 133/2011;
- The number of cases in which the information of the personal data subject was made after the cessation of the situations that conditioned the application of the exceptions and restrictions regulated by art. 15 par. (1) of Law no. 133/2011 and the manner of informing the subject;



- The number of cases in which the information of personal data subject was omitted after the cessation of the situations that conditioned the application of the exceptions and restrictions regulated by art. 15 par. (1) Law no. 133/2011, highlighting the reasons that conditioned such an omission;
- The existence of some internal verification regarding the assurance of the observance of the date subject's right to information, subsequent to the lapse of the situations that conditioned the establishment of the exceptions and restrictions established in art. 15 par. (1) of Law no. 133/2011.

It should be noted that the most of the mentioned entities presented vague information, not providing clear answers to the questions submitted both in terms of some statistical data and in terms of the possible existence of certain organizational and technical mechanisms and measures implemented to ensure the effective record of the persons in respect of whom restrictions on the exercise of rights have been established, as well as of the persons in relation to whom the rights have been / are to be exercised following the exhaustion of the purpose for which these restrictions were previously imposed. However, **the circumstances found indicate the urgent need to establish the appropriate legislative mechanisms and levers, including the undertaking of the necessary measures to ensure and streamline the realization of the rights of personal data subjects, by the entities concerned, which unfortunately, were not achieved.**

• **Legality of processing of personal data stored in state automated information resources**

Following the analytical activity performed in relation to the information gathered from the Public Services Agency, the statistics of the operations for accessing personal data stored in various state information systems was systematized per institution: State Register of Population, Real Estate Register, State Register of Drivers, State Register of Transports, Register of Law Units, separated by years, performed by users: Minister of Internal Affairs, National Anticorruption Center, General Prosecutor's Office, National Authority for Integrity, Ministry of Defense, Customs Service, State Tax Service, entities that were identified as having made the largest number of personal data accesses.

In this context, we highlight in the following table the information on the number of operations for accessing personal data in the mentioned state information resources, performed by the authorized users of the authorities indicated above:

The institution concerned	Number of accesses made in state information systems: RSP, RBI, RST, RSCV, RUD via SIA «Web Access» and IOC		
	2018	2019	2020
Ministry of Internal Affairs	3541231	20887797	11213170
Information and Security Service	93897	78939	65180
National Anticorruption Center	96017	112235	86891
General Prosecutor's Office	20109	24611	19985
Customs Service	28509	25551	12381
Ministry of Defence	347	2050	1002
National Authority for Integrity	no information was requested for 2018	20740	17217
State Tax Service		3541231	3535927

Thus, in order to ensure compliance with the legislation on personal data protection, the Center requested those entities to submit, within 60 days, information on some aspects related to the operations of accessing personal data stored in the aforementioned information systems, and namely:



- The category of subjects whose personal data stored in the information systems indicated in the approaches, are likely to be accessed and the type of personal data that are accessed by each category of subjects;
- The factual, legal grounds and purposes that usually underlie the operations of accessing personal data stored in the indicated information systems;
- Operations that are carried out in relation to personal data stored in the indicated information systems (consultation, printing and subsequent storage, copying, disclosure, combination, transmission, including cross-border transmission, etc.);
 - a) In case of subsequent printing, copying and storage operations, we request to specify the details of the measures implemented and aimed at preventing unintended actions, which may lead to destruction, unauthorized copying, loss or damage of the material on which the personal data are stored or taken off from the indicated information systems;
 - b) The terms of personal data storage that have been taken off from the indicated information systems;
 - c) For what purposes is the operation of taking personal data from the indicated information systems;
 - d) Confirmation / refutation of the information regarding the detection / identification of some security breaches triggered as a result of accessing, printing, copying and subsequent storage operations, of the personal data stored in the indicated information systems;
 - e) Measures implemented in order to prevent, overcome, combat and escalate security incidents and remedy security vulnerabilities;
- Existence of a record and evidence of persons performing operations to access personal data, stored in the indicated information systems;
- List of authorized persons who have the right of access to information systems;
- Whether accessing through the IOC provides the possibility to identify the persons performing the accesses;
- The reason for avoiding accesses through the SIC application “WEB Access” and the massive use of IOC

It should be noted that even in this case, the entities concerned either offered vague and incomplete answers or did not respond to the Centre’s request, the latter had to intervene repeatedly in order to gather the necessary information, **fact that proves, unfortunately, the inefficiency / insufficiency of the measures taken by the concerned controllers in order to ensure the efficient keeping of the records of the operations for accessing personal data, stored in various state information resources, carried out by their authorized users.**

Additionally, in the context of ensuring the prevention of non-compliant personal data processing, the Center reiterates that **the lack / insufficiency of implemented measures to ensure the security and confidentiality of personal data, in practice, and the lack of rigorous control over the correctness of processing operations of the personal data carried out, may lead, imminently, to non-compliant processing of personal data of the data subjects concerned,** ultimately leading to possible civil disputes with reparation of material and moral damages, imposing the Center to issue suspension decisions and / or cessation of personal data processing operations.

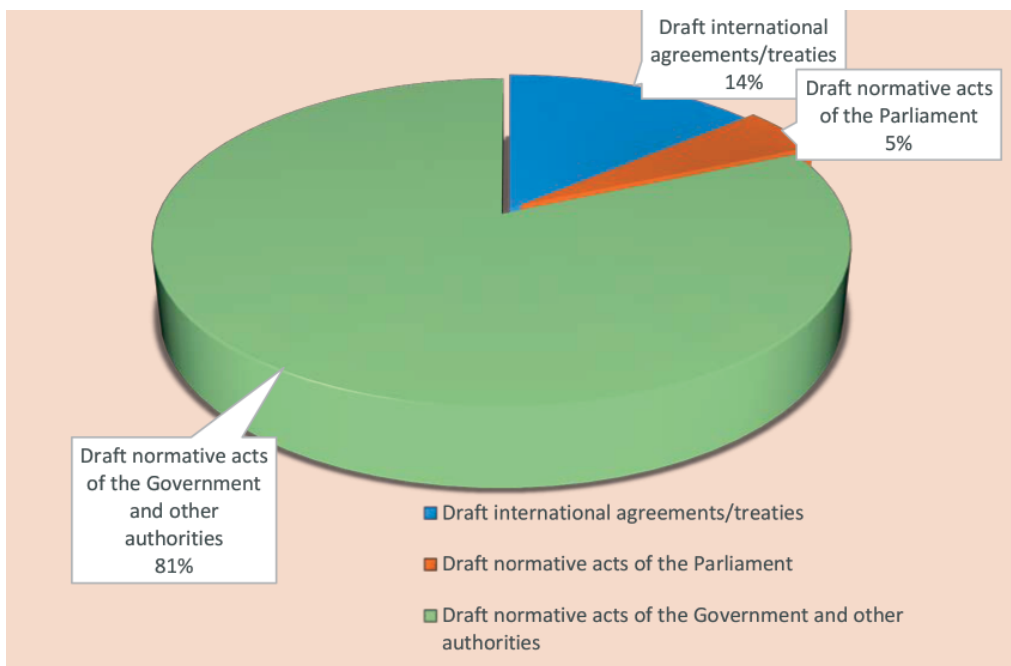
At the same time, it is necessary to mention the obligation of personal data controllers to review the personal data security policy and related documentation, at least once a year, as a result of changes or reassessments of its components, taking into account the evolution information technologies used for the processing of personal data, the legal regime of personal data protection, and the need to ensure the implementation of the principles of personal data protection, implicitly, till the development and functioning of automated information systems.

VI
CHAPTER VIAPPROVAL AND ELABORATION OF THE
DRAFT NORMATIVE ACTS**Approval of normative acts**

Following the provisions of Art. 32 paragraph (2) of the Law no.100/2017 on normative acts, the draft normative acts related to the field of personal data protection are transmitted for approval to the National Center for Personal Data Protection.

As a result, during the year 2020, **65** drafts of national / international normative acts were submitted to the Center for approval, which were examined in terms of respecting the principles of personal data protection, as well as ensuring the rights and freedoms of individuals in relation to the processing of personal data, of which:

- **9** draft international agreements / treaties;
- **3** draft normative acts on amending laws, codes;
- **53** draft normative acts of the Government and other authorities.

The percentage of opinions offered by the Center during the year 2020

It should be mentioned that the issues regulated by the normative acts submitted for approval were diverse, each act dealing with distinct areas and procedures that required careful study in order to ensure the objectivity and legality of the opinions provided. Even in these conditions, in most cases, when approving the draft normative acts, was determined that it is necessary to complete and revise the texts of those acts, being submitted objections and proposals in view of the need to comply with legal regulations on personal data protection.



Therefore, in relation to most of the draft normative acts analyzed, recommendations for their adjustment and harmonization with the legal provisions on personal data protection were made.

It should be noted that, compared to previous years, during the reference period there was an increase of about 15% of the opinions submitted to the National Authority for Personal Data Protection for the approval of acts corresponding to the implementation of automated information systems in which personal data are to be processed.

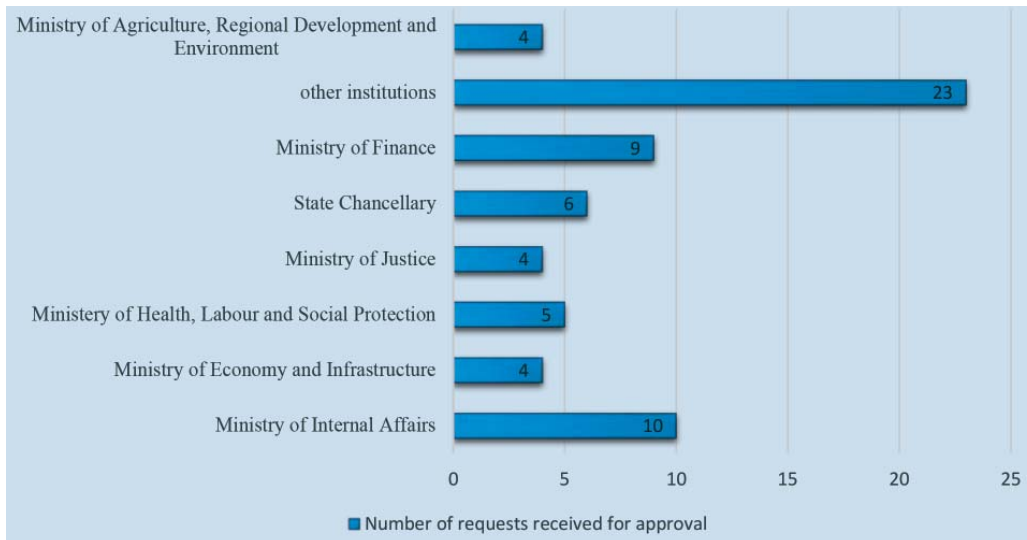
Below we present some of the most relevant drafts of approved normative acts:

- Draft Government Decision on approving the Concept of the Governmental Platform e-Learning and the Regulation on its use and administration, in relation to which it was proposed to link the concept to the regulatory framework in the field of personal data protection and inclusion in the text of the prescribed project of the new provisions that would ensure the observance of the rights of the personal data subject.
- Draft Regulation on the use, administration and development of the citizen's government portal, where it was proposed to revise points 5, 7, 9, 11, 13, 19, 20 and 24 of the mentioned draft Regulation, based on the need to ensure security and confidentiality of personal data for all participants in the data exchange on the interoperability platform.
- Draft Government decision on approving measures necessary to ensure cyber security at government level.
- Draft Government Decision on the approval of the Concept of the Government Electronic Notification Service (MNotify) and the Regulation on the operation and use of the Government Electronic Notification Service, where it was proposed to revise the deadlines for personal data retention and their automated deletion in SI MNotify.
- Draft Government Decision on the approval of the Regulation on the organization and operation of the automated information system "E-Integrity", where it was proposed to link the technical and organizational measures necessary to protect personal data against destruction, modification, blocking, copying, liability, as well as against other unlawful actions in accordance with the Requirements for ensuring personal data security when processing them in the context of personal data information systems.
- Draft Government Decision on the approval of the draft law on the amendment of some normative acts, by which was proposed, including, the amendment of the Law on personal data protection, more exactly art. 23, 24 and 25, by which was intended to replace the obligation to notify personal data processing controllers with other procedures, such as: assessment of the impact on personal data protection, prior consultation, appointment of the data protection officer. Thus, in the light of the considerations set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing the Directive 95/46 / EC (GDPR), which sets out the reasoning behind the need to repeal the obligation to notify the processing of personal data and replace it with certain effective procedures and mechanisms, the Center considered the proposal as being appropriate.

At the same time, due to the fact that the changes proposed by the author of the draft law did not cover all the procedures to be implemented by the controller and the processor, following the exclusion of the notification, the Center came up with a series of proposals to improve the draft law.



Number of requests for approval received from other institutions in 2020



Development of draft normative acts

Modification of
art. 27 of Law
133/2011

During the year 2020, the activity of the Center on the legislative line was focused on the development of the draft law on amending and supplementing art. 27 of Law 133/2011 on personal data protection, which was approved by the Parliament of the Republic of Moldova on July 9, 2020 and entered into force on August 24, 2020.

The essential condition that backgrounded the initiation of this draft law was also the urgent need to optimize and streamline the procedure of conducting investigations / controls on compliance of personal data processing by the Center, in terms of regulating a deadline to be proportional to the complexity of the procedure for verifying the conformity of the processing of personal data.

Thus, by this draft law it was proposed that the deadline for examination and resolution of the complaint submitted to the Center to be 3 months, having the possibility to justify an extension at every 30 days, depending on the complexity of the case, the volume of information to be obtained and analyzed, the behavior of the participants concerned, the conduct of the relevant authorities and the importance of the administrative procedure for the interested parties, but not more than 6 months.

On the other hand, this draft law included amendments aimed at informing the personal data subject on the situation of examination of his complaint, at the request of the latter or every extension, indicating the objective reasons for extending the examination period. Respectively, provided that personal data subject is not satisfied with the way of examining his petition, will have the possibility to contest the actions of the state controller who is examining his petition, in court or at the Center.

Another condition that preceded the development of the mentioned draft law was the urgent need for separation and clear organization of the responsibilities of the Centre's employees in the process of examining complaints and conducting the procedure for verifying the conformity of personal data processing, to streamline the work process and avoid internal institutional shortages, as well as to regulate the possibility of delegating responsibility for issuing / signing decisions of the Center, besides the director, deputy director of the authority, and the authorized staff with control functions of the Center, according to competencies assigned by the order of the Director.



CHAPTER VII

INTERNATIONAL COOPERATION

VII



The establishment and development of international cooperation in the field of personal data protection continued to be one of the key elements in strengthening the functional capacities of the Center in 2020.

Even though 2020 was a year of challenges, arising from the global epidemic situation, the Center sought to focus on strengthening bilateral and multilateral relations with external partners both within international organizations and individually. In order to achieve this goal, Center's employee participated in the working meetings of the European and International Committees. It should be noted that due to the global pandemic situation, 2020 was a limited year in terms of international meetings in the format in which they took place previously. However, some progress has been made. During 2020, the Centre's representatives participated in various conferences, meetings, and workshops.



- **Plenary meetings of the European Data Protection Board**

During 2020, representatives of the Center participated in the plenary meetings organized by the European Data Protection Board (EDPB) held in Brussels, Belgium. Among the most important meetings are the plenary meeting of 28-29 January 2020 and the plenary meeting of 18-19 February 2020.

These meetings are valuable in trying to develop mechanisms for international cooperation to facilitate the effective enforcement of personal data protection legislation, providing international mutual assistance in enforcing personal data protection legislation, including



by notification, assistance in investigations and exchange of information, subject to adequate safeguards to protect personal data and other fundamental rights and freedoms. They provide the opportunity for the involvement of relevant stakeholders in discussions and activities aimed at enhancing international cooperation in the field of enforcement of personal data protection legislation, and allows for the promotion of mutual exchange and documentation of data protection legislation and practices, including in relation to jurisdictional conflicts with third countries.

The globalization of data flows requires the international strengthening of people's rights to data protection. To this end, strong principles for the protection of personal data must be adopted, designed to facilitate the cross-border flows of personal data, while ensuring a high and coherent level of protection, free from gaps and unnecessarily complex. Thus, one of the functions of the plenary sessions of the EDPB is a structured collaboration with the other personal data protection authorities, which the Center's representatives are trying to achieve.



• Plenary meetings – Council of Europe

Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108)

Data protection is a fundamental right protected since the 1980s by international treaties, the first international convention to enter into force was drafted by the Council of Europe. Data protection is undergoing a rethinking process not only in the European Union but also within the Council of Europe. Here the reforms are characterized by the protection of the citizens of the Member States according to the development of technology. Discussions on the modernization of Convention 108 have started since October 2011, with the Consultative Committee (T-PD) reaching the adoption in 2012 a text of the protocol of review. The Committee of Ministers decided to establish an ad hoc Committee on the protection of data composed of representatives of the Member States of the Council of Europe with a mission to complete the modernisation of the Convention 108 through formal negotiation of the text of the Protocol of amendment.

The process of modernisation of Convention 108 has as purposefulness its transformation into an international legal instrument with a universal value applicable also to the States outside the Council of Europe. We note that, according to the situation at the end of 2020, of the 47 member states of the Council of Europe and 8 non-members (55 in total), the Amending Protocol to the Convention for the Protection of Individuals with regard to the Processing of Personal Data was signed by 33 states out of the total number and ratified by 10.

During the reporting period, the Center participated in two plenary meetings of the Consultative Committee of Convention 108, which held via videoconference. These meetings focused primarily on the Secretariat's presentation on major data protection activities and developments in 2020, in particular on the publication of the compiled text, which contains updates provided by delegations, but also on the three Joint Statements issued by the Chair of the Committee of Convention 108 and the Data Protection Commissioner of the Council of Europe:



- a) on the right to data protection in the context of the COVID-19 pandemic (published on 30 March 2020),
- b) on Digital Contact Tracing (published on 28 April 2020) and
- c) on “Better protection of individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services (published on 7 September 2020)”

These presentations/statements made by the Secretariat or experts come to explain and clarify some aspects in the field of personal data protection which can be resolved only through effective international cooperation. In general, in view of the fast technological development of information processing and the development of the international data flows, it is desirable to establish mechanisms at the international level and to develop existing ones, which would allow States to inform and consult on data protection. In this regard, the plenary meetings of the Consultative Committee of Convention 108 come as international instruments of a regional nature that contribute to the development and evolution of the field of data protection.

Also during the reporting period, the representative of the Center participated in the international meeting on cooperation with electronic service providers, which took place during 26 -28 February 2020 in Tbilisi (Georgia). The meeting was organized as part of the Cyber East project, as a follow-up to the Cybercrime @ EAP projects, which aim to support Eastern Partnership countries in building and maintaining partnerships with private sector entities, mainly Internet service providers, to strengthen mechanisms for cooperation and trust between the private sector, citizens and criminal justice authorities.



• Implementation of the provisions of the RM-EU Association Agreement

In this regard, it should be noted that during the reporting period the Center prepared and presented to the Ministry of Foreign Affairs and European Integration and the Ministry of Economy and Infrastructure the final general report on implementation of actions in the National Action Plan on Implementation of the Association Agreement 2017-2019. Also within the limits of this chapter, was made the approval of the new Association Agenda 2021-2027.

• Cooperation with European Union agencies

In accordance with the provisions of Article 19 (2) of the Cooperation Agreement between the Republic of Moldova and Eurojust, according to which the Data Protection Officer of Eurojust and the Data Protection Authority of the Republic of Moldova shall report to each other, at least once a year, on the implementation of the provisions of the Agreement, was send to Eurojust the information regarding the activity of the Center and the implementation of the legal provisions of personal data protection, as well as the collaboration with the General Prosecutor's Office.

We mention that the cooperation with Eurojust represents a key point in the development of



relations of international legal assistance in criminal matters in compliance with the European standards and in the sense of European integration vector of the Republic of Moldova.

This allows Eurojust to support, through the various modern mechanisms at its disposal, efforts to prevent, counter and prosecute a number of serious violations, as well as to support the law enforcement agencies of the Republic of Moldova.

• Cooperation with European Data Protection Authorities

During 2020, the Center requested the opinion and experience of several Data Protection Authorities of the member states of European Union such as Romania, Austria, Belgium, Bulgaria, Italy, France, Germany, Greece, Spain, Portugal, Netherland, etc., on the use of video surveillance cameras in prisoners' cells. This request occurs as a result of multiple addresses regarding the legality of the use of video surveillance cameras (CCTV) installed in the cells of detainees in penitentiaries and / or in pre-trial detention facilities under the auspices of the police. The purpose of this approach was to take over the good European practices, as well as to apply the legal normative framework in solving the problems related to the video surveillance installed in the cells of detainees. To this end, the DPAs were asked to share their experience on the following topics:

- Is it allowed to use video surveillance cameras (CCTV) installed in detainees' cells in prisons and / or in remand centers?
- Which normative / legislative acts regulate the legal basis of their use?
- What are the stated purposes of using video surveillance cameras (CCTV) in these cases?
- What is the allowed period of storage of the information held?
- Under what conditions can CCTV images be disclosed to third parties?
- If the rights of the data subject concerned may be restricted, in this case, the rights provided by Convention no. 108, GDPR and / or Directive 680/2016, in particular, can data subjects object to the personal data processing via CCTV?, etc.

The information already received from DPAs on the exposed topic, as well as the one being received by the Center, is / is to be systematized in order to study the good practices and to decide further on their applicability at national level.

International Projects

During 2020, the Center applied and received support in several international projects, as follows:

Programme Erasmus+

NCPDP participated in the Call for Proposals 2020 – EAC/A02/2019 Erasmus+ Programme Key Action 2 (KA2) – Cooperation for innovation and the exchange of good practices Capacity building in the field of higher education. Within the above-mentioned call, it has proposed to carry out the following Project: *EU digital career opportunities via data protection training for people with disadvantaged backgrounds*. The overall objective of the project is boosting entrepreneurship of people with disadvantaged backgrounds via tailor-made approach, based on best practices for demonstrating compliance with the EU data protection legal framework. Under the Erasmus + Program, the Center participated as a member of a consortium together with partners from Bulgaria, Italy, Greece and Poland.



TAIEX project – the Technical Assistance and Information Exchange instrument

Mass media

- ***“The right to freedom of expression and personal data protection in the context of possible global challenges! (COVID - 19 pandemic)”***

Public health

- ***“Processing and protection of personal data in the field of public health in the context of possible global challenges! (COVID - 19 pandemic)”***

In the context of a global pandemic, namely the fight against COVID-19, appear more and more legal questions regarding the use and disclosure of health data by media representatives in accordance with the provisions of GDPR. To this end, the NCPDP has planned to organize an international conference *“The right to freedom of expression and personal data protection in the context of possible global challenges! (COVID – 19 pandemic)”*, for media representative’s, the purpose of the conference being to present information, examples of good practice and innovative solutions for the purpose of establishing the right balance between freedom of expression and the right to privacy, as well as to exchange experiences between the parties. The application to the mentioned project was made through the online platform TAIEX, but in the end, the project was not accepted.

TAIEX
project
obtained

In the field of public health, Center applied in 2020 and received support from the TAIEX project in organizing the workshop ***“Processing and protection of personal data in the field of public health in the context of possible global challenges! (COVID – 19 pandemic)”***.

The aim of the workshop is to strengthen and enhance the skills of public health representatives on possible challenges that may arise globally (in the context of the pandemic COVID – 19), while respecting the fundamental rights and freedoms of individuals on personal data protection when the processing is necessary for reasons of public interest in the area of public health as well as the adoption of good practices based on relevant case law; setting a balance between the processing, storage, and disclosure of health data and the right to privacy; promoting clarity and specialized analysis, oriented towards the provisions of the law on data protection in the specific field of application – that of health; familiarization of medical representatives with the new challenges related to the processing of personal data.

The event will be organized for representatives of the Ministry of Health, Labor and Social Protection as well as medical institutions, the Ministry of Justice, the Ministry of Internal Affairs and the General Inspectorate of Police. Personal data protection experts from Croatia, Slovakia and representatives of the Center, will moderate the event. Based on the global situation of the SARS-COV – 2 pandemic, the event will take place online at the end of January 2021 for approximately 300 people, from three different regions: Central, North and South.

In 2020, the Center continued its training and awareness-raising activities. The reference period was marked by the COVID-19 pandemic, which influenced the number of training activities. For the same reasons, in 2020 most of the training and awareness-raising activities took place online.

In 2020, the trainings were organized for both the public and private sectors, especially in Chisinau. Even if these activities took place online, the participants showed an increased interest in the desire to strengthen their knowledge in the field of personal data protection and to comply with the activity related to the processing of personal data to the legal provisions in the field.

Raising awareness actions

The main information and awareness-raising activities of the society on the importance of personal data protection field carried out by the Center during the reporting period:

– On January 17, 2020, representative of the Center, trainer certified by the European Union Twinning Project, promoted a dialogue of free discussions with the students of the Law Faculty of the Free International University of the Republic of Moldova, third year, on the topic “*Personal data protection for the young audience: awareness, principles, necessity, risks and challenges*”. About 50 students participated in discussions.



– On January 28, 2020 – for the Data Protection Day, the Center organized, for the first time, a public event for parents and children entitled “*Protect your child in the online environment*”. The event was organized in collaboration with General Police Inspectorate, “Moldcell” – mobile network operator, Public Association “Solidary Parents” and General Department for Education Youth, Sport and Culture. The event gathered about 60 parents, including children, from the parent committees and students from primary, secondary and general educational institutions, Botanica sector.



– On January 29, 2020 – The Center continued the round of events dedicated to Data Protection Day, by organizing the information event for students – “*The right to access of information*”



and the right to privacy” with the participation of students of the Faculty of Law, ULIM and Faculty of Journalism, SUM, including, with the participation of civil society representatives – Promo-Lex, Center for Legal Resources, Center for Journalistic Investigations, etc. The event was attended by 14 participants.



In the context of awareness-raising activities on the importance of personal data protection, with support of the EU Twinning project “Capacity Building of the National Center for Personal Data Protection” funded by the European Union, **various information materials were developed for different categories of data subjects (including minors, parents) as well as personal data controllers.** The informative materials were used during 2020 in the multiple activities organized by the Center, **they aim at both the information about the rights of the data subjects and their responsibility for the compliant processing of personal data, as well as the legal assurance of personal data processing by controllers.** Some models of information materials can be viewed in the appendix section of [this report](#).

Training activities

During the period January-December 2020, the Center held 7 working meetings with representatives of public and private institutions on issues related to: assistance in developing codes of conduct in various areas of activity, examination of sectoral laws, guidance and consulting, etc.

At the same time, the representatives of the Center organized 4 trainings which were attended by about 500 participants from Chisinau and districts of the Republic of Moldova.

– On February 27, 2020, at the invitation of the Center for International Police Cooperation, the employees of the Conformity Department of the Center held a training meeting of the staff of the Center for International Police Cooperation.



– On June 4, 2020, at the invitation of the Congress of Local Authorities of Moldova (CLAM) leadership, the representatives of the Center had a speech at the webinar for secretaries of local councils, members of the Network of Secretaries of CLAM, on “Development of security policy and the Regulation on the processing of personal data under the LPA”. About 85 secretaries of local councils attended the webinar.



- On July 27, 2020, at the request of the Training Center in the Field of Labor Relations, the representative of the Center participated as a trainer, moderating a seminar on personal data protection.
- On November 17, 2020, the Center organized a training on personal data protection at the request of the Training Center in the Field of Labor Relations. About 150 people – from schools, kindergartens, gymnasiums, but also employees in the medical field, attended the event. The training took place online.

Center activity highlighted in the media

At the beginning of 2020, the new website of the Center was launched www.datepersonale.md, which is an important achievement for both the institution and society in general, or it is an indispensable source of information that facilitates users' access to all the information regarding the activity of the National Authority for the control of personal data processing, as well as the news related to the field of data protection at national and international level.

The Centre's current website is innovative and meets all current technical and organizational requirements and needs. It should be noted that this achievement was possible thanks to the support provided by the EU Twinning Project "Capacity Building of the National Center for Personal Data Protection of the Republic of Moldova" funded by the European Union.

49034
Views on the
NCPDP website
in 2020

During 2020, were developed and published on the Centre's website www.datepersonale.md. – 80 media articles. At the same time, during the reference period, the Center developed and published four quarterly newsletters, including statistical information about the Centre's activity, as well as useful and current information at national and international level in terms of personal data protection.

During the reference period, about the activity of the Center was mentioned in about 70 media articles. The figure has halved from the previous year amid the pandemic crisis, which has led to the suspension of several events of the Center. Among the media sources that covered the activity of the institution were: Agora, Moldpres, TVR Moldova, Moldova1, Bizlaw, Sputnik Moldova, privesc.eu, Agenția de știri – Info Prim Neo, Curentul.md, Noi.md, tribuna.md, Radio Chișinău, democracy.md, Ziarul Moldova Suverană, publika.md, TV8.md, jurnal.md.

14712
Views on
Facebook/
NCPDP in 2020

The increasing interest of the citizens towards to the activity of National Authority for personal data protection is also deduced from the online environment. In context, the official Facebook page of the Center – www.facebook.com/CNPDCP, according to the posts, it registers about 1500 visitors, monthly. The number of followers it is also on the rise – 2338 with 37% more in 2020 compared to 2019.



CHAPTER IX

HUMAN RESOURCES MANAGEMENT

IX

The staff is the most valuable resource of the Center, which actively contributes to increase the efficiency and effectiveness of the institution. Thus, the support, stimulation and appreciation at the fair value of the employed staff are the essential factors for maintaining a positive organizational and psychological climate at work.

The National Authority of personal data processing carries out its activity through the staff that ensures the achievement of the public interest in the field of competence, namely, officials of public dignity, civil servants and auxiliary staff.

The director and the deputy director exercise functions of public dignity that fall under the incidence of Law no. 199/2010, and the activity of civil servants is regulated by Law no. 158/2008 on the civil service and the status of the civil servant. The rights and responsibilities of auxiliary staff are set out in labor law.

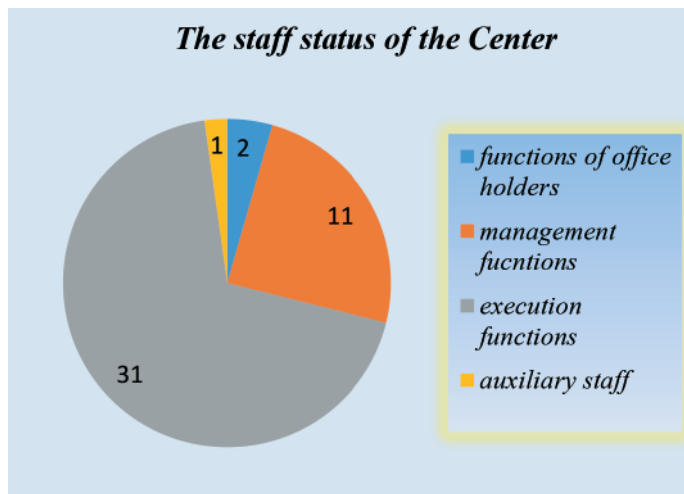
When performing the tasks, the staff of the Center takes into account the public interest in the field of personal data protection, in accordance with the provisions of the Law on personal data protection no. 133/2011.

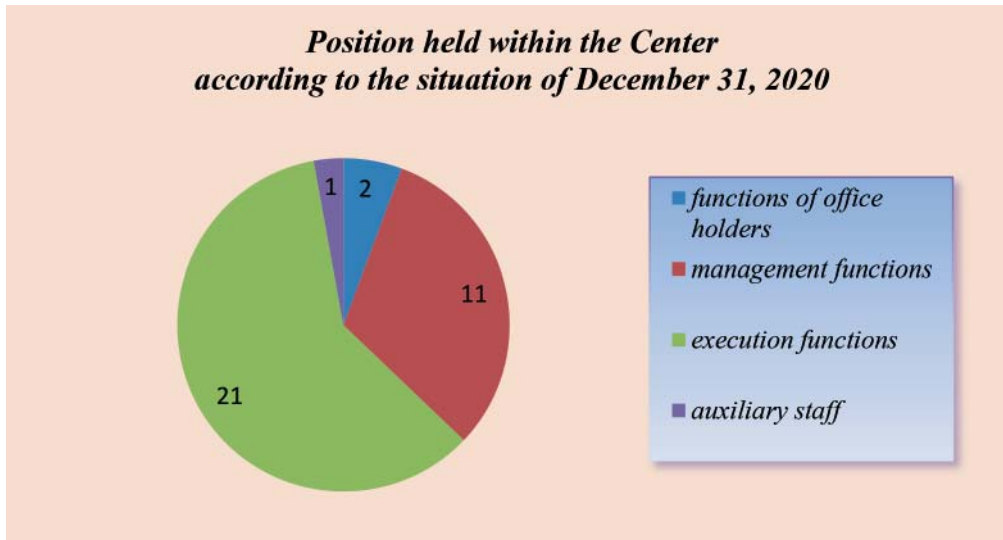
According to Law no. 182/2008, the structure of the Center consists of 8 structural subdivisions, and the limit staff is 45 units which are distributed as follows:

- 2 functions of office holders (director and the deputy director) ;
- 42 public functions; including 11 – management functions and 31 – execution functions;
- 1 – Auxiliary staff (driver).

Thus, on December 31, 2020, the total number of the Centre employees constituted 35 staff units, with an occupation rate of only 77, 8%, of which:

- 2 functions of office holders;
- 32 public functions; including 11 – management functions; 21 – execution functions of which 16 are inspector (main state inspector – 4, senior state inspector – 4, state inspector – 8), 3 consultants (main – 1, senior – 1, consultant – 1) and 2 main specialists;
- 1 – Auxiliary staff (driver).





Thus, compared to the previous reporting year, the occupation rate of positions increased by approximately 3.8 percentage points.

Degree of employment with staff in the period 2018-2020

Year	Approved units	Effectively, employees	Share, %
2018	45	32	71
2019	45	33	73
2020	45	35	77,8

The Center has advocated and continues to advocate for a policy of gender equality and equal treatment between men and women in the process of recruiting and managing human resources. However, out of the total number of employees, at the end of the reference period, the share of men was 40%, and that of women, respectively, 60%.

In this context, the diagram below shows that the share of women is higher than that of men, both in the performance of executive and managerial positions.





The staff of the Center is relatively young, and the average age of employees in 2020 was 36 years. As in the previous year, in the structure by age categories, the highest share of people aged between 35-45 years (40% of the total) and those aged 25-35 (31.4% of total).

The employment of young specialists within the Center is a continuous phenomenon, positively influencing the structure of the age profile of the staff, and only this fact, unfortunately, does not bring a positive influence on the activity of the authority. Thus, there is an increase in the share of employees under the age of 25, which is 5.7% of the total number of employees, being twice as high compared to 2019. The other age groups had lower weights.

Center staff by age categories

Year 2020	Total effective persons	Functions of office holders	Public management positions	Public execution functions	Auxiliary staff
Number of persons	35	2	11	21	1
• < 25 years old	4	–	–	4	–
• 25-35 years old	11	–	1	10	–
• 35-45 years old	14	1	7	6	–
• 45-55 years old	4	1	2	1	–
• 55-63 years old	1	–	1	–	–
• 63 years old <	1	–	–	–	1

The youngest employee in 2020 was 24 years old and the oldest corresponding – 65 years old.

The recruitment policy of the Center aims to ensure the optimal need for staff based on the principles of open competition, transparency, equal opportunities and professional merit. These principles are necessary for the recruitment of staff who will achieve the objectives proposed by the authority in the future.

During the reference period, were organized and held 8 contests for filling the vacant public positions, out of which 2 extended competitions.

Here it should be underline that 4 contests were suspended for a period of more than 2 months, in connection with the establishment of the state of emergency situation in public health, in the Republic of Moldova, based on the epidemiological situation both in the country and worldwide, as well as in order to implement measures to prevent and control new type of Coronavirus infection (COVID-19), after being resumed.

In 2020, 11 vacant and temporarily vacant public positions were put up for competition, out of which 1 management position and 10 executive positions, such as: 1 position of Head of Information Service, Media Communication and e-Transformation, 4 positions of state inspector in the Conformity Department, 2 positions of inspector in the Prevention, Surveillance and Evidence Department, 1 consultant position in the External Relations and European Integration Department, 1 consultant position in the Human Resources Service, 1 position of main specialist in the Documentation Service and Archivist and 1 position of internal auditor in the Internal Audit Service.

For participation in competitions were submitted 68 candidates' files. In order to ensure the transparency of the contest organization process, the information on the organization and conduct of the contests was published on the institution's website (www.datepersonale.md) and on the government website (www.cariere.gov.md).



Therefore, as a result of the competitions held, 9 people were hired, of which 7 were civil servants debutants. During the reporting year, 3 civil servants debutants were confirmed in public functions, obtaining the qualification “good” when evaluating the activity spend of the probationary period, at the same time being awarded the qualification degree “counselor of the class III “. It should be mentioned that the other 4 civil servants debutants are to be evaluated and, as the case may be, confirmed in the public positions held, in the first semester of 2021.

As in previous years, the Center faces the problem of the lack of an internal auditor. Already for several years, starting with 2017, the internal audit function was permanently exposed to competition, but without results, due to the lack of candidates, due to the disproportionate correlation between the salary level, related to the workload and responsibilities requested in the job description.

At the same time, it should be mentioned that the competition for filling the vacant public position of consultant in the Human Resources Service was canceled, because the winner of the competition refused to enter the public position, the reason being the unattractive salary. In 2021 this contest will be resumed.

At the same time, it should be specified that, on the basis of merit, 4 employees were promoted to senior positions, 2 civil servants were transferred to other subdivisions of the Center, for service purposes and 2 civil servants ensured and continue to provide up to currently the interim of 2 management positions, during the suspension of the service relations of the incumbents.

In 2020, there is a lower **staff turnover** compared to 2019, the number of people whose employment relationships ended was 6, compared to 8 in the previous year, of which 2 persons transferred to other public authorities, and the other 4 resigned upon request.

It should be mentioned that the staff turnover with tasks and control attributions within the Center are maintained this year as well, thus registering a share of 50% of the total number of resigned. This increase was caused by the level of irrelevant pay in relation to the complexity of the activity of verifying the legality of the personal data processing.

Fluctuation phenomenon at a very high level, which increases the risk of loss of institutional memory and distortion of the work of the institution, is determined by shortcomings in legislation on wages. Thus, the reference salary of the Centre’s employees is approximately 50% lower compared to the salary granted within other entities in the budgetary sector with similar activities and competencies.

Moreover, after investing considerably in the good professional training of employees, in raising the level of knowledge, skills and job skills required, especially in the field of competence, employees decide to go to other public authorities for a more attractive salary. As an example, currently, 3 of the former employees of the Center work within the National Integrity Authority, a much more attractive entity in terms of salaries offered to its employees.

An important element in the human resources management policy is the trend of continuous professional development of employees. In this regard, the annual professional development plan was developed, according to which the employees of the National Authority for Personal Data Protection attended 5 internal training courses and 17 external training courses. Thus, the number of training hours of the participants was 474 astronomical hours.

The continuous professional development of the civil servants within the Center in the reference year was mainly achieved at the Academy of Public Administration, through training activities carried out less normally than in previous years, in connection with the situation caused by the COVID-19 pandemic.

Thus, the professional development courses took place in different formats:

- In the classroom (off-line);



- Remote (online);



- mixed: distance through the “e-Learning Platform”, as well as with the physical presence on the last day of the course at the Academy of Public Administration.



At the Academy of Public Administration, which is the provider of training services and the center for promoting state policy in the field of professional development of civil servants of all levels, 18 employees of the Center participated in 16 professional development courses, obtaining professional development certificates in the following competencies: *Professional integration in public office, Professional ethics and integrity, Efficiency of professional activity in public administration, Development and coordination of draft regulations, Conflict management, Public service management, Strategic and operational planning in public administration, Effective management of stress at work.*

At the same time, 2 employees of the Center participated in the Workshop entitled “Cyber Incident Management”, organized by P I. “Information Technology and Cyber Security Service” in partnership with I.P. “Electronic Government Agency” and the Estonian e-Government Academy.



A strong emphasis in 2020 was on internal employee training. Thus, in the context of the global pandemic, the Center's management periodically trained staff on key measures in the prevention and mitigation of COVID-19 infection in the workplace. In this regard, has been developed a guide with concrete rules to help employees to maintain their health and safety at work.

Similarly, it should be noted that general introductory training in occupational safety and health, including new employees, was also provided. Likewise, during the reference period, other internal professional development courses with various topics were carried out, such as: "use of electronic signature", "use of the Centre's website (www.datepersonale.md)", etc.

During the reporting year, for the efficient exercise of the attributions, special merits in activity, manifestation of the spirit of initiative and special contribution in accomplishing specific tasks, for long and impeccable activity within the institution, as well as on the occasion of the Civil Servant's Day, an employee of the Center was awarded the Government Diploma.

In order to ensure an efficient management of human resources in 2020, 391 internal administrative acts were elaborated, related to the labor relations of the employees, as well as a series of internal documents that regulate the activity of different commissions, such as: Gift evaluation and record commission, Discipline commission, etc.



CHAPTER X

ECONOMIC-FINANCIAL ACTIVITY

X

ECONOMIC-FINANCIAL ACTIVITY

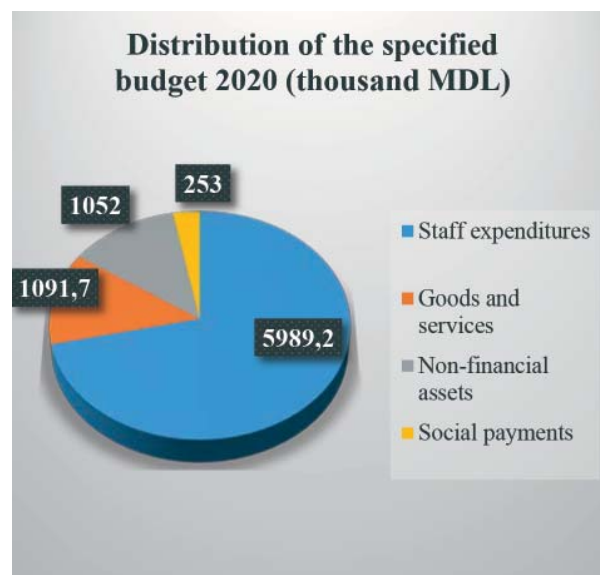
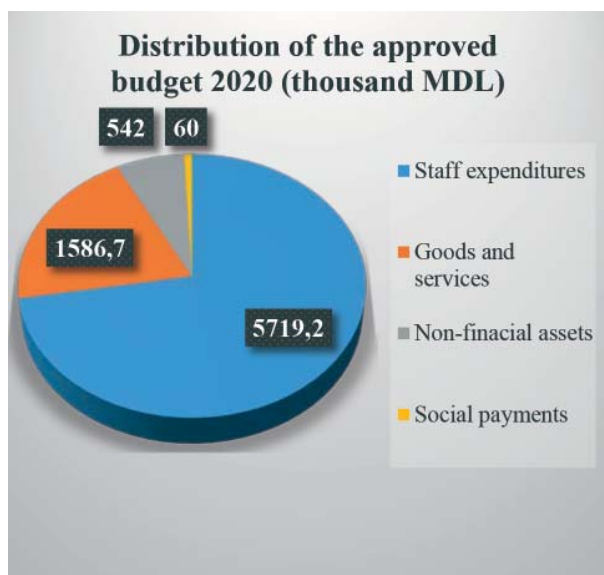
The budget of the Center was elaborated according to the provisions of the Public Finance Law and the budgetary-fiscal responsibilities no. 181/2014 and the rules established by the Ministry of Finance. According to the Law on the State Budget 2020 no. 172 /2019, for the Center was approved the total budget of **7 907, 9** thousand MDL, the general resources component.

At the same time, by Government Decisions no. 854/2020 and no. 896/2020 on amending the Law on the state budget for 2020, the Centre's allocations were increased by 70.0 thousand MDL and, respectively, with 200,0 thousand MDL, in order to partially cover the expenses for the implementation of the provisions of Law no. 270/2018 on the unitary salary system in the budgetary sector, in the chapter "labor remuneration", as well as for paying the annual award to the staff from budgetary units for activity results in 2019, established by Government Decision no. 811/2020.

In addition, they allocated to the Center financial means in the amount of 208.0 thousand MDL for granting the single allowance to employees infected with COVID-19 during the exercise of their duties, in accordance with Law no. 69/2020 on the establishment of measures during the emergency period in public health, according to Government Decision no. 895/2020.

Thus, the **specified budget** of the Center for 2020 constituted **8,385.9 thousand MDL**.

Analysis of budget allocations for 2020



As of December 31, 2020, the Centre's budget was executed in the amount of 7 583, 3 thousand MDL, which constitutes 90, 4% of the specified budget, being increased compared to the period 2017-2020.

**Budget execution in the period 2017-2020**

The financial means allocated from the state budget were directed to cover the expenses necessary for the maintenance of the activity of the National Authority for Personal Data Protection in the following directions:

Execution of expenses in 2020 (thousand MDL)

Approved	Approved	Specified	Executed	Executed compared to specified (%)
Staff expenditure	5719,2	5989,2	5946,3	99,3
Goods and services	1586,7	1091,7	775,6	71,1
Social payments	60,0	253,0	249,1	98,5
Non-financial assets, inclusive:	542,0	1052,0	612,3	59,0
<i>fixed assets</i>	217,0	807,0	413,1	51,2
<i>stocks of circulating materials</i>	325,0	245,0	199,2	81,3
TOTAL	7907,9	8385,9	7583,3	90,4

In the structure of expenses, the largest share is held by “staff expenditure”, but it should be specified that the financial means allocated in the amount of 5,719.2 thousand MDL were insufficient to remunerate the work of employees, as well as to pay the annual award for the results of the activity from 2019. Thus, as a result of submitting the corresponding approach to the Ministry of Finance, the specified allocations amounted to 5989,2 thousand MDL.

The budget specified in the chapter “goods and services” amounted to 1 091, 7 thousand MDL. The expenses executed in this category were of 775,7 thousand MDL, forming an unused balance in the amount of 316,0 thousand MDL. This has led to savings in rental services, business travel and other services.

In the chapter “social payments” were initially approved allocations in the amount of 60, 00 thousand MDL. However, following the allocation of financial means from the Government’s reserve fund in the amount of 208, 0 thousand MDL (payment of the single allowance to employees who became infected with COVID-19 during the exercise of their duties), the specified allocations increased to 253,0 thousand MDL.

With the change of the structure of the Center and the increase in 2017 of the staff limit, there was a need to expand the workspace, which was achieved only in the middle of 2020.



In this sense, the Center received in use additional space located on the fourth floor of the headquarters where it operates, in order to ensure the optimal conditions for the proper conduct of business and the performance of basic duties. Thus, goods (furniture, computer technology, etc.) were purchased, expenses reflected in the chapter “**non-financial assets**”.

In accordance with the Government Decision no. 1419/2016, the **public procurement Plan** for 2020 of the institution was developed and published on the website of the Center: <https://datepersonale.md/wp-content/uploads/2020/02/Planul-de-achizitie-2020.pdf>.

In order to carry out this plan, during the reference period, 35 public procurement contracts were concluded, of which:

- 34 low value contracts for the purchase of goods and services;
- 1 contract through the negotiation procedure without prior publication of a notice of participation, related to the technical administration services of SIA “Register of evidence of personal data controllers”.

It should be mentioned that, point 11 letter f) of the Government Decision no. 883 of 25.11.2011 regarding the approval of the Technical Concept of the automated information system “State Register of personal data controllers”, stipulates that S.I. “Special Telecommunications Center”, currently I.P. The “Information Technology and Cyber Security Service” has the quality of an entity that will provide the assistance and technical means necessary for the implementation and operation of the Register, will represent the entity that will take over the IT solution and will assist the implementation and administration of this IT system.

All contracts were registered with the State Treasury.

It should be noted that, at the conclusion of low value contracts, factors such as: the timeliness of expenditure and the lowest price criterion, together with carefully established technical requirements, were taken into account, which led to the efficient use of financial resources allocated to the Center.

The application of public procurement procedures ensured the contracting of qualified and experienced economic controllers in the field of execution of public procurement contracts.

All procurement contracts concluded to ensure the needs of the Center were executed in full and on time.



PROBLEMS AND OBJECTIVES

Problems faced by the Center

Regrettably, over several reporting periods already reveals the same spectrum of concerns / issues faced by the National Authority for Personal Data Protection. It should be noted that the major concerns reflected from year to year, including in the activity reports of the Center, generate increasing impediments both in the institutional and organizational activity and in the development of personal data protection field at national level. However, given that solving the pressing problems facing the Center is largely beyond the competence of this authority, it becomes even more difficult to ensure the development of the area of competence.

In this sense, **the legal, institutional, perception and applicability issues**, which require a rigorous solution in order to overcome the stagnation of personal data protection field at national level, are the following:

- **disparity between the national legal framework in the field of personal data protection and the new regulations existing at European level, namely**, 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 and 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.
- **discriminatory salary level of the civil servants within the Center** as compared to the one provided to other supervisory bodies, with similar status, and taking into account the specific activities that undoubtedly presume the processing of personal data, are subject to verification of legality of data processing by the Center. As example may be mentioned the following entities: Security and Intelligence Service, Ministry of Internal Affairs, Prosecutor's Offices, National Anti-Corruption Center, National Integrity Authority, Anti-Money Laundering Service, etc.;
- **the small number of employees of the Center according to the staffing of 45 units, in relation to the increasing workload**, especially in the basic subdivisions of the authority: the General Department for Surveillance and Conformity, the Legal Department, especially in the context of investing recent years with multiple additional responsibilities (for example through: the Law on electronic communications, the Law on the prevention and combating money laundering and terrorism financing, the Law on the prevention and combating of terrorism, etc.), without being created / assured and reliable institutional mechanisms for carrying out the prescribed tasks;
- **staff turnover** and insufficiency/lack at national level of qualified specialists in personal data protection field;
- **the inefficiency and insufficiency of the coercive levers for the unlawful processing of personal data**, the reason being the double, contradictory and susceptible character of the procedures for examining the findings resulting from the checking lawfulness of the processing of personal



data, manifested by doubling examination in court, in the same period, the same documents and findings issued by the Center, both in administrative order and in contravention procedure. Or, the decisions issued by the Center according to art. 27 of the Law on personal data protection, which establishes a violation of the legal provisions in the field of personal data protection, on the one hand are subject to challenge in administrative litigation order, and on the other hand, they serve as a basis for establishing the contraventions facts and the preparation of the minutes regarding the contravention, which is sent for examination in the court. Thus, besides the fact that for committing the same act / violation, the controller is subject to liability / sanction 2 times – circumstances contrary to the principles of individualization and subject to liability, there are also situations in which, same controller, for the same offense, in contravention order the controller was convicted by the court, while, in administrative contentious order, he was declared innocent, with the annulment of the Center's decisions or vice versa. However, the situation described is even more bizarre considering the fact that in both cases (the contravention procedure and the administrative contentious procedure) at the base there was the same decision to find the infringement committed in the processing of personal data. In this context, the existence of such contradictory procedures led, in some cases, in determining the inefficiency of the actions taken by the Center to counteract non-compliant data processing and to prevent the committing of other violations concerning the right to the inviolability of the intimate, family and private life of personal data subjects. However, the circumstances described are even more bleak and disarming for the National Authority for the control of personal data processing, taking into account the number of employees of the Centre sub-divisions, which is minimal in relation to the excessive volume of work.

- ***abusive use, in particular by representatives of public authorities, of the legal provisions in the field of personal data protection***, the alleged argumentation of the refusal to present the requested information through the realization of the right of access to information;

- ***lack of mechanisms, procedural guarantees and effective control in the case of law enforcement bodies*** when carrying out special investigative measures, ***which would ensure a fair balance between the interest of the prosecuting body to accumulate certain evidence and the rights of the personal data subjects concerned***. For example, there is no record of the fact whether personal data subjects who have been subjected to special investigative measures have been granted the right to be informed in this regard or if it was restricted informing them and the reasons that led to the postponement of informing, etc. However, at present there is no mechanism for post-factum information of personal data subjects on their telephone interception or on the conduct of other special investigative measures against them, or the obligation to exercise the rights of personal data subjects, once with the exhaustion of the purpose for which these rights have been restricted (the right to information, access to data, etc.) is provided both by art. 15 of the Law on personal data protection as well as by the legal provisions specific to the field of activity (Criminal Procedure Code, Law on the special activity of investigations, etc.). In this context, it is worth mentioning the **non-existence of an electronic register** of telephone interceptions, electronic communications or other special investigative measures, such as wiring, etc., **the establishment of which would be an effective solution to overcome the deficiencies indicated above**. The more detailed information on the given topic is highlighted above, in the section Activity for the prevention of non-compliance of personal data processing;

- ***the huge number of personal data access operations stored in state automated information resources, carried out in the absence of a legal purpose*** and basis, in particular by employees of law enforcement agencies, as well as the ***lack or insufficiency of measures necessary to implement in order to keep efficient records of personal data processing operations***. More information regarding the aspect of tests is reflected above, in the section Activity for the prevention of non-compliance of personal data processing.



Objectives for the year 2021

The basic objectives of the Center for the year 2021, but without limiting those described below, will focus on:

- ensuring **compliance of the national legal framework in the field of personal data protection with the new regulations at European level**, by approving by the Parliament of the Republic of Moldova in final reading two draft laws: on personal data protection and on the National Center for Personal Data Protection. At the same time, following the achievement of the objective, it is necessary to elaborate and implement the normative and internal framework related to the implementation of the new legal provisions;
- ensuring **the salary increase of the Center's staff**, linked to that provided for other control bodies of similar status, which, having regard to the specific nature of the activity, are subject to verification of the data processing legality by the Center;
- **increase of the staff limit** of the National Authority for the control of personal data processing, **in relation to the workload and competencies assigned to the Center**, or, based on the current specific activity, for a good development of legal competencies it is necessary to increase staff up to 150 units;
- further fulfilling of the Action Plan for the implementation of the Association Agreement Republic of Moldova – European Union;
- continuation and enhancement of actions to **raise awareness of the importance of personal data protection**, both from the point of view of respecting the rights of the data subjects and from the perspective of ensuring the implementation of the obligations related to the personal data controllers;
- contributing **to raising the level of correct interpretation and compliance with the legal provisions in the field of personal data protection** by the actors involved in the processing of personal data, including by ensuring the balance between the legal provisions related to the rights of access to information, the freedom of expression and the personal data protection;
- contributing to the **creation of an uniform judicial practice** on the application of provisions of legislation on personal data protection;
- raising awareness the development partners in carrying out joint projects, in order to ensure the adequate level of personal data protection in the Republic of Moldova.