CENTRUL NAȚIONAL PENTRU PROTECȚIA DATELOR
CU CARACTER PERSONAL AL REPUBLICII MOLDOVA

ACTIVITY REPORT FOR THE YEAR 2023

NATIONAL CENTER FOR PERSONAL DATA PROTECTION OF THE REPUBLIC OF MOLDOVA

ACTIVITY REPORT FOR THE YEAR 2023

CONTENTS

WHO ARE WE?

The National Centre for Personal Data Protection (NCPDP) is an autonomous public authority, independent and impartial from other public authorities, natural persons and legal entities, which exercises its legally awarded attributions by the Law no. 133/2011 on personal data protection.

The NCPDP aims to protect the fundamental freedoms and rights of natural persons, especially the right for private life regarding the processing and cross - border transfer of personal data.

In its activity, the NCPDP is guided by the Constitution of the Republic of Moldova, by the Convention for the protection of individuals with regard to automatic processing of personal data, by the Additional Protocol to the Convention, by other international agreements that the Republic of Moldova is part of, by the Law on personal data protection, the Law No. 182/2008 on the approval of the National Center for Personal Data Protection Regulation, structure, staff-limit and its financial arrangements, as well as other normative acts.

MISSION

The NCPDP contributes to protect the privacy of citizens and to ensure compliance with data protection legislation being assigned with the following tasks:

INFORMATION AND GUIDANCE BY:

- raising public awareness in order to understand the risks, rules, safeguards and rights relating to personal data processing;
- raising the awareness of data controllers and processors regarding their obligations.

CONSULTATION THROUGH:

- submitting proposals for the improvement of existing legislation in the field of processing and personal data protection;
- informing public authorities about the situation in the field of personal data protection, as well as responding to their requests and complaints;
- promoting best practices and publishing thematic recommendations;
- providing advice on the implementation of data protection impact assessments and prior consultation;
- providing data subjects with information on their rights.

SURVEILLANCE AND TRANSPARENCY THROUGH:

- monitoring compliance with personal data protection legislation;
- issuing the necessary instructions to bring the processing of personal data in compliance with the law;
- checking the compliance of the personal data processing with the requirements of the law on the basis of complaints or in case of self-reporting;
- issuing decisions finding no breach or a breach of personal data protection law, with the ordering of corrective measures where necessary;
- establishing contraventions and drawing up minutes of contravention in accordance with the Contravention Code.

COOPERATION WITH:

- similar supervisory bodies from abroad, international organisations and work towards strengthening relations with them in order to harmonise national legislation with international legal instruments and to implement best practices.

OVERVIEW

Year 2023 in numbers

REQUESTS/COMPLAINTS

12695 correspondence documents:

4434 inbox
5163 outbox
2002 internal
1096 complaints

ACTIVITY OF CONTROL

356 initiated controls
318 issued decisions
236 decisions of the absence of violations found
187 decisions of violations found
107 cases of contraventions found
117 minutes drawn up

ENDORSEMENT ACTIVITY OF DRAFT NORMATIVE ACTS

154 approved proposals
37 draft agreements/ international treaties;
31 draft normative acts amending laws, codes;
86 draft normative acts of the Government and other authorities

ACTIVITY OF THE REPRESENTATION IN THE COURTS

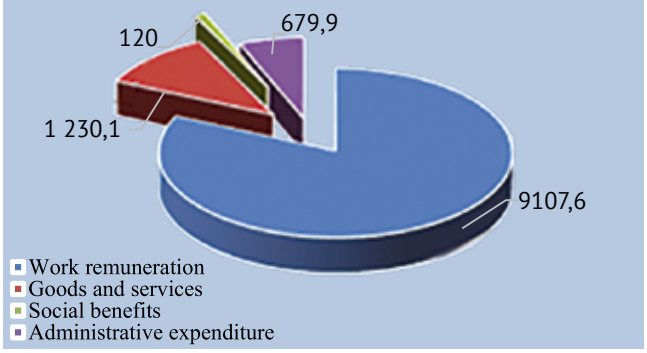
545 court proceedings:

386 in contravention proceedings
159 in administrative litigation

PREVENTION ACTIVITY

115 entities with designated data protection officers;
45 trained DPO

Specified budget for year 2023, thousands of MDL



HUMAN RESOURSES

32 out of 45 staff-limit
3 competitions held

8 persons employed / 5 debutants
6 persons resigned
20 training courses

TRAINNING AND AWARNESS ACTIVITY

3795 trained persons
61 training activities
6 information and awareness-raising activities

119 elaborated and published press releases

CHAPTER I

EXAMINATION OF COMPLAINTS AND OTHER REQUESTS

During 2023, the NCPDP continued its actions aimed at raising public awareness of the risks, rules, safeguards and rights related to personal data processing, as well as of data controllers/ processors about their obligations in relation to personal data processing. The statistical analysis of the correspondence documents registered during 2023, reflects the increasing public interest in the field of personal data protection and its careful monitoring of the developments recorded, which is also a sign of confidence in the performance of the tasks and duties entrusted to the NCPDP by Law No 133/2011 on personal data protection.

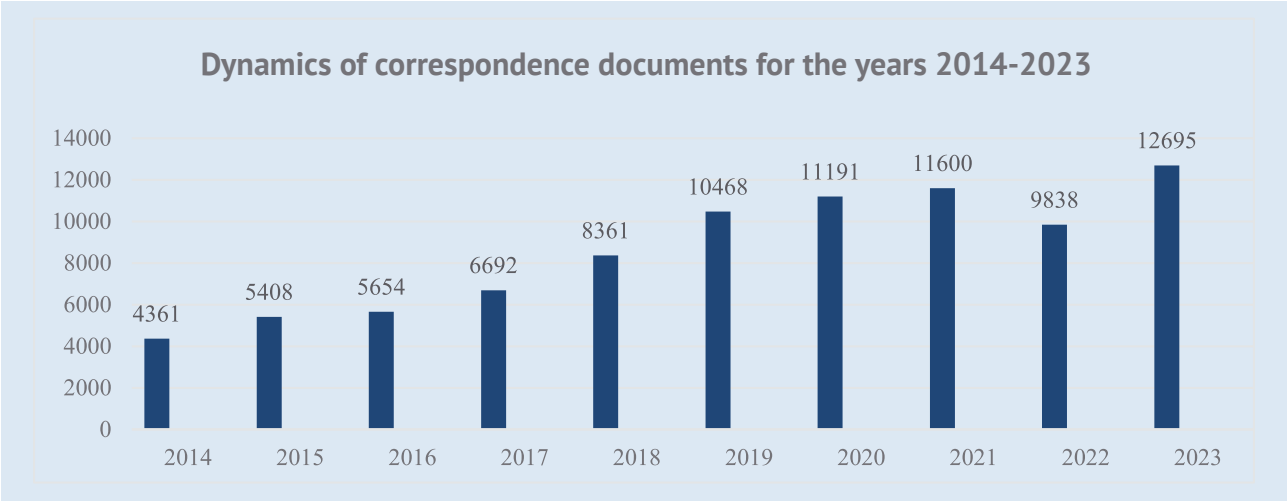
Thus, the reporting period was marked by a significant number of addresses relating to personal data processing received both from individuals, as data subjects, and from various actors in the public and private sector on various subjects regarding the compliance of peronal data processing, on issues of legality, the enforcement of data subjects' rights, the timing of data storage, cross-border data transmissions, etc.

During 2023, NCPDP examined **12695** correspondence documents, including **4434** inbox documents, **5163** outbox documents and **1096** complaints of personal data subjects.

Comparative statistics of correspondence documents, for the years 2014-2023

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
2021	11600	5083	4549	860	1108
2022	9838	3529	4045	825	1439
2023	12695	4434	5163	1096	2002

The dynamics of the number of correspondence documents registered by the NCPDP during 2014-2023 can be analysed in the below diagram.



The year 2023 reflects an increase in the flow of documents examined within the NCPDP, marked not only by the growing number of complaints received by the NCPDP, thus attesting to an awareness on the part of natural persons regarding issues related to the protection of their personal data, but also by the number of documents drafted and submitted by the NCPDP as a result: the submission of proposals on the improvement of the legislation in force on the segment of processing and personal data protection; the information provided to data controllers on the correct implementation of the legal provisions in this field; the controls carried out on the compliance of personal data processing with the requirements of the law; the information requested in connection with the conduct of the control activity; the procedural documents drawn up and submitted to the courts both in the administrative litigation and in the contravention procedure; the complaints submitted on the problematic issues identified; the training actions carried out on the basis of the requests received, as well as on the initiative of the authority; the actions to promote the field, organised in collaboration with external and internal partners from both the public and private sectors.

The analysis of the topics addressed in the correspondence documents reveals individuals' concern about the scale of the use of information technologies, which creates new challenges for personal data, especially in the context of consultation/access, collection, disclosure in the public domain and exchange of personal data, the number of which is increasing significantly. As technology enables both private entities and public authorities to use personal data to an unprecedented scale in their activities, individuals are increasingly looking for control over their personal data and guarantees to ensure their security and privacy. At the same time, there is a growing trend to ensure that a fair balance is maintained between the right to personal data protection and the rights guaranteed by the Constitution of the Republic of Moldova, such as: the right of access to information, the right to freedom of expression, honour, dignity and professional reputation, etc.

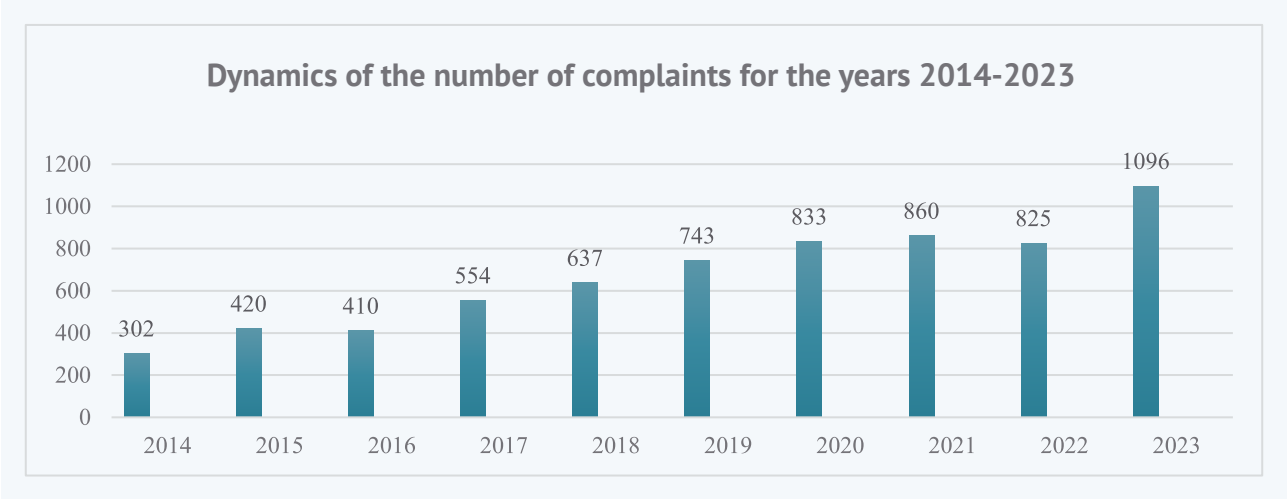
The public interest in the protection of personal data, resulting from the volume of correspondence, reflects the fact that the Law on personal data protection and the rights and obligations arising from it, shows a growing concern for data subjects. This increased awareness of the regulations is also reflected in the number of complaints and inquiries received by the NCPDP from individuals who consider that the processing of their data does not comply with the requirements of the law.

At the same time, the dynamics and specificity of correspondence documents demonstrate, above all, the need for dialogue to resolve increasingly complex and latest issues, sometimes requiring legislative or regulatory intervention.

Activity of examination of personal data subjects' complaints

During the reporting period, **1096** complaints were received by the NCPDP from natural persons - personal data subjects.

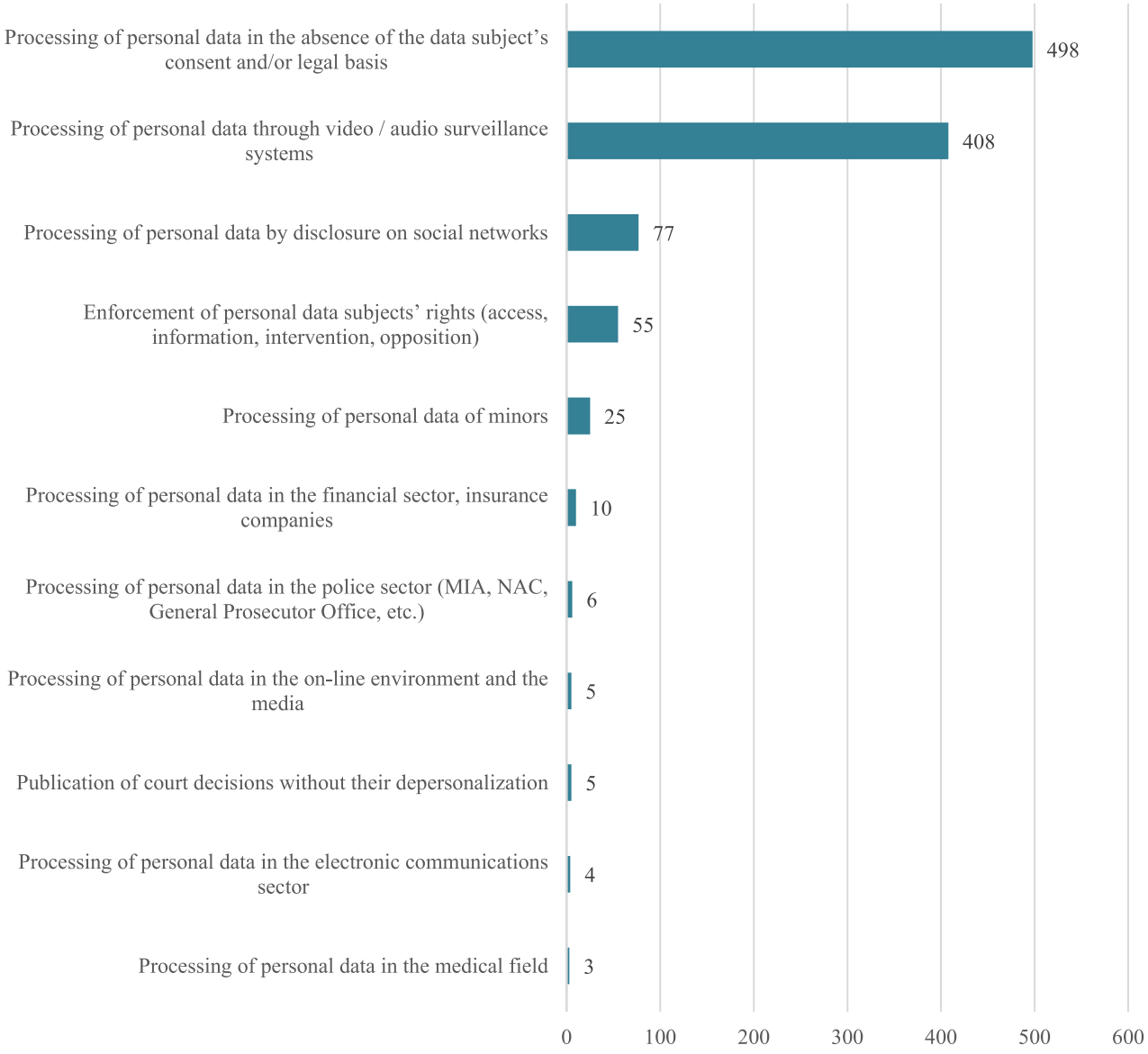
From the total number of complaints registered in the reporting period, in **356** cases, controls on the compliance of personal data processing were initiated.



Thus, in 2023, the complaints received by the National Personal Data Protection Authority mainly concerned the following topics:

- ✓ Processing of personal data in the absence of the data subject's consent and/or legal basis: **498** cases;
- ✓ Processing of personal data through video / audio surveillance systems: **408** cases;
- ✓ Processing of personal data by disclosure on social networks: **77** cases;
- ✓ Enforcement of personal data subjects' rights (access, information, intervention, opposition): **55** cases;
- ✓ Processing of personal data of minors: **25** cases;
- ✓ Processing of personal data in the financial sector, insurance companies: **10** cases;
- ✓ Processing of personal data in the police sector (MIA, NAC, General Prosecutor Office, etc.): **6** cases.
- ✓ Publication of court decisions without their depersonalization: **5** cases;
- ✓ Processing of personal data in the on-line environment and the media: **5** cases;
- ✓ Processing of personal data in the electronic communications sector: **4** cases;
- ✓ Processing of personal data in the medical field: **3** cases;

General situation regarding the complaints under examination in 2023



CHAPTER II

ACTIVITY OF CONTROL

In order to ensure consistency in the monitoring and enforcement of the Law on personal data protection, the NCPDP has established effective tasks and powers, including powers to carry out controls on the compliance of the processing of personal data with the requirements of the legislation in force, in particular when processing complaints submitted by individuals, powers to apply coercive measures as well as contraventions, powers to advise and participate in judicial proceedings. Thus, in the event of a finding a breach of personal data protection legislation, the NCPDP may order, as appropriate, the suspension, cessation, rectification, blocking or destruction of unlawful or illegally obtained data.

The NCPDP is exercising its powers to control the lawfulness of personal data processing in accordance with the appropriate procedural safeguards provided by the legislation in force, in particular the Law on personal data protection, the Administrative Code and the Contravention Code, impartially, fairly and within a reasonable time. Appropriate, necessary and proportionate measures shall be taken in the examination of each case in order to ensure compliance with the provisions of the law, taking into account the circumstances of each individual case, while respecting the right of any person to be heard or to present separately his/her views on the matters alleged in the complaint, before any individual measure is taken which might adversely affect him/her, thus ensuring that unnecessary costs and excessive inconvenience to the parties concerned/ affected by the case under examination are avoided. Each legally binding measure/ decision taken by the NCPDP is set out in written form, is clear and unambiguous, sets out the reasons for the finding no violation or finding a breach of personal data protection law, with an order, where necessary, for the suspension, cessation of personal data processing, rectification, blocking or destruction of unlawful or illegally obtained data and refers to the right to an effective remedy.

The procedure for receiving and handling complaints by the NCPDP is laid down in Article 27 of Law on personal data protection, according to which:

(1) Personal data subjects who consider that processing of their personal data does not comply with the requirements of this law, may address a complaint to the Centre within 30 days from the date of detecting violations with the prior realization, as the case may be, of the rights provided in art. 12, 13, 14, 16 and 17. If the subject of personal data fails to exercise his rights, as well as other important aspects related to the presentation of relevant evidence, the Center shall inform him within 30 days from the date the complaint was received.

(2) In the process of settling complaint, the Centre may hear the personal data subject, the controller and, as the case may be the processor, the witnesses and may order the conduct of an unscheduled control.

(2^1) The term for examination and settlement of the complaint submitted in compliance with par. (1) is 3 months, with the possibility of justified extension 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 concerned party, but not more than 6 months. After obtaining all the information

and analyzing it, the Center completes the examination and settlement of the complaint within a maximum of 30 days. If the object of the complaint exceeds the scope of this law, the complaint is not examined, a fact about which the subject of personal data is informed. Ensuring compliance with the deadline for examining and resolving complaints is the responsibility of the Centre's staff, and the control over compliance with the deadline is the responsibility of the heads of the Centre's subdivisions. The Center shall inform the subject of personal data regarding the progress in the examination and settlement of the complaint in case of an extension of the deadline for the examination and settlement of the complaint or at the request.

(3) Following the complaint examination, the Centre shall issue a grounded decision either on no violations of the legal provisions, or on the suspension of personal data processing operations, or on rectification, blocking or destruction of inaccurate data or obtained unlawfully. In case of the absence or insufficiency of the evidence proving the infringement, the Center shall ascertain, by reasoned decision the lack of infringement. The decision regarding the finding of the violation of the legislation in the field of personal data protection and the accumulated evidence serves as a basis for drawing up the report on the contravention, under the Contravention Code of the Republic of Moldova.

(3^1) The decision shall be issued by the Director of the Center, the Deputy Director and the Center authorized staff with control functions, in accordance with the powers assigned by order of the Director. The decision shall be communicated to the data subjects within 10 working days from the date of issue by any means that confirms its receipt.

(4) Provisions of paragraphs (2)-(3^1) shall apply appropriately where the Centre takes action ex officio with regard to the commission of a violation of the personal data subjects' rights acknowledged by this law.

(5) The controller, the processor or personal data subject may appeal the decision of the Centre to the competent administrative court.

In this context, the procedure of prior realisation, where necessary, of the rights provided by the Law on perosnal data protection is relevant.

It is pointed out that Articles 12-14, 16-17 of Law No 133/2011, enshrine personal and inviolable rights (right to information, right of access, right to intervention, right to object, right not to be subject to an individual decision), which the data subject realizes on his own, giving to the latter not only the possibility to have control over his personal data, but also to remedy jointly with the controller any uncertainty regarding the alleged non-compliance, if he considers that certain data processing operations carried out by certain controllers are unlawful.

After exhaustion of the access remedy, or if personal data controller/processor refuses, without justification, to provide relevant information or to respond to the data subject's request(s), the data subject is entitled to appeal his/her actions or inactions to the NCPDP.

On the basis of the above-mentioned reasoning, after receiving the information on the audit of personal data processing operations in state information resources (for example: from the Public Services Agency, the e-Government Agency, the Ministry of Internal Affairs, etc.) the personal data subjects should address personally to the controllers/processors who carried out the access to personal data for the purpose of realizing the rights guaranteed by the Law on personal data protection, in particular the right of access to personal data, including for requesting information on the purpose and legal basis of access to personal data from state information resources.

The complaint addressed to the NCPDP shall include all the details, including material/ evidential documents, regarding the steps taken in order to realize, as personal data subject, the rights provided for by Law No 133/2011, in relation to the alleged personal data controllers/ processors. However, in the case of complaints from personal data subjects submitted to the NCPDP without first addressing to the controller, the NCPDP informs the individuals concerned of the need to comply with the pre-established procedures for fulfilling the conditions for receiving and handling complaints.

During the reporting period, the NCPDP continued its monitoring and conformity activity of personal data processing carried out by public and private sector controllers as well as individuals, by carrying out controls on the basis of complaints from personal data subjects and self-reporting by the authority, following referrals received for examination including from public authorities/institutions.

Thus, **356** control materials were initiated and examined of which **331** on the basis of complaints from personal data subjects and **26** on the basis of self reporting initiated at the request of legal entities or ex officio.

Comparative information on the control activity, for the years 2018 – 2023

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
Year 2021	243	27	2	9	148/117
Year 2022	227	21	2	13	125/110
Year 2023	357	26	15	18	107/117

The control required by the Law on personal data protection is carried out by the State Inspectors of General Department for Surveillance and Conformity and the Legal Department. If necessary, depending on the subject and tasks of the control performed, the NCPDP may attract specialists and experts from fields requiring special knowledge to participate in the process of prior verification and control of the lawfulness of personal data processing. The control activity represents actions to investigate the facts and circumstances in relation to personal data processing and the collection of evidence necessary for the objective examination, in accordance with the legal provisions, of the complained case.

In most of the cases under examination, the objective of carrying out controls is to establish:

- the purpose and legal basis of personal data processing;
- the necessity of personal data processing;
- the proportionality, relevance and actuality of the data processed;
- respect for the rights of personal data subjects;
- respect for the degree of security and confidentiality of personal data processed etc.

It should be noted that, during the reference period, were carried out controls on the compliance of personal data processing with the requirements of the Law on personal data protection in connection with the following facts complained by data subjects:

- disclosure of personal data in the absence of the data subject's consent;
- violation of principles and rights guaranteed by law;
- processing of personal data through video surveillance systems by natural and legal persons;
- accessing personal data from state information systems without a legal basis;
- publication of personal data online etc.

During the reporting period, as a result of the controls, **318** decisions were issued. For clarification purposes, it should be noted that, when issuing a decision, the NCPDP may order either the absence of violation of legal provisions or their violation, depending on the subject of the control and the number of participants in the control procedure. Thus, when issuing decisions, in **236** cases the absence of infringement was found, in **187** cases the infringement of legal provisions in the field of personal data protection in the processing of personal data was found. As a result of the examination of the control materials with a finding of violation of the legal provisions in the field of personal data protection, depending on the seriousness of the violation of the principles of personal data protection in their processing, coercive measures were ordered manifested by:

- ✓ Suspension of personal data processing – **26** cases;
- ✓ Destruction / erasure of personal data processed regarding the infringement of legal provisions – **18** cases;
- ✓ Cessation of personal data processing – **15** cases.

Finally, it should be noted that in the case of violations found as a result of the verification of personal data processing lawfulness, there are penalties of a contravention nature. However, the legislator has expressly established that the decision on the finding of a breach of the legislation on personal data protection and the evidence gathered serve as a basis for the drawing up of the report on the contravention under the terms of the Contravention Code.

Respectively, as a ascertaining agent in relation to the provisions of Articles 74^1 - 74^3 of the Contravention Code related to the violation of legal provisions in the field of personal data protection, during the year **2023**, **107 reports** were drawn up **on contraventions**, **117 contraventions** were established, and the contravention cases were sent for examination to the competent court, pursuant to the provisions of the Contravention Code.

The spectrum of contraventions found in the light of the articles covered by the Contravention Code shows that the most frequent violations admitted in the processing of personal data were manifested as follows:

- Art. 74[1] para. (1): infringement of personal data processing, storage and usage rules, except in the cases provided for in paragraph (5) – **94 cases**;

- Art. 74[1] para. (3): infringement of personal data subject's rights, the right to be informed, to have access to personal data, to intervene on personal data, to object and not to be subject to an individual decision – **9 cases;**

- Art. 74[2] para. (1): refusal to provide the information or documents requested by the National Centre 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 – **14 cases**;

ACTIVITY OF CONTROL IN NUMBERS

318

ISSUED DECISIONS

107/117

CASES OF CONTRAVENTIONS FOUND/ MINUTES DRAWN UP

(regarding the infringement of Articles 74[1] - 74[2] of the Contravention Code)

18

EMPLOYEES WITH CONTROL POWERS

(in relation to 27 persons, according to the Staff Limit)

CHAPTER III

ACTIVITY OF REPRESENTATION IN THE COURTS

In civil and administrative litigation

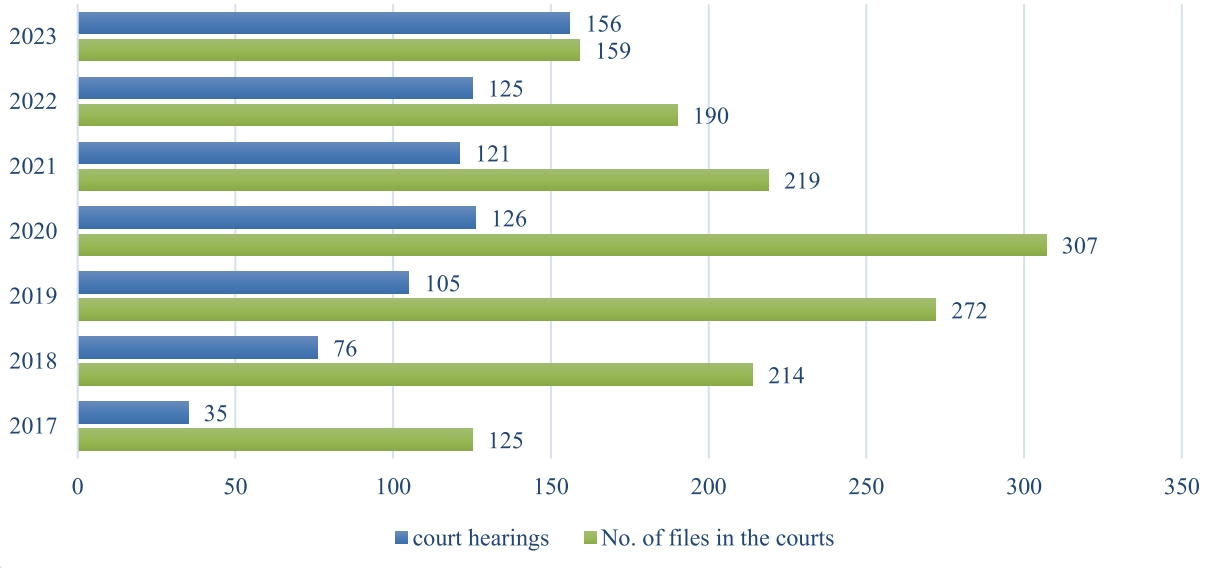
In accordance with the legislation in force, the decision, actions and inactions of the NCPDP may be appealed by the controller, the processor or data subject directly in court, in accordance with the provisions of the Administrative Code, without prior procedure, within 30 days from the date of communication or notification of the administrative act.

During 2023, the NCPDP's interests were represented in the administrative litigation courts in **156** court hearings, amongst which: **152** as a defendant; **4** as a public authority which draws conclusions, some of which were initiated even in previous years.

In 2023, the representatives of the NCPDP participated in **159** court hearings of administrative litigation, drafting **130** procedural documents necessary for an efficient examination of court cases.

At the same time, we note that in 4 court hearings the NCPDP was called as a public authority that submitted conclusions, in accordance with the provisions of Art. 74 para. (1) Code of Civil Procedure, which demonstrates the tendency of individuals to realise their right of access to justice, conferred by Art. 18 of the Law on personal data protection, by requesting compensation for material and moral damages, if they complain that they have suffered damage as a result of unlawful processing of personal data or that their rights and interests guaranteed by law have been infringed.

Comparative dynamics of the number of cases and court hearings in administrative litigation, for the period 2017-2023



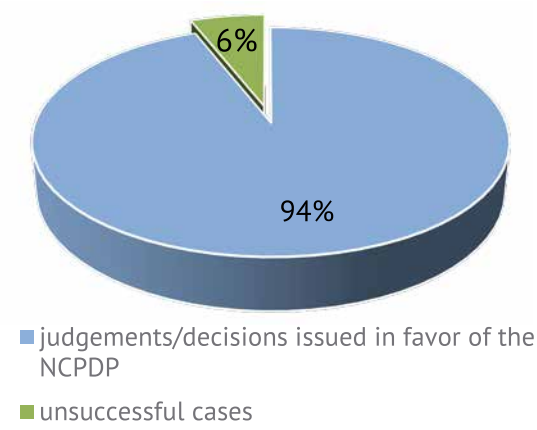
We also mention that during 2023, the examination of **18** court files was completed where the judgments/ decisions of the courts remained final and irrevocable, of which:

– 17 judgements/decisions of the court were issued in favor of the NCPDP;

– 1 case were unsuccessful for the NCPDP.

Thus, we find that in **94%** of the number of completed court files, the actions taken by the NCPDP were considered legal and justified by the courts.

Dynamic of court files in 2023



In this context, given the specific nature of the issues addressed in the complaints, in most cases the subject of the administrative litigation is the annulment of decisions issued following investigations carried out by the NCPDP regarding the finding/failure to comply with personal data protection principles.

Case no. 1

The NCPDP received a complaint from a data subject expressing his disagreement with the actions of the medical institution of which he is an employee, in relation to the disclosure of personal data to the Single Monitoring and Traffic Control Centre (CUMCT) without his consent. According to the explanations submitted by the complainant, the disclosure of personal data was carried out in connection with the investigation of contravention cases, which he considered to be abusive and carried out in violation of the provisions of the Law on personal data protection.

Following the examination of the complaint and the evidence gathered during the control, by administrative act, the NCPDP found no violation of the provisions of the Law on personal data protection by the medical institution when processing the personal data of the complainant, by disclosing them to the Single Monitoring and Traffic Control Centre.

Not agreeing with the provided measures, the complainant filed an action for annulment of the administrative act. The court dismissed the action as unfounded.

On the appeal filed, the Chișinău Court of Appeal rejected the appeal filed by the complainant, upholding the decision of the court of first instance.

When examining the admissibility of the appeal submitted by the complainant, the Supreme Court of Justice declared it inadmissible on the ground that the complainant's appeal was not sufficiently serious from the point of view of the allegation of genuine and essential breaches of procedural and substantive law capable of overturning the contested decision of the court of appeal in a possible examination on the merits and ex officio invocation of errors of law.

In its position, presented to the courts, the NCPDP stated that the legal basis which the controller invoked in disclosing the complainant's personal data arises from the legal obligation of the owner/ user of a vehicle to inform the competent police authorities about the identity of the person to whom the vehicle has been entrusted for driving.

In this regard, reference was made to the Constitutional Court Decision No 28 of 18.11.2014, for the constitutionality review of Article 234 of the Contravention Code of the Republic of Moldova, which also provides a valid explanation of the basis for personal data processing by the authorized institutions.

*In this regard, the Court explained that the road traffic safety is of major public interest and therefore **ensuring safety is a positive obligation of the State**. The transport unit, as a participant in traffic, represents a source of increased danger, and the driver is obliged to comply with certain regulations imposed by the authorities in order to avoid the risks arising from the use of vehicles. The owner of the vehicle is also liable for damage caused by the use of the vehicle in his possession.*

*The Court held that, applying mutatis mutandis the reasoning of the European Court of Human Rights (Falk v. Netherlands, 19 October 2004), the liability rule (applied to owners of registered cars) was introduced in order **to guarantee the effectiveness of traffic safety by ensuring that any breach of the road rules by technical or other means, committed by drivers whose identity cannot be established at the time of the offence, will not go unpunished.***

*Therefore, a public interest of major importance, such as road traffic safety, makes it possible to impose responsibilities on citizens, in particular to inform the police about the person entrusted with the driving of the vehicle, with the aim of protecting road users from accidents and negative consequences, as well as **creating the legal conditions for holding liable persons who have infringed road traffic rules.***

*The Court finds that there are no **less restrictive means** of achieving the aim of ensuring road safety and, therefore, the establishment of such a liability **is proportionate** to the aim pursued and the imposition of such obligations **is not excessive.***

*Thus, in the examined case, the legal obligation of the car owner or, if applicable, the authorized representative, in the part **concerning the processing of personal data** by transmitting/disclosing them to the police authorities, is dictated by the reasoning listed above.*

Case no. 2

Following the submission of a complaint by a citizen, he claimed that the housing fund manager had allegedly violated the provisions of the Law on peronal data protection by sending the payment invoices for communal services and placing them to outside the mailbox without an envelope and allowing free access to them, thereby disclosing his personal data. Following the examination of the case, a decision was issued on the finding of violation of the provisions of the Law on personal data protection by the manager of the housing fund.

The housing fund manager appealed the decision issued by the NCPDP in the court on the basis that it was unclear how, by sending the payment invoices to the mailbox, it would disclose the individual's personal data and requested the annulment of the decision as unfounded and unlawful.

The Chișinău Court, Râșcani headquarters, admitted the action filed by the complainant and annulled the decision of NCPDP.

Subsequently, the Chișinău Court of Appeal rejected the appeal filed by the NCPDP and upheld the decision of Chișinău Court, Râșcani headquarters.

By its decision, the Supreme Court of Justice upheld the appeal filed by the NCPDP, annulled the decision of the Chișinău Court of Appeal and returned the case to the Chișinău Court of Appeal for retrial, in another panel. At the same time, the complainant was admitted to the process as a third party.

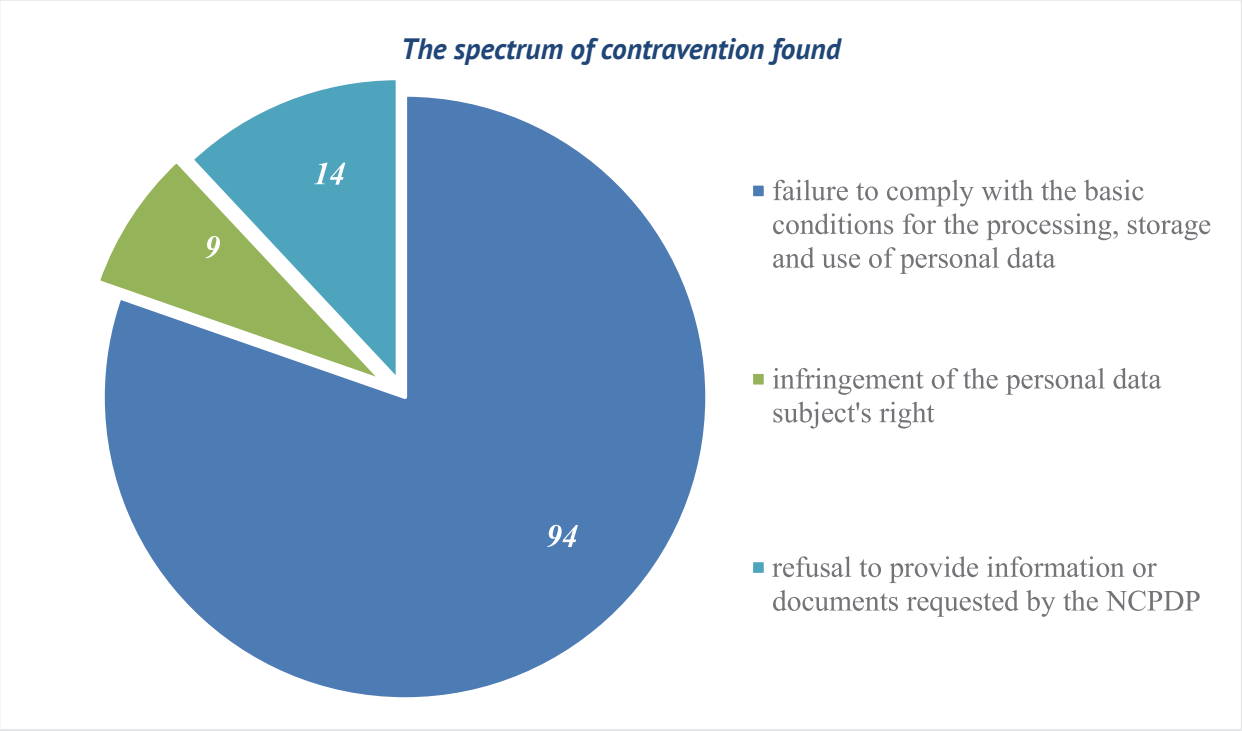
As a result, the Chișinău Court of Appeal annulled the decision of the Chisinau Court and issued a new decision dismissing the action of the housing fund manager as unfounded. The Chișinău Court of Appeal concluded that the conclusions of the first instance did not correspond to the factual circumstances, namely that the court of first instance had not admitted the action on the merits.

However, the manager of the housing fund concerned filed an appeal against the last decision of the Chișinău Court of Appeal, requesting that the appeal shall be admitted, the decision of the court of appeal be annulled and the decision of the first court be upheld.

Examining the bases of the appeal filed, the specialised panel for the examination of actions in administrative disputes of the Civil, Commercial and Administrative Litigations Chamber of the Supreme Court of Justice held that the appeal was inadmissible, did not meet the conditions for the admissibility of an appeal and did not contain convincing and well-founded grounds.

In contravention procedure

In accordance with the provisions of Article 27 para. (3) of the Law on personal data protection, based on the decisions issued, by which violations of personal data processing were found, the ascertaining agents of the NCPDP, during the reference period, drew up **107** minutes on contravention, being ascertained **117** contravention facts. In accordance with Art. 423^4 of the Contravention Code, the minutes on contravention were submitted for examination in the competent court.



In the reference period, the NCPDP's ascertaining agents participated in **386** court hearings on contraventions under examination, both in the court of first instance and at the Chișinău Court of Appeal. Furthermore, it should be noted that out of the total number of contravention cases sent for examination in the court during the reference period and in the previous years, in **90** contravention cases NCPDP 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. At the same time, during the reported period, **14** minutes on contravention were ceased/cancelled. In addition, it should be noted that other **125** contravention proceedings are pending, including on some of the infringement cases initiated in the previous years.

Cases regarding the representation in the courts, having a difficult character for the activity of the NCPDP

During the year 2023, the pressing issue continued to persist, which hindered the activity of the authority, manifested by the **examination in the courts, both in administrative proceedings and in contravention proceedings of the same acts and findings issued by the authority following the verification of the lawfulness of personal data processing.**

This essentially refers to the **double, contradictory and equivocal character** regarding the examination in the courts, during the same period, of the same acts and findings issued by the NCPDP in different proceedings. However, as a result of the examination of the control materials on the lawfulness of personal data processing, pursuant to Art. 27 para. (3) of the Law on personal data protection, [...] the NCPDP issues reasoned decisions regarding the finding of the violation of the legislation in the field of personal data protection and the accumulated evidence serves as a basis for drawing up the report on the contravention, under the Contravention Code.

Thus, the decision finding the violation of legal provisions in the field of personal data protection is liable to be challenged in order of administrative litigation.

At the same time, in accordance with Article 423^4 para. (4) of the Contravention Code, as a result of the finding of violations committed in the processing of personal data, the NCPDP draws up minutes of the contravention and sends them for examination to the competent court to resolve the cases, by pleading guilty and imposing a financial penalty, with the possibility of applying as an additional penalty the deprivation of the right to process personal data for a period of 3 months to 1 year.

Therefore, for committing the same act/violation, the personal data controller is subject to liability/sanctioning twice - circumstances contrary to the principles of individualization and subject to liability.

In particular, it should be noted that, according to the practice in this regard, there are situations where for the same act, in the contravention proceedings, the controller is found guilty by the court and in the administrative proceedings, the same controller is declared innocent by the court, with the annulment of the NCPDP's decision or vice versa. The situation described is all the more bizarre in view of the fact that in both cases (in the contravention proceedings and in the administrative proceedings) there is one and the same decision finding that a violation of the personal data processing has occurred.

In this context, **the existence of such contradictory procedures led, in some cases, to determining the inefficiency of the actions taken by the NCPDP 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 NCPDP's sub-divisions, which is minimal in relation to the excessive volume of work.

CHAPTER IV

EXAMPLES OF CASES EXAMINED IN 2023

Periodically, the NCPDP informs the society about problems and irregularities established in the activity carried out by personal data controllers in relation to personal data processing.

To this end, the Authority shall present, including by means of the annual activity report, significant cases and issues identified during the controlls carried out on the compliance of personal data processing. Thus, among the cases examined by the NCPDP in 2023, were the following:

Case no. 1: Processing of personal data without the consent of the data subject and without another legal basis

The NCPDP examined the request received from the State Tax Service (STS) informing that, as a result of the fulfilling of tax administration duties, it was found that an economic agent has been collecting and using personal data contrary to the provisions of Article 5 para. (1) of the Law on Personal Data Protection, which served as grounds for initiating the verification/investigation of the compliance of personal data processing operations.

In fact, according to the materials attached to the STS application, it was found that the economic agent processed the personal data of 35 natural persons, without their consent or that of the successors of deceased persons and in the absence of any other legal basis provided for in Article 5 para. (5) of Law No 133/2011 on personal data protection.

Following the investigations carried out by the NCPDP, in accordance with the provisions of Article 27 of Law No 133/2011 on the personal data protection, by the decision of the NCPDP, it was found a violation of the provisions of Article 4 para. (1) letter a), art. 5 para. (1), (4) and art. 12 of Law no. 133/2011 on personal data protection by the economic agent in question in the processing of personal data of the data subjects concerned in the STS application.

At the same time, the NCPDP also ordered the cessation of the personal data processing operations of the data subjects concerned in the STS procedure and the destruction of the copies of the identity cards unlawfully used/obtained by the economic agent.

Consequently, in accordance with the provisions of Article 20 para. (1) letter m) of Law No. 133/2011 on personal data protection, the NCPDP has referred the matter to the criminal prosecution body of the STS, regarding the existence of reasonable indications of falsification of documents for the purchase of goods, an act provided for in Article 335[1] of the Criminal Code.

Case no. 2: Disclosure of personal data via social networks

The NCPDP examined the complaint of a natural person who requested verification of the lawfulness of his personal data processing, manifested by placing on the social network "Facebook", a post accompanied by photos of the identity documents of the complainant.

During the investigation it was determined that the data controller is the administrator of the Facebook account where two images of ID documents (ID card and passport) were published, but the post was published not by him, but by another person with whom he is related, to whom he gave access to his account. During the control, the data controller (Facebook account administrator) admitted his guilt and realised that a breach of the rules on personal data protection had occurred.

In this context, the NCPDP, by Decision, found that the processing of personal data manifested by posting/publishing identity documents on the social network "Facebook" was carried out without a legal basis in this regard and without ensuring the confidentiality of the data processed, actions that led to the finding of violation of the provisions of Article 4 para. (1) letter a), art. 9 and art. 29 paragraph (1) of Law No. 133 of 08 July 2011.

Case no. 3: Disclosure of personal data concerning health status

The NCPDP has examined the complaint of a data subject requesting the intervention of the supervisory authority, in accordance with the powers assigned by the Law on personal data protection, to determine and sanction the person(s) within the public entities responsible for knowingly disseminating of confidential information, protected by law, which has been transmitted via work e-mail to all employees, documents containing personal information, including information on the health status of the data subject, violating his right to personal data protection on health status.

As a result of the examination of the complaint submitted, the NCPDP found that the employee of the public entity acted individually in determining the purpose and means of personal data processing relating to the health status of the data subject, without taking into account the instructions/provisions of the management of the entity, in relation to the transmission/disclosure to all employees of the information contained in the medical certificate issued in the name of the data subject, in the absence of a legal obligation/legal framework, without ensuring the confidentiality of personal data, an action which is contrary to the legal conditions laid down in Article 4 para. (1) (a), Art. 6 para. (1) and Art. 29 para. (1) of the Law on personal data protection.

Case no. 4: Non-compliant processing of personal data stored in the Register of Immovable Property

As a result of the examination of multiple complaints from various data subjects, as well as taking into account the widespread public media coverage of the fact that an NGO has accessed the personal data of an excessive number of personal data subjects stored in the Central Data Bank of the Real Estate Cadastre, the NCPDP initiated an inspection to establish the circumstances that led to the situation created.

As a result of the actions carried out during the control in question, it was determined that the NGO, as data controller, had contracted an authorised person to verify the discrepancies identified between the assets declared and those reflected in the RIP, relating to candidates for membership of the Superior Council of Magistrates and candidates for membership of the Superior Council of Prosecutors.

In this regard, from May 2022 until the time of the termination of access to the mentioned information resource - July 2022, the processor accessed an enormous amount of personal data of an enormous number of data subjects, i.e., making 680263 accesses to the Real Estate Register to approximately 378261 real estates, each of them having one, two and more owners, new and old. The number of natural persons whose personal data was accessed was 362533.

According to the data controller, the accesses to personal data of the data subjects would have occurred due to the use of an automated search robot. The search was carried out exclusively by address or cadastral number, which were the basis for the choice of the automated sample of the search group.

Another circumstance that led to excessive accesses was found to be the lack of action taken by the controller in relation to the processor to assess the correctness of personal data processing. During the above-mentioned period, the NGO, as controller, did not take any action to verify the implementation of technical and organisational measures by the processor regarding the correct and lawful processing of personal data in the RIP, although, based on the provisions set out in the Declaration on the obligation of confidentiality and security of personal data, this obligation was obvious.

Based on the circumstances described, the NCPDP found a violation of Article 4 para. (1) (a), (b) and (c), Art. 5 para. (1) and Art. 9 of the Law on personal data protection by the processor, as well as the provisions of Art. 4 para. (1) (a), (b) and (c), Art. 5 para. (1) and Art. 30 of the same law by the NGO concerned.

In addition, the NCPDP concluded that the public institution, as the owner of the state information resource and which provided access to the Central Real Estate Cadastre Database (Real Estate Register), had a legal obligation to take the necessary organisational and technical measures for the protection of personal data stored in this state information resource, which it ignored at the appropriate stage.

Taking into account the circumstances described above, the NCPDP found that the actions of the above-mentioned institution resulted in a violation of the provisions of Article 30 para. (1) of Law No. 133/2011 on personal data protection.

Taking into account the exaggerated volume of information containing personal data accessed in the circumstances elucidated during the inspection, pursuant to Art. 20 para. (1) letter m) of the Law No. 133/2011 on personal data protection, the NCPDP referred the matter to the General Prosecutor's Office for verification of the circumstances set out in the decision, in the light of the powers of the prosecution body.

Case no. 5: Non-compliant processing of personal data via a website

The NCPDP has investigated the legality of placing certain categories of personal data concerning a large number of individuals on the website www.numar.md.

Following the analysis of the information placed on the web page in question, it was found that, through it, any person could leave a comment, visible to everyone, on the owner of any mobile phone number in the Republic of Moldova. The comments on the web page contained various types of biographical information, such as: name, surname, education, place of work, age, locality, home address, type of activity carried out, etc., as well as libellous and defamatory information. Disclosure of such information online for unrestricted viewing could seriously undermine citizens' constitutional rights and freedoms.

As a result of the inspection, the NCPDP determined that the means provided for personal data processing, by publishing on the website www.numar.md of the information reflecting the categories of personal data listed above, was not in compliance, as it was neither established the existence of a specific, explicit and legitimate purpose, nor the existence of a legal basis for personal data processing concerning the holders of mobile phone numbers in the Republic of Moldova, actions committed contrary to the provisions of Article 4 para. (1) (a), (b), (c) and Art. 5 para. (1) of Law 133/2011 on personal data protection.

It should be noted that, following the intervention of the NCPDP during the control actions carried out, the website www.numar.md became unavailable/inactive.

In this context, taking into account the provisions of Art. 27 para. (3) and para. (5) of the Law on personal data protection, the NCPDP has ordered by Decision the finding in rem of violation of the provisions of Law No. 133/2011, the processing of personal data through the page www.numar.md, the finding of unavailability on the Internet of the page www.number. md, as well as the referral to the PE "Information Technology and Cyber Security Service" in order to examine the possibility of intervening in the light of the competences set out in point 33 subpoint 7) of the Regulation on the management of the top level domain .md, approved by ANRCETI Decision no. 42/2020.

Finally, it is noted that the objective of counteracting the non-compliant processing of personal data, which was on the basis of the NCPDP's self-reporting, was achieved with the unavailability/ becoming inactive of the www.numar.md website, which constituted a way of abusive disclosure of personalised information of a significant number of data subjects.

Case no. 6: Non-compliant use of personal data when applying for a credit

The NCPDP examined the complaint of a data subject concerning the alleged non-compliant processing of personal data (first name, surname, date/month/year of birth, IDNP), realized by their fraudulent storage and use.

During the investigation, the NCPDP found that the complainant had previously transmitted his personal data to the owner of a shop in order to help him to to pay a fine via the RunPay terminal located in the shop premises. The latter wrote down the personal data on a sheet and complied with the data subject's request.

Subsequently, the shop owner used the complainant's personal data such as IDNP, date/month/year of birth when submitting an application on behalf of his daughter to obtain credit via the same terminal. Although, the shop owner claimed that he mistakenly entered the complainant's ID data, believing it to be his daughter's personal data, the NCPDP did not determine the existence of a plausible justification for entering the data concerning the complainant in the credit application.

The NCPDP stated that according to Article 11 of the Law on personal data protection, the conditions and time limits for storing personal data are provided for by law, taking into account the provisions of Article 4 para. (1) letter e). At the end of personal data processing operations, if the subject of these data has not given his consent for another purpose or for further processing, they will be destroyed.

Since the data subject did not consent to further processing of personal data for other purposes, the record with his identification data was to be destroyed immediately after the fine was paid via the terminal.

Therefore, the NCPDP, having verified the fulfilment of the mandatory elements implying the conformity and legality of the processing operations, held that there was no purpose and legal basis justifying the actions of the shop owner to store and further use the personal data of the data subject, manifested by their transmission to a credit company, actions which contrave to the provisions of Article 4 para. (1) (a) and (e), Art. 5 para. (1) and Art. 11 of the Law on personal data protection.

Case no. 7: Failure to ensure regular review and adjustment of internal acts containing provisions on personal data processing

The NCPDP has received a referral from a public institution, which has sent a Decision on the results of an investigation into the performance of duties by one of its employees.

According to the findings of the public institution, it was noted that the employee, being at the reception desk in the Multifunctional Centre, would have accessed, after the personal identification number (hereinafter - IDNP), through the SIA "LegalCad", the information stored in the State Register of Population concerning a data subject, without a legal basis.

During the examination of the case, it was determined that the applicant (natural or legal person), who approaches at the reception desk, may verbally request, for advisory purposes, information, which may be communicated upon presentation/voicing of the IDNP of the owner of the real estate or the cadastral number of the real estate, without having the intention to submit requests for services. Respectively, the registrar carries out the search by accessing the "LegalCad" system,

which presumes simultaneous access also to the State Register of Population, as it is connected/ linked to the Real Estate Register.

According to the documents submitted by the public institution - as a data controller, in particular, according to the employee's job description, the latter has the following basic duties: provision of information from the real estate cadastre and the qualitative and timely execution of the duties set out in the job description; receipt, examination and execution of requests for the provision of information from the real estate cadastre, as well as the identification of real estate belonging to a person, accessing the central database, where appropriate, SIA "LegalCad".

Thus, the NCPDP has determined that the public institution has provided access to the central database in order to "address the SRP for viewing, entering or correcting data about the owner, which is done through the SIA "LegalCad", module "Update data about the owner according to the State Register of Population", order in which, in the exercise of duties, the employee is guided by the provisions of the Law on Real Estate Cadastre, taking into account the methodological recommendations, internal Instructions and Regulations, of the central body specialized in the field of cadastre and of the public institution concerned, acts which are mandatory for all employees.

After examining the regulations and instructions submitted by the public institution, the NCPDP did not identify any organisational measures put in place by the owner of the automated information system, which would have established rules on the performance of service tasks in the case of providing information from the central database to the applicant who approached the counter, whether a natural or legal person or a person empowered by a power of attorney, there is no description of the actions to be taken with regard to requests for access to information from the information systems managed by the public institution, which are made orally in accordance with the provisions of Art. 12 para. (4) of the Law on Access to Information.

For these reasons, the NCPDP found that the controller did not take sufficient organizational measures necessary to protect personal data/information stored in the managed information systems, in particular did not expressly provide for the processing of personal data stored in the managed information systems, including in the job description, the employee was assigned tasks of executing requests for the provision of information from the real estate cadastre, as well as the identification of the real estate belonging to a person, by accessing the central database, on the basis of personal data that were verbally communicated by the applicant, if necessary, through the SIA "LegalCad", in case the applicant does not want/wants to submit a request at the counter.

In the circumstances described above, the NCPDP did not find any admitted breaches by the employee in the processing of personal data through the use of the SIA "LegalCad", in circumstances where he, as registrar, was not obliged to make any records related to the purpose of access, made prior to the receipt of a request for the provision of information/provision of services.

As a result, the NCPDP informed the public institution of the need to undertake the necessary actions in order to revise the internal acts and adjust the regulations concerning the processing of personal data, in particular in the case of addressing for consultation purposes, at the reception desk, without having the intention of submitting any requests for the provision of services, actions which were carried out by the latter.

Case no. 8: Failure to update authorised users' access rights to information systems on time

The NCPDP examined the complaint of a public authority, submitted in accordance with its competence, requesting verification of the lawfulness of the processing of personal data of a data subject and his/her child, following access/consultation/extraction of personal data stored in the Integrated Information System of the General Inspectorate of the Border Police of the Republic of Moldova[1] (hereinafter – IIGIBP), which were subsequently transmitted to a third party, the actions in question being carried out by employees of a public authority with a right of access to the IIGIBP.

During the investigation, it was determined that, via the "WebClientPF" search system, from a user account that was assigned to a former employee of the public authority concerned, who resigned in 2019, using the work computer of a current employee, the information on the crossing of the state border by the data subject was searched, and subsequently the information was saved in PDF format, printed and transmitted to third parties.

Thus, it was held that the user account of the former employee was active three years after his resignation, being disconnected only two months after the access referred to in the complaint, a fact acknowledged by the public authority.

Subsequently, it was determined that the work computer that was used for the processing of the data subject's personal data was located in the work office of a subdivision of the public authority. At the time the access was carried out, the employee in charge of the computer concerned was not in the office. At the same time, it was established that other service computers were connected to the IP-device (remote VPN user) and that the service office where the targeted computer was located served as a common office for several officials, physical access to the computer was not restricted.

In these circumstances, it was not possible to identify with certainty the person who processed the personal data, in which order the NCPDP found in rem that the processing of personal data of the data subjects concerned was carried out contrary to the provisions of Article 4 para. (1) (a), (b), (c) and Art. 5 para. (1) and para. (3) of the Law on personal data protection, without a legal basis and without the consent of the data subject.

At the same time, the security incident was generated due to improper management and organization of the tasks set for the institution's staff, which, through malicious actions, either errors or negligence in the use of information resources, generated the given incident, or, according to the approved Personal Data Protection Policy, the public authority was obliged to review the access rights to the state information resource of authorized users at regular intervals, as well: - reviewing the access rights of the SIIV user - once every 6 months and after each change of employment relations that occurred in the user's activity and reviewing the granting of access rights of privileged roles - once every 3 months.

Following this, the NCPDP determined that the public authority is liable for violating the provisions of Article 30 para. (1) of the Law on personal data protection, as it failed to ensure the necessary organizational and technical measures for personal data protection made available to it, which consequently led to the illegal access to the IIGIBP and the processing of personal data of data subjects.

[1] ***The technical concept of the Integrated Border Police Information System*** *was approved by Government Decision No. 834 of 07.07.2008 "on the integrated Border Police Information System"*

In addition, the entity that manages the information system was requested to take, in the near future, the necessary actions to implement the MPass governmental authentication and authorization service, as the only method of user authentication in the IIGIBP, in accordance with Government Decision no. 1090/2013 on the electronic governmental authentication and access control service (MPass), and the public authority concerned by the control was requested to review and adjust the policies and procedures for ensuring the security and confidentiality of the processing of personal data by implementing the necessary measures to ensure that similar incidents do not occur.

Case no. 9: Illegal use of personal data belonging to others

The NCPDP received several petitions from individuals who complained about receiving numerous phone calls from various credit companies in the Republic of Moldova informing people about the examination of applications for credit, which contained their personal data, being submitted online.

As a result of the actions carried out in the framework of the control, in the light of the Law no. 133/2011 on personal data protection, the NCPDP has identified the persons who have illegally processed personal data, being found violation of Article 4 para. (1) letters a), b), c), art. 5 para. (1), Art. 9 and Art. 29 para. (1) of Law No. 133/2011 on personal data protection in connection with the disclosure to credit companies of personal data belonging to other persons, namely name, surname, state identification number (IDNP) and contact details.

In addition, in the context of the case described above, the NCPDP has made recommendations to the public regarding the need to ensure vigilance when transmitting/offering personal data.

Case no. 10: Processing the IDNP as a tax code when having a self employment activity

The NCPDP received a complaint from a group of persons who alleged that the Law No. 356/2022 on the amendment of some normative acts introduced amendments to the Law No. 93/1998 on the entrepreneur's patent, which would have created conditions for the violation of personal data protection of entrepreneurs' patent holders.

Thus, entrepreneurs operating in the markets and who have complied with the new tax regime, have found that the tax receipts issued to buyers contain personal data, in particular, the state identification number, indicated in the tax code field - C. F.

From the stipulated provisions, it was determined that the tax legislation regulates the record of tax liabilities of individuals on the basis of tax codes assigned in the prescribed order, resulting from the exercise of independent economic activity.

After examining the relevant legal provisions, including Article 5 point 28), Article 162 paragraph (1) letter b), Article 163 of the Tax Code, point 10 letter i) of the Instruction on the registration of taxpayers, and point 24 of the Regulation on the Unique Register of currency exchange and control equipment, it is clear that the processing of individuals' ID numbers in the context of independent activity is subject to regulation. Starting from 1st July 2023, the commercialization of goods and the use of only home equipment and control connected to the automated information

system „Electronic Sales Monitoring" will be documented, in conjunction with the provisions of Art. 5 para. (5) lit. b), Art. According to section 9 lit. b) of Law No. 133/2011, it was noted that the processing of personal data in the case mentioned is carried out to fulfill an obligation that the controller has under the law.

At the same time, it would seem vulnerable that any self-employed natural person is required by the existing legal framework, in particular the one concerning the algorithm of operation of currency exchange register and control equipment, to make public/known his IDNP in the tax receipts issued daily.

Similar regulations have been subject to constitutional review by the Constitutional Court, which has assessed the positive obligation of the competent authorities, as in the case under examination by the NCPDP, to ensure the protection of the IDNP of self-employed data subjects.

As a result, the NCPDP has attested the existence of a defective legal framework governing the legal regime of tax records of self-employed individuals, namely, the fact of recording the IDNP in the tax receipt issued by the licence holder to each client, interferes with the privacy of the person, being a disproportionate measure in relation to the intended purpose.

Subsidiarily, it was recommended to the Ministry of Finance/State Tax Service to put in place technical and organisational measures to ensure the protection of personal data of self-employed persons, by identifying and implementing appropriate and efficient mechanisms for keeping tax records, without prejudice to the right to personal data protection for example: by depersonalising the IDNP of the self-employed natural person recorded on the tax invoice or by assigning a new unique tax code distinct from the IDNP.

In its Decision, the NCPDP stressed the need to ensure a balance between tax obligations and individual rights to personal data protection. The problem identified should be addressed by measures that ensure that both principles are respected without prejudice to the right to privacy of self-employed individuals.

Case no. 11: Failure to comply with organisational and technical measures necessary for personal data protection

The NCPDP has received multiple requests from the police bodies, through which it has been informed about the alleged non-compliant processing of personal data by a political party, manifested by the collection of personal data from citizens.

According to the facts established during the control carried out by the NCPDP, it was found that, on behalf of the political party, personal data of citizens in certain localities were collected, such as: name, surname, year of birth, signature, telephone number and home address, for the purpose of "carrying out the campaign to collect signatures in support of the initiative to declare the unconstitutionality of a political party".

Having analysed the circumstances in which the personal data reflected in the lists concerned were accumulated/collected; including the establishment of these lists; the possibility of duplication/copying from these lists; the lack of safeguards relating to adequate security and organisational measures regarding the processing carried out, it was held that, taken together, these circumstances may lead to the use of the personal data collected for purposes other than those originally declared/determined by the party and of which individuals were informed at the

time they provided their personal data and for the processing of which they gave their consent.

Thus, from the information gathered, the NCPDP found that the data controller would not have: established a clear description of personal data processing, including after collection; regulated and implemented concrete technical and organisational measures to ensure the security of the personal data collected; designated a person who will ensure compliance with the safeguards relating to appropriate technical and organisational security measures regarding the processing to be carried out; it would also not regulate the personal data processing by processors by means of a contract or other written legal act ensuring in particular that they act only on the instructions of the data controller, in which order it has been established that the data controller - the political party - has infringed the provisions of Art. 4 para. (1)(a) and Article 30(1)(a) of the EC Treaty. (1), (2), (3) and (31) of Law No. 133/2011 on the personal data protection.

As a result, the NCPDP recommended that the political party put in place appropriate measures to ensure that the personal data processing complies with the legislation on the personal data protection. These measures include establishing a clear description of the processing, implementing appropriate security measures and designating a person responsible for managing these issues.

CAPITOLUL V

RECOMMENDATIONS AND OPINIONS OF THE NCPDP

In order to prevent breaches of the rules on personal data processing, as well as to ensure that society is informed of the problems and situations it faces, the NCPDP issues recommendations and opinions in the field of personal data protection, which can be consulted on the Authority's website under ***General Recommendations on data protection*** or under ***Data controller/NCPDP recommendations.***

During the reporting period, the NCPDP came up with several clarifications and recommendations for both data subjects and public authorities:

To the attention of Yandex Go app users

In the context of recent media reports regarding access to personal data processed through the "Yandex Go" application (such as: mobile device data, names, phone numbers, email addresses, banking information, and addresses for taxi routes), the NCPDP has encouraged data subjects to be vigilant and to inform themselves about the conditions stipulated in the Yandex Privacy Policy before installing the Yandex Go application on their mobile devices: once this application is installed, the processing of personal data is based on the consent of the data subject.

Moreover, in the case of using foreign systems/ platforms, managed/created by non-resident controllers, whose servers are located outside the country, the situation of cross-border transmission of personal data collected/processed through these systems/platforms implicitly arises, which determines the mandatory applicability of Article 32 of Law No. 133/2011 on personal data protection.

In these circumstances, the cross-border transmission of personal data to states that do not ensure an adequate level of protection (such as the Russian Federation) may take place under the conditions laid down in Article 32(2)(5) of the Law on personal data protection.

At the same time, it should be noted that in the case of taxi order management platforms owned by non-resident owners, but operating and/or producing legal effects on the territory of the Republic of Moldova, the competent state authorities will face obstacles and/or will not be able to exercise effective control over their possibly harmful actions.

Moreover, in the circumstances set out above, including the personal data subject will lose control over his or her personal data and will find it difficult to exercise his or her rights enshrined in the Law on personal data protection.

In the context of the above-mentioned information, as well as taking into account the fact that personal data, transferred across borders to states that do not ensure an adequate level

of protection, could be used to the detriment of data subjects or for purposes other than those declared by the controller, in the opinion submitted to the Government on the draft legislative initiative no. 252 of 13.07.2023, the NCPDP proposed including:

... in the context of ensuring effective protection of personal data processed, it would be appropriate to examine the possibility of establishing the rule on the use of electronic management systems (platforms) managed/kept/stored on the territory of the Republic of Moldova. However, taking into account the provisions of Articles 4 and 5 para. (5) (b) of the Law No 133/2011, the obligations/rules on personal data processing (such as for example: use of national electronic management systems/ platforms, as well as keeping the servers on the territory of the Republic of Moldova, without allowing cross-border transmission of personal data) must be provided for by law.

The text of the recommendations can be viewed by clicking on the link: https://datepersonale.md/ in-atentia-utilizatorilor-aplicatiei-yandex-go/

The NCPDP recommends maximum attention when transmitting/offering personal data

In view of the multitude of cases in the media, as well as the specifics addressed in the increasing number of complaints and complaints under examination, the NCPDP urged data subjects to exercise the utmost caution when disclosing, transmitting, disseminating personal data concerning them.

The NCPDP recalls that identity documents (such as identity cards, passports), civil status certificates, pensioners' cards, bank cards, etc. contain lots of personal data, which require effective protection on the part of their owner/holder.

Thus, giving/transmitting copies of these documents, as well as writing personal data in various lists/documents by the data subject for purposes other than those expressly provided for by law, may result in their unlawful use for purposes contrary to those originally intended, to the detriment of the data subject. Likewise, the personal data subject could lose control over his/ her personal data.

If data subjects are asked to show identity documents and/or to provide copies of these documents, as well as personal data such as name, surname, IDNP, home address, bank card details, income, amount of pension, etc. under different reasons from third parties, theyhave to make sure about the lawfulness of the collection of personal data and the subsequent use of these data.

However, according to the provisions of Law 133/2011 on personal data protection, personal data subject to processing must be: processed fairly and lawfully; collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

Nevertheless, the NCPDP emphasizes that when personal data is voluntarily provided or transmitted, recorded on various documents or included in lists, the collection of this personal

data is based on the consent of the data subject (Article 5(1) of Law 133/2011), even if the subsequent use of this data proves to be for other purposes or to the detriment of the data subject.

The recommendations text can be viewed by accessing the link: https://datepersonale.md/in-atentia-subiectilor-de-date-cnpdcp-recomanda-vigilenta-maxima-la-transmiterea-oferirea-datelor-cu-caracter-personal/

Recommendations for publishing personal data on social media

With the emergence of social media platforms such as Twitter, Tumblr, Facebook, Telegram, Instagram, LinkedIn, TikTok, Snapchat, etc., social life has undergone a radical change. People easily share news, images, personal opinions, and almost anything that happens in their lives. These platforms have become powerful tools for socializing, making new friends and acquaintances, sharing photos and videos, and promoting information. Disclosure of personal data creates a favourable environment for advertising companies, individuals who launch allegedly charitable appeals (false fundraising for humanitarian purposes), individuals who intend to take revenge, cybercriminals, and this could involve collecting sensitive data about the activities, interests, personal characteristics, political opinions, online habits and behaviours of individuals.

Therefore, social media users must exercise utmost caution in disclosing personal information, sharing public posts, uploading photos/videos or audio recordings, and trusting others on a social network.

However, NCPDP warns that the collection and processing of personal data on social networks, as well as any data processing, must be carried out in strict compliance with the provisions of the Law on personal data protection, and the personal data, that are subject to processing must be: processed correctly and in accordance with the law; collected for specific, explicit, and legitimate purposes, and not further processed in a manner incompatible with these purposes; adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or subsequently processed.

Therefore, NCPDP urges data subjects to protect their privacy prior publishing or sharing any information on social networks or any other online platform.

It is important for social media users to carefully read and understand:

- The privacy policy should include information on what content can be shared with third parties, as well as the ability to delete content from the site;
- The website's features should specify who can see messages, whether they will only be visible to specified recipients or all users on the platform, among other details;

- What biographical information should be provided (e.g. biographical data such as full name, year of birth, age or address should only be used when registering your account and not given to other users on social networks),
- Account information (e.g. sensitive information such as: school attended, political affiliation, bank account information, place of living/domicile, etc. should never be provided);
- Who the potential "Friends" are (e.g. by analysing their profile to understand who they are, what they do and what kind of content they distribute);
- The need to disable the location sharing features of the gadget being used;
- Extreme caution when posting photos/video or audio recordings online (it could be very difficult to delete them, as in the case of metadata or if someone has copied, shared or distributed them on other sites or social networks) etc.

The text of the recommendations can be viewed by accessing the following link: https://datepersonale.md/in-atentia-subiectilor-de-date-recomandari-privind-publicarea-datelor-cu-caracter-pesonal-pe-retelele-de-socializare/

NCPDP recommends taking necessary measures to protect personal data when accessing state registers/information systems

Following the compliance control procedures for personal data processing requirements set out in Law No. 133/2011 on personal data protection, initiated based on complaints received from data subjects, NCPDP identified the following non-conformities: *the tendency to use access credentials (username and password) for a single user account authorized by multiple employees of the beneficiary entity; the use of usernames and passwords by third parties should be avoided. It is important to update the list of authorized users when employment or job position changes occur within the entity. The personal data of the authorized user (IDNP, number or contact address) should not be included in the user lists. The system owner should be informed of any changes in the administrator responsible for accessing the aforementioned information portals listed in the user list. The systematic updating of user passwords and the lack of manual and/or electronic evidence of accessing/consulting personal data stored in state information systems etc.*

The NCPDP does not doubt or deny the right of the public authority to collect/access/consult or verify personal data from various state information systems, which are necessary for the performance of tasks resulting from the exercise of the prerogatives of public authority it is entrusted with, but, all these potential personal data processing operations are to be carried out in compliance with all the conditions for processing personal data laid down by the Law on personal data protection, and the situations identified generate imminent risks with regard to ensuring the confidentiality and security of personal data processed/stored in state registers/information systems, which concern practically all citizens of the Republic of Moldova.

In this context, based on the provisions of art. 20 para. (1) let. a), c), o), q) of Law No. 133/2011 on personal data protection, in order to ensure an adequate level of integrity, confidentiality and security of personal data and with the aim of preventing similar violations to those indicated, NCPDP has made recommendations to public authorities regarding:

a) Regularly revise and update the list of authorized users attached to service contracts concluded in the context of granting access to state information systems, especially those managed by ASP.

b) Establish a mechanism for authorized users to keep a manual and/or electronic record of accessing/consulting personal data. Ensure that employees are informed about the prohibition of unauthorized access/use of personal data from record-keeping systems.

The recommendations text can be viewed by accessing the following link: https://datepersonale.md/in-atentia-autoritatilor-publice/

CHAPTER VI

ACTIVITY OF SURVEILLANCE OF PERSONAL DATA PROCESSING

The work of providing methodological and advisory support from the NCPDP is a key purpose in the correct implementation of national legislation on personal data protection. This activity focuses on several key issues, such as:

- clarifying legal provisions and providing methodological recommendations to ensure correct understanding and proper application of the relevant legislation;
- managing the personal data protection impact assessment process, which is crucial for identifying and addressing potential data protection risks;
- guidance on the implementation of personal data security measures through specific guidelines/recommendations to ensure the protection of sensitive information and the prevention of unauthorised access;
- identifying and explaining the actions and measures required for certain types of sectoral processing to ensure that the processing of personal data complies with the relevant legislation. This is crucial in order to avoid misperception/inaccurate perception of personal data processing rules and to enhance compliance.

By providing this support, the NCPDP contributes to strengthening a strong data protection practice, ensuring that data controllers comply with legal requirements and implement appropriate measures to protect the confidentiality and integrity of personal data.

However, it should be noted that a crucial role in ensuring the compliance of personal data processing in the work carried out by personal data controllers lies with Data Protection Officers.

According to the information provided by personal data controllers, **115** entities have designated Data Protection Officers, which demonstrates the existence of deficiencies in the appointment/ establishment of these persons/subdivisions.

As a reminder, the Data Protection Officer is responsible for coordinating and supervising data protection activities within the organisation, ensuring an integrated and consistent approach to data protection.

By appointing a Data Protection Officer within the organisation and empowering him/her accordingly, it ensures that the management of personal data processing is carried out in accordance with legal rules, while promoting transparency and trust among data subjects.

In the process of appointing the Data Protection Officer, the data controller or the processor shall take into account criteria such as professional qualities, expert knowledge of data protection

regulations and practices, *in particular in the field of law and IT security relating to personal data*, and the ability to perform the tasks laid down. The designated person must have sufficient independence and authority to carry out his/her responsibilities effectively. The controller or processor shall ensure that none of these tasks and duties give rise to a conflict of interest. This may be an employee of the organisation or an external person such as a consultant or data protection expert. A single data protection officer may be appointed for more than one public law legal entity or for more than one private law legal entity entrusted with a general interest mission or concessionaire of a public service. A group of companies may also appoint a single Data Protection Officer provided that he or she is easily available.

It is also important that the Data Protection Officer has a good understanding of the processing operations carried out by the organisation, the IT systems used by the organisation and its data protection needs.

It should be pointed out that according to Art. 25^2 para. (1) of Law No. 133/2011, some of the main tasks of Data Protection Officer in relation to the data controller are:

a) informing and advising the controller or the processor and the employees who process the data of their obligations under this law and other legislation;

b) monitoring c ompliance with this Law and other legislation on data protection and the controller's or processor's policies on personal data protection and the allocation of responsibilities, including for awareness-raising and training of staff involved in processing operations and related audits;

c) providing advice on request on data protection impact assessment and monitoring its functioning.

Thus, in the context of the above, we consider that the person appointed to the position of Data Protection Officer must be in a clear position to be properly and timely involved in all aspects of personal data protection and, at the same time, must not be involved in determining the purposes and means of their processing, including not being responsible for certain processing operations/recording systems of personal data managed, or, from the analysis of the information submitted to the NCPDP address, there are possible risks of conflict of interest in the appointment of the Data Protection Officer. In this regard, reference will be made, for guidance, to the Article 29 Working Party's Guidelines on Data Protection Officers ("DPOs") (GL 243 rev. 01), according to which conflicting positions within the organisation may include senior management positions (**such as Chief Executive Officer, Chief Administrative Officer, Chief Financial Officer, Chief Medical Officer, Head of Marketing, Head of Human Resources or Head of IT Departments**), but also other roles lower in the organisation chart if such positions or roles lead to the determination of the purposes and means of data processing.

Processing of personal data stored in the main automated state information resources

The situation regarding access to the main state registers/information systems carried out through the Search Information System (SIC) "Access-Web" and Common Object Interface (COI) technology has been in the sights of the National Authority for Personal Data Protection for several years.

In this context, the NCPDP dynamically analyzes the statistics of accesses made in recent years by users: the Ministry of Internal Affairs, the National Anti-Corruption Centre, the General Prosecutor's Office, the National Integrity Authority, the Ministry of Defence, the Customs

Service, the State Tax Service, entities that have been identified with the highest number of accesses of personal data undertaken. The information in the following table is based on data provided by the Public Services Agency and the e-Government Agency, entities that provide access to information contained in the main state registers/information systems for various public institutions and private organisations.

Institution concerned	Number of accesses to state information systems: RSP, RBI, RST, RSCV, RSUD				
	via SIA „Acces-Web" and COI			Via the interoperability platform (MConnect)	
	2021	*2022*	*2023*	*2022*	*2023*
Ministry of Internal Affairs	**13259515**	**22446877**	**26781106**	**15429**	**3125054**
Intelligence and Security Service	**69196**	**70184**	**73624**	**43080**	**65042**
National Anticorruption Center	**74493**	**75486**	**53727**	**10468**	**9691**
General Prosecutor's Office	**22405**	**30797**	**15066**	**6**	**0**
Customs Service	**14063**	**17715**	**14102**	**6**	**151067**
Ministry of Defence	**503**	**727**	**498**	**115301**	**302896**
National Integrity Authority	**18823**	**19127**	**15661**	**11759**	**19825**
State Tax Service	**3007799**	**4071998**	**9685627**	**9566872**	**15996061**

As it can be seen from the table, the accesses carried out in 2023 by the targeted institutions through the access technologies offered by the Public Services Agency and the eGovernment Agency show that: the Ministry of Internal Affairs, the Intelligence and Security Service, the National Anti-Corruption Centre and the General Prosecutor's Office carried out accesses mostly through the SIC "Access-Web" and COI and the Customs Service, the Ministry of Defence, the National Integrity Authority and the State Tax Service accessed the targeted state information resources preferentially through the interoperability platform (Mconnect).

At the same time, the overall analysis of the situation in this chapter showed that in 2023, compared to previous reporting periods, there was a clear upward trend in the number of accesses through the interoperability platform (MConnect).

Last but not least, the number of accesses by the State Tax Service, the Ministry of Internal Affairs, including its subdivisions, and the Ministry of Defence increased substantially compared to the previous year.

We recall that, according to the provisions of Article 13 para. (3) and (5) of Law No. 142/2018 on data exchange and interoperability, the existing bilateral data exchange contracts or agreements concluded between public participants will be terminated by law, once the corresponding data exchange through the interoperability platform is carried out, **except for the case** when special legal provisions are applicable in the field of supervision of financial sector entities, national defence, state security, maintenance of public order, counteracting crime, preventing and combating corruption, acts related to corruption and acts of corrupt behaviour, as well as protection of the rights and freedoms of individuals.

The above-mentioned provisions are the basis for the continued use of Common Object Interface (COI) technology, which does not provide for the nominal identification of users who have carried out data access operations, but who are required to justify the purpose and legal basis of these operations.

At the same time, as regards access to the state information registers/systems managed by the Public Services Agency, in particular through the e-Cadastre information portal and the SIC "Web Access", during 2023, in the framework of the controls initiated, the NCPDP noted the admission by various entities benefiting from information access services to state information resources of violations of personal data processing, such as:

- *the tendency for the access credentials (username and password) of a single authorised user account to be used by several employees of the beneficiary entity;*
- *possession/use of username and password by third parties;*
- *lack to update the list of users after termination of employment, change of job or position in the entity;*
- *failure to include personal data of the authorised user (IDNP, contact number or address) in user lists;*
- *failure to inform the owner of the information system about the change of the administrator responsible for access to information resources, indicated in the user list;*
- *failure to systematically update user passwords etc;*
- *failure to keep manual and/or electronic records of access/consultation operations of personal data stor*ed in state information systems.

In order to prevent unauthorized access to personal data and/or unauthorized use of personal data, the NCPDP came up with recommendations, which were sent to all central public authorities, which disseminated the NCPDP's approach to subordinate institutions, territorial offices of the State Chancellery and first and second level local public administration authorities, in order to inform the Personal Data Protection Authority about the measures taken in relation to the issues highlighted above.

As a result, the NCPDP received 36 responses from the recipient entities, informing them of the organisational and technical measures taken in order to comply with the recommendations submitted.

It was gratifying that some of the central public authorities mentioned that they were aware of the provisions highlighted in the NCPDP's approach and ensured compliance with the personal data protection principles laid down in Law No 133/2011 on personal data protection.

In the context of actions to prevent non-compliant processing of personal data, the NCPDP has undertaken a series of actions, including: referral to the relevant public authorities

on the problematic issues identified in the personal data protection segment, providing recommendations to both data controllers and data subjects, including by publishing them on the NCPDP's website as follows:

- *transmission of personal data to the "Yandex Go" app;*
- *giving/transmitting personal data, including copies of ID documents to various persons;*
- *publishing personal data on social networks;*
- *taking the necessary measures to protect personal data when accessing state registers/ information systems.*

Similarly, in order to ensure the information and awareness of society on the field of personal data protection, during 2023 a multitude of trainings were conducted for representatives of data controllers on the rules for personal data in the context of the Law on personal data protection, being trained about **3795** people.

CHAPTER VII

ENDORCEMENT OF DRAFT NORMATIV ACTS

In accordance with its tasks, the NCPDP makes proposals for the improvement of the legislation in force in the field of personal data protection and processing, including by submitting opinions on draft laws and other normative acts.

Where processing is carried out by the controller pursuant to a legal obligation or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing shall be regulated by normative acts.

In the endorsement process, the NCPDP comes with proposals that the act should include clear regulations on the purpose of the processing, the general conditions governing the lawfulness of personal data processing, the criteria for establishing the controller, the categories of personal data subject to processing, the data subjects, the entities to which personal data may be disclosed, purpose limitations, the storage period, the realisation of the rights of the data subjects and other measures to ensure lawful and fair processing of personal data.

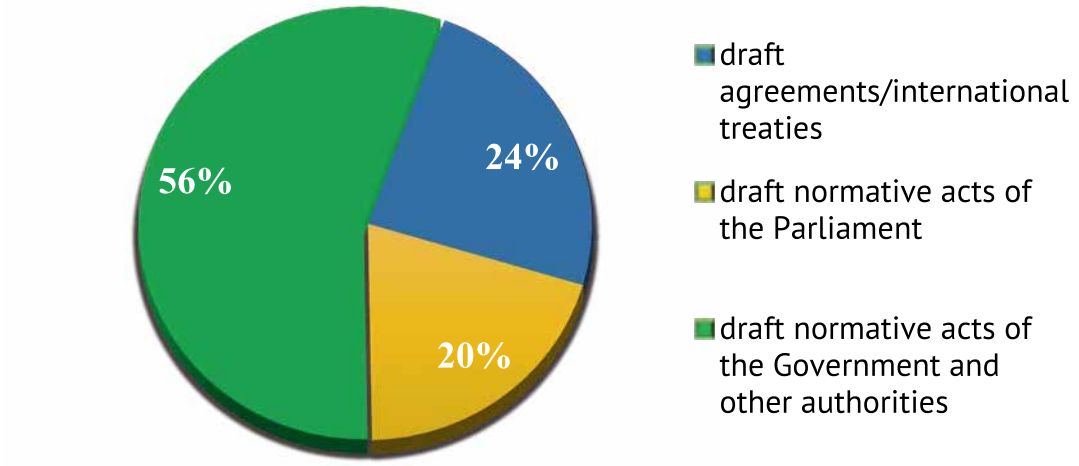
The work of endorsing draft laws focused on the submission of proposals on a significant number of draft normative acts and the elaboration of points of view on the adequate application of the rules in the field of personal data protection.

The opinions were aimed at informing the general public and providing legislative advice to the competent public authorities or institutions, as well as to other entities, in order to ensure a uniform and correct application of the principles of personal data protection.

In this regard, during the year 2023, **154** draft national regulations/international treaties were submitted to the NCPDP for approval in relation to the protection of the rights and freedoms of individuals with regard to the processing of personal data, including:

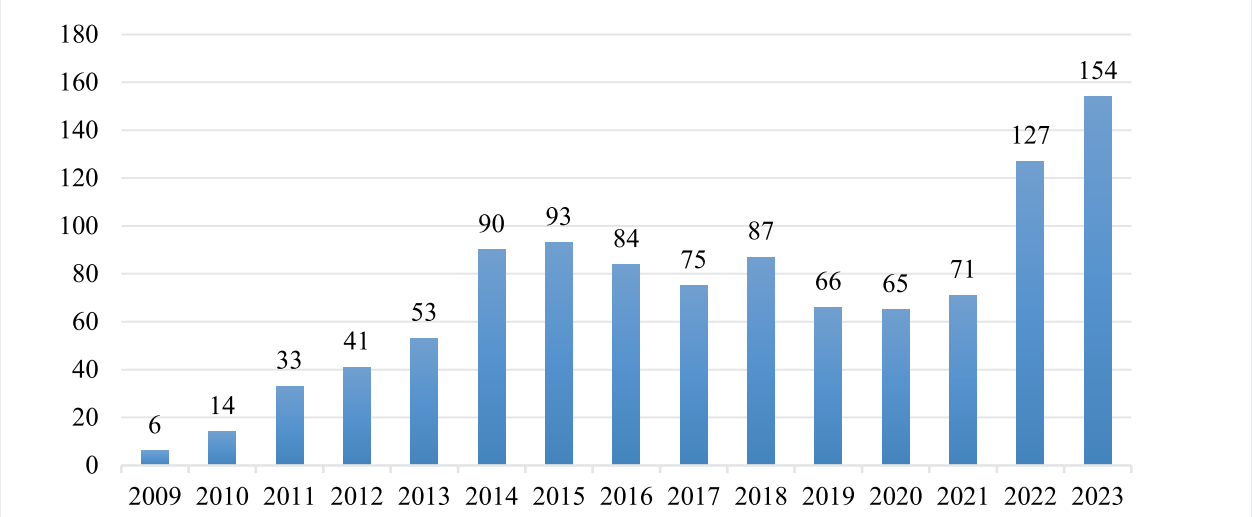
- 37 draft agreements/international treaties;
- 31 draft normative acts on amending codes and regulations;
- 86 draft normative acts of the Government and other authorities.

Procentage of opinions given by NCPDP in 2023



In the case of most of the drafts proposed for endorsement, the NCPDP considered that it was necessary to complete, amend or revise the respective texts, presenting a series of recommendations and proposals with a view to adjusting/conforming certain provisions of the respective drafts to the principles and conditions for processing personal data, in order to guarantee respect for the rights of personal data subjects.

Dynamics of draft laws submitted for approval 2009-2023



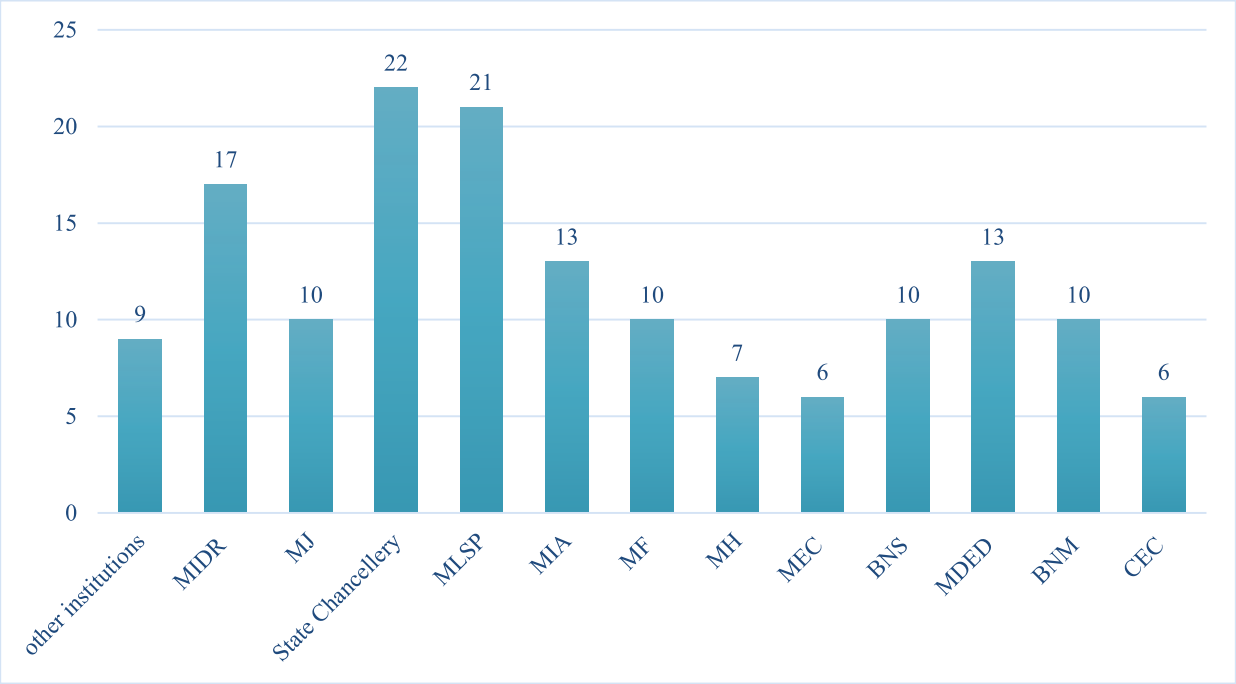
Separately, we present below the most relevant draft normative acts endorsed, as follows:

- *draft laws on the Intelligence and Security Service, on the status of intelligence and security officer, and on counterintelligence and foreign intelligence activity;*
- *draft decision on the approval of the draft law on the amendment of some normative acts (ensuring access to information of public interest);*
- *draft law on amending Article 5 para. (8) of the Law No. 308/2017 on preventing and combating money laundering and terrorist financing;*

- *draft law on the amending of some normative acts, submitted as a legislative initiative by a group of deputies in the Parliament of the Republic of Moldova (use of platforms in the provision of road transport services in taxi service);*
- *draft Government Decision on the initiation of negotiations and approval of the signature of the Financing Agreement between the Government of the Republic of Moldova and the European Commission on the „EU Resilience and Governance" Programme;*
- *draft decision on the approval of the Regulation on the organisation and functioning of the Demographic and Social Statistics Information System;*
- *draft decision on the approval of the procedure for remote identification of persons using digital means;*
- *draft decision on the approval of the draft law on access to information of public interest;*
- *set of materials on the initiation of negotiations on the Agreement between the Republic of Moldova and the International Federation of Red Cross and Red Crescent Societies on the legal status, privileges and immunities of the International Federation of Red Cross and Red Crescent Societies in the Republic of Moldova;*
- *draft resolution on the approval of the draft law on the amendment of some normative acts (facilitation of the business environment);*
- *draft Government Decision "On the approval of the National Statistical System Development Programme for 2023-2026";*
- *draft Agreement between the Government of the Republic of Moldova and the Government of the Republic of Iceland on the readmission of persons residing illegally;*
- *finalised draft of the Government Decision on the amendment of Government Decision No 128/2014 on the common government technology platform (MCloud);*
- *draft decision "on the approval of the Regulation on the peculiarities of nomination and registration of candidates for local elections";*
- *draft decision on the amendment of Annex No. 1 to Government Decision No. 1310/2003 on the approval of the Regulation on obtaining, recording, storing, systematizing and using fingerprint data and the List of positions held by persons subject to mandatory fingerprint registration;*
- *draft „Agreement between the Republic of Moldova and Ukraine in the field of social security"*
- *draft Agreement between the Government of the Republic of Moldova and the Government of the Italian Republic on the mutual recognition of driving licences for the purpose of conversion";*
- *draft Agreement between the Republic of Moldova and Canada in the field of social security;*
- *draft decisions "on the approval of the Regulation on the State Register of Voters" and "on the approval of the Regulation on the drawing up, administration, distribution and updating of electoral lists";*
- *draft decision on the approval of the concept of the information system "Migration";*
- *draft decision on the approval of the Concept of the Unified Information System „e-Admission" in higher education";*

- *draft decision on the modification of Government Decision No 834/2008 on the Integrated Information System of the Border Police;*
- *the draft Government Decision on the approval of the Regulation of the Information Resource formed by the Information Subsystem „Autotest";*
- *draft decision on the Concept and Regulation on the organization and functioning of the Information System „National Cancer Registry";*
- *draft decision on the approval of the "Concept of the Information System for Recording Human Resources in the Health System (SI ERUSS)";*
- *draft decision on the approval of the draft law on the use of data from the Passenger Name Register (PNR);*
- *draft decision on the amendment of some normative acts (revision of the functionality of the Government Entrepreneur Portal and the Government Citizen Portal;*
- *draft decision on the approval of the draft law on the modification of some normative acts (in the field of state control over entrepreneurial activity);*
- *draft Government Decision on the amendment of Government Decision No. 951/2022 on the organization and conduct of the population and housing census in the Republic of Moldova in 2024;*
- *the draft decisions "on the approval of the Regulation on the State Register of Voters" and "on the approval of the Regulation on the drawing, administration, dissemination and updating of electoral lists";*
- *draft Memorandum of Understanding with A.O. „Red Cross Society of Moldova" on financial assistance to be provided to vulnerable families affected by the crises: rising prices, war in Ukraine;*
- *draft bilateral agreement on cooperation in the field of repatriation of unaccompanied children to their place of habitual residence between the Republic of Moldova and Romania;*
- *the draft Decision of the National Commission for Financial Markets on the approval of the Regulation on the conditions and procedure for registration in the Register of insurance and bancassurance agencies;*
- *draft decision "on the approval of the Regulation on the financing of political parties";*
- *draft Government Decision for the approval of the Concept of the Information System "State Register of Genetic Data" and the Regulation on the way of keeping the Information System "State Register of Genetic Data";*
- *draft Memorandum of Understanding and Annex on the obligations of the parties in the process of processing personal data in relation to the provision of currency assistance to vulnerable Moldovans and integration of the response to challenges in the national social protection system of the Republic of Moldova.*

Number of requests for endorsement received by NCPDP in 2023



Below, for information purposes, we present some of the most important opinions issued by the NCPDP on draft laws in the reporting year:

1.On the draft law on access to information of public interest, the NCPDP noted that the adoption of a new law is an important step in the process of ensuring the transparency of government activity and in the accountability of information providers, in the part aimed at providing public access to information held.

At the same time, it was pointed out that the content of the draft contains general and insufficient regulations, which do not facilitate access to information, do not bring clarity and ease the burden on information providers in examining requests for access to information according to explicit and accessible criteria.

Even though the content of the Information Note to the draft is extensive and comes with explanations to bring clarity, in particular, to the application of the rules of Articles 6 and 7 of the draft, which regulate the limitation of access to information of public interest and the application of the criterion of proportionality of limitation, it was considered imperative that these wordings/interpretations be reflected, to an appropriate extent, in the actual content of the draft law. However, they will be useful and necessary for information providers, who are obliged to apply the criterion of proportionality of limitation, especially in view of the fact that the provisions of the Information Note to the draft cannot be binding on the subjects concerned and, after the adoption of the law, they have no legal value and are no longer accessible.

It was noted that the new law on access to information of public interest must be clear, predictable and sufficiently accessible to enable data subjects to act in accordance with the law and to enable information providers to correctly apply the proportionality test in limiting access to information of public interest so as not to unduly interfere with the rights and freedoms enshrined in a democratic society.

At the same time, the notion of information of public interest reflected in Article 2 of the draft is too general and not comprehensive, referring to all information held by information providers, regardless of the storage medium (paper, electronic or any other format). In this respect it was noted that not all information held by an information provider could be of public interest, for example: data on border crossing or tax payments by a certain person, who does not hold a public position, is not a public person and has not been involved in public facts/actions.

At the same time, the draft law places the task and responsibility on the information provider to assess and analyse the information requested in the access request in terms of whether it is of public interest or relates to private life, with no benchmarks to guide them. In these circumstances, the information provider is made difficult to make an assessment as, according to Article 14 of the draft, the applicant is not obliged to give reasons/justification for the request and to demonstrate a specific interest in obtaining the information.

The protection of the legitimate purposes listed in Article 6 of the draft is an exception to providing access to official information, and information providers, regrettably, do not have clear criteria to guide their determination, in which order there is a risk of discretionary application/ interpretation of access to protected categories of information, which will consequently lead either to an illegitimate restriction of the right of access to official information or to a violation of the protection of legitimate purposes granted by law.

In this chapter it was mentioned that the version of Law 982/2000 is much more substantial, as Art. 7 para. (2)(c) states that access to official information may not be restricted, except for personal information, the disclosure of which is considered as an interference in the privacy of the person, protected by the legislation on personal data protection.

Such an approach is found in Law 544/2001 on free access to information of public interest in Romania, which clearly defines in the content of the normative act what information on personal data is.

Subsequently, Article 14 of the Romanian law regulates that information on the citizen's personal data may become information of public interest only to the extent that it affects the capacity to exercise a public function.

It has been noted that when balancing two related interests, e.g. the right of access to information and one of the legitimate aims listed in Art. 6 para. (1) of the draft, for the information provider, the primary/sectoral regulatory act governing the legitimate purpose (*e.g. Law no. 245/2008 on state secrecy*) is paramount, to which the latter can easily refer when basing its refusal to provide the requested information.

Regrettably, Article 6 of the draft did not contain any rules that would clarify the concept of privacy, when information about private life can become information of public interest and the applicable regulatory framework governing the conditions of processing *(access, provision, disclosure, publication, etc.*) of information about private life, including personal data.

In addition, it was considered relevant to complete Article 6 of the draft with a new paragraph with the following content: *"Access to personal data which in accordance with the regulations are of a public/open nature may not be restricted."*

At the same time, it was noted that the fact that the proportionality criterion of limitation, reflected in Article 7 of the draft regulation, is to be left to the information provider, will generate a number of obstacles in the cumulative and reasoned implementation of the three conditions set out in a generalized form, and it is not clear how the damage to the privacy of the individual caused by the disclosure of the requested information will be estimated.

At the same time, the assessments to be made by the information provider, in the light of the provisions of Article 7(b) and (c) of the draft, regarding the damage that will/could be caused in connection with the provision of the requested information in relation to the legitimate purpose identified by the latter, cannot always be objective and directly related to the person - the right holder. However, the assessment of the damage, when we are talking in particular about a natural person, depends directly on the personality of the subject, who proves and assesses the extent of the damage himself.

It was reiterated that the requirements set out in Article 7(b) and (c) of the draft will, in practice, create major obstacles for information providers in examining requests for access to official information, to whom such conditions are attributed a discretionary role of arbiter in balancing fundamental rights, a role which is currently exercised by the court.

Furthermore, with reference to the text of Article 8, it was proposed to supplement paragraph (1) with a new letter after letter b) to be worded as follows: "c) *the surname, first name, position held by the employees of the authority, e-mail addresses and telephone number*". At letter (h), given that not only the heads of the Authority and the heads of subdivisions go on working trips, it was considered appropriate to add after the words *'heads of subdivisions'* the words *„and other employee"*. Letter l) of the same paragraph was too general in content, as it was not clear to which data/type of controls it referred: statistical/disaggregated/compiled data or access to all information on the results of controls carried out, which could have negative consequences for the persons concerned by the control, in which order it was recommended to revise the rule, and the obligation to publish/non-publish information on the carrying out of controls should be regulated by special laws regulating the procedure of carrying out controls in various areas, for example, as in the case of the Law on State Control over Entrepreneurial Activity.

With regard to the provision in para. (2) of the mentioned article, the wording provided, creates uncertainties, as it is not clear to which categories of disabilities reference is made, also taking into account that this imposed obligation implies additional costs, which are quite high.

According to the provisions of Article 13 of the draft, the information provider is obliged to establish/implement a new special Register of requests for disclosure of information of public interest, given that practically every public authority currently registers requests for access to information as an integral part of the correspondence of public authorities through the electronic document management system "E-Management documents". The creation and development of a special Register for this purpose is inappropriate, as each entity manages its correspondence within the limits of the general regulatory framework.

With reference to Articles 21 and 22 of the draft, it was noted that, in addition to the grounds provided for refusal of the request/refusal to disclose information of public interest, there could be situations where the request for access to information of public interest is too vague to identify the documents concerned, or the request is manifestly unreasonable, the information provider having no legal powers to react to it, in which case it is necessary to give the possibility to the information provider to request additional information to clarify the request.

In the part dealing with Chapter V of the draft, the classification of the acts of non-disclosure of the number and date of registration of the application, the total or partial re-registration of the application, as being liable, was considered unjustified and disproportionate in view of the insignificant degree of damage and the minor consequences of these actions of the provider of information of public interest.

Generally speaking, the establishment of legal liability for information providers generates other unfavourable sides, or the responsible persons, for fear of being fined, will provide any

information requested, without making a demarcation whether access to it is limited or not, whether the requested data are of public interest or not.

The limited deadlines for examining requests for access to information of public interest, plus the complexity of basing a refusal to provide information on the 3 proportionality criteria, will predispose/determine the information provider to satisfy, for the most part, requests for access to information without carrying out a proper analysis.

On the other hand, according to the draft in question, it was noted that the means of defence of the applicant for information are regulated, when he considers that his rights have been prejudiced, may request compensation for moral and material damages in court, with an order to the information provider to release the requested information.

It has been emphasised that the right of access to information is not an absolute right and must be applied with respect for the scope of other competing rights, requiring a complicated balancing exercise amongst competing rights, which can be carried out by the court, which has the task of verifying whether the information requested concerns information of public interest. As the CJEU has also stressed in its judgments, balancing the fundamental right to privacy with other rights is "by no means a precise science", making national courts responsible for finding the right balance between competing rights.

In addition, in order to meet the requirement of predictability of the provisions of the normative act, it was considered appropriate to exclude/revise the words "*other public authorities*" in Art. 28 let. c) of the draft, as it makes the rule imprecise and unclear.

In the light of the above, it was proposed to revise the draft in the context of the comments submitted, which will make a substantial contribution to compliance with the principles of transparency and accountability of information providers, as well as to the non-admission of interference in the fundamental rights and freedoms of individuals, in particular the right to inviolability of privacy with regard to the processing of personal data.

2. *In the draft Government Decision approving the Concept of the Information System "State Register of Genetic Data" and the Regulation on how to keep the Information System "State Register of Genetic Data",* the NCPDP noted that the draft normative acts are developed in accordance with Article 7(1) of Law No. 235/2017 on legal genetic registration, as well as with a view to implementing point 9, subpoint 9.8 of the Government Action Plan for 2023, approved by Government Decision No. 90/2023.

At point 30 subpoint 1) of the draft Concept of the Information System "State Register of Genetic Data" (hereinafter SI RSDG), it was proposed to replace the term "*personal numerical identifier*" with the term "*state identification number of the natural person*", in accordance with Law No 273/1994 on identity documents in the national passport system.

It has been determined that point 41 of the SI RSDG Concept describes the interaction of the SI RSDG with shared government information systems, the use of which is mandatory for specialised central government authorities. At the same time, the State information systems and resources that will interact and ensure data exchange with the SI RSDG are not specified concretely and precisely, similarly to point 71 of the draft Regulation on the way of keeping the SI RSDG. However, at the implementation stage, the interaction of the SI RSDG with the basic and additional external information systems belonging to public authorities is to be ensured from a legal point of view, in compliance with the legal limits.

It was proposed to revise and correlate point 41 of the draft SI RSDG Concept and point 71 of the draft Regulation on the way of keeping the SI RSDG, with the express specification of

the external information systems/resources that will ensure the exchange of data with the SI RSDG, the categories/flows of personal data, necessary to be retrieved in order to achieve the purposes.

At point 50 it was recommended that, when transmitting confidential information, the method of protection of information transmitted through all types of communication channels against interception, alteration or falsification of information should be encryption of the information, without exception, and at short distances - the use of protected optical fibres as communication channels.

In this context, it was reported that the use of cryptographic data security means with guaranteed strength for the required level of confidentiality and the electronic key system ensures message authentication and secure information exchange.

Also, at this point, it was considered appropriate to define/describe the information security mechanisms used, not only by indicating, but also by supplementing them with the following notions:

> *"confidentiality: guarantees that the data exchanged between the person requesting it and the provider cannot be intercepted or accessed by an unauthorised third party and cannot be accessed at an inappropriate time;*
>
> *integrity: ensures that the data flow between the requester and the provider has not been altered or manipulated by an unauthorised third party or the data has not been accessed before a certain term or a certain time;*
>
> *non-repudiation: a measure ensuring that, after sending/receiving information, the sender/ receiver cannot falsely deny having sent/received information;*
>
> *maintenance: the SI RSDG must be provided at all times with the necessary support and maintenance in accordance with the agreed level of service."*

With reference to point 86 of the draft Regulation on the way of keeping the SI RSDG, which provides for the obligation to register the SI RSD in the Register of personal data controllers, it was noted that, in the light of the new amendments made to Law No 133/2011 on personal data protection, this task was excluded by Law No 175/2021 amending some normative acts.

3. On the draft decision on the approval of the draft law on the amendment of some normative acts (facilitation of the business environment activity) the NCPDP noted that the draft law intends to supplement Art. 2 and Art. 15 of the Law No. 133/2011 on personal data protection with exceptions and restrictions to certain legal provisions.

According to the Information Note to the draft, *the purpose of these amendments is to grant the right to persons subject to state control of entrepreneurial activity to make audio and/or video recordings of inspectors who are in the exercise of their duties and carry out state control, without the obligation to warn about this fact in advance or to obtain the inspector's consent. Similarly, the note mentions that currently such an exception exists only in relation to law enforcement bodies in relation to citizens, but not vice versa, so in order to be able to film an inspector or police officer who is in the exercise of his duties anyway permission must be obtained in advance. The amendment will provide a viable tool in the fight against corruption and abuses by law enforcement bodies.*

Thus, in the context of the information note to the draft, it was noted that the right of law enforcement bodies to make audio and/or video recordings is provided for in the normative acts directly regulating the activity of these bodies/authorities and not in Law No. 133/2011.

Therefore, the amendments made to the articles mentioned of the Law on personal data protection are irrelevant, inappropriate and unjustified in relation to the current content/ meaning of these articles, which, at the moment, have a well-defined purpose and are strictly addressed to law enforcement bodies.

It has been specified that, currently, the Law on Personal Data Protection provides a viable and legal tool for the inspected persons to carry out personal data processing operations, by means of audio and/or video recording of inspectors in the exercise of their duties and carrying out state control, actions which can be covered by the provisions of Article 5 para. (5) (e) of the above-mentioned law, in which case the intervention on letter (d) of Art. 2 para. (2) of Law 133/2011 is neither necessary nor justified.

At the same time, attention was drawn to the fact that the rule laid down in Article 2 para. (2) letter d) exclusively concerns the activity of law enforcement bodies, which process personal data in the framework of criminal or misdemeanour proceedings under the law and, given the specific nature of the activity carried out, are entitled to apply restrictions/exceptions to the processing of personal data and the realisation of the rights of data subjects, in order not to prejudice the actions/objectives pursued in the exercise of legal powers. Thus, the activity of law enforcement bodies cannot always be proportional or equal to the scope of state control over entrepreneurial activity.

In the part concerning the addition of a new paragraph to Article 15 of Law 133/2011, with the following content "(5) *The exceptions and restrictions provided for in paragraphs 1 and 2 may also be applied by natural or legal persons interacting with public authorities in the situations referred to in paragraph 1 in order to ensure respect for the rights and freedoms of individuals and/or family members and to prevent possible abuses or illegal actions by representatives of the public authorities concerned*", it was noted that these supplemets go beyond the scope of the regulation and do not fall within the article concerned, which has a different meaning and purpose.

It has been specified that the legislator's intention was to establish in Article 15 exceptions and restrictions only in the context of the actions provided for in Article 2(2)(d) and Art. 5 (5) (g) of Law No 133/2011 and only for the purposes of national defence, state security and the maintenance of public order, the protection of the rights and freedoms of the data subject or of other persons, if by applying art. 4(1), Art.12 (1) and (2), art.13, 14 of the Law is prejudiced the effectiveness of the action or the purpose pursued in the exercise of legal powers of the public authority.

Similarly, this chapter pointed that Article 15 of Law 133/2011 does not provide for exceptions to the provisions of Article 5 of the Law on personal data protection, but the alleged audio/ video recordings are to be made on the legal basis provided for in the legislation of the field of activity, which ensures that the processing of data falls within the legal grounds set out in Article 5(5) of the above mentioned law.

As a result, all personal data controllers, without exceptions and limitations, shall process personal data on the basis of a well-founded legal basis, including law enforcement bodies, to which Article 15 of Law 133/2011 is applicable.

It was reiterated that consent is not the only legal basis for processing personal data and Article 5(5) of Law 133/2011 would provide data controllers, including persons subject to control, with the legitimacy to carry out personal data processing operations by means of audio and/or video recording of inspectors performing their duties and carrying out state control, especially in the context of the proposed amendment to Art. 25 of Law 131/2012.

Under these circumstances, for the establishment, exercise or defence of a right in court, either in judicial proceedings or in administrative proceedings, the inspected persons could have a legitimate interest in the processing of personal data by means of audio and/or video recording of the inspectors, under the conditions laid down in Article 5(5). (5) let. e) of Law No. 133/2011.

It was pointed out that the amendments made to Article 25 of Law No. 131/2012 on state control over entrepreneurial activity, which is proposed to be supplemented with a new letter with the following content: *"k) to make video and/or audio recordings of the actions of inspectors throughout the duration of the control activity, without the obligation to inform about this fact or obtain the consent of the inspectors or the control body;"* would be sufficient and complete in order to classify the actions of processing personal data carried out by the persons subject to inspection in accordance with the provisions of the legislation on personal data protection.

In the light of the above, the NCPDP did not endorse the proposed amendments to Law No 133/2011 on personal data protection.

4. On the draft law on the amendment of some normative acts, submitted as a legislative initiative by a group of deputies in the Parliament of the Republic of Moldova, the NCPDP communicated that, according to the Information Note, the draft law regulates the obligations and legal framework concerning the holders of the rights of ownership and/or operation on the territory of the Republic of Moldova of electronic systems (platforms) for the management, placement/reception of orders and/or payments for the providing of road transport taxi services.

It was mentioned that through these systems/platforms made available to natural persons - customers/employees by the legal holders, through which it is intended to place/receive orders for the providing of road transport taxi services, personal data processing processes/operations will take place.

It is specified that the processing of personal data, regardless of the means used, shall be carried out in compliance with the provisions of Law No. 133/2011 on personal data protection.

The NCPDP noted that para.(2) (d) of Article 81 of the Road Transport Code refers to "*and the security of personal data processed*", but in the context of the proposed amendments, the rule stated/prescribed is not sufficient/adequate to determine/guarantee the minimum rules to be observed when processing personal data.

In this context, it is proposed to exclude from letter (d) para. (2) of Art. 81 of the Road Transport Code of the text "*and the security of personal data processed*" with the addition of a new paragraph in the same article or of para. (2) with the following new wording:

"When processing personal data through electronic management systems/platforms, compliance with the legal conditions for processing personal data shall be ensured, also the confidentiality and security measures of the personal data processed, guaranteeing the realization of the rights of data subjects, in accordance with the provisions of the Law on personal data protection shall be ensured."

At the same time, it was noted that, on the basis of the provisions of the draft law in question, the owners of the electronic management systems (platforms) specified above will be obliged to register legally on the territory of the Republic of Moldova, in order to provide the service of intermediation of the purchase of taxi transport service between the final beneficiary and taxi transport providers.

In the same vein, in the context of ensuring effective protection of personal data processed, it was considered appropriate to examine the possibility of establishing the rule on the use of electronic management systems (platforms) managed / kept / stored on the territory of the

Republic of Moldova. However, taking into account the provisions of Articles 4 and 5 para. (5) (b) of the Law No 133/2011, the obligations/rules on processing of personal data (*such as for example: use of national electronic management systems/platforms, as well as keeping the servers on the territory of the Republic of Moldova, without allowing cross-border transmission of personal data)* must be provided for by law.

In the same context, it was pointed out that in the case of taxi order management platforms owned by non-resident owners, but operating and/or producing legal effects on the territory of the Republic of Moldova, the competent state authorities will face obstacles and/or will not be able to exercise effective control over their possibly harmful actions.

Implicitly, the NCPDP will not have sufficient tools to be able to control the compliance of the processing of personal data, in the light of the provisions of Law No 133/2011, if the personal data of data subjects (customers/taxi drivers) would be transmitted, in particular, to countries that do not ensure an adequate level of personal data protection.

It has been specified that, in the circumstances set out above, including the personal data subject will lose control over his personal data and will be unable to exercise his rights enshrined in Law No 133/2011.

In the context of the aspects highlighted above, as well as the information in the media regarding the use of personal data processed through international platforms (e.g. "Yandex Taxi") to the detriment of data subjects or for purposes other than those declared by the controller, it was considered appropriate to request, on the basis of the given draft, including the opinion of the Intelligence and Security Service, from the perspective of ensuring information security.

It was pointed out that in the case of use by providers in the Republic of Moldova of foreign systems/platforms, managed/created by non-resident providers, whose servers are located outside the country, the situation of cross-border transmission of personal data collected/ processed through these systems/platforms automatically arises, which determines the mandatory applicability of Article 32 of Law 133/2011.

5. *On the draft law amending Article 5 para. (8) of the Law no. 308/2017 on preventing and combating money laundering and terrorist financing NCPDP* communicated that, according to the information related to the draft, the presentation of identity documents when performing currency exchage

exchange operations becomes mandatory, regardless of the amount, representing an important measure to prevent money laundering and terrorist financing, which helps to protect the financial system and ensure a safe and transparent financial environment.

In this context, the NCPDP specified that such amendments to Law No. 208/2017, generate massive/major personal data processing operations, to be carried out in strict compliance with the provisions of Law No. 133/2011 on personal data protection.

However, according to the official website of the National Bank of Moldova[1], as of 01 August 2023, there are 408 currency exchange offices (legal entities) that hold the license of the National Bank of Moldova to perform currency exchange operations with natural persons on the territory of the Republic of Moldova.

Similarly, 747 foreign exchange offices (including foreign exchange machines) of licensed banks performing currency exchange operations with natural persons on the territory of the Republic of Moldova and 7 hotels holding the license of the National Bank of Moldova for

[1] *https://www.bnm.md/ro/content/informatie-aferenta-caselor-de-schimb-valutar*

currency exchange activity with natural persons (purchase operations) through their own foreign exchange bureau were certified.

The above-mentioned figures raise concerns regarding the level of awareness/preparedness of the foreign exchange entities and their level of equipment, both technically and physically/ organizationally (*given the large number of them operating on the territory of the Republic of Moldova*), in the application and implementation of the new provisions, in order to ensure compliance with the processing of personal data, including respect for the rights of data subjects and ensuring the confidentiality of personal data[2] and the security of personal data when processing them[3].

It was noted that Article 5 of Law No 133/2011 sets out the legal grounds for personal data processing. For example, as appropriate to the case at hand, the consent of the personal data subject is not required in cases where the processing is necessary for the performance of an obligation of the controller by law.

In this situation, for the legal obligation to be valid and binding, the law must be known to the person to whom it applies, it must be accessible, it must meet the criterion of foreseeability and it must also comply with the legislation on personal data protection, including the requirement of necessity and proportionality in relation to the intended purpose, in order to exclude any unjustified intrusion into the privacy of the natural person, as well as safeguards to ensure the rights of data subjects, to ensure the security of personal data processing and the confidentiality of such data.

Also, it should be taken into account the principles of lawmaking, as reflected in Law No 100/2017 on normative acts, in accordance with which the draft normative act must be clear, predictable and sufficiently accessible.

However, the format in which para. (8) of Art. 5 – *currency exchange operations shall be carried out only upon presentation of identity documents, and the data therein shall be recorded by the foreign exchange entity,* leads to some ambiguities, in particular: what categories of personal data shall be processed from customers, in their capacity as data subjects, however, the term *"data"* is a general and interpretative one; what would be the mode of personal data processing by cas exchange entities, electronic/manual/mixed; to which persons/authorities such data may be disclosed and for what purposes, etc.

At the same time, according to the information note to the draft law, financial institutions have a legal responsibility to verify the identity of customers and to ensure that financial activities are legal, at what point it was noted that it is not clear to which financial activities the note refers and by which means the institutions concerned will ensure that financial activities are legal.

Thus, it was considered appropriate to supplement Article 5 of Law no. 308/2017 with clear provisions, which would place responsibility on the National Bank of Moldova to establish and regulate a secure and uniform mechanism for the collection and management of personal

[2] *Art. 29 para. (1) of Law 133/2011, controllers and third parties who have access to personal data are obliged to ensure the confidentiality of such data, except in the following cases: a) the processing relates to data voluntarily and manifestly made public by personal data subject; b) the personal data have been depersonalized*

[3] *Article 30 (1) of Law 133/2011, when processing personal data, the controller is obliged to take the necessary organizational and technical measures to protect personal data against destruction, alteration, blocking, copying, dissemination and other unlawful actions, measures designed to ensure an adequate level of security with regard to the risks presented by the processing and the nature of the data processed.*

data by currency exchange entities - in the form of a register/system, ensuring sufficient and adequate safeguards for the rights and freedoms of data subjects, conditions that would give citizens confidence that their personal data are processed securely, and to the state an effective control over the data contained in this register.

6. On the draft decision on the approval of the "Concept of the Human Resources Information System for the Health System (SI ERUSS)", the NCPDP proposed the following:

In Chapter IV, the organisational space of the SI ERUSS, it was proposed to determine/identify the users and data providers, as participants in the SI ERUSS, in accordance with the provisions of the Law No 71/2007 on registers, this is why it was recommended to expressly nominate them.

At point 18, sub-point 1 of the draft, which lists the characteristics of the data subject "Employee", it was mentioned that personal data relating to health constitute special categories of data whose legal protection regime is more stringent and requires appropriate and compliant processing, in compliance with the principles of non-excessiveness and proportionality, and that the purposes and functions outlined in the draft do not justify the processing of these categories of data.

It was noted that, according to point 28, the validation of employees' personal codes will be ensured through the electronic government service MConect *for retrieving data on the employee's personal code*, name, surname, address, date of birth and *information on children* (personal code, name, surname, date of birth).

In this context, it was noted that the primary purpose of the IS ERUSS is the *automation of human resources management processes in health at the system level,* the creation of the single electronic register of staff in the health system, the automation of the processes of registration and management of medical staff and *not the collection of personal data of minors of employees in the medical/health system*. Thus, the causal link between the processing of personal data of minors and the purpose stated in the draft Concept proposed for endorsement cannot be established, which makes it necessary to review the volume of data proposed to be collected.

Point 25 of the SI ERUSS specifies that the infrastructure of presentation of the web portal www.eruss.gov.md shall present a complex interactive interface, composed of several modules and working levels, having the capacity to operate with different content, textual, files of different formats, accessible to users both in *open and closed form*, without specifying which information will be open.

In this context, it was recommended to the author of the draft to expressly determine the categories of personal data, which will be open/public, in order to exclude as much as possible the prejudice to the interests and rights of the personal data subjects concerned.

Last but not least, attention has been drawn to the problematic nature of recording the state identification number (IDNP) by health employees in the documents related to the provision of healthcare, through the method of disclosure and inclusion in observation records, prescriptions for compensated medicines, etc.

It has been stated that the IDNP of the natural person falls under the notion of personal data, whose legal regime of confidentiality and security must be respected by any person, and its processing must be carried out in strict compliance with the law.

It has been specified that, by recording the state identification number, the name/surname of the medical staff in the observation records, prescriptions for compensated medicines, etc., these data become public, circulating, which generates increased risks for the privacy of the data subjects.

In these circumstances, given that the SI ERUSS is part of the Integrated Medical Information System, as well as of the Medical Register, which will be responsible for the human resources component and will ensure functional control of human resources in health, it was proposed, at this stage of development/implementation of the information system, to assign and validate for medical staff an identification/registration number different from the IDNP, which will be recorded on the medical documentation.

It was recommended to add a new letter to the information object *"Doctor/pharmacist/medical assistant"* or to supplement letter b) point 22 subpoint 3) with rules on the identification of the doctor, including on the basis of a separate/supplementary numerical code/registration number, replacing the IDNP and to be indicated in the observation records, prescriptions for compensated medicines, etc.

It has been specified that this mechanism of randomly assigning a code to each individual medical staff member, different from the IDNP, which will be made public, does not cancel the right of the data controller to process the IDNP of medical staff within the SI ERUSS system for the purpose of functional control relating to the recording and management of human resources.

This mechanism is designed to ensure the compliance of personal data processed by the Ministry of Health and to strengthen respect for the right to personal data protection.

Subsequently, it was reiterated that the issue of requiring personal data subjects to disclose their IDNP to an undefined circle of persons was subject to constitutional review by the Constitutional Court in its judgment of 22 May 2014[4], in which it found unjustified interference in the privacy of persons engaged in liberal activities.

7. On the draft law on the amendment of some normative acts (amendment of the Criminal Code and the Contravention Code) registered at the State Chancellery under the unique number 533/ MJ 2022, the NCPDP noted that according to paragraph 35 of the draft submitted for approval, the Criminal Code is supplemented with Article 177[1] *"Falsification of identity"*.

In this regard, it was specified that in accordance with Article 15 of the Criminal Code, the degree of the offence is determined according to the signs characterising the elements of the offence: object, objective side, subject and subjective side.

Accordingly, Article 126 of the Criminal Code entitled *"Extremely large proportions, large proportions, considerable damage and essential damage"* sets out the situations when *large proportions* and *extremely large proportions* are considered, as well as the criteria for determining whether the damage caused is considerable or essential.

In the context of the mentioned provisions, an essential condition for the initiation of criminal proceedings is the occurrence of the harmful consequences in the form of large or extremely large damages, which in turn are increased from year to year, depending on the forecast average monthly salary per economy, established by the Government Decision in force at the time of the offence.

[4] *https://www.constcourt.md/public/ccdoc/hotariri/ro-h_13_2014_ro.pdf*

The analysis of the new offence " *falsification of identity*", which was to be introduced into the Criminal Code, does not indicate that the victims have suffered large or extremely large material damage, but is conditioned only on the action of misleading or maintaining error in order to produce a legal consequence, rules which are general and interpretable from case to case.

For these reasons, the criminal act that is intended to be criminalized, in the wording set out, could create a conflict of norms with the offence set out in Article 74^1 of the Contravention Code, according to which *failure to comply with the basic conditions for the processing, storage and use of personal data, with the exception of the cases provided for in paragraph 1 of Article 74^1 of the Criminal Code, may result in a breach of the rules of the Criminal Code. (5), is punishable by a fine from 60 to 90 conventional units imposed on the natural person, by a fine from 90 to 180 conventional units imposed on the person holding a position of responsibility, by a fine from 120 to 300 conventional units imposed on the legal person with or without deprivation, in all cases, of the right to carry out a certain activity for a period from 3 months to one year.*

In this regard, it has been noted that acts of unlawful use of personal data of a data subject without the consent of the data subject are frequently committed, either with the purpose of causing consequences, or by presenting a false identity or attributing such identity to another person, in particular by registering and/or using user accounts on social media platforms, web portals, e-mail addresses, telephone numbers, access cards or other information society services, in order to mislead or deceive in order to produce a legal consequence - acts which, in the absence of clearly determined damage, may be qualified, including in terms of the criminal offence provided for in Art. 74^1 para. (1) Contravention Code.

Thus, there is a risk that an act of unlawful processing of personal data may be classified as a crime and/or a offence on the basis of arbitrary and discretionary criteria by those who have the power to enforce criminal and contravention law.

In summary, it was concluded that the new criminal offences are formulated in an vague and unclear manner in relation to the offence and will give the authorities who are to apply them an excessive margin of discretion, where, it was considered appropriate to make changes to the content of Article 177^1 of the draft from the perspective of the damage caused, so that the regulatory framework offers the possibility of effective investigation of these categories of offences and does not create conflicts with the contravention offence.

The reasoning set out above was also presented as valid in relation to the offences provided for in Articles 259 and 260 of the draft amendment to the Criminal Code.

8. *During the public consultation process, the NCPDP presented its opinion on the draft law on counter-intelligence and foreign intelligence activities*, examining the provisions of the draft law in the light of the provisions of international human rights treaties ratified by the Republic of Moldova, but also taking into account the case law of the ECHR in this field, the following general conclusions were presented:

- The purpose of the draft may fall within the exceptions provided for in Article 54 (2) of the Constitution of the Republic of Moldova and Art. 8 (2) of the Convention for the Protection of Human Rights and Fundamental Freedoms;
- The Republic of Moldova, as a State party to the Convention for the Protection of Human Rights and Fundamental Freedoms and to the Convention for the Protection of

Individuals with regard to Automatic Processing of Personal Data, has a certain degree to determine the best policy in the field of ensuring State security;

- It can be considered that the draft pursues a legitimate aim and the adoption of such regulations might be necessary in a democratic society **only if certain minimum safeguards for the protection of the persons concerned by the secret surveillance measures are respected and if it is possible to challenge them before an independent judicial authority, preferably in court.**

However, according to the wording of the draft provisions, the provisions of the international human rights treaties ratified by the Republic of Moldova and the case law of the ECHR in this field were not taken into account when drafting the draft, and the following was generally found:

1. The provisions of the draft not only restrict the exercise of the right to privacy, the inviolability of the home and the secrecy of correspondence, but also affect the very existence of these rights (*lack of minimum guarantees of protection, lack of procedural guarantees for challenging secret surveillance measures, lack of mechanisms for effective and permanent control by an independent judicial authority);*
2. The authors, including in the information note to the draft, have not provided arguments that could reasonably justify that, in establishing the regulatory framework in the field of national security, the margin of appreciation of a state party to the international conventions in the field of human rights ratified by the Republic of Moldova has not been exceeded;
3. The draft law does not comply with the requirements of clarity, predictability and accessibility, since its provisions do not clearly and exhaustively define the nature of the offences which may allow the initiation of surveillance measures and the categories of persons who may become the subject of such measures;
4. The provisions of the draft do not contain sufficient safeguards (at least minimum safeguards of protection) to eliminate abuses and ensure respect for fundamental human rights and freedoms;
5. The issue of notification of persons concerned by secret surveillance measures is not sufficiently regulated (*at least a posteriori, when the purpose is achieved*);
6. The provisions of the draft do not ensure an effective measure of challenging or repairing their consequences for the persons concerned by the surveillance;
7. The authors have not provided sufficient arguments justifying the proportionality of the intention to increase the term of the surveillance measures up to 2 years in relation to the consequences of the interference in the private life of the persons subject to these measures;
8. There is a gap in the regulation of the procedures for the retention, consultation, examination, use, transmission and destruction of intercepted data;
9. There are no safeguards in place to exclude abuse and risk in relation to the procedure for authorising surveillance measures by the heads of the authority competent to carry out such measures;

10. The draft law provides for inadequate control mechanisms in order to exclude potential abuses it is crucial to establish effective and permanent control mechanisms, which can be achieved in particular by an independent judicial authority.

In conclusion, it was noted that failure to adapt the draft law on information and counter-information activity to the requirements and criteria mentioned above would undermine the existence of fundamental rights guaranteed by the Constitution and would create the conditions for the Republic of Moldova to be condemned as a party to international human rights treaties.

Afterwards, the NCPDP representative participated in the public debates organized on the platform of the Committee on National Security, Defence and Public Order of the Parliament of the Republic of Moldova, coming up with comments and proposals to improve the content of the draft.

CHAPTER VIII

INTERNATIONAL COOPERATION

International cooperation continues to be the advocate of institutional development goals: the accomplishments in this area being achieved through sharing the experience, the expertise and the best practices with other Data Protection Authorities and through the training provided by EU experts within TAIEX projects and the GIZ Eastern Partnership Regional Fund for Public Administration Reform, as well as through the adoption and practical application of international standards for the personal data protection.

Cooperation, both at European and international level, is a strategic issue that requires involvement in all developing initiatives.

In 2023, the strengthening of international collaboration was accomplished through the active participation of representatives of the NCPDP at the plenary meetings of the European Data Protection Board (EDPB) and the Council of Europe. It is to be noted that the Republic of Moldova has been the observer in the EDPB since 2017.

During the year 2023, international meetings and sessions were held both online and in person.

Plenary meetings of the European Data Protection Board

During the 2023, the NCPDP representatives participated in 6 online plenary meetings, as well as in three of them were held in Brussels with physical presence. A number of important documents were adopted during the European Data Protection Board plenary meetings, including:

- Guidelines 03/2021 on the application of Article 65 (1) (a) GDPR;
- Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR;
- Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them;
- Guidelines 04/2022 on the calculation of administrative fines under the GDPR;
- Guidelines 07/2022 on certification as a tool for transfers;
- Statement 1/2023 on the first review of the functioning of the adequacy decision for Japan;
- Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023;
- EDPB-EDPS Joint Opinion 02/2023 on the Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro;
- EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals.

The purpose of these meetings is to determine the requirements for international cooperation in order to enhance the implementation of personal data protection legislation, as well through the notification, assistance with investigations and exchange of information, subject to adequate safeguards for the personal data protection.

Plenary meetings within the Council of Europe

The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108)

During the year 2023, the NCPDP's management attended two plenary meetings of the Advisory Committee of Convention 108 which were held in person.

The meetings focused on various topics of high importance, including the Convention 108+ and the status of current ratifications and accessions, personal data protection for anti-money laundering measures and combating the terrorism financing, in the context of crossborder data flows, interpretative document to Article 11 of the Convention 108+, personal data protection in the electoral process (including biometric data), cooperation with other bodies and entities of Council of Europe, as well as major improvements and actions in the field of data protection.

The delegation of the NCPDP reported about the status of ratification of Protocol CETS No. 223

on amending the Convention 108, pointing out that the draft ratification document has been submitted to the Ministry of Justice for the necessary actions to ensure submission of the draft by the Government of the Republic of Moldova to the Parliament of the Republic of Moldova. The Republic of Moldova is in the process of guaranteeing the transposition of Regulation (EU) 2016/679 and Directive (EU) 2016/680 into the national legislation.

The delegation also reported about developments and actions in the field of data protection at the national level.

Simultaneously, we mention that, of the 46 member states of the Council of Europe and 9 non-member states (total of 55 states), the Protocol amending the Convention 108 for the protection of individuals with regard to automatic processing of personal data was signed by 45 states from the total number and ratified by 31.

Cooperarea cu Eurojust, European Data Protection Authorities and national institutions in the field of personal data protection

➢ 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, NCPDP had reported 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.

➢ On 10-12 May 2023, the representatives of the NCPDP participated in the **31st Spring Conference of the European Data Protection Authorities** in Budapest, Hungary.

During the working sessions, topical data protection issues were presented, such as assessing the social impact of the use of new technologies in different areas; interaction

between Data Protection and Competition law; court decisions: resolutions and amendments to the Rules of Procedure; best practices/case studies in enforcement cooperation between EEA and non-EEA countries.

For the first time at a Spring Conference of the European Data Protection Authorities, an Open Day was organised. This practice gave the opportunity to several institutions, NGOs or other organisations that expressed interest in the topics covered during the event to participate online.

The event was attended by the representatives of Central and Eastern European Data Protection Authorities, the Council of Europe, the European Data Protection Board, the European Data Protection Supervisor, where they had the opportunity to exchange experience and best practices in the field of personal data protection, including the role of the Data Protection Officer within a public or private entity.

➢ From 1 to 3 November 2023, the NCPDP's representative participated in the ***Internet Freedom Summit 2023,*** which took place in Ohrid, Republic of North Macedonia.

The event included interactive sessions, workshops, roundtables and training sessions, focusing on topical issues in the field of personal data protection and privacy, such as:

- Privacy in a connected world: Navigating and Challenges of Data Protection in the Digital Age;
- International data protection standards and the importance of harmonisation for efficient cross-border data transfers;
- Balancing privacy and technological innovation;
- The role of regulators in promoting a privacy-sensitive innovation culture;
- Strategies for monitoring and enforcing data protection regulations on online platforms;
- The role of data protection authorities in ensuring compliance and addressing detected breaches;
- The future of privacy: emerging technologies and trends, etc.

At the event, the NCPDP's representative addressed the topic - "***Balancing privacy and data protection from a South-East European perspective***". Participants also shared their views on strategies for monitoring and enforcing data protection regulations on online platforms, in particular, on the future of privacy in an era of artificial intelligence, blockchain and other new technologies impacting privacy

➢ From 8 to 9 November 2023, the NCPDP's representatives participated in ***the European Case Management Workshop 2023***, held in Bern, Switzerland, an annual event that provides a forum for participatory dialogue between Data Protection Authorities on the challenges they face and the solutions they apply in their daily practice.

The aim of the event was to focus on topical issues in the field of personal data protection and privacy, in particular such as:

- Handling unfounded or excessive requests - as per Article 57 (4) of the GDPR;
- Essential personal data protection safeguards for law enforcement cooperation between data protection authorities in the EEA;
- GPS tracking in employment relationships;
- Facial recognition and detection through the lens of personal data protection etc.

The European Case Management Workshop 2023 was attended by 82 representatives from 29 countries and 37 Data Protection Authorities

➢ From 13 to 15 December 2023, the NCPDP's representative participated in ***Cyber Security Policy Summit*** and ***Closing Conference of the CyberEast Project***. The event took place at the Palace of the Parliament in Bucharest, Romania, and was a part of the *Octopus 2023* Conference.

The Cyber Security Policy Summit in the Eastern Partnership Region was dedicated to the discussion of regional priorities and the adoption of the second *Regional Declaration on Strategic Priorities*, 10 years after the first version of this document (*Declaration on Strategic Priorities for the Cooperation against Cybercrime in the Eastern Partnership Region*, adopted in Kiev in 2013). *The Closing Conference of the CyberEast Project* has addressed the topics related to legislation and policies, as well as the development of capacity and cooperation from the perspective of national partners which demonstrate the impact and relevance of the project in improving their capacities on cybercrime and electronic challenges.

➢ On 25 January 2023, the NCPDP and the General Police Inspectorate (GPI) approved and signed the ***Training plan in the data protection field*** for the GPI subdivisions, as well as the ***Additional Protocol to the Cooperation Agreement*** signed by the Parties in 2019. The main purpose of the Training Plan was to increase the awareness of GPI subdivisions' employees about the principles of personal data protection and to ensure the proper implementation of the relevant legal provisions in their work.

The Additional Protocol aims to strengthen cooperation and information exchange in the field of data protection, to organise joint training and events, as well as to ensure continuous efforts to improve the protection of citizens' rights and freedoms with regard to personal data processing in accordance with national and international standards.

➢ On October 17, the NCPDP representatives participated in the Conference "***GDPR4BUSINESS***", organized by the National Association of ICT Companies within the ABA Rule of Law Initiative Project "*Personal Data Protection – Rights and Obligations in the Republic of Moldova*" in partnership with the European Business Association (EBA Moldova).

At the opening session, the Deputy Director of the NCPDP, Angela COLOMIICENCO, thanked the National Association of ICT Companies and its partners for their contribution to the initiation and organisation of the conference, welcoming the participation of business, civil society and representatives of public institutions in the event, which she described as testimony to the strengthening of cooperative relations in the field of personal data protection.

Mr. Alexei STRAHOV, Head of the Prevention, Surveillance and Evidence Department, participated in the conference as an expert on behalf of the NCPDP, who addressed the topic ***"Data Protection Officer" (DPO)***, highlighting the newest and important aspects required by the provisions of Law 133/2011 on the protection of personal data, appointment of the DPO, DPO function, and DPO tasks.

At the same time, the conference presented practices with applicable content for business and representatives of public authorities, such as:

- key aspects of the draft law on Personal Data Protection
- international and regional experience in the application of GDPR
- solutions and responses to situations, cases and challenges faced by business and public authorities in implementing the harmonised legal framework.

During the event, as speakers, participated state officials, national and international experts in the field of data protection.

EU projects

During 2023, the CNPDCP applied for, won and received support from the ***TAIEX*** project ***- Technical Assistance and Information Exchange Instrument*** in the organisation of national conferences, study visits and expert missions for the public sector, namely:

Expert mission
"Personal data processing for statistical purposes"

In the period 29-30 March, the NCPDP in collaboration with TAIEX project experts organised the ***Expert Mission "Personal data processing for statistical purposes" in online format***. The objective of the Expert Mission was to present the European legal and operational best practices on the mechanisms of processing and storage of personal data for statistical purposes by the National Bureau of Statistics (NBS).

The event took place for two days, featuring discussions between EU experts, the NCPDP the NBS in order to identify issues related to personal data processing for statistical purposes, ensuring guarantees on the of personal data processing and respect for the rights of data subjects. On the second day, a training course was held for representatives of several public institutions. The Expert Mission was moderated by data protection experts from Romania and Greece, addressing topics such as general conditions of data processing, data storage for statistical purposes, access to informational systems and data protection regulations in this context. The event was attended by 24 representatives of public sector.

National Conference "Data Protection Impact Assessment
and the Role of the Data Protection Officer"

On 10 July, the NCPDP held the national conference "***Data Protection Impact Assessment and the Role of the Data Protection Officer***".

The aim of the workshop was to takeover the legal and operational best practices by the representatives of public institutions on Data Protection Impact Assessment (DPIA) mechanisms, processing operations requiring a DPIA, and the role of the Data Protection Officer (DPO) within public sector personal data controllers.

The event was opened by NCPDP's Director Victoria MUNTEAN, who emphasized the necessity for vigorous personal data protection in the context of the increasing level of the digitization of society.

The conference, moderated by data protection experts from Italy and Malta, addressed topics such as the necessity and proportionality of DPIAs, scenarios for data protection impact assessment, prior consultation in situations of increased risk, the necessary resources for a Data Protection Officer, as well as best practice examples for assigning and supporting DPOs. Around 60 representatives of the public sector attended the event.

Study visit "Reconciling the right of access to information and the personal data protection"

In the period 18-19 October, the representatives of the NCPDP carried out a study visit entitled ***"Reconciling the right of access to information and personal data protection"***. The event was hosted by the French National Commission for Information Technology and Civil Liberties (CNIL).

The purpose of the event was to take up the best legal and operational practices on mechanisms to reconcile the right of access to information and the protection of personal data. During the study visit, moderated by experts in the field of personal data protection from the CNIL and CADA – Commission for Access to Administrative Documents, topics of importance such as: protection of personal data in the exercise of the right of access to information; reconciling the right of access to information and the right to protection of personal data; request for access to administrative documents or exercise of the right of access by the data subject, how to distinguish them and what is the impact; publication and re-use of data of public interest; re-use of data of public interest for scientific research purposes, etc. have been analysed and discussed.

Collaboration with the GIZ Eastern Partnership Regional Fund for Public Administration Reform)

In 2023, thanks to the fruitful collaborative partnership with the Eastern Partnership Regional Fund for Public Administration Reform *(implemented by the German International Cooperation Agency (GIZ) and funded by the German Federal Ministry for Economic Cooperation and Development (BMZ),* NCPDP's members participated in four Academies on "*Service Design and Delivery in a Digital Age*". These Academies contributed to capacity building in the fields such as user-centric digital public services, digital transformation, quality management systems and quality culture, information collection and user feedback.

CHAPTER IX

AWARENESS AND TRAINING ACTIVITIES

During the year 2023, the NCPDP has made remarkable progress in the area of awareness and training activities in the field of personal data protection. Trainings were conducted with physical attendance as well as in online or hybrid formats for a record number of public institutions. Trainings were also organised for the subdivisions of the General Police Inspectorate and for medical institutions both in Chisinau municipality and in the country.

At the same time, an information and awareness campaign in the school community continued during the same period under the title: ***"Personal data protection and the safety of children in the online environment".*** Similarly, during the reference period, the NCPDP also organised street actions with different topics in the context of several events.

AWARENESS ACTIONS

During the 2023, the information and awareness-raising campaign for school communities continued under the title: "Personal data protection and the safety of children in the online environment". The aim of the campaign was to provide the school community with high visibility on data protection and child safety online at local and national level by promoting empowerment and best practice for intervention and support. The topics covered in the training included: general notions on personal data; correct use of pictures/video online; risks and threats online; communication on social networks etc. Four training courses were organised in the school community:

27 January - Public Institution "Gheorghe Asachi Theoretical Lyceum""

17 May - Public Institution "Mircea Eliade Theoretical Lyceum"

18 May - Public Institution "Ion Creanga Theoretical Lyceum"

07 December - Public Institution "Dante Alighieri Theoretical Lyceum"

In this context, about **160** pupils were trained.

➢ On 27 January 2023, a street action was organised by NCPDP's representatives in the context of the celebration of the European Data Protection Day. In this context, a group of NCPDP employees distributed informational materials to passers-by in front of the Triumphal Arch in Chisinau municipality. People were informed about the meaning of "*Data Protection Day*", the concept of personal data, the rights of personal data subjects, data security and confidentiality measures, as well as the principles of personal data protection. At the same time, they were informed about the possible situations of non-compliant processing of personal data, providing them with practical guidance and recommendations that should be undertaken in such situations

➢ On 13 May 2023, the NCPDP joined the initiative of the EU Delegation to the Republic of Moldova and participated in the inauguration event of the European Village, organised annually on the occasion of Europe Day. This year's edition was held under the slogan "*European Moldova*", the event took place in the Great National Assembly Square in Chisinau. Participants had the opportunity to interact with the representatives of public institutions, diplomatic missions of

EU Member States accredited in Chisinau, to get acquainted with projects carried out with the support of the European Union, to participate in various educational, creative and interactive activities, to taste European cuisine and to participate in information sessions on current topics. The representatives of the NCPDP set up a stand with educational-informative materials and promotional fliers, and the general public was informed about the field of personal data protection. Amongst the topics of interest both for adults and children, the following can be mentioned: the concept of personal data, the rights of data subjects, data security and confidentiality measures, principles of personal data protection etc.

Also, during 2023, the NCPDP developed and published on the official website www.datepersonale.md **119** press releases. Likewise, the authority has developed and published information newsletters with reference to statistical information regarding the activity of NCPDP, as well as other useful information at the national and international level in the field of personal data protection.

TRAINING ACTIVITIES

During the 2023, NCPDP organized a record number of trainings courses for representatives of public institutions, General Police Inspectorate's subdivisions and medical institutions both in Chisinau and in the territory.

➢ On 25 January 2023, the NCPDP and the General Police Inspectorate (GPI) approved and signed the ***Training plan in thefield of data protection*** for the GPI subdivisions, therefore several training courses were organised during the year. The purpose of these training courses was to increase the awareness of GPI subdivisions' employees about the principles of personal data protection and to ensure the proper application of the relevant legal provisions in their work. During the trainings, some of the important topics were addressed, such as: definition of general notions of personal data protection; the legal way of personal data processing in the activity carried out by the employees of the GPI subdivisions; the requirements for personal data protection, in the exercise of official duties; the obligations of the police body as a data controller in relation to the data subject; the correct procedure of accessing personal data through the State Information Systems, as well as keeping correct audit records of such accesses; personal data security and confidentiality measures etc. Thus, training courses were organised for the following subdivisions:

- 1st February – Anenii Noi Police Inspectorate of the GPI;
- 6th March – National Inspectorate of Investigation (NII) of the GPI;
- 24th March – National Centre for Combating Trafficking in Human Beings of the NII;
- 7th April – National Public Security Inspectorate, Regional Directorate "Centre" of the GPI;
- 25th April – Buiucani Police Inspectorate of the Chișinău Police Department;
- 5th May – Ciocana Police Inspectorate of Chișinău Police Department;
- 22nd May – Râșcani Police Inspectorate of Chișinău Police Department;
- 5th June – General Directorate for Criminal Prosecution of the GPI;
- 23rd June – Police Department of ATU Gagauzia;
- 11th July - Ialoveni Police Inspectorate of the GPI;
- 17th July - National Public Security Inspectorate (INSP), Southern Directorate of the GPI;
- 3rd August - Botanica Police Inspectorate of the Police Directorate;
- 29th August - National Public Security Inspectorate (INSP), Northern Directorate of the GPI;
- 5th September – Sîngerei Police Inspectorate of the GPI;
- 19 September - Straseni Police Inspectorate of the GPI;
- 3rd October - Telenesti Police Inspectorate of the GPI;
- 10th October - Taraclia Police Inspectorate of the GPI;
- 7th November - DAI, DCPI Interpol of GPI, DPC and DPI of GPI;
- 27th November - Central Police Inspectorate of Police Directorate;
- 5th December - Police Department of Chisinau municipality.

In this context, about **1200** representatives of the GPI subdivisions were trained.

✓ Also, the training courses were organized for a number of medical institutions on "***Legal provisions in the field of personal data protection***". The aim of the training courses was to strengthen the capacities of medical staff by familiarizing, raising awareness and informing them about the field of personal data protection. Thus, the trainings took place:

- 9th June – Family Doctors Center from Bălți municipality
- 21st June – Central Territorial Medical Association
- 28th June – Nicolae Testemițanu University Primary Health Care Clinic
- 27th September – Municipal Children's Hospital No. 1
- 4th October – IMPS "*Ungheni District Hospital*"
- 16th October – IMPS "*Glodeni District Hospital*"
- 3rd November – Institute of Physiopneumology "*Chiril Draganiuc*".

In this context, about **550** representatives of medical institutions were trained.

✓ Throughout 2023, the NCPDP has demonstrated its openness and a spirit of collaboration, organising multiple training courses for representatives of public institutions at their request. The training courses aimed at familiarizing representatives of public sector with the aspects of personal data protection in the public service, the regulation of processing procedures, as well as the personal data confidentiality and privacy in accordance with the actual legislation. Training courses were organised for the following institutions:

- 31st January - representatives of the libraries in the Chișinau municipality and other districts of the Republic;
- 12th May - National Health Insurance Company;
- 26th May - Cahul General Directorate of Education;
- 29th May - State Tax Service;
- 14th June - Ministry of Internal Affairs;
- 16th June - National Agency of Road Transport;
- 13th September - Ministry of Finance;
- 28th September - National Anticorruption Centre;
- 29th September - Agency for Court Administration, Southern Region;
- 2nd October - General Inspectorate of Carabineers;
- 6th October - General Inspectorate of Carabineers Training Centre;
- 11th October - Regional Directorate "Centre" of the General Inspectorate of Carabineers;
- 12th October - Agency for Court Administration, Northern Region;
- 13th October - Agency for Court Administration, Centre Region;
- 18th October - Regional Directorate "Centre" of the General Inspectorate of Carabineers;
- 20th October - Regional Directorate "South" of the General Inspectorate of Carabineers;
- 25th October - Regional Directorate "North" of the General Inspectorate of Carabineers;
- 31st October - Ministry of Energy;

- 1st November - General Directorate of Education, Youth and Sport of the Chisinau Municipal Council;
- 9th November - National Integrity Authority;
- 16th November - State Chancellery;
- 17th November - Directors of early education institutions in Chisinau municipality;
- 22nd November - Directors of educational institutions in Chisinau municipality;
- 23rd November - Ministry of Infrastructure and Regional Development;
- 28th November - Ministry of Labour and Social Protection;
- 29th November - Republican Psycho-Pedagogical Center;
- 6th December - State Protection and Guard Service;
- 8th December - Ministry of Agriculture and Food Industry;
- 18th December - National Agency for Food Safety.

Around **2000** public authority representatives were trained during the events.




At the same time, the NCPDP has organised **5** training courses for the persons designated by the controller or the processor as Data Protection Officer.

This obligation is established by the provisions of Law no.133/2011 on personal data protection of personal data, which establishes the duty of the controller and the processor

to appoint a Data Protection Officer in the cases provided by the Article 25 of the above-mentioned law. The purpose of the training courses was to develop theoretical knowledge in the field of personal data protection and practical skills in applying the relevant regulations and legislative requirements. During the trainings, important topics were discussed, such as definition of general notions related to the field of personal data protection; rights of personal data subjects; processing of special categories of personal data; principles and legal grounds for processing personal data; ensuring security and confidentiality of processed personal data; issues related to the Data Protection Officer (DPO); issues related to Data Protection Impact Assessment, etc. So far, about **45** DPOs from both the public and private sectors have been trained.

CHAPTER X

MANAGERIAL ACTIVITY OF THE NCPDP

Management of human resources

Human resources are the core element of any institution, contributing significantly to the achievement of the entity's objectives and having a significant impact on its performance.

Effective human resource management not only contributes to the long-term success of the authority, but also to creating a motivating and fair working environment for employees.

In the performing of its tasks, the NCPDP consists of 8 structural subdivisions (departments and services), in accordance with the structure approved by Law No 182/2008, which remains unchanged since 2017.

The National Authority for the Control of Personal Data Processing is staffed by law graduates, supplemented by specialists in the field of international relations, public administration, economists, as well as auxiliary staff, with a total of 45 units according to the following categories of functions:

- 2 positions of public dignity (Director and Deputy Director);
- 42 public functions, including 11 managerial public functions and 31 executive functions;
- 1 auxiliary staff (driver).

Thus, at the beginning of the reporting period, 33 employees were actually working in the institution, and at the end of the period - 32.

Staff level for 2023

	Positions of public dignity	Managerial public functions	Execution functions	Auxiliary staff	Total number of persons
The staff limit on 31.12.2023, units	2	11	31	1	45
Public positions/ positions occupied on 31.12.2023, persons	2	11	18	1	32
Occupancy rate of public offices/ posts, %	100	100	58,1	100	71

Within the National Data Protection Authority, a gender equality policy is applied in the recruitment and human resources management process, however, there is a prevalence of female employees over male employees, i.e. the share of women in 2023 is 69% (22) and that of men is 31% (10).

The average age of employees per authority is 39 years. In the age structure, the trend of the last few years continues with the employment of people aged 35-45 years having the highest share - 43.8% of the total number of employees actually employed.

In the table below we see the share of employees of the NCPDP by age and gender, by type of function.

NCPDP staff by age and gender categories

Year 2023	*Total number of persons*		*Positions of public dignity*		*Managerial public functions*		*Execution functions*		*Auxiliary staff*	
	Women	*Men*	*Women*	*Men*	*Women*	*Men*	*Women*	*Men*	*Women*	*Men*
Number of persons	***22***	***10***	***2***	***-***	***9***	***2***	***11***	***7***	***-***	***1***
< 25 years	*4*	*1*	-	-	-	-	*4*	*1*	-	-
25-35years	*3*	*3*	-	-	*1*	-	*2*	*3*	-	-
35-45 years	*11*	*3*	*1*	-	*7*	*2*	*3*	*1*	-	-
45-55 years	*3*	*1*	*1*	-	*1*	-	*1*	*1*	-	-
55-63 years	-	*1*	-	-	-	-	-	*1*	-	-
> 63 years	*1*	*1*	-	-	-	-	*1*	-	-	*1*

Although the national framework regulating salary policies in the budgetary sector, in place in 2023, conditioned the resigning of many NCPDP's specialists to budgetary institutions with more attractive salary conditions, in the reporting year the turnover rate was 18%, significantly lower than in 2022 (37%).

Staff turnover

Years	Average number of employees	No. of persons whose service/ employment relationship ended	Turnover %
2018	*32*	*8*	*23*
2019	*33*	*8*	*24*
2020	*36*	*6*	*18*
2021	*39*	*13*	*35*
2022	*32*	*13*	*37*
2023	*32*	*6*	*18*

During 2023, 6 employees resigned and 8 people were hired, 5 of whom were beginners. It should also be noted that during the reporting year, the employment relationships of 3 civil

servants were suspended in connection with their request for partial paid leave for childcare up to 3 years old.

Thus, at the end of the reporting year, the occupancy rate in the NCPDP was approximately 71.1%, at the same level as in 2022.

Staff levels in the period 2018-2023

Year	*Units approved*	*Effectively, empoyees*	*Share, %*
2018	45	32	71
2019	45	33	73
2020	45	35	78
2021	45	39	89
2022	45	32	71
2023	*45*	*32*	*71*

In the process of ensuring the necessary staffing in 2023, the NCPDP has relied on the procedures for occupying public positions by competition and transfer. Among the procedures for filling public posts, the procedure for occupying public posts by competition prevailed.

In this regard, during 2023, 3 competitions were organized and held, 2 of which were extended several times, to fill 8 public vacancies, for which 37 candidates' applications were submitted and accepted. 1 executive civil service post was filled by external transfer.

In the reporting year, the NCPDP faced a shortage of qualified staff. The reasons for the reduced capacity of the Authority to cover the staffing needs were due to the level of salaries not corresponding to the complexity of the tasks and competencies required by the work to be performed, the high workload for existing staff and a low number of candidates in competitions for executive public positions.

Staff turnover increases the risk of continuity of the institution's work and creates the risk of loss of institutional memory. During 2023, there was an essential increase in the proportion of staff with the experience between 1 and 2 years in the NCPDP, i.e 31%.

Thus, after a good professional training and assimilation of the necessary knowledge, skills and working abilities, employees decide to leave for other public authorities for a more attractive salary package.

The phenomenon of staff turnover represents a number of significant disadvantages for the work of the NCPDP and the procedure for selecting and hiring new staff is difficult and complicated due to the lack of competent and experienced specialists in the field of personal data protection.

Professional training

In order to strengthen institutional capacities, the NCPDP pays particular attention to the development of human resources as an important vector for increasing the quality of the work carried out.

To this end, an Annual Continuous Professional Development Plan was drawn up, according to which 33 employees received training, including those who resigned.

The training activities took place in different types and forms and were organised with the aim of deepening and updating knowledge, developing skills and modelling skills/behaviours necessary for the effective exercise of the duties of the service.

Thus, during the year 2023, employees of NCPDP participated in 20 training sessions, of which:

- 14 external training sessions, organized and conducted mainly by the Institute of Public Administration, being the elite center for promoting the state policy in the field of training and professional development of civil servants of all levels;
- 6 internal training sessions, moderated by the institution's internal trainers.

In the continuous professional development of employees, a key role was played by a study visit to the French Data Protection Authority (CNIL), organised with the support of the Technical Assistance Project (TAIEX), with the topic "Reconciling the right of access to information and personal data protection". Thus, 5 employees of the NCPDP had the opportunity to learn best legal and operational practices on the mechanism for reconciling the right of access to information and personal data protection.

Last but not least, we would like to mention that in order to implement the provisions of the national legislation on occupational safety and health, a number of measures have been put in place within the NCPDP to ensure the safety and health of staff in the workplace. To this end, in order to prevent occupational hazards, trainings such as introductory-general training, on-the workplace training and on medical first aid, fire safety training, etc., were organized and held periodically during the year.

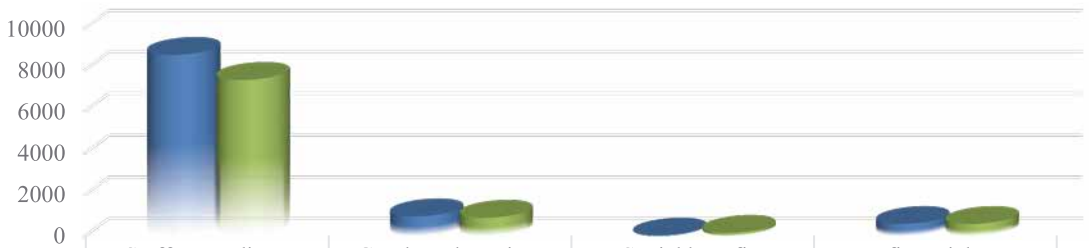
Economic and financial activity

In accordance with Article 19 of the Law on personal data protection, the activity of the NCPDP is fully financed from the state budget within the limits of the budget allocations approved by the annual budget law.

The limits specified in the year 2023 for NCPDP according to the Law no. 359/2023 on state budget for the year 2023, amounted to 11 137,6 thousand MDL.

According to the situation on 31 December 2023, the budget of NCPDP was implemented in the amount of 10 290,7 thousand MDL, which is 92.4%, being in increase compared to the previous year.

Budget execution for the year 2023 compared to the year 2022 (thousand MDL)



	Staff expenditure	Goods and services	Social benefits	Non-financial assets
2023	8711,8	956,1	35,9	586,9
2022	7504,5	889,1	159,9	584

2023 2022

On the basis of the approved/specified financial resources framework, the distribution of allocations by category of expenditure has been carried out in accordance with the needs of the NCPDP in the implementation of the tasks within its sphere of competence, as shown in the table:

Indicators	Approved	Specified	Executed 31.12.2023	Execution rate, %
TOTAL	**11 137,6**	**11 137,6**	**10 290,7**	**92,4**
Expenditure	**10 457,7**	**10 457,7**	**9 703,8**	**92,8**
Staff expenditure	*9 107,6*	*9 107,6*	*8 711,8*	*95,6*
Goods and services	*1 230,1*	*1 230,1*	*956,1*	*77,7*
Social benefits	*120,0*	*120,0*	*35,9*	*29,9*
Non-financial assets	**679,9**	**679,9**	**586,9**	**86,3**
Fixed assests	*351,4*	*351,4*	*338,7*	*96,4*
Stocks of circulating materials	*328,5*	*328,5*	*248,2*	*75,5*

Thus, the major share of expenditure is allocated to the chapter "*Staff expenditure*", in this regard, financial means in the amount of 9 107,6 were allocated in the proportion of 81,8% of the total budget of the NCPDP, intended for the remuneration of staff and payment of mandatory state social security contributions.

The financial means approved under the chapter "*Goods and services*" amounted to 1 230,1 thousand MDL, which is 11, 0% of the total budget of the NCPDP. Expenditure in this category amounted to 956,1 thousand MDL, which includes: expenses for renting the premises, maintenance of technical equipment and software, means of transport necessary for carrying out controls, ensuring the security of the institution's premises, expenses for ensuring the participation of representatives of the NCPDP in working groups, forums and international conferences.

For the chapter "*Social benefits*", financial means in the amount of 120,0 thousand MDL or 1.1% of the total allocated budget were foreseen, and the amount of 3,9 thousand MDL was executed.

With reference to the chapter "*Non-financial assets*" we mention that the amount of 679,9 thousand MDL was allocated in the proportion of 6,1% of the total budget of the NCPDP, thus executing expenditures in the amount of 586,9 thousand MDL, being purchased computing equipment, chairs and other goods needed for the proper conduct of daily activity.

In accordance with the objective on the realization of the annual and quarterly plan for conducting public procurement procedures for the year 2023, as well as its implementation by organizing and conducting public procurement procedures, for the reporting period, low-value contracts on the purchase of goods and services were drawn up and registered, as necessary, at the State Treasury, also organizing procurement as necessary with the request for price quotations - for low-value goods and services.

Budget expenditure was carried out in compliance with the principles of legality, timeliness, continuity and efficiency. All documents subject to own preventive financial control have been checked and certified for compliance/within budget limits.

In the period September-December 2023, the audit team of the Court of Accounts of the Republic of Moldova carried out the external public audit mission. The mission was carried out in accordance with the Audit Activity Programme of the Court of Accounts for the year 2023, aiming to assess the conformity of the formation, management and use of public financial resources and public assets by the National Centre for Personal Data Protection in the period 2018-2022.

The recommendations of the Court of Accounts audit team on some of the practices in place will be used to review/improve some internal processes on the use of budgetary resources, and some of the recommendations have been implemented by the end of the audit mission.

As a conclusion on the management of the allocated budgetary funds, it can be stated that they have been used as efficiently as possible in a period which has continued to be challenging and that the amounts of the institution's budget have been carefully managed.

Internal Audit Service activity

The Internal Audit Service is an internal subdivision of the NCPDP, which ensures that the mission and core functions are carried out in the following areas:

- carrying out audit missions;
- assessment of the internal management control system.

The mission of the Internal Audit Service is to perform internal audit assignments, provide advice and objective assurance on the effectiveness of the system of managerial internal control, provide recommendations for improvement and contribute to the improvement of the work of the NCPDP.

In order to perform the mission of the Internal Audit Service, the scope of internal audit work includes all systems, processes and activities of the NCPDP.

The NCPDP Internal Audit Service carried out its work in accordance with the Internal Audit Activity Plan for the year 2023, performing the **4** planned audit missions.

The audit missions carried out covered the main areas of activity of the NCPCDP, namely:

- the execution of the NCPDP budget for 2022;
- the liquidation of the Register of personal data controllers;
- compliance of public procurement of goods and services in 2022;
- archiv*ing of NCPDP files*.

The internal audit reports have been submitted to the Director of the NCPDP and to the managers of the audited subdivisions for action as appropriate.

During 2023, Internal Audit monitored the implementation of 13 recommendations submitted as a result of audit missions, including from the audit mission at the end of 2022.

The degree of implementation of **9** recommendations from audit missions for which the implementation deadline had expired was **100%.**

The implementation of **4** recommendations from the last audit mission carried out, for which the reporting deadline is May 2024, is in progress.

The monitoring of the implementation of the recommendations is kept under continuous control.

The assessment of the Annual Report on Internal Managerial Control (IMC), for the year 2022 was carried out within the deadline.

As a result of the assessment of the IMC report, as well as the internal training on the given area, in order to develop and improve the IMR system, several core processes were identified and described within General Department for Surveillance and Conformity and the Economic and Financial Service of the NCPDP during the reporting year.

At the same time, in order to implement the proposals and objections presented in the process of assessment of the internal management control system, 3 internal regulations were developed/updated and approved within the Authority:

- *Updated the GDSC's Internal Regulation by excluding from them the provisions relating to the RODCAP;*
- *Updated the Rules of Procedure of the NCPDP;*
- *Developed and approved the Internal Regulation on the evaluation of professional performance, as well as the way of establishing the performance bonus for NCPDP's employees.*

In the process of implementing and developing the IMC system and the proposals set out in the report, the managers were consulted on the managerial internal control responsibilities of the heads of NCPDP's subdivisions.

In addition, during the year, advice and counselling was provided to NCPDP's staff on public internal financial control in over **70** cases.

The risk management procedure within the NCPDP is approved.

Risks are updated and assessed in relation to the approved objectives and actions of the activity. The risk management control measures ensure an acceptable level appropriate to the risk tolerance. Monitoring of control measures within the Authority's subdivisions shall be carried out regularly, depending on the type of risk.

In order to implement the annual training plan for NCPDP's staff, the Internal Audit Service has developed methodological training material and held 2 internal training sessions on the implementation and development of the internal managerial control system (IMC).

This training provided guidance and techniques for managers and employees in various aspects such as: managerial control responsibilities, objective setting, process documentation, risk management, control activities, as well as important tools for correct and transparent management in accordance with the current legislation and regulations of resources.

The internal training sessions were attended by more than 80% of the NCPDP civil servants.

PROBLEMS AND OBJECTIVES IN THE ACTIVITY OF THE NCPDP

Analysing the period covered by this activity report, it can be noted that it was marked by a series of activities and events aimed at promoting the field of personal data protection and fulfilling the commitments of the NCPDP, as well as strengthening its institutional capacities and relations with internal partners in the public and private sector, as well as with external partners for technical cooperation.

At the same time, the concerns reflected previously, show their unchanged practicality from year to year and generate increasing difficulties both in institutional and organisational activity and in ensuring compliance of personal data processing and creating a climate of confidence for individuals to exercise control over their personal data and legal and practical security for individuals, economic actors and authorities at national level. However, taking into account the fact that solving the urgent problems faced by the NCPDP, mostly exceeds the limit of competence of this authority, it becomes even more difficult overcome/achieve them.

Thus, at the national level, remains top priority to harmonise the national legal framework with the relevant EU acquis, namely with 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, as well as 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.

In this regard, it should be noted that in the summer of 2022, at the initiative of the NCPDP, on the platform of the Ministry of Justice, which is the authority responsible for promoting the drafts (the NCPDP is not a subject with the right of legislative initiative), an inter-institutional working group was created, with a view to further analysing and finalising/elaborating draft normative acts that will ensure the alignment of national legislation with the latest standards in the field of personal data protection enshrined at European Union level.

The Working Group included representatives from the Parliament of the Republic of Moldova, the State Chancellery, the Economic Council under the Prime Minister of Moldova, the NCPDP, the Ministry of Justice, the Ministry of Economy, the Ministry of Internal Affairs, the Prosecutor General's Office, the National Anti-Corruption Centre, the American Chamber of Commerce in Moldova, the European Business Association, the Foreign Investors Association, the National Association of ICT Companies.

The active and constructive participation in the activities of the working group of NCPDP representatives, the Ministry of Justice, as well as representatives of the private and public sectors, qualifies this fact as testimony to the desire of the actors involved to align national legislation with European standards as soon as possible and to strengthen their cooperation in the field of personal data protection.

Two draft documents have been elaborated within the working group:

- *the draft law on personal data protection*, including rules on the establishment, powers and tasks of the National Centre for Personal Data Protection and the staff of the authority,
- *the draft law on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties*.

The draft law on the protection of personal data passed two approval procedures and will be submitted to the Government of the Republic of Moldova.

It is imperative to accelerate the finalisation process of these draft laws in order to bring them back on the agenda of the Parliament of the Republic of Moldova, as they will ensure the implementation of a complex and undivided legal framework by incorporating all the rules and methods enshrined by current European regulations in the field. However, the inconsistency between the national legal framework in the personal data protection field and the existing European regulations generates a multitude of deficiencies both in terms of the development of the field at the national level and in the correct and unequivocal implementation of the requirements related to personal data processing.

The process of legislation harmonization is essential to maintain an upward trend in personal data protection and not to allow a regression of the field, as well as to ensure that the rights of personal data subjects are genuinely respected. Furthermore, this harmonization promotes a legally secure environment for personal data controllers.

The Republic of Moldova must establish balanced and clear rules, without deviating from the European regulatory framework in this field, a comprehensive legislative framework for personal data protection, because recent changes in the social sphere have shown that the complexity of personal data processing operations depends on various new circumstances related to the development of information technologies that the state often fails to regulate.

It is noted that there is, currently, a major trend of companies paying increasing attention on the level of personal data protection, including when deciding to establish themselves economically in an EU member country. Thus, the existence of a legal framework in the field of personal data protection equivalent to that of the European Union will be a guarantee for foreign and national economic agents, but also for their customers, whose data stored in the Republic of Moldova will be processed under adequate security conditions and transferred on the basis of principles and rigors unanimously recognized within the European Union.

The harmonization of the legislation in the field of personal data protection with the European Union legislation will be a progressive step towards the recognition of the Republic of Moldova as a state that ensures an adequate level of personal data protection, which will enhance the credibility of the Republic of Moldova, create optimal conditions for attracting investment and developing sustainable economic relations.

Another problem that marked the work of the NCPDP is the deep institutional crisis faced by the NCPDP during the last years, conditioned by the major fluctuation of staff due to the unattractive salary in relation to the skills, the volume and the specifics of the activities carried out.

However, an analysis of the information and statistical data reflected in this report shows that the specific nature and volume of the activities in which the employees of the NCPDP are involved have increased considerably, it is crucial and mandatory to strengthen and ensure the efficient functioning of the supervisory authority for the compliance of personal data processing.

The issue of increasing the salary for employees of the NCPDP has been regularly addressed in the multitude of meetings and approaches to the Parliament of the Republic of Moldova, the Government of the Republic of Moldova and the Ministry of Finance.

The redressing of the institutional crisis within the NCPDP was also addressed in the Plenary of the Parliament of the Republic of Moldova, where deputies noted and supported the fact that, in order to ensure the independent exercising of their powers, employees of the NCPDP must be adequately remunerated, on an equal basis with other employees of independent institutions, and have a salary equal to that existing in the authorities falling within the scope of activity of the NCPDP, subject to verification by the NCPDP on the lawfulness of the processing of personal data.

Thus, by the Decision of the Parliament of the Republic of Moldova no. 103 of 28 April 2023, the Government was entrusted with the task of taking the necessary actions to solve the problems related to the system of salaries of the institution's staff and to adjust the regulatory framework in the field of personal data protection in accordance with European regulations, in order to strengthen the institutional capacities of the NCPDP.

It should be noted that, in the context of European integration aspirations, the field of personal data protection remains a priority on the agenda of the Republic of Moldova, which is conditioned not only by the harmonization of the national legal framework with the Community acquis in this field (which is currently being finalized by the Ministry of Justice), but also by the existence of qualified specialists to monitor the correct application of the legislation in this field.

It should be noted that both the Law on personal data protection and the future regulatory framework that will faithfully transpose Regulation (EU) 2016/679 and Directive (EU) 2016/680, which is a very complex legal framework, cover all areas implying the processing of personal data: public sector, financial-banking, information technology, educational, health, commercial, law enforcement, etc., and the correct application and implementation of the legal rules in this area is essential for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data.

For these reasons, during 2023, the NCPDP has not been able to hire and maintain qualified specialists, especially in the field of information technologies, which are indispensable in the work of the authority, due to the multiple skills that require advanced knowledge in this field to meet the current challenges.

The considerable increase in the workload of activities in which NCPDP's employees are involved has increased the flow of staff, caused by **the poor level of payment in relation to the complexity and volume of activities**. Thus, it has become urgent and imperative to strengthen and ensure the efficient functioning of the Personal Data Processing Control Authority.

During the year 2023, the imbalance and gap between the salary level of employees of the NCPDP and employees of other institutions is substantial, maintaining the same differential salary level, which has resulted in a major NCPDP's staff turnover and it is absolutely necessary to increase the salary of employees.

In the circumstances described above, in order to remedy the institutional crisis by means of legislative levers, which would guarantee an adequate level of salaries for the employees of the institution concerned, at the end of 2023, by the State Budget Law for 2024, the reference value of the staff of the NCCPDP was increased.

Thus, ***the problems faced by the NCPDP over the years continued in the reporting period*** and are reflected in detail in the content of this report - these are of a legal, institutional, perception

and enforcement nature and require urgent resolution in order to develop the field of personal data protection at the national level and which, if largely reviewing them, are as follows:

- ***inconsistency between the national legal framework and the existing European regulations in the field of personal data protection;***

- ***the discriminatory level of the salary of the NCPDP's employees*** compared to that provided for other surveillance bodies with similar status or authorities which, taking into account the specific nature of their activity, are processing considerable volumes of personal data and are subject to verification of the legality of data processing by the NCPDP, circumstances which generate ***staff turnover*** and the shortage/lack of qualified specialists in the field of personal data protection at national level;

- ***small number of staff in relation to the specific and increasing workload***, especially in the core subdivisions of the authority: General Department for Surveillance and Conformity and Legal Department, especially in the context that the same employees examine petitions, participate in the drafting and endorsement of draft normative acts, carry out controls/investigations of the compliance of personal data processing, perform the tasks of the ascertaining agent, participate as trainers in trainings, represent the NCPDP in the courts in administrative litigation and in the contravention proceedings, without being created/ensured and reliable institutional mechanisms in order to perform the assigned tasks;

- ***the lack of adequate safeguards for the NCPDP's employees*** regarding the risks generated by the control activity and the actions of interference of some law enforcement bodies subject to control by the NCPDP with the aim of intimidating the employees of the NCPDP;

- ***the inefficiency and insufficiency of the coercive levers for unlawful processing of personal data***, the reason having the double, contradictory and susceptible character of the procedures for examining the findings resulting from the verification of the lawfulness of personal data processing, manifested by the duplication of the examination in the courts, in the same period, of the same acts and findings issued by the NCPDP, both in administrative litigation and in contravention proceedings (detailed information reflected in the chapter Activity of representation in the courts);

- ***the abuse of legal provisions in the field of personal data protection***, in particular by representatives of public authorities, when allegedly arguing the refusal to provide the requested information in the light of the realization of the right of access to information;

- ***the large number of operations to access personal data stored in automated state information resources using the SIC "Access-Web" and COI technology, which creates difficulties in identifying the user who accessed the personal data and the purpose and legal basis of the access, respectively, or, where appropriate, the need to ensure access to state registers/information systems through the interoperability platform (MConnect).***

The objectives of the NCPDP for 2024 are essentially to take appropriate action to address the concerns highlighted above. Thus, the basic objectives outlined for the immediate future, but not limited to those described below, will focus on ensuring:

- ***to bring the national legal framework in the field of personal data protection in line with the new regulations existing at European level***, through the approval by the Parliament of the Republic of Moldova of the draft laws: on personal data protection and on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, detection, investigation or prosecution of criminal offences or the execution of criminal offences;

- ***strengthening the administrative and institutional capacities of the NCPDP*** in terms of both financial and human resources, including activities to improve staff skills and knowledge;
- ***further implementation of the tasks resulting from the National Action Plan for the Accession of the Republic of Moldova to the European Union for 2024-2027;***
- the continuation and amplification of actions ***to raise society's awareness of the importance of the field of personal data protection***, both from the perspective of respecting/knowing the rights of data subjects and ensuring the exercise of the obligations of personal data controllers;
- contribute to ***raising the level of correct interpretation and consistent application of the legal provisions in the field of personal data protection*** by the actors involved in the processing of personal data, including by ensuring a ballance between the legal provisions related to the rights of access to information, freedom of expression and personal data protection;
- ***raise the awareness of development partners in the implementation of joint projects*** in order to ensure an adequate level of personal data protection in the Republic of Moldova.