



**NATIONAL CENTER FOR PERSONAL DATA PROTECTION  
OF THE REPUBLIC OF MOLDOVA**

**ACTIVITY REPORT FOR THE YEAR 2024**

# CONTENTS

**WELCOME SPEECH.....71**

**OVERVIEW.....72**

**CHAPTER I**

**EXAMINATION OF COMPLAINTS AND  
OTHER REQUESTS .....73**

**CHAPTER II**

**ACTIVITY OF CONTROL .....76**

**CHAPTER III**

**ACTIVITY OF THE REPRESENTATION  
IN THE COURTS .....79**

**CHAPTER IV**

**EXAMPLES OF CASES EXAMINED IN 2024 .....83**



<b>CHAPTER V</b>	<b>RECOMMENDATIONS AND OPINIONS OF THE NCPDP .....</b>	<b>90</b>
<b>CHAPTER VI</b>	<b>ACTIVITY OF PREVENTION AND SURVEILLANCE OF PERSONAL DATA PROCESSING .....</b>	<b>98</b>
<b>CHAPTER VII</b>	<b>ENDORSEMENT AND DEVELOPMENT OF DRAFT NORMATIVE ACTS.....</b>	<b>103</b>
<b>CHAPTER VIII</b>	<b>INTERNATIONAL COOPERATION .....</b>	<b>111</b>
<b>CHAPTER IX</b>	<b>AWARENESS AND TRAINING ACTIVITIES.....</b>	<b>119</b>
<b>CHAPTER X</b>	<b>MANAGERIAL ACTIVITY OF NCPDP .....</b>	<b>128</b>
	<b>PROBLEMS AND OBJECTIVES IN THE ACTIVITY OF THE NCPDP .....</b>	<b>134</b>



***“Ladies and Gentlemen,  
Dear Colleagues and Distinguished Guests,***

... “Convention 108+ is an essential pillar in ensuring an adequate level of personal data protection for data subjects globally. In an age where data is the currency of progress, it is crucial to ensure that it is treated with respect and security.

This conference is a significant step in the right direction, bringing to the attention of both public institutions and the private sector a comprehensive perspective on Convention 108+ and its impact in facilitating international data flows. The topicality of this issue is all the more important in the context of the signing by the Republic of Moldova, on 9 February 2023, of the Protocol amending Convention 108+. We are now at a crucial moment in the process of securing the ratification of this document, which brings with it new and modern rules in the field of personal data protection. The Protocol amending Convention 108+ is a clear manifestation of our firm commitment to international standards and to the fundamental rights of individuals with regard to the processing of personal data.

The Treaty addresses the challenges to privacy resulting from the use of new information and communication technologies and strengthens the Convention mechanism to ensure its effective implementation. We face complex challenges and a rapid dynamic of technological change, and the ratification of this protocol is a vital step to ensure that our laws are up to the new digital challenges. In an interconnected and ever-changing world, this conference becomes a springboard for a deeper understanding of the implications of Convention 108+ and how it can contribute to a safer and more equitable digital society.

...Together, we will contribute to building a solid legal framework to ensure safe navigation in the evolving digital world. This is an excellent opportunity to reflect on the progress made in the field of data protection and to underline the importance of a responsible approach to handling personal information.

...We want to raise the awareness of all actors involved - from public authorities and institutions as well as the private sector. Only through collaboration and active involvement can we build an environment where personal data is treated with respect and trust.”

Extract from the speech of Mrs. Victoria MUNTEAN, Director of NCPDP  
in the context of the opening of the National Conference on  
*“Raising Awareness on Convention 108 +”*,  
event organized on 26 January 2024 on the occasion of  
the European Data Protection Day



## OVERVIEW

### Year 2024 in numbers

#### REQUESTS/COMPLAINTS

##### 13037 correspondence documents:

5596 inbox, of which 1160 complaints



5699 outbox

1742 internal

#### ACTIVITY OF CONTROL

312 initiated controls

372 issued decisions

268 decisions of the absence of violations found

173 decisions of violations found

135 minutes drawn up

143 cases of contraventions found



#### ENDORSEMENT ACTIVITY OF DRAFT NORMATIVE ACTS

##### 170 approved proposals

42 draft agreements/  
international treaties;

48 draft normative acts  
amending laws, codes;

80 draft normative acts of the  
Government and other authorities



#### ACTIVITY OF THE REPRESENTATION IN THE COURTS

##### 692 court proceedings:

487 in contravention proceedings

205 in administrative litigation



#### PREVENTION ACTIVITY

1893 consultations provided



139 entities with  
designated data protection  
officers

#### The level of budget execution NCPDP, %



#### HUMAN RESOURCES

34 out of 45 staff-limit

5 competitions held



7 persons employees/5  
debutants

7 persons resigned

16 training courses for  
employees

#### TRAINING AND AWARENESS ACTIVITY

5690 trained persons

76 training activities

10 information and awareness-raising  
activities

119 elaborated and  
published press  
releases





## CHAPTER I

EXAMINATION OF COMPLAINTS  
AND OTHER REQUESTS

The complaints received by NCPDP concern various sectors, such as: video surveillance, social networks, telecommunications, labor relations, health, education, financial, public sector, etc. In their examination, the NCPDP applies the same principles and rules/conditions provided by Law no. 133/2011 on personal data protection, but the issues raised in the complaints are very different and each time new topics/aspects are highlighted due to the evolution of the field and its interaction with the daily activities of citizens, which involve the processing of personal data. The emergence of new technologies is constantly generating new questions, and it is certain that the issues complained will continue to evolve, making the mission of NCPDP more and more complex but interesting. Every day, the NCPDP responds to dozens of requests, often complex, dealing with situations in its field of competence, from a wide variety of audiences.

During 2024, NCPDP examined and issued **13 037** correspondence documents, including **5596** inbox documents of which **1096** complaints of personal data subjects and **5163** outbox documents.

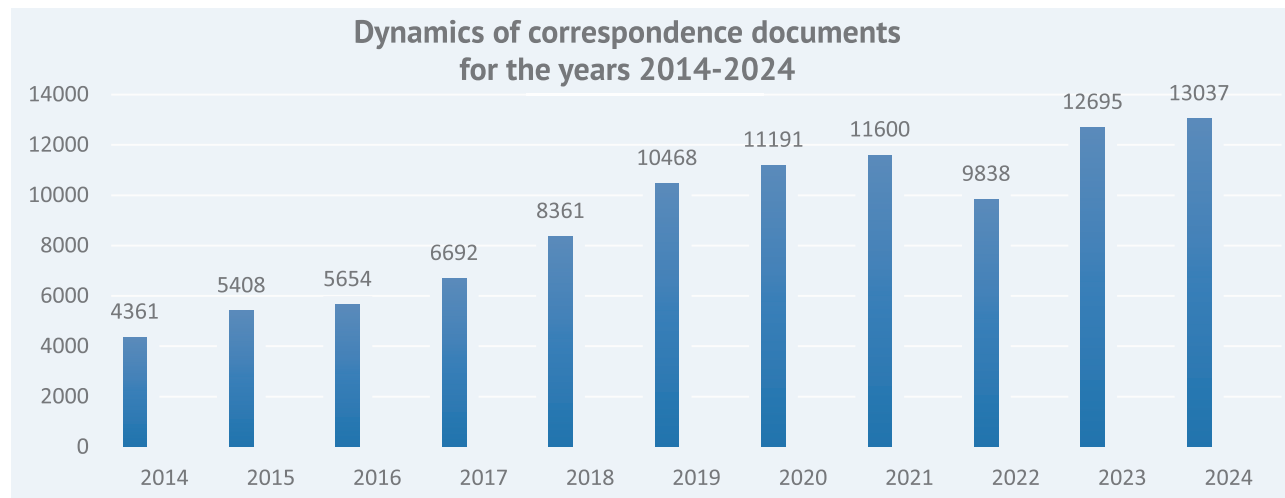
*Comparative statistics of correspondence documents, for the years 2014-2024*

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
2024	13 037	5596	5699	1160	1742

In order to face this flow of documents, the NCPDP has mobilized its efforts on offering information and advisory support both to personal data subjects, providing them with qualified legal information about the exercise of their rights, and to data controllers, assisting them with the compliance of personal data processing operations to personal data protection legislation, responding and providing advices both in writing through the post office, by e-mail or verbally, by phone or in audiences.



The dynamics of the number of correspondence documents registered by the NCPDP during 2014-2024 can be analysed in the below diagram.

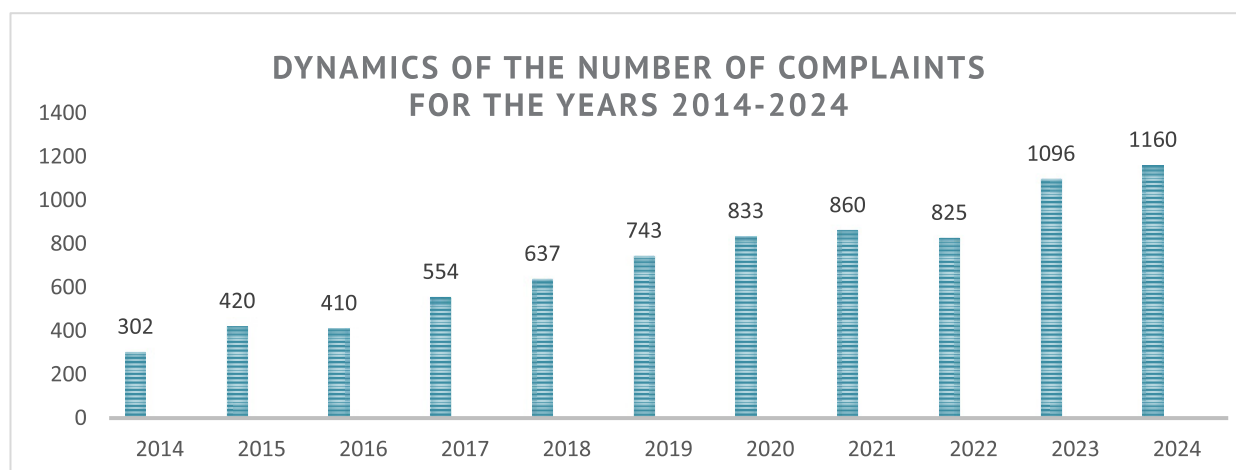


The topics addressed in the correspondence documents reveal the increased concern of personal data controllers in ensuring compliance with personal data processing requirements established by Law no. 133/2011 on personal data protection and related national legislation, in implementing the necessary organizational and technical measures to ensure the confidentiality and security of personal data processed, including in the context of processing personal data through automated filing systems, the use of automated decision-making based on the categories of personal data collected, which have generated new challenges for the field of personal data protection, as well as the interest of personal data subjects in order to actually realize the rights afforded by Law no. 133/2011 and the growing tendency of the latter to have control over their own personal data, in particular in the light of the increasing exchange of personal data between public and private actors, including individuals, associations and companies.

#### Activity of examination of personal data subjects' complaints

During the reporting period, **1160** complaints were received by the NCPDP from natural persons - personal data subjects.

From the total number of complaints registered in the reporting period, in **312** cases, controls on the compliance of personal data processing were initiated.





Thus, in 2024, the complaints sent to the National Authority of Personal Data Protection continued to raise, mainly issues related to:

- ✓ Processing of personal data through video / audio surveillance systems: **435** cases;
- ✓ Processing of personal data without the data subject's consent and/or legal basis, including the processing of personal data from state information resources: **346** cases;
- ✓ Processing of personal data by disclosure on social networks: **179** cases;
- ✓ Enforcement of personal data subjects' rights (access, information, intervention, opposition): **134** cases;
- ✓ Processing of personal data of minors: **16** cases;
- ✓ Processing of personal data in the police sector (MIA, NAC, General Prosecutor Office, etc.): **15** cases;
- ✓ Processing of personal data in the financial sector, insurance companies: **8** cases;
- ✓ Processing of personal data in the healthcare sector: **6** cases;
- ✓ Processing of personal data in the electronic communications sector: **5** cases;
- ✓ Processing of personal data in the on-line environment and the media: **4** cases;
- ✓ Checking the legality of processing operations: **4** cases;
- ✓ Processing the data subject's IDNP: **4** cases;
- ✓ Publication of court decisions without their proper depersonalization: **2** cases;
- ✓ Disclosure of personal data to unrecognized entities acting on the left bank of the Dniester (Transnistria): **1** case;
- ✓ Cross-border transfer of personal data: **1** case.





## CHAPTER II

## ACTIVITY OF CONTROL

ACTIVITY CONTROL, KEY FIGURES 2024		Measures coercive/corrective ordered:
<b>312</b> Controls	<b>372</b> Decisions issued	<b>47</b> - Suspension
<b>12</b> Exit controls on the spot	<b>268</b> Finding the absence of violations	<b>28</b> - Cessation
	<b>173</b> Finding the violations	<b>8</b> - Destruction / erasure
		<b>17</b> - Organizational and technical measures to be implemented

The control of compliance of personal data processing is initiated upon complaint of personal data subject or on the basis of NCPDP's self-report, in accordance with Article 27 of Law no.133/2011, upon having information/indications, supported by evidence, about the existence of situations of violation of the fundamental rights and freedoms of natural persons with regard to the processing of personal data, in particular the right to inviolability of intimate, family and private life.

The control activity consists in verifying the lawfulness of the processing of personal data by personal data controllers and/or processors. When examining each control material, appropriate, necessary and proportionate steps are taken 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 interviewed/heard or to present his/her position on the issues raised in the complaint separately.

The control performed allows the NCPDP to understand the nature and purpose of the personal data processing carried out by a controller and/or processor and, as a result of the control, the NCPDP may order actions/measures to bring the personal data processing operations into compliance with the requirements of the law and/or request the court to impose a fine.

The control is carried out by the State Inspectors of General Department for Surveillance and Conformity and the Legal Department, who are authorized with control functions.

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 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.





Control activity means carrying out checks on personal data controllers to clarify the facts and circumstances in relation to the processing of personal data and to collect the evidence necessary for the objective examination of the complained case.

Thus, during the reference period, **312** control materials were initiated and examined, based on the complaints of personal data subjects/self-reports initiated at the request of legal entities or ex officio, with a decrease in the number of controls initiated compared to 2023. In this regard, it should be noted that when a complaint is submitted, depending on its subject matter, the NCPDP reminds individuals of the need to address in prior to the controller or the processor and, however, compliance with the procedure established by art. 27 para. (1) of the Law on personal data protection is necessary in order to meet the conditions for receiving and resolving complaints. Finally, this is a procedure to jointly remedy with the controller or processor any uncertainty regarding the alleged non-compliance, in which order the need to apply to the NCPDP for a control is no longer necessary. It should also be noted that the control is initiated at the complaint of the data subject. In general, the data subject complains about the actions of a single controller, however, there are increasingly frequent cases where, in a single complaint, the data subject contests the processing of his or her personal data by several controllers in different cases, and in these cases too, the NCPDP initiates a single control. Such controls are much more complex and require more time to gather the relevant information and evidence, to hear all the persons involved, and to carry out a multi-aspectual analysis of the operations complained. Despite the effort made, this has a direct impact on the increase in the number of controls initiated.

It should also be noted here that the control is initiated upon the complaint of the data subject. In general situations, the person complains about the actions of a single controller. However, cases are increasingly recorded when in a single complaint, the person contests the processing operations of his personal data carried out by several controllers regarding different circumstances. However, such controls are much more complex and require a longer time to accumulate relevant information and evidence, to hear all the persons involved, as well as a multi-aspect analysis of the operations complained about. In these cases, NCPDP initiates a single control and, even if the efforts made to examine such controls are much more imposing/complex, this fact directly influences the number of controls initiated.

It should be noted that, during the reference period, controls on the compliance of personal data processing with the requirements of the Law on personal data protection were carried out in relation to the following actions 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, **372** 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 **268** cases the absence of infringement was found, in **173** 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* – **47 cases**;
- *Cessation of personal data processing* – **28 cases**.
- *Destruction / erasure of personal data processed regarding the infringement of legal provisions* – **8 cases**;
- *The need to implement the necessary organizational and technical measures for personal data protection* - **17 cases**.

At the same time, as a ascertaining agent in relation to the provisions of Articles 74<sup>1</sup> - 74<sup>3</sup> of the Contravention Code related to the violation of legal provisions in the field of personal data protection, during the year **2024, 135 reports** were drawn up **on contraventions, 143 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<sup>1</sup> para. (1): infringement of personal data processing, storage and usage rules, except in the cases provided for in paragraph (5) – **111 cases**;

- Art. 74<sup>1</sup> 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 – **10 cases**;

- Art. 74<sup>2</sup> 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 – **18 cases**;

- Art. 74<sup>3</sup>: failure to fulfill within the established term the decision of the National Center for Personal Data Protection on the reinstatement of the personal data subject's rights, including the suspension or cessation of personal data processing, on blocking, partial or complete destruction of personal data processed in violation of personal data protection legislation - **4 cases**.

### *Comparative information on the control activity, for the years 2018 – 2024*

Period for comparison	Number of controls initiated	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 /
Year 2018	326	16	Minutes issued	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	356	26	15	18	107/117
Yaer 2024	312	47	28	8	143/135



CHAPTER III

ACTIVITY OF REPRESENTATION  
IN THE COURTS

ACTIVITY OF REPRESENTATION IN THE COURTS

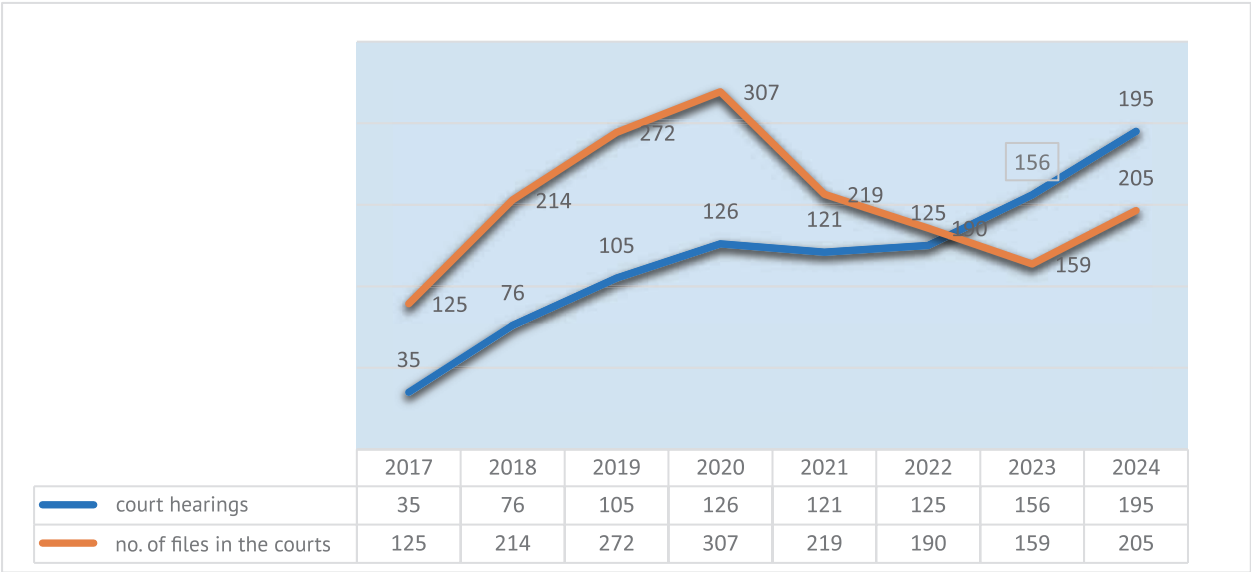


*In civil and administrative litigation*

During 2024, the NCPDP’s interests were represented in the administrative litigation courts in **224** court hearings, amongst which: **210** as a defendant; **14** as a public authority which draws conclusions.

Therefore, the representatives of the NCPDP participated in **205** court hearings of administrative litigation, drafting **130** procedural documents necessary for an efficient examination of court cases.

*Comparative dynamics of the number of cases and court hearings in administrative litigation, for the period 2017-2024*





Similarly, during 2024, the examination of **29** court files was completed where the judgments/decisions of the courts remained final and irrevocable, of which:

- **26** judgements/decisions of the court were issued in favor of the NCPDP;
- **3** case were unsuccessful for the NCPDP, which concerned administrative acts issued in the years preceding the reporting period: one decision on the control of the lawfulness of personal data processing operations and two replies to petitions.

Thus, we find that in **90%** of the number of completed court files, the actions taken by the NCPDP were considered legal and justified by the courts.

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:

*On November 20, 2019, the NCPDP received a collective complaint from some judges who alleged the violation of the Law no. 133/2011 by their colleague, as a result of the publication / dissemination on Internet (on a social network) of personal data, such as: name, surname, signature and domicile of judges, without their consent. Following the examination of the case, the NCPDP noted that the category of personal data that poses a higher risk to individuals is the data on their domicile, and unlike the other categories of personal data that have been published/disclosed, which can be considered public despite the position held by the petitioners, the domicile cannot be categorized as public information.*

*After examining the case, the NCPDP found, by decision, that the provisions of the law had been infringed in the alleged case.*

*Disagreeing with the decision of the NCPDP, the claimant filed an application for a contentious administrative appeal. Following the examination, the court admitted the action and annulled the administrative act issued by the NCPDP.*

*However, following the appeal submitted by the NCPDP against the judgment of the trial court, the Chişinău Court of Appeal appealed the judgment of the first instance and issued a new decision, dismissing the action filed by the respondent as unfounded.*

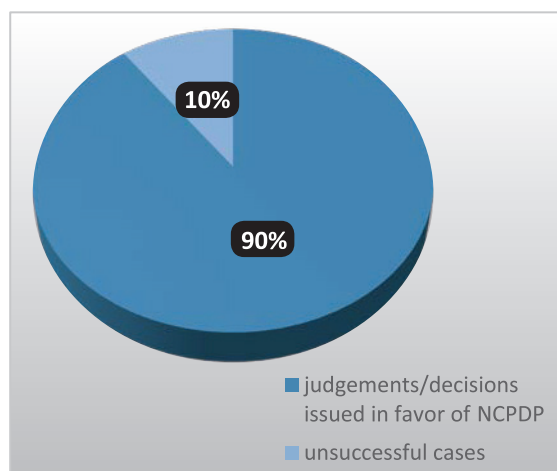
*The Chişinău Court of Appeal confirmed that the NCPDP decision complies with the legal rules and fundamental principles of personal data protection, corrected the errors of assessment of the court of first instance and emphasized the importance of a proper and detailed assessment of all relevant evidence and legal issues.*

*The Supreme Court of Justice has still to decide on the case.*

#### Case no. 2:

*Following the examination of the complaint submitted by a citizen on behalf of the administrator of a condominium association in mun. Chisinau - which alleged violations of the provisions of the Law no. 133/2011 on personal data protection, namely, by accessing in the Real Estate Register (RBI) the information on the real estate owned by title of ownership, the NCPDP initiated the control procedure and issued the Decision finding the violation of the provisions of Law 133/2011.*

**Dynamic of court files in 2024**





Thus, the condominium association, whose administrator accessed the personal data of the petitioner, had signed a contract for the providing of services from the RBI with the Public Services Agency in order to perform the tasks of the association.

At the same time, the association signed a contract with another condominium association, of which the petitioner was a member, for the provision of consulting services. Following the examination of the case, it was held that the condominium association that accessed the personal data of the petitioner was not entitled to access the personal data of the tenants of another association, in which order the NCPDP found a violation of the provisions of the Law no. 133/2011, as the legal basis for the processing of personal data was not established.

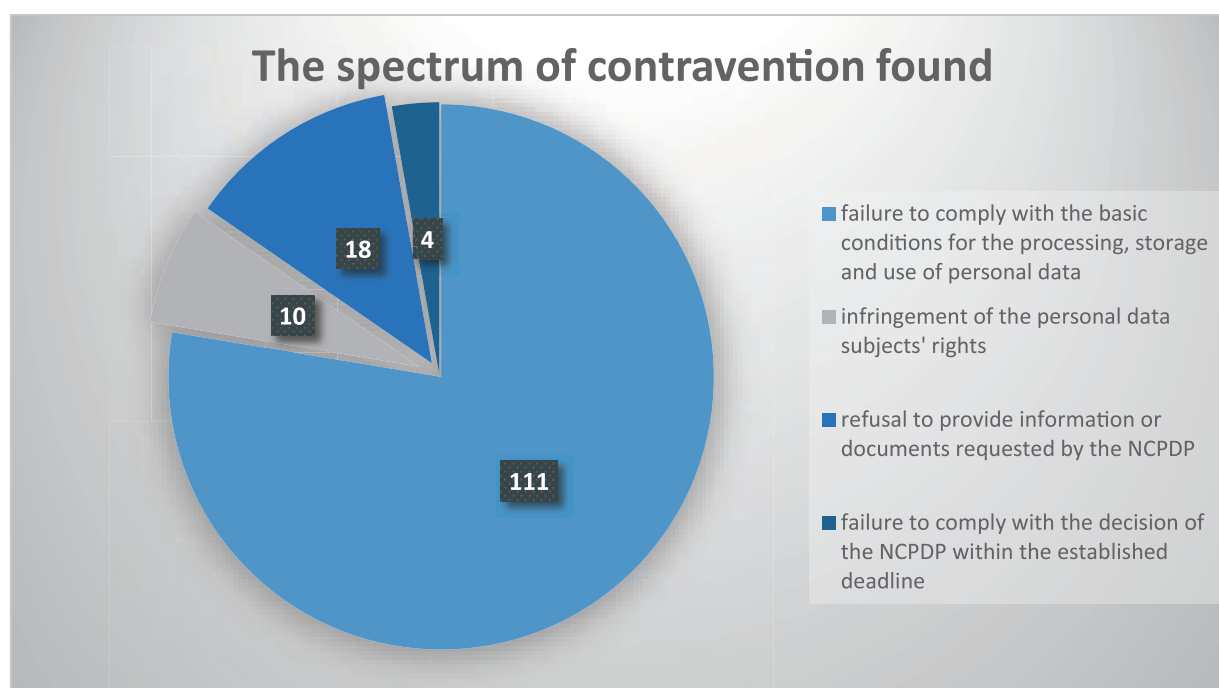
Finally, the condominium association appealed the decision issued by NCPDP in court and requested its annulment as unfounded and illegal.

On 12.06.2024, the Chisinau District Court, Rascani Branch, issued a judgment dismissing the administrative action filed by the association.

The judgment in question was not subject to any appeal, thus it remained final and irrevocable as of the date of the judgment.

### ***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 **135** minutes on contravention, being ascertained **143** contravention facts. In accordance with Art. 423<sup>4</sup> 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 **487** court hearings on contraventions under examination. Furthermore, it should be noted that during the reference period, in **162** contravention cases NCPDP won the case, the court acknowledging the guilt of the persons in respect of whom minutes on contravention were drawn up, including on cases submitted to the court prior to the reporting period, establishing sanctions in the form of a fine. At the same time, during the reported period, **5** minutes on contravention were ceased/cancelled. In addition, it should be noted that other **106** contravention proceedings are pending, including on some of the infringement cases initiated in 2023.

**Examination in the courts, both in administrative proceedings and in contravention proceedings of the same acts and findings issued following the verification of the lawfulness of personal data processing significantly hinders the work of the authority.**

However, as a result of the examination of the control materials on the lawfulness of personal data processing, in the order stipulated by Article 27 para. (3) of the Law on personal data protection, [...] the decision issued by NCPDP on the finding of infringement of personal data protection legislation and the evidence gathered serve as a basis for the drawing up the report on the contravention, under the conditions of the Contravention Code.

It should be noted that, according to the practice, there are contradictory solutions adopted by the courts, in which, for the same act, in administrative proceedings, the controller is found guilty by the court, and in contravention proceedings, the court finds the absence of the contraventional act, annulling the minutes on the contravention or vice versa.

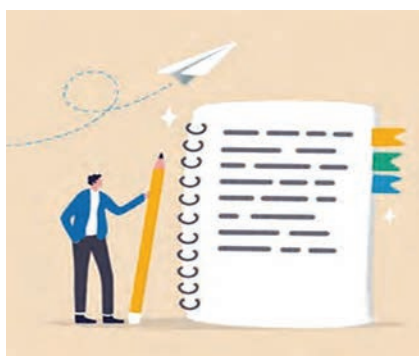
**The existence of such contradictory procedures led, in some cases, to determining the inefficiency of the actions taken by the NCPDP to counteract non-compliant data processing and to prevent the committing of other violations concerning the right to the inviolability of the intimate, family and private life of personal data subjects.**



## CHAPTER IV

EXAMPLES OF CASES  
EXAMINED IN 2024

## IV



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.

In this respect, Authority shall present, including by means of the annual activity report, significant cases and issues identified during the controls 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: Regarding the excessive processing without a legal basis of personal data relating to the first-degree relatives of the offender when the report on the infringement is drawn up, in respect of the latter***

*The NCPDP examined the complaint of a data subject who alleged unauthorized and excessive processing of his personal data by an employee of a public authority, without any legal basis, carried out by an employee of a public authority as an ascertaining agent.*

*Within the investigation it was determined that the employee of the public authority, in order to establish the identity and domicile of the person against whom the contravention case was initiated, processed her personal data through the government portal [www.date.gov.md](http://www.date.gov.md), accessing in addition the personal data related to her first-degree relatives, in which order, in the report generated by the portal, there are personal data about her mother, husband and son, which, being printed, was attached to the material of the contravention proceedings initiated against the petitioner.*

*Examining the circumstances of the case, it was determined that the ascertaining agent was to access/consult only those personal data that were strictly necessary for the drawing up the report on contravention, in accordance with Art. 443 para. (1) lit. c) Contravention Code.*

*Even if the extract/personal file automatically generated by the governmental portal [www.date.gov.md](http://www.date.gov.md), included the personal data of the relatives of the person for whom the administrative procedure was initiated, the ascertaining agent had to take measures to depersonalize these data, if the file was intended to be attached to the administrative file, if it was not technically possible to separate them from the data on the offender, which were necessary for the proper conduct of the administrative procedure.*





However, in this case, it was found that the ascertaining agent excessively processed the personal data relating to the offender's mother, husband and son, which had no relevance to the case under examination and did not need to be attached to the case materials, not being established the existence of a legal basis, a specific, explicit and legitimate purpose and the causal link between the purpose and the identifiers of the offender's relatives, being found the violation of the provisions of Art. (1) lit. a), c) and art. 5 of Law no. 133/2011 on personal data protection, which determined the existence of the constitutive elements of the offense provided for in Article 741 paragraph (1) of the Contravention Code (failure to comply with the basic conditions for the processing, storage and use of personal data)

In the context of the findings, the NCPDP has requested the public authority to re-evaluate the categories of personal data processed, in the light of the tasks entrusted to it, in relation to the set of data to which it was granted access and, if necessary, to address the public institution that provides access to the government portal in order to remedy the situation by identifying and implementing organizational and technical measures that would prevent situations of excessive processing of personal data by its employees, as in the case in question.

#### **Case No. 2: Regarding the attachment of a copy of the identity card to a file in which the person was not concerned**

The NCPDP examined the complaint by which the petitioner requested verification of the legality of the processing operations of his personal data following the attachment a copy of his identity card to a civil file in which he was not concerned.

Thus, during the investigation, it was found that the copy of the identity card belonging to the petitioner was collected and attached to personal file drawn up upon hiring a third party, which is not provided for in the regulations or instructions related to keeping the personal file.

Subsequently, the copy of the identity card belonging to the petitioner was attached, together with other documents of the third party, to the civil file in which the latter was concerned.

Following the above, the NCPDP determined that the processing operations of personal data belonging to data subject contravene the provisions of art. 4 para. (1), letters a) and b) and art. 5 of the Law on personal data protection, or, they were carried out by the data controller - where applicable, a public authority, in the absence of a specific, explicit and legitimate purpose.

#### **Case No. 3: Regarding the disclosure of personal data recorded in the Decision of the Equality Council, without ensuring their confidentiality**

The NCPDP examined the complaint of a data subject, who complained about the non-compliant processing of his personal data, such as: name, surname, health data, by the director of the kindergarten where he worked, following the dissemination/publication of this data on the social network „Facebook”.

During the investigation, the kindergarten director acknowledged the publication/dissemination Decision of the Equality Council, without depersonalization of personal data, on the profile created and managed by her on the social network „Facebook” and claimed that the decision was published to ensure transparency and to eliminate discrimination against her. At the same time, she claimed that, upon employment, within the preschool educational institution, the petitioner signed the agreement on the processing of employees' personal data, which would have provided her with a legal basis in this regard.



Although the kindergarten director had a legal basis for processing the personal data of the petitioner as an employee, in the employment relationship, the dissemination/publication on the social network „Facebook” of the Decision of the Equality Council, which contains information such as name, surname, health data, cannot be justified by the petitioner consent for the processing of personal data at the date of employment, or, accordingly, the person did not express consent to the publication of her data on any social networks.

For these reasons, the NCPDP found that the controller processed the personal data of the petitioner without a legal basis, without ensuring the confidentiality of the processed personal data, actions that contravene the provisions of art. 4 para. (1) lett. a), art. 5 para. (1) and art. 29 para. (1) of the Law on personal data protection.

Subsequently, pursuant to art. 20 para. (2) of the aforementioned normative act, the NCPDP ordered the deletion of the Decision of Equality Council containing the personal data of the data subject, published on the social network „Facebook” or the depersonalization of the personal data, so that the details regarding the personal or material circumstances no longer allow their attribution to an identified or identifiable natural person or to allow attribution only under the conditions of an investigation that requires disproportionate expenditure of time, means and manpower.

#### **Case No. 4: Regarding the publication of personal data on social networks**

The NCPDP examined the complaint of a data subject, through which it notified the alleged fact of non-compliant processing of personal data concerning him, following the publication on social networks of a video sequence containing the latter's personal data.

Thus, by analyzing the content published on the social network, the existence of a video sequence was identified, which begins with the presentation of two photographic images of the petitioner printed on a sheet (it is assumed that these are part of a file), containing: image, name, first name, father's first name (patronymic), date of birth, gender, place of birth and citizenship. At the same time, on the same tab there is a table in which other information regarding the petitioner is inserted. Furthermore, the video sequence presents a request submitted by the petitioner to the police body, which contains the personal data of the data subject, as follows: name, first name, patronymic, domicile, day, month, year of birth, identity card series, mobile phone number.

During the investigation, it was determined that the user with an unidentified pseudonym, revealing the disputed video on the TikTok social network, did not implement any actions to ensure the confidentiality of the data subject's personal data, thus violating the principles of personal data protection.

Accordingly, following the examination of all the information/materials administered, no evidence that would undoubtedly identify the person who collected the personal data of the data subject and subsequently published the disputed video sequence on the TikTok social network could be accumulated, it being only noted that citizen I. E. took over the disputed video sequence from a public source and republished it on his profile page on the Facebook social network.

Therefore, NCPDP was unable to intervene in other ways to identify the person who is registered on the TikTok social network with the username (unidentified pseudonym), because the platform does not make such information public for confidentiality reasons.

However, given that the purpose and legal basis for the publication/dissemination of personal data on the TikTok social network was not identified from the accumulated materials, NCPDP found in rem that the user of the above-mentioned social network with the username (unidentified



pseudonym) published a video sequence containing the personal data of the petitioner, contrary to the provisions of art. 4 para. (1) lett. a), c) and art. 5 para. (1) of the Law on Personal Data Protection.

At the same time, in relation to citizen I.E., who republished on his profile page on the social network Facebook, the same video, which includes: image, name, first name, patronymic, domicile, day, month, year of birth, ID card series, mobile phone number of the petitioner - data that were and can be consulted by users of the social network Facebook who view the respective post, invoking in this regard the information of the general public/freedom of expression, it was ordered that he make changes (e.g. blanking/blurring) of personal data, published, in order to ensure their confidentiality, being excessive in relation to the declared purpose, or, in the case, even if it is claimed that the person targeted in the post is a civic activist/public figure, and in relation to him the principle of reducing personal data to a minimum is to be ensured, to the extent that they are adequate and not excessive in relation to the declared purpose.

#### **Case No. 5: Processing of personal data during the live broadcast of the local council meeting**

The NCPDP examined the complaint regarding the alleged non-compliant processing of personal data, following the live broadcast of the local council meeting, during which the subject of providing material aid to a vulnerable person was discussed.

During the investigation, the NCPDP found that personal data concerning the person in question were published on the social network „Facebook”, following the live broadcast of the local council meeting by a councilor, in order to ensure the transparency of the decisions taken by the council. As a result, the name, surname, the illness the person suffers from and the amount of aid were disclosed.

According to art. 4 par. (1) lett. a), b) and c) of Law no. 133/2011 on personal data protection, personal data that are the subject of processing must be processed fairly and in accordance with the provisions of the law; collected for specified, explicit and legitimate purposes, and not subsequently processed in a manner incompatible with these purposes, adequate, relevant and not excessive in relation to the purpose for which they are collected and/or subsequently processed. Thus, the local councilor should have stopped the live broadcast as soon as he was informed that information containing sensitive personal data of individuals was to be discussed, especially being aware that information regarding health status constitutes a special category of personal data.

In the context, in resolving the complaint, the NCPDP found a violation of the provisions of art. 4 para. (1) lett. a), b), c), art. 5 para. (1), art. 7 and art. 29 para. (1) of Law no. 133/2011 on personal data protection by the local councilor, when disclosing the personal data of the data subject.



### **Case No. 6: Publication of personal data on social networks of vulnerable persons**

Following a complaint, the NCPDP took action on the alleged illegal processing of personal data concerning people from various localities in the country, following the publication on the social networks „Facebook” and „YouTube” of video sequences regarding the offering of food packages to elderly people, including those bedridden, with the disclosure of their image, voice, as well as data about their age, physical characteristics and residence.

During the investigation, it was found that the person, while performing acts of charity, made numerous video recordings at the homes of the persons concerned, which were subsequently disseminated/published on social media, in the absence of the consent granted by the latter for the processing of personal data.

The NCPDP does not deny the benefit of the charitable actions carried out, in this case, but the publication on social networks/internet of personal data of the data subjects, in the absence of their consent, violates the conditions for personal data protection, especially when information about social/vulnerable status or/and health status is disclosed, which constitutes a special category of personal data and poses high risks for the rights and freedoms of individuals.

Consequently, the NCPDP found that the processing of personal data of the persons found in the published video sequences was carried out in violation of art. 4 para. (1) lett. a), b) and c), art. 5 para. (1) and art. 29 para. (1) of the Law on personal data protection.

### **Case No. 7: Processing of personal data for commercial prospecting purposes by a preschool educational institution**

The parents of a minor child contacted the NCPDP, deploring the actions of a preschool educational institution following the broadcasting of video spots on its Instagram page, which allegedly contain images of the child, without their consent.

During the investigation, from the materials accumulated, the NCPDP noted that the parents had concluded an educational contract, which stipulated that upon signing it, the students and parents/legal representatives consent to the school using photo-audio-video recordings of their activity and their names, for exclusively educational purposes or for promoting, on various channels, the school's image and the results of school and extracurricular activities.

Thus, during the investigation it was found that the use/publication of the child's personal data took place after the termination of the educational contract, or, according to the circumstances indicated in the complaint, a consent accepting the processing of personal data, after the termination of the contract, by the legal representative of the minor child, was not expressed. Although the parents requested the deletion of personal data, the videos in which the image of the minor child appears, ran on the institution's Instagram page for more than 3 months, without their consent, and the preschool educational institution was found to have violated the provisions of art. 4 para. (1) lett. a), c), art. 5 para. (3) of Law no. 133/2011.



**Case No. 8: Failure to comply with the organizational and technical measures necessary for the personal data protection**

The NCPDP examined the complaint of an individual, who requested verification of the legality of personal data processing operations concerning him, carried out through several state information resources.

During the examination of the accumulated material, it was found that one of the controllers to verification did not take the necessary organizational and technical measures for the protection of personal data, actions aimed at ensuring an adequate level of integrity, confidentiality and security with regard to the risks related to the processing of personal data recorded in the Central Data Bank of the Real Estate Cadastre, or, upon termination of the employment relationship with the employee, who was assigned a user account at the central data bank of the real estate cadastre for the exercise of his/her job duties, the controller (local public authority) did not withdraw the right of access to the mentioned information resource, which led to the access of personal data for purposes other than those resulting from the powers assigned to the controller.

In these circumstances, in relation to the user, who accessed the personal data, NCPDP found a violation of the provisions of art. 4 para. (1) lett. a), b), c), art. 5 para. (1) of the Law on personal data protection and in relation to the controller, a violation of the provisions of art. 4 para. (1) lett. a) and art. 30 of the same law, when processing the personal data of the data subject.

**Case No. 9: Processing of personal data through a video surveillance system installed within the perimeter of a residential building**

The NCPDP received a complaint from an individual who complained about his neighbor's actions regarding the processing of personal data through a video surveillance system that was installed in the staircase of a residential building, as well as on the exterior wall of the building.

In the case, the NCPDP found that the personal data (image) of the residents of the apartment building and of the visitors/passers-by are processed through the video surveillance system, since the angle of capture of the surveillance cameras monitors/records video the space that constitutes a common part of the apartment building (entrance to the apartment building, stairs of the apartment building, common yard) and the public road. Thus, the personal data that are the subject of processing through the complained video surveillance system are excessive for the declared purpose, which cannot be considered as an activity carried out exclusively „for personal or family needs”, operations that present an interference in the private life of the persons subject to monitoring.

However, in the case of apartment buildings, a video surveillance system could only be installed by the Condominium Co-Owners Association, for example, at the entrance/exit to/from the apartment buildings, within the perimeter of the building, as well as in the spaces adjacent to them (parking spaces, access roads, etc.) in accordance with the provisions of art. 34 para. (3) lett. f) of the Condominium Law, art. 546 para. (1) and para. (2) of the Civil Code.

At the same time, it was determined that the video surveillance camera had an „audio recording” function.



*Before installing video surveillance cameras with audio recording, the controller must always critically examine whether this measure is, firstly, appropriate for achieving the desired objective and, secondly, proportionate and necessary for its purposes, in relation to the fundamental rights and freedoms of the data subjects. However, during data processing, not only private conversations of family members are recorded and stored, but also of third parties who fall within the range of the video/audio recording devices, which constitutes an excessive and disproportionate measure in relation to the declared purpose, thus violating the right of other persons to the inviolability of their private life.*

*In this case, it was determined that the processing of personal data, through the video surveillance system complained of, was carried out in violation of art. 4 para. (1) lett. a) and c), art. 5 para. (1) of the Law on personal data protection, and the processing of personal data through the video surveillance system was ordered to cease.*

#### **Case No. 10: Processing of personal data for the purpose of pursuing a legitimate interest**

*The NCPDP examined the case regarding the alleged non-compliant processing of personal data of 96 employees by a former employee of the entity.*

*During the investigation, from the accumulated materials, the NCPDP deduced that the latter, having access to the entity's archive during the period when he worked within it, collected and disclosed information containing personal data of the institution's employees such as: name, surname, position and salary to the Ministry of Education and Research by submitting a complaint regarding certain abuses committed by the institution's administration during the period when he was employed, and the documents attached to the complaint served as evidentiary material to prove those invoked by the latter.*

*In this context, it should be noted that the disclosure of information containing personal data must not contravene the principles of personal data protection, as long as it is necessary for addressing the competent authorities, reporting certain frauds, and presenting evidence in this regard, or for defending one's rights and interests or the interests of society as a whole. Thus, in the case under examination, the processing of personal data was relevant to the purpose for which it was disclosed, given that the complaint submitted to the Ministry of Education and Research also concerned employees whose personal data were recorded in the documents attached to the complaint. According to Article 5(5) lett. (e) of Law 133/2011, the consent of the data subject is not required if the processing is necessary to fulfill a legitimate interest of the data controller or a third party to whom the personal data is disclosed, provided that this interest does not harm the interests, rights, and fundamental freedoms of the data subject.*

## CHAPTER V

RECOMMENDATIONS AND OPINIONS  
OF THE NCPDP

## RECOMMENDED



In order to prevent the violation of personal data processing rules, as well as to ensure the public is informed about the issues and situations encountered in the area of its competence, the NCPDP issues recommendations and opinions in the field of personal data protection. *These can be consulted on the authority's website in the section „General Recommendations on Data Protection” or in the section „Data Controller/Recommendations of NCPDP”.*

During the reference period, the NCPDP provided several clarifications and recommendations both for data subjects and for data controllers, such as:

*Guidelines regarding security measures for the protection and processing of personal data within information systems*



Currently, the obligation to ensure the security of personal data processing is stipulated in Article 30 of Law no. 133/2011 on personal data protection. This provision is of a general nature, which can create difficulties for controllers and processors in understanding the specific responsibilities related to data security. The references made in the guidelines will contribute to a better understanding and application of the legal requirements regarding the security of personal data.

Identifying appropriate measures to protect personal data is always a challenge for controllers and processors as there is no universally applicable rule. Therefore, the document cannot provide a single model applicable to all types of personal data processing. However, its aim is to present the essential elements of the related procedures, in order to facilitate a generally shared understanding of “who, how and when should act”.

*The full text of the guidelines can be viewed by accessing the link: [https://datepersonale.md/wp-content/uploads/2025/01/cerinte-masuri-securitate-acualizat\\_26\\_02\\_24.pdf](https://datepersonale.md/wp-content/uploads/2025/01/cerinte-masuri-securitate-acualizat_26_02_24.pdf)*



### Things to know about personal data



#### ➤ What is personal data?

Name, surname, home address, telephone number, e-mail address, location data, IP address, civil state, photo face, habits and preferences, online identifiers and any other data related to the physical, physiological, economic, cultural or social identity that can be used for the direct or indirect identification of a natural person.

#### ➤ Special category of personal data

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, data concerning health, genetic data, and biometric data for uniquely identifying a natural person, or data concerning a natural person's sex life or sexual orientation. The processing of these data is allowed only in cases strictly stipulated by law.

#### ➤ When can I transfer my personal data to other persons?

In case personal data is requested, you may send your personal data independently when this is necessary for the fulfillment of obligations, or when this fact is provided by law. For example, provide the home address of an online store for the delivery of the order, present the identity card to confirm the age when you buy alcohol in a store, give the personal data to hospital for receiving treatment, etc.

#### ➤ When can I disclose the personal data of other persons?

You may process the personal data of other persons if this data is necessary for the achievement of a legal purpose, for example: provide this information when requested by law enforcement agencies, submit personal data to the court to defend your rights. In general, the volume and categories of data transmitted must not exceed the stated purpose.

#### ➤ When should you comply with the provisions of the Law on personal data protection?

You should comply with the legislation in the field of personal data protection, whether you collect, store, transfer, disclose by transmission or if, by automated means, you process personal data, which is part of a record system in connection with a professional or commercial activity. The legislation in the field does not apply to the processing of personal data for personal or domestic purposes (the phone numbers recorded in the phone book, the family photo album, the use of data when selling the property).



➤ **Companies can only use personal data for certain purposes**

A company must determine the purpose and legal basis for which it will collect personal data, as well as how it will use it. A company can only process this data for the purpose for which it was collected. The company must inform data subjects about the purposes of the collection and use of the data. The company can only use personal data for other purposes if the new purpose is compatible with the purpose for which the data was originally collected (a related agreement, legitimate interest or vital).

➤ **Consent is not the only legal basis for processing personal data**

Giving consent is not the only legal basis for processing data. The legislation also provides for other possibilities that may be more appropriate than consent, such as a contract to which the data subject is a party (for the provision of services), an activity in the public interest (an obligation provided by law), the protection of the vital interests of individuals or the legitimate interests of an entity or individual.

➤ **Copies of identity documents can only be made in cases provided for by law**

A company or other organization may request a copy of an identity document only if this is necessary to fulfill an obligation provided for by law. For example, a bank may make a copy of an identity document to open a bank account. However, in order to sign a service contract, it is usually sufficient to present the identity document in order to transcribe the necessary data from it. The identity document will be presented only to verify/confirm the identity of the person.

➤ **Video surveillance by a natural person can only be carried out on the territory of his property**

You can install video surveillance cameras on the territory of your property for personal or family activities/needs. In this case, as long as the space subject to video surveillance does not exceed the property of the manager/controller, the legislation on personal data protection does not apply, unless the rights of the data subject are violated. However, when the video surveillance camera covers a public space (street, sidewalk or neighbor's property) the legislation on the protection of personal data applies.

➤ **Companies that must appoint a data protection officer**

A company must appoint a data protection officer in cases provided for by personal data protection legislation. For example, if the company's core activities involve the processing of personal data that requires regular monitoring of a large number of individuals or if the company processes special categories of data on a large scale.

*The text of the recommendations can be viewed by accessing the link: <https://datepersonale.md/wp-content/uploads/2024/08/Lucruri-bune-de-%C8%99tiut-despre-datele-cu-caracter-personal.pdf>*

**Clarifications regarding the processing of personal data  
in the context of the Population and Housing Census in 2024**

In the light of the multitude information disseminated in the public space in relation to personal data processing in the context of conducting the Population and Housing Census of the Republic of Moldova in 2024, the National Centre for Personal Data Protection (NCPDP) comes with the following clarifications:

The purpose of Law No 133/2011 on personal data protection is to ensure the protection of the fundamental rights and freedoms of natural persons with regard to the processing of



personal data, in this regard establishing framework requirements to ensure compliance of the processing of personal data in various sectors, such as: medical, financial, police, education, telecommunications, etc.

Accordingly, the law in question contains general provisions and, through sectoral normative acts, specific rules may be provided regarding the purpose of processing personal data, the categories of data that are the subject of processing, the data subjects, the conditions under which processing takes place, the measures to ensure the confidentiality and security of personal data, the entities to which personal data may be disclosed, etc.

The reasoning presented above is also valid in relation to the normative acts regulating the organization and conduct of the Population and Housing Census of the Republic of Moldova in 2024.

It should be noted that, in the light of the assigned powers, NCPDP actively participated in the process of approving the normative acts regulating the processing of personal data related to official statistics, submitting relevant comments and proposals to improve their content, in order to comply with the requirements set out in the legislation in the field of personal data protection.

Considering the issues addressed in the public space regarding the processing of personal data in the process of conducting the Population and Housing Census in 2024, it was emphasized that the processing of personal data is considered lawful when it is carried out on the basis of the legal grounds provided for in art. 5 of the Law on personal data protection. In this regard, para. (5) of the aforementioned article provides for situations when the consent of the data subject is not required for the processing of personal data, for example, as appropriate, for: fulfilling an obligation incumbent on the controller under the law or for the performance of tasks of public interest or resulting from the exercise of public authority vested in the controller or the third party to whom the personal data are disclosed.

*Thus, in order to provide public interest information about the resident population and housing for the development, monitoring and evaluation of policies, for the justification of human development decisions, for scientific research and the development of the business environment, the legislator adopted Law No. 231/2022 on the population and housing census, subsequently approving the related secondary regulatory framework, acts that involve/generate the processing of personal data for the purpose of conducting the census.*

Accordingly, **the processing of personal data within this exercise is carried out based on the normative acts regulating the organization and conduct of the Population and Housing Census of the Republic of Moldova in 2024, however**, the Law on personal data protection does not come with specific regulations/conditions in this regard.

Thus, the provisions of art. 7 of the Law on population and housing census, which provide for mandatory participation in the census, are relevant. For example: in para. (1) of this article it is provided *that participation in the census of persons who meet the conditions of art. 3 para. (1) point 1) letters a)–c) is compulsory*. Further, para. (5) states *that if one or more members of the household are missing, the enumerator completes the census questionnaires based on the information provided by the other members who have full capacity to exercise, if they know the answers to the questions in the questionnaires. The necessary information about minor children is provided by the legal*

representatives. Article 23 of the same Act provides that violations of the provisions of the Act shall give rise to disciplinary, civil, criminal and/or misdemeanour liability, as appropriate.

In its capacity as data controller, the National Bureau of Statistics is empowered by law to collect, process and store personal data, ensuring the confidentiality and adequate security of individual data, including protection against unauthorized or illegal processing and against accidental loss, destruction or damage, through technical, organizational and administrative measures implemented, according to the Personal Data Protection Policy and other regulatory acts related to the notified field.

In accordance with Art. 14 para. (4) of the Law on population and housing census, the NBS is prohibited from transmitting to other natural or legal persons the personal data collected for the purpose of conducting the census.

In the context of the above subject, it should be noted that, to date, the NCPDP has not received any complaints from data subjects regarding the possible non-compliant processing of their personal data carried out in the framework of the Population and Housing Census of the Republic of Moldova 2024, including with regard to alleged transmissions of personal data to unauthorized persons.

Finally, the NCPDP recommends the population to get information from official sources, and when there are any uncertainties regarding the legal regime of personal data protection or official statistics, to contact the competent authorities.

The text of the press release can be viewed by accessing the following link: <https://datepersonale.md/7829/>

### **A new fraudulent scheme! Be careful when providing personal data!**



In the context of the media information regarding the collection of personal data by alleged persons accredited by the NCPDP, the authority came up with the following clarifications and recommendations for data subjects:

The NCPDP is an autonomous, independent and impartial public authority vis-à-vis of other public authorities, natural and legal persons, which exercises the powers conferred on it by the Law on personal data protection. As a body responsible

for the processing of personal data, the NCPDP has a number of powers, such as: monitoring compliance with the legislation on the protection of information and controlling its application, in particular the right to information, access to data, intervention in data and opposition; providing personal data subjects with information on their rights; ordering the suspension or cessations of personal data processing carried out in violation of legal provisions; **carrying out control of the legality of personal data processing**; notifying law enforcement agencies in the event of indications of the commission of crimes related to the violation of the rights of personal data subjects; ascertaining contraventions and concluding reports in accordance with the Contravention Code of the Republic of Moldova, etc.

**NCPDP employees may process personal data only for the purpose of exercising the above-mentioned duties/competences, requesting specific information about the subject of the complaint under examination or the initiated/carried out control. The official institutional contact details can be checked on the authority's website.**



**At the same time, NCPDP drew attention to the fact that it does not accredit/authorize persons to process personal data and/or to act on its behalf.** Moreover, people who request information through such dubious means are scammers and most likely their goal is to deprive you of financial means, using personal data.

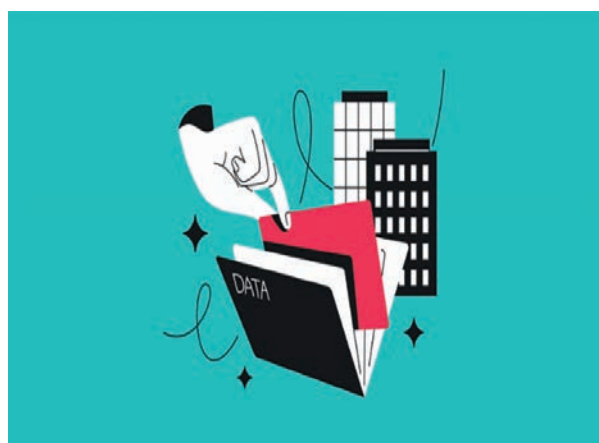
**In this context, CNPDCP recommended citizens:**

- **Do not access links in suspicious messages or advertisements;**
- **Avoid registering and completing dubious online surveys;**
- **Do not provide information containing personal data on unverified sites;**
- **Do not respond to suspicious messages and mark them as SPAM;**
- **Download applications only from official sources;**
- **Do not enter personal data upon request, even if fabulous winnings are offered;**
- **Do not provide unknown persons with remote access to devices through specialized applications (for example, AnyDesk and TeamViewer);**
- **Do not communicate bank card details to anyone;**
- **Do not transfer money to unknown persons and do not transmit funds to anyone through unknown third parties, regardless of the purpose.**

*The text of the recommendations can be viewed by accessing the following link:* <https://datepersonale.md/o-noua-schema-frauduloasa-atentie-la-furnizarea-datelor-cu-caracter-personal/>

**To the attention of the data subjects! NCPDP recommends maximum vigilance when transmitting/providing personal data**

Based on the multitude of cases in the media, as well as the specifics addressed in an increasing number of complaints and notifications under examination, NCPDP urged data subjects to demonstrate maximum caution when disclosing, transmitting, and disseminating personal data concerning them. Identity documents (such as identity cards, passports), civil status certificates, pensioner cards, bank cards, etc. record a multitude of personal data, which require effective protection from their holder/owner.



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

**If you are asked to provide your identity documents and/or to provide copies of these documents, as well as to provide personal data such as: your name, surname, IDNP, home address, bank card details, income, pension amount, etc. under different pretexts by third parties, you have to make sure about the legality 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, the personal data that are the subject of 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.

In the conditions of voluntary provision/transmission of personal data, recorded on various documents or by entering them in some lists/documents, the basis for the collection of these personal data is the existence of the consent of the personal data subject (art. 5 para. (1) of Law 133/2011). At the same time, it can later be proven that these data would have been used for other purposes/to the detriment of the data subject concerned, in which order each citizen is responsible for ensuring the protection of his/her personal data, or, the security and confidentiality of these data must be a priority.

*The text of the recommendations can be viewed by accessing the following link: <https://datepersonale.md/in-atentia-subiectilor-de-date-cnpdcp-recomanda-vigilenta-maxima-la-transmiterea-oferirea-datelor-cu-caracter-personal/Atenție! Fraude cu utilizarea datelor cu caracter personal. CNPDCP recomandă repetat vigilență maximă la transmiterea datelor cu caracter personal>*

**[Attention! Fraud with the use of personal data. NCPDP repeatedly recommends maximum vigilance when transmitting personal data](#)**



In the context of the lamented aspects regarding the collection of personal data recorded in identity cards, by the exponents of a political party, for the purpose of registering on the «PSB» platform in order to benefit from financial resources from banking institutions in the Russian Federation, **this fact essentially consisting in identifying the existence of loans in the names of data subjects that are to be repaid by the latter, NCPDP urged data subjects to demonstrate maximum caution when disclosing/transmitting personal data concerning them, as identity documents (such as identity cards, passports) record a multitude of personal data, which require effective protection from their holder/owner.**

**Thus, if the presentation of identity documents and/or the provision of copies of these documents is requested, under different pretexts, individuals should ensure that the collection of personal data and the subsequent use of these data are legal.** However, the provision/transmission of personal data from these documents by the data subject, for purposes other than those expressly provided for by law, **may generate their illegal use, for purposes contrary to those originally provided, to the detriment of the data subject.** Likewise, the personal data subject could lose control over his or her personal data.

**In this case, the cases filed with the NCPDP clearly demonstrate that the transmission by the data subjects of copies of their identity cards for an alleged benefit of some sums of money led to the opening, in the latter's name, of loans at banking institutions on the territory of**



**the Russian Federation, which currently claim the repayment of accumulated credit debts** (for example, by «Promsvyazbank» (PSB Bank) from the Russian Federation).

The text of the recommendations can be viewed by accessing the following link: <https://datepersonale.md/atentie-fraude-cu-utilizarea-datelor-cu-caracter-personal-cnpdcp-recomanda-repetat-vigilenta-maxima-la-transmiterea-datelor-cu-caracter-personal/>

### **Attention personal data controllers!**



In accordance with the provisions of point 2.1 of Government Decision no. 678/2024 on the amendment and repeal of certain Government decisions (facilitation of business environment activity VI), which entered into force on November 15, 2024, **Government Decision no. 1123/2010 on the approval of the Requirements for ensuring the security of personal data when processing them within personal data information systems (Requirements) was repealed, the obligation of personal data controllers to submit annual, by January 31, generalized reports to the NCPDP on**

**security incidents of managed personal data information systems being excluded.**

At the same time, the repeal of the aforementioned Requirements did not exclude the obligation of controllers, as well as of processors (if applicable), provided for in art. 29 and art. 30 of Law no. 133/2011, to implement the organizational and technical measures necessary to protect personal data against destruction, modification, blocking, copying, dissemination, as well as against other unlawful actions, measures intended to ensure an adequate level of security in terms of the risks presented by the processing and the nature of the processed data, including ensuring their confidentiality.

In this context, on the official website of the authority, in the chapter NCPDP Recommendations (<https://datepersonale.md/data-controllers/ncpdp-guidelines/>), you can consult the Guidelines on security measures for the protection and processing of personal data within information systems, which are published.

The text of the press release can be viewed by accessing the following link: <https://datepersonale.md/in-atentie-operatorilor-de-date-cu-caracter-personal-4/>



## ACTIVITY OF PREVENTION AND SURVEILLANCE OF PERSONAL DATA PROCESSING



In order to achieve its mission, the NCPDP is tasked with monitoring and ensuring the application of the law; raising public awareness in order to understand the risks associated with processing, the rules, guarantees and rights regarding processing, and raising awareness among controllers and processors regarding their obligations under the law.

Thus, in order to carry out the advisory tasks, in addition to the multiple answers provided, in an advisory capacity, during the reporting year, 1893 telephone consultations were provided, either via e-mail or at the authority's headquarters.

The most frequently addressed topics during the consultations were video surveillance carried out by individuals when the personal data processing is carried out exclusively for personal or family needs; the conditions/methods of informing data subjects when video surveillance is carried out; the actions to be taken to adjust the angles of capture of video cameras when they monitor spaces outside private property, such as public roads or neighbors' households without their consent; the publication of personal data on websites and online social media; the mechanisms for realizing the rights of data subjects, as well as aspects related to the processing of personal data carried out by public sector authorities/institutions.

Providing consultations and educating citizens, including representatives of legal entities (as part of consultations and inspections) on matters of personal data processing, as well as recommending measures/actions to ensure compliance with personal data processing, contributes substantially to preventing possible violations.



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

Accessing the main state registers/information systems represents in itself a large-scale personal data processing process, being constantly under the watchful eye of the NCPDP over the past few years.

As in previous years, the NCPDP dynamically analyzes the statistics of accesses made in 2024 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)		
	2022	2023	2024 SIA „Acces-Web”/COI	2022	2023	2024
Ministry of Internal Affairs	22.446.877	26.781.106	326.527/ 24.699.955	15.429	3.125.054	2.863.276
Intelligence and Security Service	70.184	73.624	24.848/ 27.725	43.080	65.042	76.261
National Anticorruption Center	75.486	53.727	0/ 25.544	10.468	9.691	686
General Prosecutor's Office	30.797	15.066	0 /1.078	6	0	0
Customs Service	17.715	14.102	11397/ 0	6	151.067	228.426
Ministry of Defence	727	498	0	115.301	302.896	288.279
National Integrity Authority	19.127	15.661	0 /8.875	11.759	19.825	1.356
State Tax Service	4.071.998	9.685.627	10.147/ 13.937.925	9.566.872	15.996.061	7.513.765

As can be seen, the share of accesses made by the targeted entities through the access technologies offered by the Public Services Agency (COI - 38,701,102 accesses) is 3.5 times higher than those offered by the Electronic Governance Agency (10,972,049).

In the context of the information presented above, it should be noted that in accordance with Government Decision No. 959/2023 on the organization and functioning of the Agency for Geodesy, Cartography and Cadastre (restructuring the field of geodesy, cartography and cadastre and amending some normative acts), from December 20, 2023, **the Public Institution Real Estate Cadastre (IPCBI) took over from the Public Services Agency the following areas of activity: creating and maintaining the real estate cadastre, other information systems and domain registers,**



performing cadastral and real estate valuation works, **administering the central data bank of the real estate cadastre**, performing state registrations of real estate and rights over them, providing public services in the field of cadastre and will be the successor of rights and obligations related to the areas of activity taken over; in which order we present below the number of accesses made to the Real Estate Register in 2024, information provided by IPCBI.

Institution concerned	Number of accesses made to RBI via E-Cadastre in 2024
Ministry of Internal Affairs	58.025
Intelligence and Security Service	11.358
National Anticorruption Center	25.741
General Prosecutor's Office	3628
Serviciul Vamal	3308
Ministry of Defence	295
National Integrity Authority	11.626
State Tax Service	36.905

Analyzing the list of public entities connected to state registers/information systems through COI, presented by the Public Services Agency, it was noted that currently there are **16** beneficiaries with the right to access personal data through the respective technology.

In this context, we note that in 2024, NCPDP addressed to the Electronic Governance Agency, the Public Services Agency, and informed the Government of the Republic of Moldova and the Committee on National Security, Defense and Public Order of the Parliament of the Republic of Moldova, regarding the fact that the continued provision of interconnection through the COI of the targeted entities contravenes the provisions of Law No. 142/2018 on data exchange and interoperability.

Unfortunately, we can note that **16** out of **18** public entities that remained connected at the beginning of 2024, still have unlimited access to the main state information resources managed by the Public Services Agency through the COI.

Moreover, from the information presented by the Public Services Agency and the Electronic Governance Agency, reflected in the table above, the enormous volume of accesses made through COI was noted, *for example: 24,699,955 accesses were made by the Ministry of Internal Affairs through that technology and only 2,863,276 through the interoperability platform, which is 8.6 times less.*

We remind you that according to art. 6 paragraph (3) of Law no. 142/2018 on data exchange and interoperability, public participants are obliged to carry out data exchange through the interoperability platform and to ensure the technical conditions necessary for data exchange, except for the cases provided for in art. 2 paragraph (4), namely, in the case of the exchange of **data classified as state secret, bank secret or other data with a special legal regime, where the special legislation in force will apply.**

In the context, over the past few years, the NCPDP has repeatedly communicated that the issue of the use of COI remains an unresolved one to date, given that state authorities access personal data contrary to legal provisions, a technology that, in fact, does not meet the requirements for



ensuring the security of personal data when processing them within automated information systems and does not ensure the nominal identification of users who have performed data access operations, having the obligation to justify the purpose and legal basis of these operations. However, in the context of the intensification of the digitalization process of public services, it is even more stringent to ensure and adequately implement the rules/norms related to the field of personal data protection.

We remind you that personal data controllers are obliged to comply with the principles set out in the provisions of Article 4 of the Law on personal data protection, according to which personal data that are the subject of processing must be: processed fairly and in accordance with the provisions of the law; collected for specified, explicit and legitimate purposes, and not subsequently processed in a manner incompatible with these purposes; adequate, relevant and not excessive in relation to the purpose for which they are collected and/or subsequently processed; accurate and, if necessary, updated, stored in a form which allows the identification of the subjects of the personal data for a period not exceeding the duration necessary to achieve the purposes for which they are collected and subsequently processed.

In this context, we emphasize that both the controller and processor (if applicable), according to the provisions of art. 29 and art. 30 of the Law on personal data protection, have the obligation to ensure the confidentiality and security of the processed personal data.

In another context, it is necessary to highlight the provisions of art. 13 para. (3) and (5) of Law no. 142/2018 on data exchange and interoperability, according to which existing bilateral data exchange contracts or agreements concluded between public participants will be terminated by law, once the corresponding data exchange is carried out through the interoperability platform, except in the case where special legal provisions in the field of supervision of entities in the financial sector, national defense, state security, maintenance of public order, countering crime, preventing and combating corruption, acts related to corruption and acts of corrupt behavior, as well as the protection of the rights and freedoms of individuals are applicable. Within 36 months from the date of publication of the law, public participants who, on the date of adoption of the law, use, each for their legal purpose, information systems that do not meet the requirements of the law will comply with the technical requirements applicable within the interoperability platform

Thus, we can note the double overrun (by more than 3 years) of the execution of these provisions by the targeted entities.

At the same time, it should be noted that situations are still being identified regarding the admission by various entities benefiting from information services for access to state information resources, such as the Real Estate Registry, based on contracts concluded with PSA, IPCBI or EGA, of violations such as:

- using the access credentials (username and password) of a single authorized user access account by multiple employees of the beneficiary entity;
- providing the username and password to third parties;
- failing to update the user list after changing the job or position in the entity;
- failing to include the user's personal data (IDNP, contact number or address) in the user lists;



- failing to inform the Public Services Agency/Public Institution Real Estate Cadastre about the change of administrator by the beneficiary;
- failing to update user passwords in a timely manner, etc.

Based on the above, the NCPDP has repeatedly requested that the relevant entities take appropriate actions to ensure the compliance of all processing/access operations of personal data stored in state information resources, by allowing access to and use of this information exclusively through methods corresponding to security and confidentiality requirements, with information on the actions taken in this regard.

For information purposes, below is presented information on the number of petitioners who have exercised the right of access to data, requesting information on accessing personal data concerning them from the registers/information systems managed by the Electronic Government Agency, the Public Services Agency and the Public Institution Real Estate Cadastre.

Year	Number of requests from data subjects submitted in the context of exercising the right of access to personal data stored in state registers/information systems		
	Public Service Agency	Electronic Government Agency	Public Institution Real Estate Cadastre
2023	649	99	-
2024	338	77	134

In this context, it should be noted that citizens have access to the Citizen's Government Portal (MCabinet) provided by the Electronic Governance Agency, through which they can view the history of access to their personal data by public authorities and institutions and other natural and legal persons under private law. The portal presents information on the legal entities that have accessed the citizen's personal data, as well as the date of access and the legal basis. The information is taken from the government logging service MLog, in which all government entities are required to enter information about data access, including in the process of data exchange through the MConnect platform.



## CHAPTER VII

ENDORSEMENT OF DRAFT  
NORMATIV ACTS

## VII

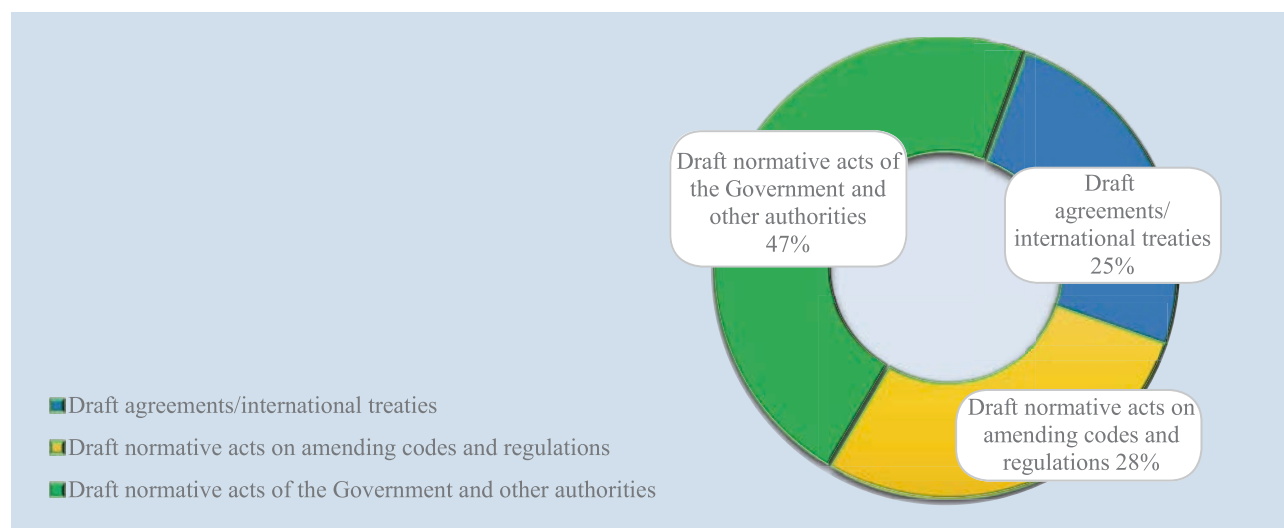


*What is the NCPDP opinion?* Draft normative acts that fall within the NCPDP's areas of competence are submitted to it for approval. The NCPDP may be contacted by various public actors regarding draft normative acts, such as laws or Government decisions, before their adoption. The opinions given help to inform public authorities on issues regarding the protection of personal data and aim to ensure the fundamental rights and freedoms of the individual with regard to the processing of personal data, in particular the right to the inviolability of intimate, family and private life, but do not constitute a "validation", an "authorization" or even a "refusal".

Submitting proposals regarding the improvement of the legislation in force in the field of personal data protection and processing is one of the NCPDP's attributions provided for by the Law on personal data protection.

During the year 2024, **170** 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:

- **42** draft agreements/international treaties;
- **48** draft normative acts on amending codes and regulations;
- **80** draft normative acts of the Government and other authorities.

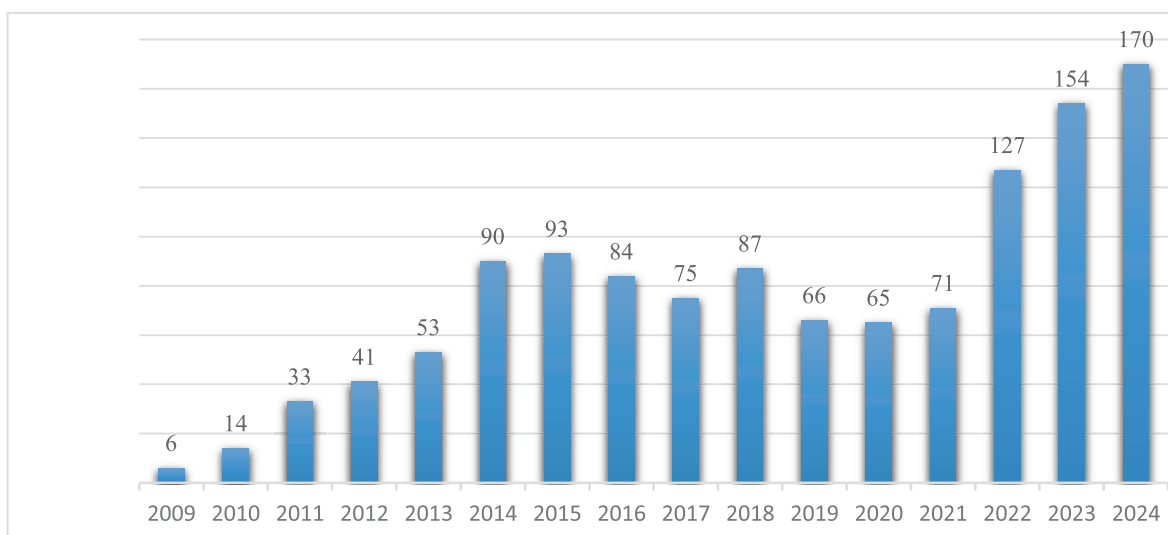






In the most of case of the drafts proposed for endorsement, the NCPDP considered that it was necessary to supplement, amend or revise the respective texts, offering a series of recommendations and proposals in order to adjust the projects with specific provisions related to personal data processing operations, such as: the conditions governing the legality of personal data processing by the controller; the types of data that are the subject of processing; the data subjects; the entities to which data may be disclosed and the purpose for which the respective personal data may be disclosed; purpose-related limitations; storage periods; processing operations and procedures, measures to ensure data security and confidentiality, etc.

***Dynamics of draft laws submitted for approval 2009-2024***



As an example, below are reflected the most relevant draft normative acts approved during 2024, as follows:

- *the draft law amending Law No. 1104-XV of June 6, 2002 on the National Anticorruption Center;*
- *the draft law to amend certain normative acts (records of offenses, criminal cases and persons who have committed offenses and records of contraventions, contravention cases and persons who have committed contraventions);*
- *the draft Government decision on the approval of the Concept and Regulation of the “Medical Certification of Birth and Death” Information System;*
- *the draft Government decision on the approval of the National Economic Development Strategy 2030;*
- *the draft Government decision on the approval of the Concept of the Information System “State Register of Controls”;*
- *the draft Government decision on the approval of the Concept and Regulation of the Information System for monitoring and evaluating HIV infection;*
- *the draft Government decision to amend some Government decisions (organization and operation of the Automated Road Traffic Surveillance System “Traffic Control”);*
- *the draft Government decision on the approval of the draft law on contracts for the provision of digital content and digital services;*





- the draft Government decision on the approval of the Concept of the “Trust Register” Information System and the Regulations of the Trust Register;
- the draft Government decision on the identification of service providers (in the context of the provisions of Law no. 48/2023 on cybersecurity);
- the draft Government decision for the implementation of the provisions of Law no. 28/2024 on the state border of the Republic of Moldova;
- the draft Convention between the Government of the Republic of Moldova and the Government of Belgium on police cooperation.

***During 2024, the NCPDP’s activity in the legislative creation segment was focused on finalizing and promoting the draft of the new law on personal data protection.***

***Thus, on July 25, 2024, the Parliament of the Republic of Moldova adopted Law no. 195/2024 on personal data protection, published in the Official Gazette of the Republic of Moldova of August 23, 2024, no. 367-369, art. 574.***

The purpose of the law is to ensure the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data, in particular the right to the inviolability of intimate, family and private life.

We remind you that, in order to achieve the national objective aimed at ensuring an adequate level of personal data protection, in accordance with the norms of the European Union and the Council of Europe, as well as to guarantee the protection of the fundamental rights and freedoms of citizens, in particular the right to privacy with regard to the processing of personal data, a Working Group was created on the platform of the Ministry of Justice, which included representatives from the NCPDP, the Ministry of Justice, the Parliament of the Republic of Moldova, the State Chancellery, the Economic Council under the Prime Minister of the Republic of Moldova, the Ministry of Economy, the Ministry of Internal Affairs, the Prosecutor General’s Office, the National Anticorruption Center, the American Chamber of Commerce in Moldova, the European Business Association, the Association of Foreign Investors, and the National Association of ICT Companies.

It is worth mentioning that the draft law was subject to expert review by the European Commission, Directorate-General for Justice and Consumers. Thus, during the bilateral screening exercise related to Chapter 23 “Justice and Fundamental Rights” which took place between 15-17 October 2024 in Brussels, the experts from the European Commission highly appreciated the efforts made and the result obtained in the development and adoption of the new legal framework in the field of personal data protection, it being clearly mentioned that the state is to ensure adequate capacities and mechanisms for the National authority for personal data protection to be able to implement the new rules that arise with the entry into force of the adopted legal framework, which is a very complex one

Law No. 195/2024 on personal data protection faithfully transposes the provisions of 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.

The regulations stipulated in the new law will grant individuals increased control over their personal data, detailing a series of aspects, such as:



- *The guiding principles regarding the processing of personal data;*
- *The rights of individuals in relation to the processing of personal data concerning them and the manner of exercising them;*
- *The responsibilities of controllers and processors in the process of processing personal data;*
- *The manner of carrying out data transfers to other states or to international organizations;*
- *Regulation of the organization and functioning of the supervisory authority - NCPDP;*
- *Procedure for submitting and examining complaints from data subjects in case of alleged non-compliant processing, as well as the manner of conducting investigations by NCPDP;*
- *Financial sanctions applied by NCPDP to controllers for violating legal provisions, etc.*

The new regulatory act, Law No. 195/2024 on personal data protection, enters into force 2 years after the date of publication in the Official Gazette of the Republic of Moldova. Until then, the provisions of Law No. 133/2011 on personal data protection apply.

In addition to the active participation and involvement in aligning the national framework with the European Union acquis in the field of personal data protection, it will be emphasized that the representatives of the NCPDP directly participate in the implementation of priority tasks in the context of the implementation of the requirements for accession to the European Union, contributing to the bilateral screening procedure and the implementation of actions from the National Action Plan for the Accession of the Republic of Moldova to the European Union for 2024-2027, including in other areas involving the processing of personal data and their cross-border transfer, within Working Group No. 2 "Free Movement of Workers", Working Group No. 10 "Information Society and Media", Working Group No. 14 "Transport", Working Group No. 19 "Social and Labor Policy", Working Group No. 23 "Judicial System and Fundamental Rights", Working Group No. 24 "Justice, freedom, security", Working Group no. 28 "Consumer protection and public health".

**On July 10, 2024, by Order No. 25 of the Director of the NCPDP, the Regulation on the control of the legality of personal data processing was approved, published in the Official Gazette No. 318-320/594 of 25.07.2024.**

The development of the document was conditioned by the adoption of Law no. 95/2024 amending certain normative acts (in the field of state control over entrepreneurial activity) by which amendments and additions were made to art. 20, 21, 26, 27 of Law no. 133/2011 on personal data protection, adjusting the legal framework regarding the control of the legality of personal data processing. Thus, in accordance with the provisions of article 26 paragraph (2) of the aforementioned law, the control is carried out in accordance with a regulation developed and approved by the NCPDP. When carrying out the control of the legality of the processing of personal data by persons practicing entrepreneurial activity, the NCPDP applies the provisions of Law no. 133/2011 and Law no. 131/2012 on state control to the extent that it does not contradict Law no. 133/2011.

In accordance with art. 19 of Law no. 133/2011, the NCPDP carries out the control over the compliance of the processing of personal data in accordance with the requirements of the Law on personal data protection, under conditions of impartiality and independence. The control of the legality of data processing is regulated in Chapter V of the law, in particular, art. 26 and 27, which establish the procedure for receiving and resolving complaints by the NCPDP.

In light of the new regulations in force, the NCPDP has developed and approved the Regulation on the control of the legality of personal data processing.



The normative act fully regulates the procedure and conditions for conducting the control, the rights and obligations of the controller and the person subject to the control, including in the case of an on-site investigation. After obtaining all the information and analyzing it, the NCPDP issues a reasoned decision by which it finds the absence of a violation or a violation of the legislation in the field of personal data protection, ordering, as appropriate, the suspension, cessation of personal data processing operations, the rectification, blocking or destruction of false or illegally obtained data. In the event of the absence or insufficiency of evidence that would demonstrate the violation, the NCPDP finds, by reasoned decision, the absence of a violation. The decision on the finding of a violation of the legislation in the field of personal data protection and the accumulated evidence serve as the basis for drawing up a report on the contravention, under the terms of the Contravention Code of the Republic of Moldova. If applicable, the instructions in the decision are included in the plan for remediation of the contravention. Therefore, when carrying out the control of the legality of personal data processing by any natural or legal person of public or private law, the NCPDP will apply the provisions of Law no. 133/2011 and the Regulation on the control of the legality of personal data processing.

The provisions of the Regulation on the control of the legality of personal data processing aim to ensure a coherent control of the processing of personal data based on complaints received from data subjects.

***The amendment of the Standard Contract for the cross-border transfer of personal data to states that do not ensure an adequate level of personal data protection, approved by Order no. 33/2022 of the Director of NCPDP was necessary following the amendments provided for by Law no. 60/2023 on the amendment of some normative acts (stimulation of e-commerce), which supplemented Article 30 of Law no. 133/2011 on personal data protection. The new amendments were approved by Order of the Director of NCPDP No. 33/2024.***

Thus, the amendments to this article introduced regulations on the conditions for the recruitment/sub-contracting by processors another processors to carry out specific personal data processing operations on behalf of the controller.

It should be noted that the transfer of personal data to countries that do not ensure an adequate level of protection may take place only under the conditions stipulated in Article 32 para. (5) of Law No 133/2011 on personal data protection.

In this context, pursuant to Art. (5) lit. i) of Law 133/2011, by Order no. 33 of April 22, 2022, the Standard Contract for the cross-border transfer of personal data to states that do not ensure an adequate level of personal data protection was approved.

The role of the Standard Contract is to lay down appropriate technical and organizational measures, including enforceable rights of personal data subjects and effective remedies with regard to cross-border data flows from controllers to controllers, from controllers to processors and/or from processors to controllers.

Given that national legislation in the field of personal data protection did not contain rules allowing controllers or processors to sub-contract third parties to be involved in personal data processing operations, the Standard Contract, approved by Order No 33/2022, did not provide for rules on the transfer of personal data from one processor to another processor.

In the light of the amendments to Law No 133/2011, the Standard Clauses have been aligned with the new legal provisions.



## PROPOSALS TO AMEND CERTAIN LEGAL ACTS

**With regard to the initiation of the ex-post impact assessment of the Law on data exchange and interoperability** following the adoption of Decision CSN-o3 no.139 of April 24, 2024, at the request of the National Security, Defense and Public Order Commission of RM Parliament, which asked the authorities concerned to inform about the implementation of the above-mentioned act, the NCPDP, with reference to the overly wide access to state information resources to interested persons, such as: individuals, non-profit associations, various legal entities of private law, etc., communicated the following:

[...] According to Art. 2 para. (1) and (2) of Law 142/2018 on data exchange and interoperability:

- (1) **The Law applies to public participants in data exchange, namely public authorities and institutions, including autonomous administrative authorities, central administrative authorities subordinated to the Government and organizational structures within their sphere of competence (subordinated administrative authorities, including deconcentrated and subordinated public services, as well as public institutions in which the Ministry, the State Chancellery or other central administrative authority has the status of founder), as well as legal entities under private law which, on behalf of public authorities and institutions, manage or own state information systems.**
- (2) **The Law applies also to legal persons under private law, including notaries, bailiffs, registrars, attorneys, authorized administrators, court experts, interpreters and translators, mediators and other persons authorized according to the legislation in force, insofar as they own information systems, hold data of interest to public authorities and institutions or other natural persons and legal persons under private law and are willing and intend to participate in the exchange of data, as well as to natural persons in the conditions in which they are data consumers.**

In this context, the provisions of Art. 11 para. (2) lett. g) and i) of the **Law on Register of Immovable Property No 1543/1998**, according to which the implementing institution: **g) owns and manages the central cadastral data bank; i) provides systematized cadastral information to public administration authorities, other legal entities and individuals.**

In accordance with Art. (11) of the same normative act, **the data on the state identification number (IDNP), date of birth and domicile of the natural person shall be released to persons having rights registered in Chapter A, B or C of the immovable property register, to their representatives, as well as to notaries, lawyers, financial institutions, enterprises providing real estate services or performing cadastral works, to persons and authorities indicated in Art. (23) lett. (3) of this Law, other persons who justify the purpose of processing personal data in accordance with the Law no. 133 of July 8, 2011 on personal data protection.**

Furthermore, para. (21) of the aforementioned article provides that information on the registered rights to immovable property **shall be provided to natural and legal persons upon request, by granting access to the central real property cadastre data bank under the conditions of the legislation in force on data exchange and interoperability.**

According to para. (3), **information on registered rights in immovable property shall be provided against payment, except in the cases indicated in Art. (3).**

Thus, according to Art. (3) of the same law, **the Methodology for calculating tariffs and tariffs for services rendered by the implementing institution and its territorial structures, services related to the registration of immovable property and rights over them, as well as other services falling within the**





*exclusive competence of the implementing institution and its territorial structures, shall be approved by the Government.*

Based on the aforementioned legal provisions, it follows that natural and legal persons may be provided with information about the registered rights to the immovable property, with the granting of access to the central data bank of the cadastre of immovable property under the conditions of Law No. 142/2018 on data exchange and interoperability.

In this context, it will be noted that **until** the entry into force of the Law on Data Exchange and Interoperability and the sectoral amendments in this field, the old wording of Art. 6 para. (21) of Law No 1543/1998 on the register of immovable property provided that information on registered rights in immovable property ***shall be provided to natural and legal persons on request, by granting access to the central data bank of the register of immovable property through local and global computer and telecommunications networks.*** In the light of the legal amendments, it follows that the contracts concluded by the PSA with the beneficiaries - natural and legal persons - before the entry into force of those amendments were to be reviewed and, possibly, revoked.

In the same order of ideas, by way of example, the provisions of the Concept of the automated information system „*State Population Register*”, approved by the Decision of the Government of the Republic of Moldova No 333/2002, should be noted.

Thus, according to point 8 of Chapter III - Functional space of the SPR, ***the information in the SPR database is provided***, in accordance with the national legislation in force, to the leadership of the Republic of Moldova, central and local public administration bodies, ***natural and legal persons*** and within the framework of data exchange. The public administration bodies, natural and legal persons, which use information from the SPR, shall be liable for its disclosure under the conditions of the law.

At the same time, according to point 15 of Chapter IV - Provision of information from SPR of the Regulation on the State Population Register, approved by the same Government Decision, the *information from SPR is provided to* ***public authorities, legal entities and individuals on the basis of contract or, respectively, request.***

*The contract or request shall contain the purpose for which the information is requested and how it is to be used, the volume and structure of the data, the form and language of the document, the type of media on which the data is provided, the periodicity of release, the measures for personal data protection, the control procedures, and the way the information is offered (with and/or without payment). If the information is provided against payment, the cost of the information shall also include the amount and the estimated material costs of its use, processing and provision.*

*The information is provided free of charge for public institutions financed from the state budget, **and for private individuals and legal entities against payment, except in the cases expressly provided by law.***

Thus, in the context of the topic addressed on granting access to a wide range of categories of persons, in terms of preventing the non-compliant processing of personal data stored in various state information systems, such as: the *Real Estate Register, the State Register of Population*, etc., even if in the recent period some changes have been made in the relevant legislation that change/improve the situation in this respect, **it is still necessary to intervene on the parliamentary/governmental platform in order to analyze the review of the legal framework**





**regulating access to data stored in state information resources**, especially considering that the volume and specificity of information stored in state information resources are of strategic national importance, which require an adequate level of security.

**In the context of the parliamentary hearings on „Electoral frauds reported in the presidential elections and the 2024 republican referendum”,** the NCPDP, based on its functional competences, in order to prevent the use of data reflecting the identity of the person for purposes that could harm the interests or rights of citizens, by the request addressed to the **Legal Committee for appointments and immunities** of the RM Parliament, proposed the amendment of the following normative acts:

- - **Art. 9 „Liability for violation of this law” of Law no. 273/1994 on identity documents in the national passport system, in para. (1)** shall be completed with two new letters, with the following text:
  - n) *the collection of copies of the identity documents, except in the situations provided for by the legislation in force or in singular cases in specific situations, which do not involve frequent and massive collection of copies of the identity documents;*
  - o) *publication in the Internet web space of copies of identity documents or data reflecting the state identification number of the natural person, the serial number and the number of the document.*
- ➤ **Art. 18 „Obligations of the organizer” of the Law no. 26/2008 on Meetings** will be completed with a new paragraph:

(3) If citizens' signatures are collected at meetings in support of initiatives or for consultation on local, regional or national issues of particular interest, the completed lists shall contain the following data on the persons expressing their position on the subject matter: name, surname, year of birth, locality, telephone number and signature.

The proposal has been submitted in the context that during the last few years, especially in the period 2023 - 2024, the collection of personal data and copies of identity documents directly from the data subjects for various alleged purposes, such as: offering aid/compensation, supporting the realization of social projects, at local or national level, or for various citizen initiatives, has been increasing, in fact, creating circumstances for the use of these data in various/multiple fraudulent schemes.

Providing/transmitting copies of identity documents, as well as writing data from identity documents in various lists/documents by citizens, may generate their illegal use for purposes contrary to those initially declared by the persons collecting such data, to the detriment of citizens. In cases where citizens are asked to provide copies of their identity documents and to submit data relating to their name, surname, IDNP, home address, bank card details, income, pension amount, etc. under various pretexts by certain persons, citizens do not usually trust the legality of the collection of the requested data, the honesty/credibility of the persons collecting them and the risks of subsequent use of such data.



## CHAPTER VIII

## INTERNATIONAL COOPERATION

## VIII



In 2024, NCPDP continued to strengthen and expand its international relations, playing an active role in promoting European principles and standards in the field of personal data protection. By participating in various international initiatives, seminars and working groups, the authority contributed to the development of a coherent framework for the protection of privacy, in the context of technological developments and emerging regulations.

Collaborations with data protection authorities from other European Union (EU) Member States and other international organisations have been essential in ensuring a safe and fair environment for the management of personal data, aligned with international best practices. At the same time, bilateral and multilateral collaborations have been essential not only for the exchange of good practices, but also for the implementation of common solutions to emerging data protection challenges.

This chapter reflects the efforts and achievements of the NCPDP in strengthening its position internationally and in promoting a continuous dialogue on the field of personal data protection.

*Plenary meetings of the European Data Protection Board*



During the year 2024, NCPDP's representatives participated in 6 online plenary meetings and 5 meetings with physical presence in Brussels. During the plenary meetings of the European



Data Protection Board, opinions and guidelines of major importance were adopted, including:

- Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR;
- Guidelines 01/2023 on Article 37 Law Enforcement Directive;
- Guidelines 04/2022 on the calculation of administrative fines under the GDPR;
- Opinion 11/2024 on the use of facial recognition to streamline airport passengers' flow (compatibility with Articles 5(1)(e) and (f), 25 and 32 GDPR).

The participation of the NCPDP in the plenary sessions of the European Data Protection Board had a significant impact both on the strengthening of the role of the authority and on the harmonization and consolidation of the national regulatory framework related to the field of data protection. This close collaboration allowed the authority to improve its internal practice, adopt good European practices and ensure a uniform application of national legislation, having a positive impact on the protection of individuals' rights in the Republic of Moldova.

### *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 2024, the NCPDP's management attended two plenary meetings of the

Committee of Convention 108 which were held in person.

Various important topics were addressed during the meetings, including Convention 108+ and the status of current ratifications and accessions, the personal data protection in combating money laundering and terrorist financing, contractual clauses in the context of cross-border data flows, the interpretation

of Article 11 of Convention 108+, privacy-enhancing technologies, cooperation with other Council of Europe bodies and entities, as well as major developments and activities in the field of data protection.



The NCPDP delegation informed about the developments and activities in the field of data protection at the national level and the status of ratification of Protocol CETS 223 to Convention 108, noting that on 25 July 2024, the Parliament of the Republic of Moldova adopted the new Law no. 195/2024 on personal data protection which was published in the Official Gazette of the Republic of Moldova no. 367-369, art. 574, on August 23, 2024, which will enter into force 2 years after the date of publication, in which order the Ministry of Justice considers it appropriate to ratify the Protocol once the new law enters into force. The draft law on the ratification of the Protocol amending the Convention for the protection of individuals with regard to automatic processing of personal data and the related documents were submitted to the Ministry of Justice for intergovernmental consultation procedures.

In this context, it will be noted 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. A minimum of 38 ratifications are required for Convention 108+ to enter into force. Convention 108+ remains the only legally binding international instrument protecting personal data and the right to privacy, aiming to ensure adequate protection for all individuals in an ever-expanding digital age.

#### *Cooperation with European Union agencies*



In accordance with the provisions of Article 19 (2) of the Cooperation Agreement between the Republic of Moldova and Eurojust, according to which the Data Protection Officer of Eurojust and the Data Protection Authority of the Republic of Moldova shall report to each other, at least once a year, on the implementation of the provisions of the Agreement, 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. Cooperarea cu Autoritățile europene de protecție a datelor cu caracter personal

#### *Cooperation with European Data Protection Authorities*

❖ In the period 14-16 May 2024, representatives of the NCPDP participated in the 32nd **Spring Conference of the European Data Protection Authorities** in Riga, Latvia.

The Spring Conference was hosted by the Latvian State Data Protection Inspectorate and brought together Data Protection Authorities from across Europe to establish a common framework





for cooperation to protect individuals' data at European level. The conference also served as a unique European platform for the exchange of experience and best practices in the field of data protection.

During the working sessions, topical issues were presented, such as:

- The role of Data Protection Authorities in the era of evolving digital regulation;
  - Managing data protection and privacy in the era of emerging technologies and innovations;
  - Health data protection in the age of digitization;
  - Shaping data protection through the cooperative experience of Data Protection Authorities;
- Managing the Anti-Money Laundering (AML) and General Data Protection Regulation (GDPR) regulations: challenges, cooperation and compliance;
  - Strengthening compliance with AML and GDPR regulations through collaborative strategies.

For the second time, an Open Day was organized as part of a Spring Conference of the European Data Protection Authorities. This gave the opportunity to several institutions, NGOs or other organizations that expressed an interest in the topics addressed during the event to participate, including online.

The event was attended by 145 representatives from 43 countries, such as: Austria, Belgium, Bulgaria, Croatia, Denmark, France, Georgia, Germany, Greece, Hungary, Italy, Malta, Moldova, Portugal, Romania, Spain, Switzerland, Ukraine, etc. Representatives of four organizations attended also the event: FRA, EDPS, EDPB and the European Commission.

❖ On 30 – 31 October 2024, the representatives of the NCPDP participated in a study visit to the Latvian Data State Inspectorate (Inspectorate), an event organized within the project entitled ***“Strengthening personal data protection in the Republic of Moldova Phase I”***.

The purpose of the study visit was to learn the best legal and operational practices from the representatives of the NCPDP on the certification of Data Protection Officers (DPOs), Data Protection Impact Assessment (DPIA), as well as to strengthen data protection mechanisms by aligning them with European standards and practices.

During the event, the Director of the Inspectorate, Jekaterina Macuka, presented the main tasks/activities of the institution, its role in promoting the field of personal data protection in Latvia, highlighting the challenges and







opportunities in the field of personal data protection of both countries, as well as the continued cooperation and exchange of best practices.

During the two days, topics of importance were addressed, such as:

- **Data Protection Officer certification:** the purpose of DPO certification, who issues DPO certifications, who can apply to receive a DPO certification, what is the feedback from different stakeholders on these DPO certifications, etc.
- **Presentation of the DPO certification scheme:** conception, development and introduction of DPO certification: experiences, failures, successes and lessons learned;
- **Privacy Impact Assessment in Latvia:** how a DPIA is conducted, who is obliged to conduct a DPIA, the necessity of conducting a DPIA, training of other persons such as employees of public authorities on issues related to the privacy of personal data, etc.

The study visit was organized with the support of the Council of Europe Data Protection Unit and the Latvian State Data Inspectorate.

### EU Projects



❖ On 26 January, the NCPDP in collaboration with TAIEX project experts organised the national conference “Raising Awareness on the Convention 108+”.

The aim of the conference was to raise awareness of both public institutions and the private sector about Convention 108 + as a viable tool to facilitate international data transfers, thus ensuring an adequate level of protection for data subjects globally.

The conference was moderated by data protection experts from Italy, Slovenia and Spain. Among the topics addressed by the experts are:

- the impact of Convention 108+ on adequacy decisions and data transfers, with a focus on compliance with the EU acquis;
- Convention 108+ as a viable tool to facilitate international data transfers while ensuring an adequate level of protection for individuals worldwide;
- Convention 108+ as a bridge between legal regimes and countries;
- the ratification process of Convention 108+;
- lessons learned and advice from ratifying countries;
- Convention 108+: the Evaluation and Review Mechanism, etc.

The event was organised and funded by the European Commission Technical Assistance and Information Exchange Instrument (TAIEX), and was attended by about 100 representatives of both public institutions and the private sector.



❖ From 11 to 13 March 2024, the representatives of the NCPDP made the study visit “**Processing of personal data through video surveillance systems**”. The event was hosted by the Spanish Data Protection Authority (AEPD) – Agencia Española de Protección de Datos.

The purpose of the event was both to take up legal and operational best practices on the use of video surveillance means, and to provide employees of the NCPDP with the skills and resources necessary to effectively address issues related to the processing of personal data through video surveillance systems, in accordance with current legislation and in the interest of protecting the rights of data subjects.



During the study visit, moderated by experts in the field of personal data protection from the AEPD, topics of importance were analysed in depth, such as: the evolution of video-surveillance regulations, the latest legislative changes and regulations related to personal data processing through video-surveillance systems, with a focus on GDPR regulations; data subjects' rights and ethics in video-surveillance; reception and classification of complaints; inspection procedures and instructions; technical and organisational measures to ensure the security of personal data; promotion of technologies applied to video-surveillance, etc.

The study visit was organised with the support of the EU TAIEX Project – Technical Assistance and Information Exchange Instrument, managed and funded by the Directorate-General for European Neighbourhood Policy and Enlargement Negotiations (DG NEAR) of the European Commission.

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



❖ In 2024, 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 the “**Learning and**



***Networking Week on Personal Data Protection in the Digital Age***, which took place in Tallinn, Estonia.

The aim of the event was to take over the Estonian experience in the implementation process of the GDPR, providing a comprehensive and practical overview of the challenges arising in its application.



Given that Estonia is known as a global leader in the digitisation of public services and ranks 3rd in the Global Cybersecurity Index as the most secure country, the information was presented on how

the processing of personal data is organised in public institutions, as well as new trends in the process of ensuring cybersecurity.

During the “*Learning and Networking Week in Estonia on Personal Data Protection in Digital Era*”, some important topics were addressed, such as:

- Challenges of the Estonian Data Protection Authority before and after the GDPR;
- Processing of personal data in public databases: processing practices and access to such data;
- GDPR case law: significant trends and findings from Estonian judicial and supervisory practice;
- Privacy vs. data reuse in the context of a digitally modernised society: challenges and recommendations;
- Data sharing and personal data protection;
- Cybersecurity etc.

The event was organised by 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 and brought together representatives of Data Protection Authorities from Moldova, Armenia, Georgia and Ukraine.

❖ In 2024, the video spot „Protect your personal data” was launched. The purpose of this social video is to inform and raise awareness of the general public about the field of personal data protection both from the perspective of respecting/ knowing the rights of data subjects and ensuring/observing the obligations of personal data controllers. Through it, the most important aspects related to the





field of personal data protection are highlighted, such as: general notions of personal data, what this data is, to whom we can disclose it, who can request it, as well as what are the obligations of data controllers in ensuring the security and confidentiality of this data.

The video spot was developed with the support of the project „Regional Fund for Public Administration Reform in the Eastern Partnership”, implemented by the German International Cooperation Agency (GIZ) and financed by the German Federal Ministry for Economic Cooperation and Development (BMZ) and can be viewed by accessing the following link: <https://datepersonale.md/videogalerie/>

Throughout 2024, the video spot was mediatized through several means of media, such as: TV devices installed in trolleybuses and buses in the capital for 1 month (January - February); TV devices installed in courthouses for 1 month (March). The video spot was also broadcast prime time (before the main news bulletin of the day) through the public television channel Moldova 1 for 2 weeks, between October 1-14.

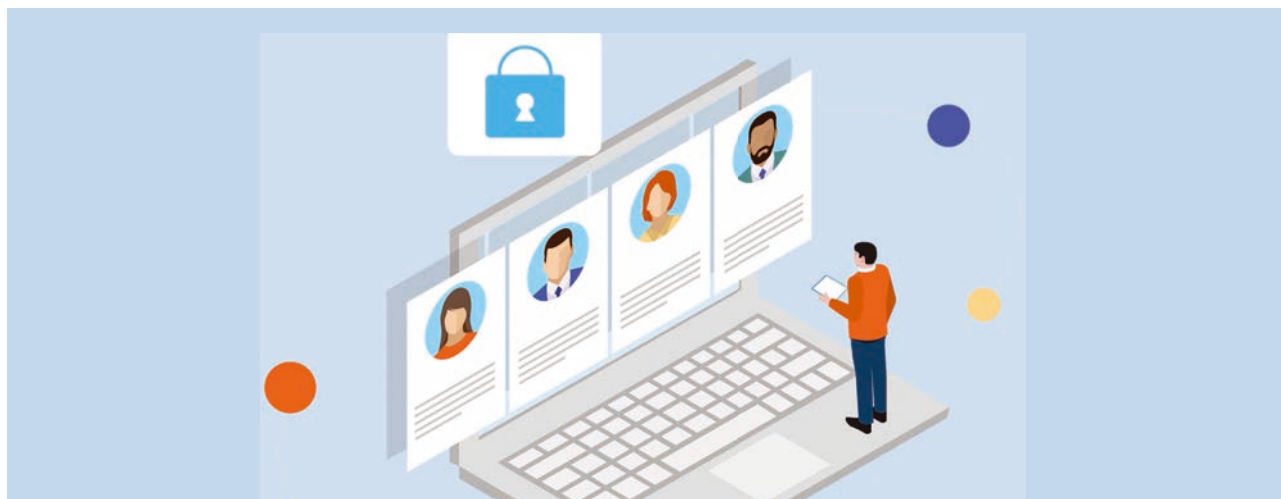




## CHAPTER IX

AWARENESS AND TRAINING  
ACTIVITIES

## IX



During the year 2024, the NCPDP has made remarkable progress in the area of awareness and training activities in the field of personal data protection.

In this respect, NCPDP continued the information and awareness campaign of the school community, organized street actions with different topics in the context of several events, organized a multitude of trainings with physical presence, as well as in online or hybrid format, for a record number of public institutions, especially for the subdivisions of the General Police Inspectorate, the General Inspectorate of Border Police and the National Office of Social Insurance, both in Chisinau and in the territory according to the training plans approved and signed by the leaders of the mentioned institutions.

#### **Awareness actions**

Given the interest among children for the campaign **“Personal Data Protection and Children’s Safety in the Online Environment”**, the campaign was also carried out in 2024. 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 addressed during the trainings focused on: familiarization of children with the concept of personal data; proper use of photos/video online; risks and threats online; communication on social networks, etc., being organized several training sessions within the school community, both in Chisinau and in the north and south of the country, namely:





## 25 January- Public Institution “Spiru Haret” Theoretical Lyceum, Chisinau



## 19 April - Public Institution “Liviu Rebreanu” Theoretical Lyceum, Chisinau



## 23 April - Public Institution “Iulia Hasdeu” Theoretical Lyceum, Chisinau



## 10 July - Republican Center for Children and Youth "Artico"



## 04 Octobre - Public Institution "Constantin Negruzzi" Theoretical Lyceum, Chisinau



## 12 November - Public Institution "Mihai Eminescu" Theoretical Lyceum, Cahul







### 03 December – Public Institution “George Cosbuc” Theoretical Lyceum, Balti

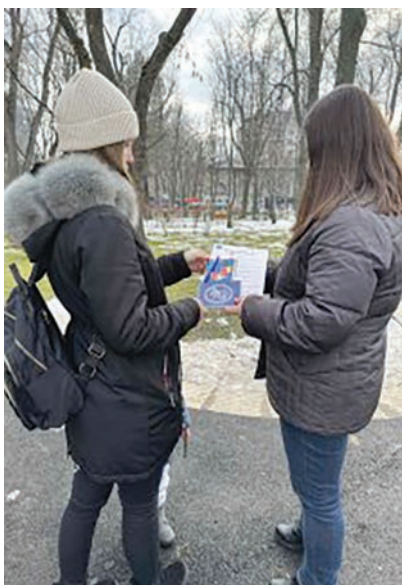


### 03 December – Public Institution “Lucian Blaga” Theoretical Lyceum, Balti



In totally, about **640** pupils were trained during the reference period.

On January 24, 2024, the *street action organized by NCPDP representatives in the context of the celebration of the European Data Protection Day* was held. In this context, a group of NCPDP employees distributed informational materials to passers-by in front of the Triumphal Arch Chisinau municipality. They were informed about the “Data Protection Day”, the concept of personal data, the rights of data subjects, data security and confidentiality measures, as well as the principles of personal data protection. Citizens were also informed about possible situations of non-compliant processing of personal data providing them with practical guidance and recommendations that should be undertaken in such situations.







On July 10, NCPDP celebrates 16 years of activity. On the occasion of this day, the institution organizes specific activities to raise awareness and promote best practices in privacy and data protection. These activities include street actions addressed to the general public to inform and sensitize them to the field of personal data protection. In this context, on July 9, several employees of the NCPDP distributed to passers-by, information

materials, in order to disseminate useful messages in the field of personal data protection, to inform and encourage Moldovan citizens to pay more attention to this field.

On 10-11 December, the NCPDP participated in the **Human Rights and Equality Forum - 3rd Edition**, organized in the context of the International Human Rights Day. The Forum created a unique platform for discussion and exchange of ideas between public institutions, civil society organizations, national and international experts in the field of fundamental human rights and freedoms. The Forum included interactive activities, games, workshops, movie screenings and information stands. In this context, NCPDP representatives set up a stand with educational-informative materials and promotional items, and the general public was informed about the field of personal data protection. At the same time, citizens were informed about possible situations of non-compliant processing of personal data and were given practical guidance and recommendations that should be taken in such cases.

The event was organized under the initiative of the Office of the People's Advocate and the Equality Council, with the support of development partners such as UN Agencies and the Council of Europe.



## Training activities

The year 2024 was marked by a record number of trainings organized for representatives of public institutions, both from the municipality of Chisinau and from the country, with a total of 5690 people trained.

**On 26 January 2024**, the NCPDP and the General Police Inspectorate (GPI) approved and signed the Training plan in the field 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.

In this context, **16 training courses** have been organized, being trained about **775 representatives of the GPI subdivisions**.



**On 21 February 2024**, the NCPDP and the General Inspectorate of the Border Police (GIBP) approved and signed the *Training plan in the field of data protection* for the GIBP subdivisions, therefore several training courses were organised. The purpose of these training courses was to increase the awareness of GIBP subdivisions' employees about the principles of personal data protection and to ensure the proper application of the relevant legal provisions in their work.





Thus, 14 training courses have been organized, being trained about 710 representatives of the GIBP subdivisions.



**On July 08, 2024**, was approved and signed by the heads of the NCPDP and the National Office of Social Insurance (NOSI), the Training Plan in the field of personal data protection for employees of the structural subdivisions of NOSI. The aim of the training courses was to increase the NOSI employees' awareness of the principles of personal data protection, as well as to familiarize them with the personal data confidentiality and security regime in accordance with the provisions of the legislation in force. During the events, important topics were discussed, such as: the definition of general notions related to the field of personal data protection; the rights of personal data subjects; the processing of special categories of personal data; principles and legal grounds for the processing of personal data; issues related to the appointment of the Data Protection Officer (DPO); aspects related to the Data Protection Impact Assessment; ensuring the security and confidentiality of personal data by NOSI employees, etc.

Thus, **10 training courses** were organized for the Central Apparatus of the National Office of Social Insurance; Territorial Office of Social Insurance, mun. Chisinau; Territorial Office of Social Insurance, North region; Territorial Office of Social Insurance, Center region; Territorial Office of Social Insurance, South region, being trained a total of **910 employees**.



Also this year, 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 legislation in force. During the events important topics were discussed, such as: definition of general concepts related to the field of personal data protection; principles and legal grounds for processing personal data; rights of personal data subjects; processing of special categories of personal data; requirements for the protection of personal data in the exercise of official duties; ensuring the security and confidentiality of personal data processed; issues related to the appointment of the Data Protection Officer (DPO), as well as his/her obligations and tasks; issues related to the Data Protection Impact Assessment (DPIA), as well as the steps of conducting a DPIA, etc. Thus, training courses were organized for the following institutions:

- February 07– Chisinau City Hall;
- February 08– National Financial Market Commission;
- February 23– Ministry of Health;
- March 15– Râșcani District Court;
- March 21– Chisinau Court;
- March 22– Agency for Intervention and Payments for Agriculture;
- March 26– Ministry of Economic Development and Digitalisation;
- April 04 – State Chancellery, territorial offices;
- April 16 – Single National Service for Emergency Calls 112;
- April 18 – State Pedagogical University “Ion Creangă”;
- May 16 – Standardization Institute of Moldova;
- May 30 – Electronic Governance Agency;
- June 05 – Chisinau City Hall;
- June 07 – Ministry of Foreign Affairs and European Integration;
- June 21 – State Tax Service;
- June 25 – Unified Center for the Provision of Public Services;
- June 26 – State Tax Service, territorial tax officials;
- June 27 – Land registration and evaluation project of the World Bank;
- August 13- Center for Strategic Communication and Combating Disinformation;
- September 26 - Psychiatric Clinical Hospital;





- October 08 – Parliament Secretariat;
- October 10 – Association of Internal Auditors;
- October 15 – National Employment Agency;
- October 17 – National Anti-Corruption Center;
- October 18 – Customs Service;
- October 24 – State Financial Control Inspectorate;
- October 25 – Territorial General Directorate “North” of the National Anti-Corruption Center;
- October 28 – General Directorate for Education, Youth and Sport of the Chisinau Municipal Council;
- October 30 – General Directorate of Education, Youth and Sport, directors of early education institutions in the Chisinau municipality;
- November 05 – General Directorate of Medical and Social Assistance;
- November 06 – General Directorate of Education, Youth and Sport, directors of educational institutions in Chisinau municipality;
- November 11 – State Tax Service;
- November 12 – General Territorial Directorate “South” of the National Anticorruption Center;
- November 13 – General Directorate for the Protection of Children’s Rights;
- November 22 – General Inspectorate for Migration;
- December 11 – Supreme Court of Justice.



Around **3295** representatives of public authorities were trained during these events.

### Management of human resources

The performance of NCPDP is dependent on the success of its employees - on their knowledge and professionalism, and the achievements and success of its employees depend on ensuring their rights through relevant management, leadership, professional and personal safety.

According to the structure, approved by Law no. 182/2008, the NCPDP consists of **8** structural subdivisions, and the number of staff is **45** units, including auxiliary staff.

At the end of 2024, the total number of employees is **34** persons, including **2** persons with the status of public dignity, **31** persons with the status of civil servants (including **10** managerial civil servants and **21** executive civil servants) and **1** person with an auxiliary function (driver).

Thus, at the end of the reporting year, the occupancy rate of functions/positions was approximately 76%.



### *Staff levels in the period 2018-2024*

Year	Units approved	Effectively, employees	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
2024	45	34	76

In the year 2024, compared to previous years, there is a small increase in the level of employment in public functions in the NCPDP, especially in executive functions.

This increase is due to the re-employment of some employees in the public executive positions in connection with the end of the suspension of service due to their being on partially paid leave for childcare up to the age of three.

Most of the institution's employees are law graduates, complemented by professionals in the fields of international relations, public administration, economics and other fields specific to the institution's activity. The employees who, in accordance with their duties, carry out activities to verify the compliance of personal data processing, for the most part, have a university degree in law and have at least graduated from a higher education institution.

The Authority applies a policy of gender equality in the recruitment and management of human resources, however, there is an essential prevalence of female employees over male employees, with the proportion of women in 2024 being **71% (24)** and men **29% (10)**.



The average age of employees per authority is 40 years. In the age structure, the proportion of persons aged 35-45 years is maintained, representing 35.3% of the total number of actual employees.

The table below reflects the share of NCPDP employees by age and gender, by types of functions.

### *NCPDP staff by age and gender categories*

Year 2024	Total number of persons		Positions of public dignity		Managerial public function		Execution functions		Auxiliary staff	
	Women	Men	Women	Men	Women	Men	Women	Men	Women	Men
<b>Number of persons</b>	<b>24</b>	<b>10</b>	<b>2</b>	<b>-</b>	<b>8</b>	<b>2</b>	<b>14</b>	<b>7</b>	<b>-</b>	<b>1</b>
• < 25 years	3	1	-	-	-	-	3	1	-	-
• 25-35 years	6	1	-	-	1	-	5	1	-	-
• 35-45 years	12	2	1	-	6	1	5	1	-	-
• 45-55 years	2	2	1	-	1	1	-	1	-	-
• 55-63 years	-	3	-	-	-	-	-	3	-	-
• 63 ani <	1	1	-	-	-	-	1	-	-	1

The national framework regulating salary policies in the budgetary sector, existing in 2024, has conditioned the resigning of 7 specialists from the NCPDP to budgetary institutions with more attractive salary conditions.

Thus, the staff turnover rate in 2024 reached **21%**, 3 percentage points higher than in 2023 (**18%**).

### *Staff turnover*

Years	Average number of employees	No. of persons whose service/employment relationship ended	Turnover,
%	32	8	23
2019	33	8	24
2020	36	6	18
2021	39	13	35
2022	32	13	37
2023	32	6	18
<b>2024</b>	<b>34</b>	<b>7</b>	<b>21</b>

In the process of ensuring the necessary staffing in 2024, the NCPDP has relied on the procedures for occupying public positions by promotion and competition. Among the procedures for filling public posts, the procedure for occupying public posts by competition prevailed, 7 persons were hired, 5 of whom were debutants.

In this regard, **5** competitions were organized and held, for which **33** applications were submitted and accepted.

During the reporting period, **3** employees had their employment relationships changed through promotion to immediately higher positions.

In the reporting year the NCPDP faced a lack of qualified staff. The reasons for the reduced capacity of the authority to cover the staffing needs were due to the disproportionate level of salaries of NCPDP's civil servants compared to other control bodies with similar status or





ministries, the complexity of the tasks and activity-specific skills, the high workload for the existing staff and the low number of candidates in the competitions for vacant public positions.

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

As in previous years, the proportion of staff with between 1 and 2 years' experience in the NCPDP is maintained at 32% in 2024.

The phenomenon of turnover has a number of disadvantages, and the procedure of selection and hiring of new staff is laborious and complicated due to the lack of competent specialists with experience in the field of personal data protection.

### PROFESSIONAL TRAINING

In order to strengthen its institutional capacity, the NCPDP pays particular attention to the professional development of human resources as an important vector in increasing the quality of the work performed.

The continuous professional development of employees is carried out in accordance with the provisions of *Annex no. 10 to Government Decision no. 201/2009 on the implementation of the provisions of Law no. 158/2008 on the civil service and the status of civil servants*, as well as on the basis of the annual plan of continuous professional development, according to which 38 employees have benefited from training courses, including those who have already resigned.

The training activities took place in different types and forms, such as:

- **7** 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;
- **9** internal training sessions, including trainings on specific areas of activity, moderated by trainers within the institution.

At the same time, the employees of the NCPDP were trained in various work trips abroad. In this regard, the exchange of experience with their counterparts abroad and the study of their best practices were ensured during study visits, workshops, conferences, as well as participation in various high-level events and meetings. During the reporting period, employees participated in **16** such activities abroad.

### Economic and financial activity

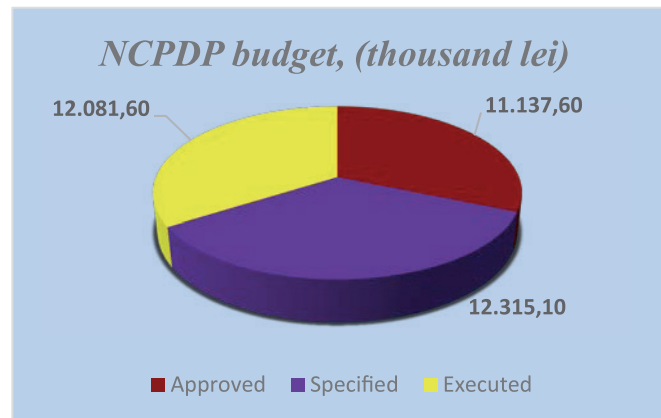


In accordance with Article 19 of the Law on personal data protection, the activity of the NCPDP is fully financed from the state budget within the limits of the budget allocations approved by the annual budget law. For the year 2024, the Authority has been allocated financial resources amounting to **12 315,10 thousand lei**, intended to ensure an optimal functioning of the Authority, to provide it with office equipment and techniques, to maintain the premises and to cover other necessary current expenses.

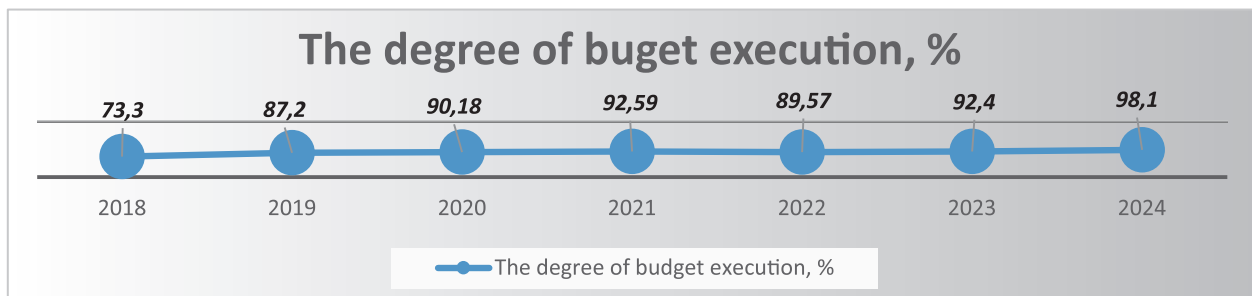


In order to fulfill the tasks assigned to its competence, during 2024, expenses in the amount of **12 081,60 thousand lei** (which constitutes 98,10 %) were executed, of which:

- **Staff expenditure** - 10 285,04 thousand lei (execution level 100,0%);
- **expenditures for goods and services** - 1 152,81 thousand lei (execution level 88,46%);
- **non-financial assets** - 587,47 thousand lei (execution level 90,83%);
- **social benefits** - 56,27 thousand lei (execution level 56,27%).



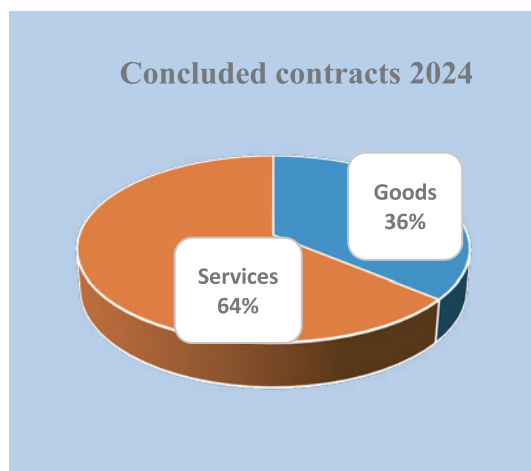
Over the years, the execution of the allocated budgets has shown an increasing trend and their evolution can be viewed below:



In accordance with the objective on the realization of the annual and quarterly plan for public procurement procedures for the year 2024, as well as its implementation through the organization and conduct of public procurement procedures, for the reporting period, low-value contracts for the purchase of goods and services were drawn up with their registration, as necessary, with the State Treasury.

The procurement procedures were managed through the MTender platform and their reporting was carried out subsequently.

Taking into account the planned needs, **50** procurement contracts (1 419,5 thousand lei) were concluded during the period, of which **32 for services** (878,1 thousand lei) and 18 for goods (541,4 thousand lei).





### *Internal Audit Service activity*

An essential role in ensuring the transparency and efficiency of the NCPDP's activity falls to the Internal Audit Service, which ensures the achievement of the mission and basic functions in the following areas:

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



The mission of the Internal Audit Service is to provide objective advice and assurance on the effectiveness of the financial management and control system, contributing to achieving added value and providing recommendations for its improvement.

In order to achieve the mission of the Internal Audit Service, the scope of internal audit activity 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 2024, performing the **4** planned audit missions.

The audit missions performed covered the following processes and activities:

- evaluation of the professional performance of civil servants within the NCPDP;
- execution of the NCPDP budget for 2023;
- evaluation of the integration process of civil servants starting out in public positions within the NCPDP;
- evaluation of the process regarding the disposal of material assets.

The internal audit reports were presented to the Director of the NCPDP and the operational managers of the audited subdivisions for action and, possibly, execution, according to their competences.

During 2024, the Internal Audit Service monitored the implementation of 15 internal audit recommendations, including 4 recommendations from the audit mission at the end of 2023.

The degree of implementation of 14 recommendations from audit missions was 100%.

The implementation of a recommendation from the last audit mission is in process, with the reporting deadline being May 2025.

At the same time, the implementation of 12 recommendations from the external audit, completed by the Court of Accounts in January 2024, was monitored. The reporting deadline for the implementation of the external audit recommendations is February 2025. Monitoring the implementation of the recommendations is kept under constant control.

As a result of the audit missions, in three subdivisions of the NCPDP in the last year of activity, several basic processes were identified, described or modified.

The assessment of the Annual Report on Internal Management Control (IMC), for the year 2023, was carried out within the established deadline with the development and presentation of the respective Report to the authority's management.

At the same time, in order to implement the proposals and objections raised in the process



of evaluating the internal managerial control system, amendments to the internal Regulation on the evaluation of professional performance, as well as the method of establishing the performance bonus for NCPDP employees, were developed and approved within the authority.

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 **80** 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.

Risk management controls ensure an acceptable level, corresponding to risk tolerance.

Monitoring of control measures within the authority's subdivisions is carried out periodically, depending on the type of risk with the respective reporting.

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). These trainings 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 **85%** of the NCPDP civil servants.



## PROBLEMES AND OBJECTIVES IN THE ACTIVITY OF THE NCPDP

*The problems that NCPDP has faced over the years persist in the reporting period*, these being of a legal, institutional, perceptual and applicability nature and requiring a stringent solution in order to develop the field of personal data protection at the national level and which, to summarize, constitute the following:

- ***inconsistency between the national legal framework and the existing European regulations in the field of personal data protection.*** It should be noted here that, on August 23, 2024, in the Official Gazette of the Republic of Moldova no. 367-369, art. 574, Law no. 195/2024 on personal data protection was published, a normative act that faithfully transposes the provisions of 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. Thus, the law takes over the community regulations on personal data protection, with the terminological, institutional and material norms being implemented accordingly.

However, the transposition of 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, remains a pressing priority.

The draft law on the *protection of individuals with regard to the processing of personal data by competent authorities for the purposes of preventing, detecting, investigating or prosecuting criminal offences or the execution of criminal penalties*, which will transpose Directive (EU) 2016/680, is being drafted and will be finalized and debated within the Working Group created for this purpose. Subsequently, it is necessary to emphasize the importance and rigor of the entry into force, on the same date, of both laws, mentioned in this chapter, exactly according to the model followed by the European Union when adopting Regulation (EU) 2016/679 and Directive (EU) 2016/680 (acts adopted and entered into force simultaneously), otherwise, there would be a risk of generating a regulatory/legislative vacuum for all data controllers in the field of preventing, detecting, investigating or prosecuting criminal offences or the execution of criminal penalties, which is unacceptable.

Accelerating the process of bringing the draft law on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of preventing, detecting, investigating or prosecuting crimes or executing sentences to the agenda of the Parliament of the Republic of Moldova and its adoption is imperative.

- ***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 makes this problem even more felt.





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 included not only by national legal harmonization with the community acquis in the field but also by the existence of qualified specialists to monitor the correct application of legislation in the field, however, attracting and maintaining them attractively may have places to ensure remuneration. However, the existing salary mechanism stratifies the public service into categories of civil servants whose statute offers attractive salaries and categories of civil servants who offer a precarious salary, which, ab initio contradicts the provisions of Law no. 270/2018 on the unitary salary system in the budgetary sector, which in art. 3 para. (1) letter b) non-discrimination, fairness and coherence, according to the statute of ensuring equal treatment and equal remuneration for work of equal value.

- ***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 complaints, 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 considerable increase in the volume of activities in which NCPDP employees are involved has increased staff turnover, caused by **the precarious level of remuneration in relation to the complexity and volume of activities**. Thus, it is urgently and imperatively necessary to consolidate and ensure the efficient functioning of the Authority for the control of processing personal data;

- ***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. It should be noted that this problem will be overcome with the entry into force of the new law on personal data protection (Law no. 195/2024);

- ***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 of public interest;

- ***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).

- ***insufficient awareness by individuals of the possible risks that may arise as a result of offering copies of identity documents to third parties, under various pretexts, as well as the presentation of data relating to: surname, first name, IDNP, home address, bank card details, income, pension amount, etc., without showing caution when disclosing and transmitting personal data, without being sure of the legality of the collection of personal data and the subsequent use of this data.***



**The objectives of the NCPDP for 2025** 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**, by the approval by the Parliament of the Republic of Moldova of the draft law on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of preventing, detecting, investigating or prosecuting crimes or executing sentences;
- **strengthening the administrative and institutional capacities of the NCPDP** in terms of both financial and human resources, including activities to improve staff skills and knowledges;
- **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 balance 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.