NATIONAL CENTER FOR PERSONAL DATA PROTECTION OF THE REPUBLIC OF MOLDOVA

ACTIVITY REPORT FOR THE YEAR 2022

CONTENTS

WELCOME SPEECH

„Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified".

The Charter of Fundamental Rights of the European Union

Dear Readers,

Strong personal data protection rules and their rigorous enforcement are essential to guarantee the right to personal data protection. They are also an important component of an increasingly data-driven economy. Digital transformation, on the one hand, offers more and more opportunities for rapid and innovative economic development, on the other hand - it brings new challenges and risks for individuals. Technological progress, centralised/automated processing of large volumes of data and the interconnection of digital devices, allow the collection and use of personal data in increasingly complex and opaque ways, thus posing significant challenges to privacy and data protection. These developments require clear rules on personal data protection and consistent enforcement by competent authorities.

The effects of using data to generate profits go far beyond the scope of individual areas of law. The internationalisation of personal data protection can also be seen when we consider the increasing use of large volumes of data or new technologies such as Artificial Intelligence and cloud services.

Personal data protection is therefore no longer just an issue for data protection authorities; it must also be on the daily agenda of legislators, regulatory authorities as well as private entities and natural persons.

Our aim, as personal data protection authority, is to ensure that a fair balance is maintained between the right to personal data protection and the rights guaranteed by the Constitution of the Republic of Moldova, such as: the right of access to information, the right to freedom of expression, the right to inviolability of intimate, family and private life, etc. At the same time, the field of personal data protection should under no circumstances be perceived as an impediment to the realisation of competing rights and interests.

Based on its tasks, the National Centre for Personal Data Protection informs institutions and society about its activity, priority issues and concerns in the field of individuals' rights protection and presents the Annual Activity Report.

This activity report presents confirmatory information and statistics in this respect, i.e. examples of cases examined by the authority, draft legislation prepared and endorsed, recommendations and guidelines drawn up, problems identified and objectives set, etc.

Victoria MUNTEAN

Director

GENERAL PRESENTATION

Year 2022 in numbers

REQUESTS / COMPLAINTS

9838 correspondence documents:
3529 inbox
4045 outbox
1439 internal
825 complaints

ACTIVITY OF CONTROL

227 initiated controls
230 issued decisions
125 decisions of the absence of violations found
105 decisions of violations found
36 decisions of suspention/cessation/erasure
125 cases of contraventions found
110 minutes drawn up

ENDORSEMENT ACTIVITY OF DRAFT NORMATIVE ACTS

25 draft agreements/international treaties
23 draft normative acts amending laws, codes
79 draft normative acts of the Government and other authorities

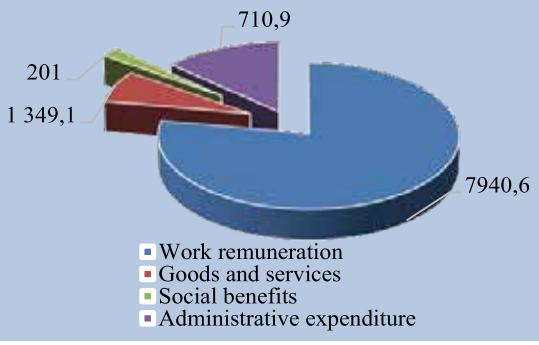
ACTIVITY OF THE REPRESENTATION IN THE COURTS

551 court proceedings:
361 in contravention proceedings
190 in administrative litigation

PREVENTION ACTIVITY

84 data protection officers designated
11 consultations/prior consultations provided in relation to the data protection impact assessment

SPECIFIED BUDGET 2022, THOUSAND LEI



HUMAN RESOURSES

32 out of 45 staff-limit
5 competitions held
6 persons employed / 2 debutants
13 persons resigned
21 training courses

TRAINNING AND AWARNESS ACTIVITY

2862 trained persons
38 training activities
5 information and awareness-raising activities
105 press releases elaborated and published

CHAPTER I

EXAMINATION OF COMPLAINTS AND OTHER REQUESTS

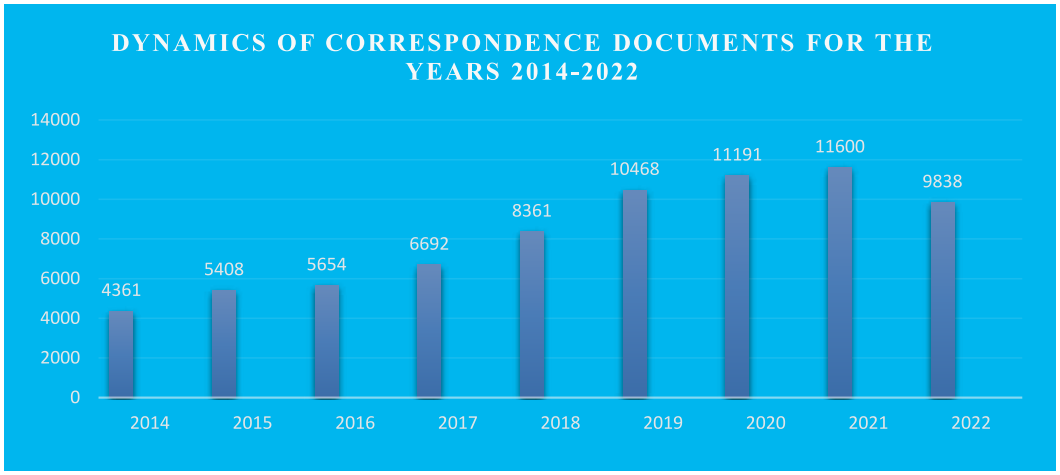
The National Center for Personal Data Protection of the Republic of Moldova (NCPDP) provides information and advisory support to personal data subjects and data controllers who wish to obtain qualified legal information on the exercise of their rights or assistance in complying with data protection legislation in the processing of personal data, providing answers both in writing through the post office and by e-mail or telephone.

During 2022, NCPDP examined **9838** correspondence documents, including **3529** inbox documents, **4045** outbox documents and **825** complaints of personal data subjects.

Comparative statistics of correspondence documents, for the years 2014-2022

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

The dynamics of the number of correspondence documents registered by the NCPDP during 2014-2022 can be analysed in the below diagram.



The topics addressed in the correspondence documents reveal the increased concern of the controllers in ensuring compliance with the rules for personal data processing established by the Law on personal data protection and related national legislation, in implementing the necessary organisational and technical measures to ensure the confidentiality and security of personal data processed, including in the context of rapid technological developments and globalisation which have created new challenges for personal data protection, as well as the interest of personal data subjects to actually realise the rights laid down in the Law on personal data protection and the tendency of the latter to have control over their personal data, especially in the light of the increasing exchange of personal data between public and private actors, including natural persons, associations and enterprises.

At the same time, in 2022 compared to the previous reporting period, there is a slight decrease in the number of correspondence documents registered by the NCPDP during the reporting period.

This is partly due to the significant changes to the Law No. 133/2011 on personal data protection, following the entry into force of the Law No. 175/2021 on the amendment of certain regulatory acts, which excluded the powers of the NCPDP to receive and analyse notifications from data controllers and to carry out prior controls on categories of personal data processing operations subject to cross-border transfer and on categories of personal data processing operations presenting special risks to the rights and freedoms of individuals, as a result of which the NCPDP authorised or refused authorisation of personal data processing operations, including the tasks of keeping the Register of evidence of personal data controllers.

Other circumstances that influenced the dynamics of the number of correspondence documents registered by the NCPDP are due to amendments to the provisions of Art. 27 of the Law on personal data protection, in force since 24 August 2020, in circumstances where the prenoted legal amendments established conditions for submitting a complaint to the authority, which indicate the prior realization by the data subject of the rights provided for in Art. 12, 13, 14, 16 and 17 of the Law on personal data protection. This was also reflected in the number of requests submitted in which the data subject only requested confirmation as to whether or not his or her personal data had been accessed in a particular state filing system. Thus, following changes the data subject first submits a request to the personal data controller holding this system, for example to the "Public Services Agency", which holds the State Population Register, the State Register of Transport, the State Register of Vehicle Drivers, the State Register of Real Estate and the Civil Status Registry. However, in view of the functional powers prescribed by the Law on personal data protection, the NCPDP does not have direct access to the personal data of data subjects stored in the databases and/or in the filing and IT systems of personal data controllers, as well as to the audit of personal data processing operations in these databases and/or filing systems.

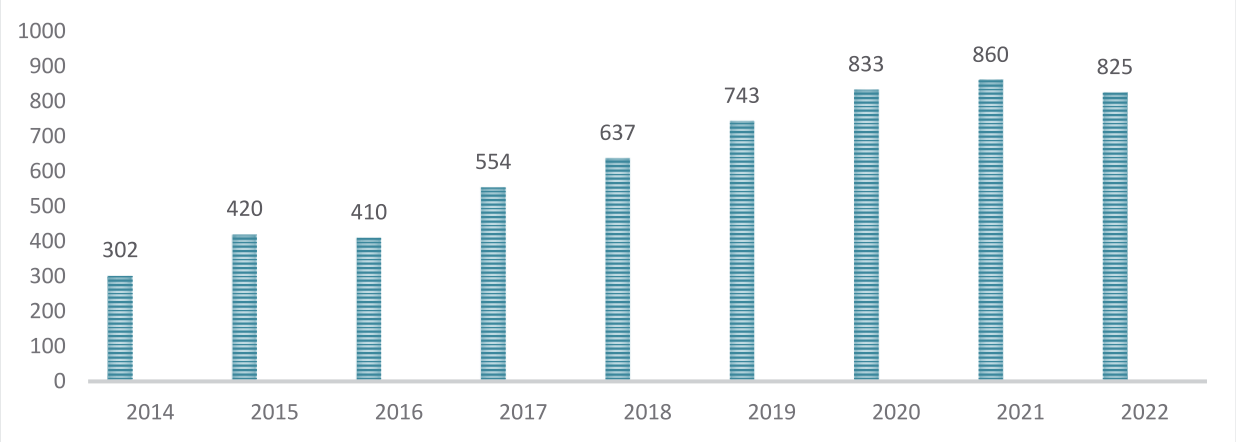
The above recitals explain the decrease in the number of documents registered during 2022 and have significantly influenced the work of the NCPDP.

Activity of examination of personal data subjects' complaints

During the reporting period, **825** complaints were received by the NCPDP from natural persons - personal data subjects.

From the total number of complaints registered in the reporting period, in **227** cases, controls on the compliance of personal data processing were initiated.

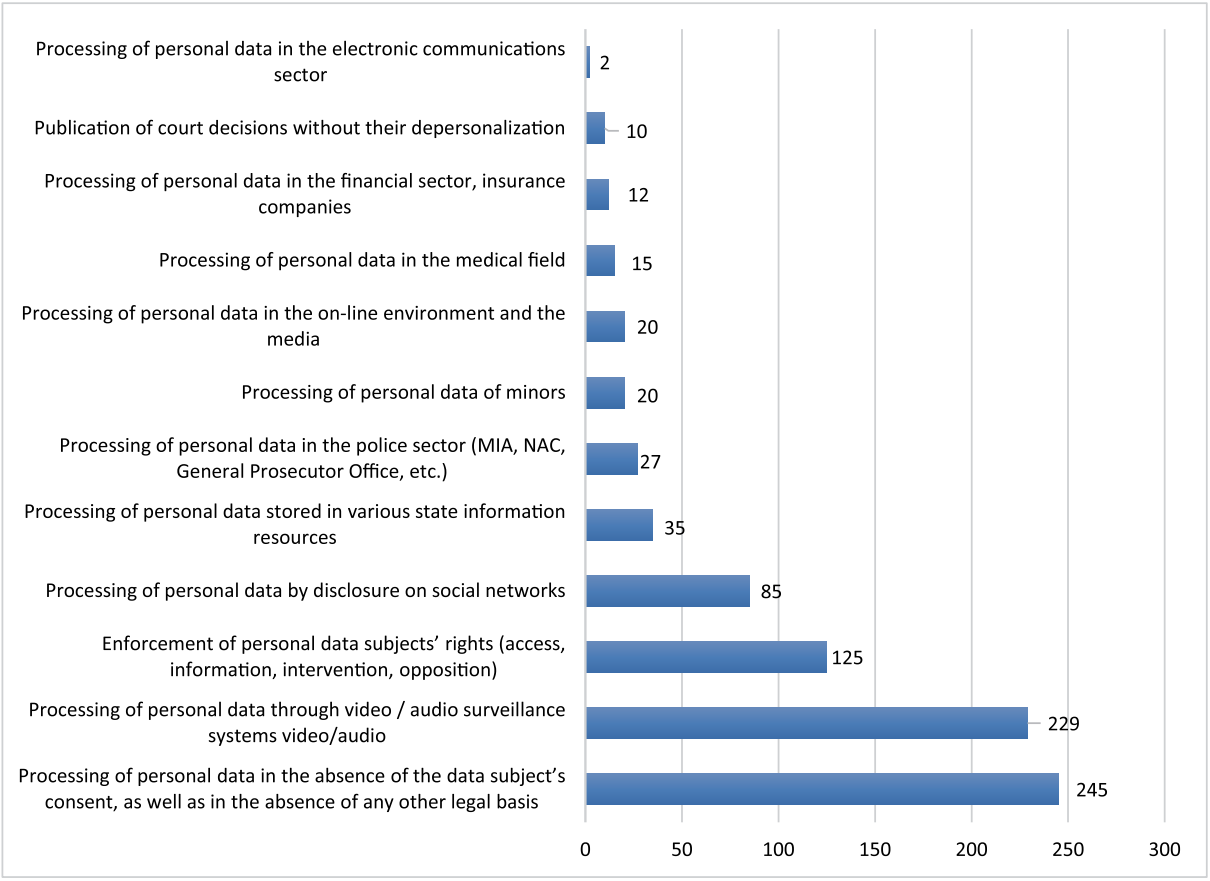
DYNAMICS OF THE NUMBER OF COMPLAINTS FOR THE YEARS 2014-2022



Thus, in 2022, complaints submitted to the National Authority for Personal Data Protection continued to raise issues mainly relating to:

- ✓ Processing of personal data in the absence of the data subject's consent, as well as in the absence of any other legal basis: **245** cases;
- ✓ Processing of personal data through video / audio surveillance systems: **229** cases;
- ✓ Enforcement of personal data subjects' rights (access, information, intervention, opposition): **125** cases;
- ✓ Processing of personal data by disclosure on social networks: **85** cases;
- ✓ Processing of personal data stored in various state information resources: **35** cases;
- ✓ Processing of personal data in the police sector (MIA, NAC, General Prosecutor Office, etc.): **27** cases;
- ✓ Processing of personal data of minors: **20** cases;
- ✓ Processing of personal data in the on-line environment and the media: **20** cases;
- ✓ Processing of personal data in the medical field: **15** cases;
- ✓ Processing of personal data in the financial sector, insurance companies: **12** cases;
- ✓ Publication of court decisions without their depersonalization: **10** cases;
- ✓ Processing of personal data in the electronic communications sector: **2** cases.

General situation regarding the complaints under examination in 2022



CHAPTER II

ACTIVITY OF CONTROL

Any natural person/data subject has the right to adequate protection of his/her personal data. The processing of personal data must be necessary, fair, lawful and proportionate.

Data provided directly or indirectly by natural persons must not be used for purposes other than those for which they were originally collected and must not be further processed in a way incompatible with those purposes. These rights apply to all persons, regardless of nationality or place of residence. The processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life is permitted only with the explicit consent of the person concerned or under the conditions laid down by law.

Data subjects have the right to receive information from the persons and companies holding part of their personal data in various filing systems, such as websites, databases, state registers, etc., and to request rectification or erasure of such data if they are incomplete or inaccurate.

Any data subject has the right to request the annulment, in whole or in part, of any individual decision which produces legal effects on his or her rights and freedoms and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him or her, such as professional competence, credibility, behavior, etc.

Thus, in order to ensure the protection of the fundamental rights and freedoms of natural persons with regard to personal data processing, the personal data protection authority remains the institution that provides support to data subjects who consider that their rights and interests guaranteed by the Law No. 133/2011 have been violated as a result of unlawful processing of personal data.

Therefore, also during the reference period, the NCPDP continued its activity of monitoring and verifying the compliance of personal data processing by public and private sector controllers by carrying out controls on the basis of complaints from personal data subjects, complaints received for examination, including from public authorities/institutions and self-reporting by the authority.

The control activity consists in verifying the lawfulness of personal data processing by personal data controllers and/or processors, which aims to elucidate the circumstances of the processing operations, to collect the evidence necessary for an objective examination of the case complained of and to corroborate them with the legal provisions related to the field of personal data protection.

The issues examined by the NCPDP are becoming increasingly complex. When examining complaints, the NCPDP follows a control procedure in accordance with the legal framework by collecting evidence/information in accordance with the provisions of the law. The procedures are largely based on written communication, which can sometimes seriously obstruct the efficiency of the decision-making process, and there are situations when the persons concerned by the case do not cooperate with the authority, refusing to receive its requests or not providing the requested information.

In most of the cases examined, the purpose of the controls is to establish:

- the purpose and legal basis of personal data processing;
- the necessity and specific nature of personal data processing;
- proportionality, relevance and actuality of processed data;
- respecting the rights of personal data subjects;
- respecting the degree of security and confidentiality of personal data processed;

The control required by the Law on personal data protection is carried out by the state inspectors of the General Department for Surveillance and Conformity and the Legal Department. If necessary, depending on the subject and tasks of the control performed the NCPDP may attract specialists and experts from fields requiring special knowledge to participate in the process of prior verification and control of the lawfulness of personal data processing. The control activity consists in verifying the legality of personal data processing by the data controllers in order to clarify the facts and circumstances related to personal data processing and collect the evidence necessary for the objective examination of the claimed case.

Thus, during the reference period, **227** control materials were initiated and examined on the basis of complaints from personal data subjects/self reporting initiated at the request of legal entities/public authorities or ex officio.

Comparative information on the control activity, for the years 2018 – 2022

Period for comparison	Number of controls initiated based on: complaints / notification, requests for cross-border transfer	Acts issued as a reaction to controls			
		Decisions on suspension of personal data processing	Decisions on cessation of personal data processing	Decisions on destruction / erasure of data processed in the breach of law	Cases of contraventions found / Minutes issued
Year 2018	326	16	4	27	191/92
Year 2019	376	26	8	24	186/105
Year 2020	303	20	6	17	170/125
Year 2021	243	27	2	9	148/117
Year 2022	227	21	2	13	125/110

Comparative analysis of the statistical data shows a slight decrease in the number of controls compared to 2021. This is due to the substantial changes made in 2021 to the Law on personal data protection. In this context it should be noted, following the entry into force of the Law No. 175/2021 on the amendment of certain normative acts (Law No. 175/2021), the powers of the supervisory body regarding the receiving and analysing notifications of data controllers' notifications, as a result of which the NCPDP authorizes or refuses the authorization of personal data processing operations, were excluded.

Respectively, from 10 January 2022 the obligation to register and notify filing systems to the NCPDP has been excluded. However, the personal data controller must still comply with the rules for personal data processing regulated by the Law No 133/2011, such as: main conditions/ principles for personal data processing; respect for the rights of personal data subjects; obligation for personal data controllers to carry out, in certain cases, prior to processing, the personal data protection impact assessment; designation of data protection officer.

Furthermore, it is noted that by the Law No 175/2021 was also amended Article 32 of the Law on personal data protection, which excluded the power of the NCPDP to examine requests / complaints from controllers to authorise the cross-border transfer of data, a power which provided for the control of the circumstances in which a cross-border transfer of data was to take place with the issuance of a reasoned decision in this regard.

However, in the circumstances set out above, the NCPDP did not initiate control activities concerning the authorisation or refusal to authorise personal data processing operations, including personal data processing operations subject to cross-border data transfer.

At the same time, the decrease in the number of controls compared to 2021 is also due to the amendments made in 2020 to the provisions of Art. 27 of Law No. 133 of 08.07.2011 on personal data protection, significantly influencing the work of the NCPDP in terms of control over the lawfulness of personal data processing, or, the amendments made have established conditions for filing a complaint to the authority, namely, the need for prior fulfillment by data subjects of the rights provided for in Art. 12, 13, 14, 16 and 17 of the Law on personal data protection, which explains the decrease in the number of controls initiated on the basis of personal data subjects' complaints, a fact that will continue in 2022, as well as the fact that at the stage of realization by data subjects of their rights in relation to controllers, the latter have resolved/clarified the situation invoked by the complainants.

In this context, it should be noted that Art. 27 of the law expressly regulates issues concerning: the deadline for examining and handling data subjects' complaints, the reasons for their extension, the deadline for issuing the decision on the case and the person who may challenge the actions and/or inactions of the NCPDP in the administrative court.

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

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

publication of personal data online, etc.

As a result, **230** decisions were issued, of which **125** decisions finding no violation, **105** decisions finding a violation of legal provisions in relation to personal data processing. Following 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 – 21 cases;
- Destruction / erasure of personal data processed regarding the infringement of legal provisions – 13 cases;
- Cessation of personal data processing – 2 cases.

Not lastly, it should be noted that in the case of violations found as a result of the verification of personal data processing lawfulness, both coercive and contraventional sanctions are imposed. Thus, the decision on the finding of a breach of personal data protection legislation and the evidence gathered serve as a basis for the drawing up of the report on the contravention under the terms of the Contravention Code.

Subsequently, in relation to the provisions of Articles 74^1 - 74^3 of the Contravention Code, the contraventions related to personal data protection for which sanctions are applied are:

- infringement of personal data processing, storage and usage rules;
- infringement 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;
- cross-border transfer of personal data with violation of personal data protection legislation;
- 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;
- obstruction the access of the staff authorized with control functions of the National Centre for Personal Data Protection to the premises and to the territory of the location of the personal data filing systems, to the personal data processed by the controllers and/or processors, to the processing equipment, programs and applications, to any document or record related to the processing of personal data;
- failure to comply, within the deadline, with the decision of the National Center for Personal Data Protection on the re-establishment of the personal data subject's rights, including on the suspension or cessation of personal data processing, on blocking, partial or complete destruction of personal data processed in breach of the legislation on personal data protection.

Fines in the amount of 30 to 300 conventional units may be imposed for the offences described above.

It should be noted that the court is responsible for the solving of the cases and the imposing of fines, which, according to the Contravention Code, once the guilty party has pleaded guilty and the financial penalty has been imposed, it also has the power to impose an additional penalty in the form of deprivation of the right to process personal data for a period of 3 months to 1 year.

Thus, according to the control activity carried out as an ascertaining body, according to the facts stated in Articles 74^1 - 74^3 of the Contravention Code, regarding the violation of the legal provisions in the field of personal data protection, during the year 2022, **110** minutes on contravention were drawn up, **125** contravention facts being established and sent for examination in the Court, according to the provisions of the Contravention Code.

It should be pointed out that, although 2 rules providing for sanctions for personal data processing without notification and/or authorisation of the supervisory body in the field of

personal data processing, where notification or obtaining authorisation is mandatory, as well as processing of personal data by a controller not registered in the prescribed manner - Art. 74^1 para. (2) and for failure to comply with the requirements for ensuring the security of personal data when personal data processing within the framework of personal data information systems - Art. 74^1 para. (1) (in the wording before the entry into force of the Law 175/2021), compared to the year 2021, the number of administrative fines has been reduced by only 6% and the number of offences has been reduced by 15%.

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

- Art. 74^1 para. (1): infringement of personal data processing, storage and usage rules, except in the cases provided for in paragraph (5) – 92 cases;
- Art. 74^1 para. (3): infringement 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 – 12 cases;
- Art. 74^2 para. (1): refusal to provide the information or documents requested by the National Centre for Personal Data Protection in the process of exercising control powers, presentation of inauthentic or incomplete information, as well as failure to submit the required information and documents within the deadline established by law – 17 cases;
- Art. 74^3: failure to comply, within the deadline, with the decision of the National Center for Personal Data Protection on the restoration of the personal data subject's rights, including on the suspension or cessation of personal data processing, on blocking, partial or complete destruction of personal data processed in breach of the legislation on personal data protection - 4 cases.

CHAPTER III

ACTIVITY OF REPRESENTATION IN THE COURTS

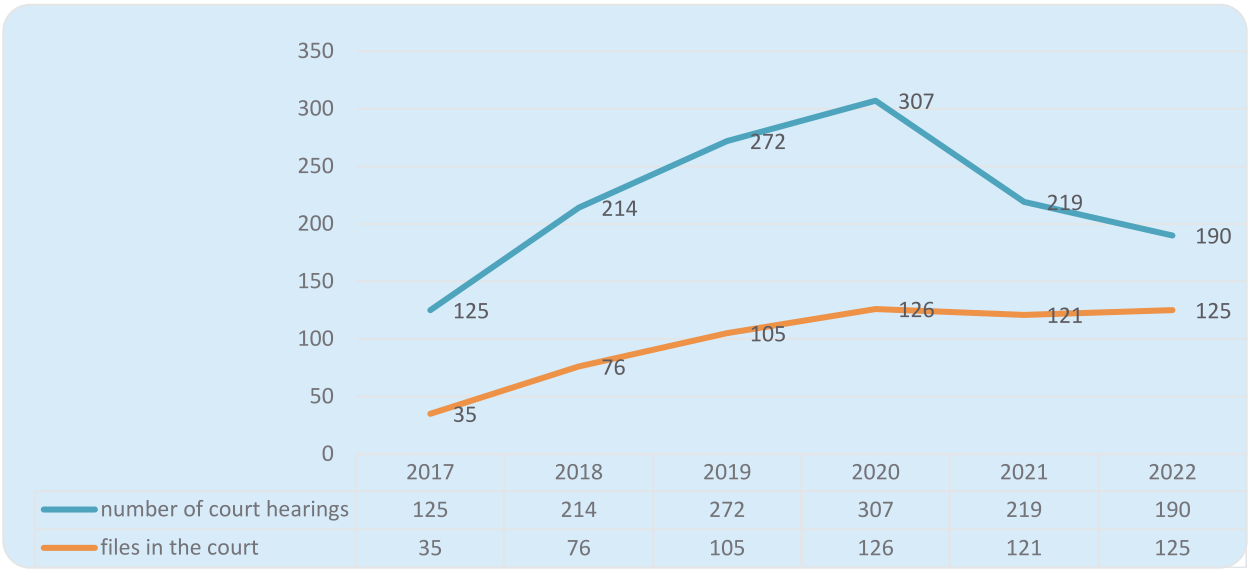
In civil and administrative litigation

During the year 2022, the NCPDP's interests were represented in the administrative litigation courts in **125** court hearings, amongst which: **118** as a defendant; **7** as a public authority which draws conclusions.

Therefore, the representatives of the NCPDP participated in **190** court hearings of administrative litigation, drafting **95** procedural documents necessary for an efficient examination of court cases.

At the same time, we note that in **7** court hearings the NCPDP was called as a public authority that submitted conclusions, in accordance with the provisions of Art. 74 para. (1) Code of Civil Procedure. However, the data subject, if the NCPDP through its decisions has found certain non-compliances in relation to the processing of his personal data, can exercise his right of access to justice, conferred by Art. 18 of the Law on personal data protection, according to which any person who has suffered damage as a result of personal data processing carried out unlawfully or whose rights and interests guaranteed by the Law No. 133/2011 have been violated has the right to appeal to the court for compensation for material and moral damages.

Comparative dynamics of the number of cases and court hearings in administrative litigation, for the period 2017-2022



	2017	2018	2019	2020	2021	2022
number of court hearings	125	214	272	307	219	190
files in the court	35	76	105	126	121	125

Furthermore, we mention that during 2022 the examination of **35** court files was completed, where the judgements / decisions of the courts remained final and irrevocable, of which **21** judgements/decisions of the court were issued in favor of the NCPDP and **14** cases were unsuccessful for the NCPDP.

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.

Thus, in addition to the many cases examined in the administrative court, the following successful cases for the National Authority for Personal Data Protection in 2022 are to be mentioned as examples:

Case no. 1

The data subject contacted a banking institution regarding access to personal data via the video surveillance system and requested to be allowed to access the video recordings taken by the surveillance cameras located outside the bank's premises, in relation to the fact that during the specified period of time he was pushed and shoved by a person who, according to the data subject, appeared to be a state agent in uniform.

As a result, the bank informed the data subject of its inability to provide the video recordings on the grounds that the information requested, i.e. the video images captured by the surveillance cameras located outside the bank's premises, constituted banking secrecy and involved the disclosure of personal data of the bank's customers.

Thus, the data subject notified the Personal Data Protection Authority about the violation of the right of access to personal data, to which, following the control carried out by the NCPDP, it issued a decision finding a violation of the provisions of Article 13 of the the Law on personal data protection by the banking institution in relation to the data subject.

Therefore, it is revealed that the personal data subject, who is the subject of personal data processing, exercised his right of access to his personal data to the banking institution, processed through the video surveillance system installed at the bank's premises.

It should be noted that, despite the legal framework on data protection, which enshrines the rights of the personal data subject, including in the banking sector, which allows the provision of information (images) containing personal data concerning only the person who requests them, the banking institution has not, however, ensured the subject's right of access to his personal data processed through the video surveillance system, contrary to Art. 13 of the Law No. 133/2011 on personal data protection.

As a result, the decision issued by the NCPDP was maintained by the court of first instance, the Chisinau Court of Appeal and the Supreme Court of Justice.

Case no. 2

At the origin of the control initiated by the NCPDP were the actions of a bailiff who accessed and printed from the State Population Register (RSP), via the SIC "Access-Web", the personal data of a third person in the framework of an enforcement procedure.

In the case, following the examination of the data subject's complaints, the NCPDP found that, in order to achieve the purpose - identification of the debtor's relatives' address - it was sufficient only to view the third party's personal data, without printing and attaching to the file the extract from the RSP containing more information than the home address.

In addition, the Personal Data Protection Authority noted that the State Population Register is an information source containing a huge amount of personal data. Therefore, printing and attaching to the materials of an enforcement procedure the extract from the RSP of a natural person - personal data subject, who is not a party to the enforcement procedure, containing a certain amount of personal

data irrelevant to the procedure, such as blood group, date of birth, etc. can take place after ensuring a balance of necessity and proportionality.

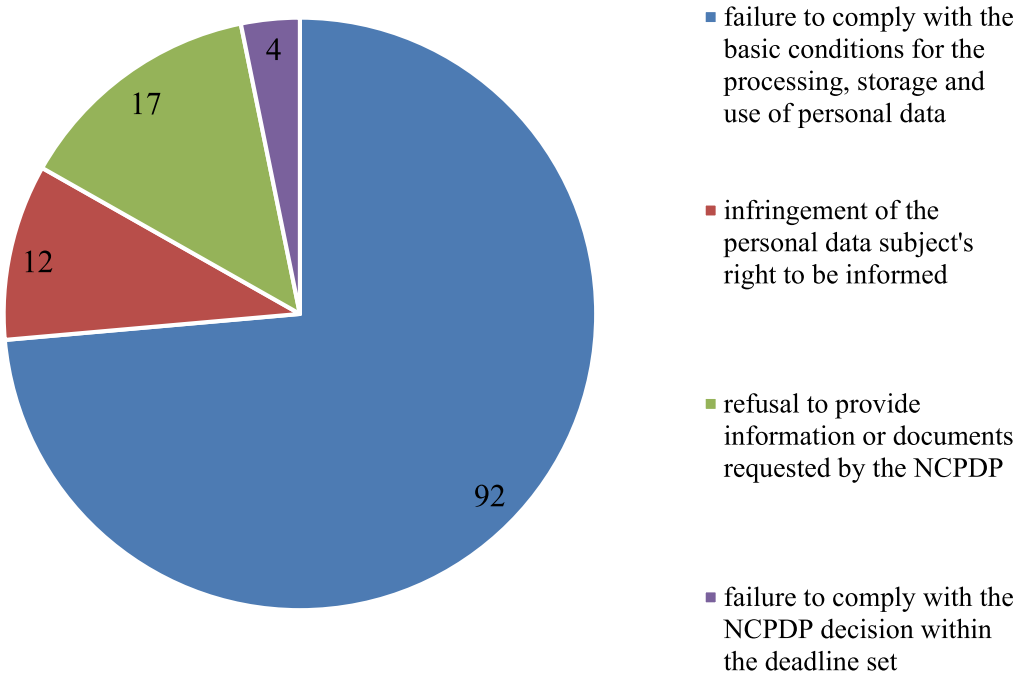
Thus, the actions of the bailiff have been qualified by the NCPDP as contrary to Art. 4 para. (1) let. c) of the Law on personal data protection.

Following this, the decision issued by the NCPDP was maintained by the court of first instance, the Chisinau Court of Appeal and the Supreme Court of Justice.

In contravention procedure

Based on the decisions issued, by which violations of the processing of personal data were found, the ascertaining agents of the NCPDP, during the reference period, drew up **110** minutes on contravention, being ascertained **125** contravention facts. In accordance with Art. 423[4] of the Contravention Code, the minutes on contravention were submitted for examination in the competent court.

The spectrum of contravention found



During the year 2022, the NCPDP's ascertaining agents participated in more than **361** court hearings on contraventions under examination, both in the court of first instance and at the Chișinău Court of Appeal. Furthermore, it should be noted that out of the total of **110** contravention cases sent for examination in the court during the reference period, in **56** proceedings examined the NCPDP won the case, the court acknowledging the guilt of the persons in respect of whom minutes on contravention were drawn up, establishing sanctions in the form of a fine. In addition, it should be noted that another **140** proceedings are currently pending before the courts, including on some of the infringement cases initiated in 2021.

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

➢ It should be pointed out that, during the reference period, the NCPDP has made considerable efforts to carry out the duties of the ascertaining body in the framework of the contravention cases, which were initiated and/or submitted to the court for examination before the entry into force of the Law No. 175/2021, but in the circumstances in which the contravention rules set out in Art. 74^1 para. (1) of the Contravention Code have been significantly amended and those of para. (4) of the same article in the context of the amendments to para. (1) have been repealed, the ascertaining agents requested the court to reclassify the contravention facts.

Thus, in cases where the court has ordered the suspension of the contravention proceedings against the offender who committed the offence referred to in Article 74^1 para. (4) of the Contravention Code, on the grounds that this act is no longer considered a contravention, the NCPDP found the statements of the court of first instance to be unfounded, since the act committed, provided for in Article 74^1 para. (4) of the Contravention Code (until the entry into force of the new amendments) is still punishable under the new provisions of Art. 74^1 para. (1) of the Contravention Code, being amended as follows: *"Failure to comply with the basic conditions for the processing, storage and use of personal data, except in the cases provided for in para. (5), shall be punishable by a fine [...]"*.

As a result, the constituent elements of the offence provided for in Article 74^1 para. (1) of the Contravention Code (in its current wording), are similar to those in para. (4) which has been repealed. However, the offence in question (previously set out in para. (4) and now in para. (1) of Art. 74^1 of the Contravention Code) is based on the same factual legal rules, falling under the provisions of the articles set out in Chapter II of the Law No. 133/2011, entitled "*Basic conditions for the processing, storage and use of personal data*", the same object, subject, objective/subjective side, contraventional nature and the sanction provided for in these paragraphs is the same.

At the same time, on similar cases, the courts (for example: Chisinau Court, Ciocana headquarters, by judgment of 24.12.2021 (case no. 4 - 2234/2021), Chisinau Court, Buiucani headquarters, by judgment of 17.03.2022 (case no. 4-22009110-12-4-22012022 (4-179/2022)), have decided that the cessation of the contravention process on the grounds of exclusion from the Contravention Code para. (4) of Art. 74^1 is unfounded, or, although the rule laid down in Art. 74^1 para. (4) has been excluded, the offence committed is still punishable under the new provisions of Article 74^1 para. (1) of the same Code. The offender's actions are to be reclassified under para. (1) of Art. 74^1 of the Contravention Code.

Therefore, in cases where the court has ordered the cessation of the infringement proceedings against an offender who has committed the offence referred to in Article 74^1 para. (4) of the Contravention Code, on the grounds that this act is no longer considered a contravention, the NCPDP's ascertaining agents considered that the court had misinterpreted Article 3 of the Contravention Code, and more than **65** appeals were submitted to the Chisinau Court of Appeal.

➢ And during the year 2022, the pressing issue persisted, which hinders the activity of the authority, manifested by the **double, contradictory and equivocal character aiming at the examination in the courts of authority's findings issued following the verification of the lawfulness of personal data processing**.

This essentially refers to the duplication of examination in the courts, during the same period, of the same acts and findings issued by the NCPDP, both in administrative proceedings and in

contravention proceedings. However, as a result of the examination of the control materials on the lawfulness of personal data processing, pursuant to Art. 27 para. (3) of the Law on personal data protection, the NCPDP issues reasoned decisions regarding the finding of the violation of the legislation in the field of personal data protection and the accumulated evidence serves as a basis for drawing up the report on the contravention, under the Contravention Code.

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

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

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

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

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

However, the circumstances described are even more bleak and disarming for the National Authority for the control of personal data processing, taking into account the number of employees of the NCPDP's sub-divisions, which is minimal in relation to the excessive volume of work.

➢ Another aspect related to the activity of representing the NCPDP in the courts in order of administrative litigation, which negatively marked the activity of the authority, **concerned the confusing situation related to the applicability of the rules on administrative litigation to the preliminary procedure**. And furthermore, the court of first instance has issued several orders in which the applications for legal action against the decisions issued by the NCPDP on the basis of Article 27 of the Law 133/2011 were declared inadmissible on the grounds that the complainants did not comply with the prior procedure, referring to Article 208 of the Administrative Code. The decisions in question were challenged by both the NCPDP and the complainants and were ultimately upheld by the Chișinău Court of Appeal, thus becoming final and irrevocable.

According to Art. 27 para. (5) of the Law 133/2011, *the controller, the processor or personal data subject may appeal the actions, inactions and the decision of the Center to the competent administrative court*. Thus, the law expressly provides for the addressing in court, without the need to carry out the preliminary procedure, provisions that come in accordance with Art. 163 let. c) of the Administrative Code. However, this procedure was conceived as a way of offering

the possibility to obtain the resolution of the dispute more quickly by recognizing the right or legitimate interest of the injured party.

In this context, it should be mentioned that, on 29 December 2021, the SCJ published the *Information Note on the judicial practice in the resolution of the issue of compliance with the prior procedure in administrative litigation*, issued in order to establish what is the factual and legal situation in the department of judicial practice and whether the courts correctly and uniformly apply the legislation on compliance with the prior procedure in administrative litigation.

The results of the generalization of the study carried out by the SCJ have shown that in all cases, when the special derogating legislative rules do not provide for a prior procedure, ***the hierarchically inferior courts incorrectly declare the actions inadmissible, pursuant to Art. 207 para. (2) let. (f) of the Administrative Code, on the grounds that the conditions specified in Art. 208 of the Administrative Code are not met.***

According to the information systematized and presented in the Information Note on the judicial practice in the resolution of the issue of compliance with the prior procedure in administrative litigation, ***the SCJ expressly and unequivocally concluded that the Law No. 133/2011 on personal data protection is part of the laws related to the Administrative Code, which does not regulate the prior procedure.***

Thus, the explanatory reasoning highlighted in the Information Note **demonstrated the legality and validity of the NCPDP's actions, in the part concerning the indication of the procedure with regard to the exercise of the right to appeal against decisions issued.**

However, despite what was presented in the Information Note of the SCJ, during the year 2022, a confusing and equivocal situation regarding the applicability of the rules on administrative litigation remained, as the opinions of the court were divided, with cases in which the court examined the legality of administrative acts issued by the NCPDP without following the prior procedure and cases in which the court indicated that the prior procedure had to be followed.

The circumstances highlighted clearly indicate the dual position of the courts in relation to the issue in question, which has certainly hindered the work of the NCPDP in the area of correct identification of the right of appeal against administrative acts issued. **Thus, not agreeing with the court's decision and, in particular, with a view to denying the violation of the right of defence of the persons concerned, the NCPDP filed appeals against the court's decisions.**

The situation was resolved with the entry into force on 5 September 2022 of Law No. 155/2022 on the amendment of some regulatory acts, which came with amendments to a number of regulatory acts, clearly establishing the procedure for filing an action in administrative litigation.

Thus, the law in question also amended Art. 27 para. (5) of Law No. 133/2011, according to which *the controller, the processor or the subject of personal data may challenge the actions, inactions and decision of the Centre directly in court, in accordance with the provisions of the Administrative Code*, **without prior procedure**.

CHAPTER IV

EXAMPLES OF CASES EXAMINED IN 2022

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

In this regard, the Authority presents, including by means of the annual activity report, significant cases and problems identified in the controls carried out on the compliance of personal data processing. Thus, among the cases examined by the NCPDP in 2022, were the following:

Non-compliant processing of personal data, materialized by accessing/consulting state information resources

- *The NCPDP received a complaint from a personal data subject, who requested verification of the lawfulness of personal data processing operations concerning him, carried out by 8 (eight) entities manifested by accessing personal data stored in several automated record systems: State Population Register (RSP), State Register of Transports (RST), Real Estate Register (RBI), etc., being more than 400 accesses. At the same time, the complainant also complained about the failure of the controllers to exercise the right of access to personal data. In these circumstances, the NCPDP ordered the examination of the lawfulness of the processing operations of the data subject's personal data carried out by each controller.*

  Thus, as a result of the investigations, with regard to three data controllers, the NCPDP found that the data controllers processed the personal data of the data subject in compliance with the requirements of Law No. 133 /2011, while in the case of five data controllers, the NCPDP found a violation of the provisions of the aforementioned Law, as the data controllers could not justify the purpose and legal basis of the processing operations of the data subject's personal data, or could not identify the data of the users who carried out certain consultation/viewing operations of the data subject's personal data and, respectively, it was not possible to identify the purpose of the processing.

  Furthermore, with regard to a data controller-legal entity, the NCPDP established that, although the complainant exercised his right of access to his personal data processed by the entity, by sending a request pursuant to Art. 13 of the Law 133/2011 to the controller, the latter did not provide him with a response to what he had requested, contrary to the aforementioned legal provisions.

  Thus, in respect of the persons concerned, minutes were drawn up on the contravention under Article 74^1 para. (1) and par. (3) and Art. 74^2 para. (1) of the Contravention Code.

- *The NCPDP has examined the complaint received from the Effective Inspection Department of the General Police Inspectorate of the Ministry of Internal Affairs, complaining about alleged unlawful acts admitted in the processing of personal data of a data subject by police employees of a territorial police inspectorate.*

  In the context, the NCPDP determined that, the characteristic and criminal record on behalf of the data subject, documents incorporating personal data extracted/collected from state information resources such as: year of birth, state identification number (IDNP), data from the registration certificate, family status, home/residence address, conduct, personal data related to traffic offences received, were issued and delivered by the person in charge of the General Police Inspectorate without a legal basis and consent of the data subject, without an address/request from the data subject or the lawyer representing his/her interests, including without a request from the court to issue these documents, actions which are contrary to the legal conditions laid down in Art. 4 para. (1) (a), Art. 5, Art. 8 and Art. 9 of the Law No. 133 of 8 July 2011 on personal data protection.

  On this basis, the NCPDP has drawn up, in respect of the person in charge concerned, a report on the infringement under Article 74[1] para. (1) of the Contravention Code.

Non-compliant processing of personal data through video surveillance system

- *During the examination of the complaint of a personal data subject regarding the alleged non-compliant processing of his personal data, the NCPDP found that the complainant's neighbour, via the video surveillance camera, processed personal data such as the voice and image of those who were/were moving in the space near the video surveillance device.*

  The video surveillance camera, being installed on the electricity pylon located opposite the house of the video surveillance system manager, monitored not only the private property of the camera manager, but also a portion of the complainant's property, as well as the public road where other persons have access. Moreover, the video surveillance camera also carried out audio recording, which is confirmed by the evidence attached to the case. Thus, the personal data processing operations were considered excessive for the alleged purpose, i.e. for the surveillance of the property and goods belonging to him.

  As a result, in this case, the NCPDP found that the video surveillance camera manager violated Art. 4 para. (1) (a), (b), (c), Art. 5 para. (1) of Law no.133/2011, with the order to stop/block the operation of processing the voice of the data subjects and to change the angle of capture of the space under surveillance, either blurring/pixelating the relevant areas and/or repositioning the location of the video surveillance device so as to capture exclusively the space belonging to the owner/manager of the camera.

  At the same time, the NCPDP determined in the actions of the person the existence of the contravention provided for in Article 74[1] para. (1) of the Contravention Code.

Unauthorised access to personal data collected through a video surveillance system

- *A complaint was received by the NCPDP from a personal data subject who requested verification of the lawfulness of the processing of his personal data by the management of a shop, which made available to strangers pictures containing his personal data, i.e. his image, pictures of his personal car (registration number), which were subsequently posted on the social network Facebook.*

  According to the case, the data subject, while driving his car in the parking lot of a store, stepped on a stray dog after leaving. Following the incident, two individuals approached the store security guard to provide video footage of the incident.

  According to the security guard, he refused to provide them with the requested information, but still allowed them to view the requested video footage. At this point, the individuals took pictures/videos from the monitor screen, which were subsequently posted on the social networking site "Facebook".

  It should be pointed out that the security guard, by his actions, allowed strangers to view the images recorded by the video surveillance system installed in the perimeter of the shop, in which order he did not ensure the confidentiality of personal data. However, the monitoring or viewing of images in the areas under surveillance must be limited to authorised staff.

  Given the circumstances of the case, the NCPDP found that the security guard, a person with the right of access to the video surveillance system, was under an obligation to ensure the confidentiality of personal data in order to comply with the internal regulations and the job description, but his actions in giving strangers access to/viewing the video recordings collected by the video surveillance system installed in the perimeter of the store was contrary to the provisions of Article 4 para. (1), Art. 5 para. (1) and Art. 29 of the Law on personal data protection.

  Furthermore, by allowing the viewing of video recordings, for which the guard was responsible, he facilitated the dissemination of personal data in the public area.

  Thus, a report was drawn up on the person in question for an infringement under Article 74[1] para. (1) of the Contravention Code.

Disclosure of personal data via social networks

- *The NCPDP, while examining the complaint of a personal data subject concerning the alleged improper processing of personal data concerning him by his wife, noted that the latter, being a user of the social network "Facebook", posted on her page several photos of the complainant's identity documents, which reflected his personal data, namely: first name, surname, patronymic, IDNP, home address, criminal record without the consent of the complainant.*

  As a result, the NCPDP found a violation of Art. 4 para. (1) (a), (b) and Art. 5 para. (1) of Law No. 133/2011 by the person who posted on his "Facebook" page the images of the documents containing the complainant's personal data.

At the same time, in the actions of the person it was determined the existence of the contravention provided for in Article 74[1] para. (1) of the Contravention Code.

- *During the examination of the complaint of a personal data subject regarding the alleged non-compliant processing of his personal data, the NCPDP found that a user of the social network "Facebook", a civic activist, had posted on his page a video recording containing personal data of the complainant without his consent, namely: his first name, surname, home address, date, month, year of birth and telephone number. The complainant's data was obtained by video recording with a mobile phone, while one of the parties was taking knowledge of the case materials in a file to which the civic activist was not a party. The online collection and dissemination of personal data took place on the premises of the court.*

  As a result, the NCPDP has determined that the interest of the natural person not to have his personal data disclosed prevails over the interest of the general public to know this information, qualifying these personal data processing operations as non-compliant, in relation to the principles of personal data protection, as set out the Law No 133/2011 on personal data protection, being found in violation of Art. 4 para. (1) (a), (b), Art. 5 para. (1) and Art. 29 para. (1) of the Law No. 133/2011 by the person who posted on his "Facebook" page the images containing the personal data of the complainant.

  In addition, in view of the lack of cooperation with the authority shown by the person who published the above-mentioned data on the social network, by not providing the information requested in the examination of the case complained of, it was found that there was a violation of Art. 20 para. (3) of the Law No.133/2011. At the same time, a report was drawn up on this person regarding the contravention for committing the acts provided for in Article 74[1] para. (1) and Art. 74[2] para. (1) of the Contravention Code.

Non-compliance with organisational and technical measures necessary for personal data protection

- *The NCPDP, in the course of examining the complaint of a personal data subject concerning the allegedly unlawful processing of his personal data, found that 2 employees of a public authority, contrary to Art. 30 para. (1) of the Law No. 133/2011 and the internal regulations of the authority, which prohibited the use of applications on non-governmental platforms and personal e-mails, used the application "Telegram" and personal e-mail for the transmission of official documents containing personal data.*

  As a result of the control carried out, it was found that the employees of the authority concerned violated the provisions of Art. 4 para. (1) (a) and Art. 30 para. (1) of the Law No. 133/2011. At the same time, they were issued with administrative fines for committing the offence referred to in Article 74[1] para. (1) of the Contravention Code.
- *The NCPDP, while examining the material submitted by one of the police inspectorates, concerning the complaint of a data subject regarding the alleged non-compliant processing of his personal data, initiated a self-investigation on the facts set out in the complaint and found that a doctor from a Public Health Centre (PHC), with the consent of his manager, without being technically secured at that time by the latter with government tools/platforms on the*

subdomain "@gov. md", via non-governmental electronic mail, transmitted to several family doctors a list containing the data of persons who had crossed the state border, namely: name, surname, date, month, year of birth, IDNP, sex, address and telephone number, which led to the disclosure by transmission of information constituting personal data, contrary to the provisions of Art. 4 para. (1) (a), Art. 29 para. (1) and Art. 30 para. (1), para. (3) let. a), b) of the Law No. 133/2011.

As a result, the NCPDP has determined in the actions of the head of the PHC the existence of the contravention provided for in Art. 74[1] para. (1) of the Contravention Code.

Non-compliant processing of personal data stored in the Real Estate Register

- *Following investigations carried out by the NCPDP, a decision was issued finding non-compliance of personal data processing by a local public authority (LPA) in relation to two data subjects, where the authority had accessed their personal data stored in the Real Estate Register (RBI) in an uncompliant manner.*

  As a result of the actions taken, it was found that the LPA, as personal data controller, did not comply with the necessary organisational and technical measures for the personal data protection and did not update the list of employees entitled to access the information stored in the RBI.

  At the same time, the data controller did not notify the Public Services Agency about the modification of the list of users with access rights to the information in the Central Data Bank (CDB) of the real estate cadastre, and did not block the access rights of the user - a former employee, but, following the end of his employment, his access rights to the CDB remained active. Moreover, these actions/inactions led to the fact that several employees of the concerned LPA's subdivisions continued to use the data (username/password) of the former employee to access the information system, not being authorized users with access rights to the information in the CDB, which made it impossible for the LPA to identify the user/employee who accessed the personal data.

  The LPA also failed to keep a record of the access/consultation of personal data through the CDB of the real estate cadastre, by recording the exact date and time of personal data processing, indicating the purpose, legal basis and necessity of the operation carried out, specifying the record system from which they were processed, the categories of data processed and, consequently, the personal data of the complainants were processed without the existence of a legal purpose and basis.

  As a result of the examination of the complaint, the NCPDP found a violation of the provisions of the Law No 133/2011 on personal data protection. In addition, the NCPDP obliged the local public authority to take all necessary measures regarding the amendment of the users' right of access to the system; to inform the P.I. "Public Services Agency" about the change of users;

to establish a mechanism for keeping manual and/or electronic records of access/consultation of personal data by authorized users, as well as to instruct subordinate employees about not allowing unauthorized access/use of personal data in the managed record systems.

The NCPDP does not doubt or deny the right of the local public authority to collect/access/consult or verify personal data from various information systems, including those relating to the real estate of individuals, which are necessary for the performance of the tasks resulting from the exercise of the prerogatives of public authority with which it is empowered, but all these potential personal data processing operations shall be carried out in compliance with all the principles of personal data processing set out in the Law 133/2011 on personal data protection.

- *A data subject, following the receipt of the access history in the Real Estate Register (RBI) of his personal data, complained to the NCPDP about the access actions as being carried out without a lawful purpose and basis, as well as without his consent.*

  Thus, during the examination of the case, the NCPDP found that a lawyer had accessed personal data in the RBI in the absence of a contract for the provision of information services signed with the Public Services Agency (ASP), which could possibly have included the accesses made in the RBI within the legal provisions.

  It should be noted that open information about the real estate contained in the Real Estate Cadastre can be accessed by any applicant through the e-Cadastre information portal, for example: type of object, cadastral number, address, mode of use, surface area of the property.

  At the same time, the information about the holder/owner of the property is not open and can only be accessed by authorised users, based on the contract concluded with the ASP, following authentication in the system by logging in, or, in the case where the authorised user accesses the information about the owner of the property, this personal data processing operation is reflected in the audit/access log, which can subsequently be presented by the ASP to the personal data subject. Open data accesses are not recorded by the nominated system.

  In addition, during the examination of the case in question, it was noted that, according to the audit provided by the ASP, the accesses complained of were carried out by another controller who had signed the contract for the provision of information services with the agency in question. Moreover, the lawyer confirmed that he had access to the RBI on the basis of the access password provided by an employee of the former S.I. "Cadastru", without having any contract for the provision of information services with the S.I. "Cadastru" or ASP. As a result of the control carried out, the NCPDP found a violation of Art. 4 para. (1) letter a) of the Law No. 133/2011 on personal data processing.

  In this context, the NCPDP notified the ASP about the irregularities found in the processing of personal data by ASP employees (institution, which following the reorganization has fused with ÎS Cadastru).

Personal data processing of political party candidates through publication/disclosure on the website of the electoral bloc

- *The NCPDP initiated a self-investigation on the publication by the president of an electoral bloc, online and in the mass-media, of information on the criminal records of counter-candidates for the position of deputy from a political party.*

  Thus, it was established that, according to the materials accumulated in the administrative procedure, the images posted by the president of the electoral bloc contained an excessive amount of personal data of the candidates for the position of deputy in the Parliament of the Republic of Moldova, for example: "name, surname of the subjects, date, month, year of birth and data from the Register of forensic and criminological information".

  Following the examination of the case, the NCPDP was unable to identify the legal basis that would justify the disclosure of the special category of personal data of the political party's candidates for the parliamentary elections by the president of the electoral bloc by publishing/disclosing them on the website, as well as on the „YouTube" channel. Consequently, following the control of the compliance of personal data processing, the personal data protection authority issued the decision on the finding of violation of the provisions of Articles 4, 5 and 29 of the Law No. 133/2011 on personal data protection, when processing personal data of the candidates of the political party by publishing/disclosing them on the website of the electoral bloc, as well as on the „YouTube" channel.

  The NCPDP has also ordered the erasure of images/videos, where information on the criminal records of some candidates for the position of deputy was illustrated/exposed.

CAPITOLUL V

RECOMMENDATIONS AND OPINIONS OF THE NCPDP

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

Thus, in 2022, several recommendations and opinions have been issued aimed at the society, including:

Guidelines on the processing of personal data through video-surveillance systems

These guidelines contain best practice recommendations for the use of video surveillance devices that provide the possibility to view or record images of individuals and may also refer to other personal information collected and stored by companies/institutions on natural persons. The processing of personal data held by companies/institutions is regulated by the Law 133/2011 and the guidelines in this document will help these companies/institutions understand their responsibilities and obligations in terms of data protection when using video surveillance means. Data protection legislation not only establishes obligations for controllers/processors but also gives to natural persons rights, such as: the right to access personal data or to have it deleted when retention is no longer necessary, insofar as the derogations do not apply.

The basic legal requirement for all controllers/processors is to comply with the provisions of the Law no 133/2011. The guidelines aim to provide guidance on how these legal requirements can be met and are addressed to a large number of potential users. This is because the Law No 133/2011 applies to all controllers/processors processing personal data in both the private and public sector.

The recommendations in these guidelines are based on the principles of personal data protection that are at the basis of personal data protection legislation and have been established to follow the life cycle and practical operation of video surveillance systems.

Some sections of these guidelines address issues that should be considered by controllers/processors to ensure that best practice recommendations would be fulfilled.

Due to the extensive and voluminous nature of these guidelines, their full text is not included in this report and can be viewed by accessing the link:

https://datepersonale.md/wp-content/uploads/2022/12/Linii-directorii-in-supraveghere-video-1.pdf

Considerations in relation to the increasing use of video surveillance systems with audio recording functions

According to the provisions of the Law No. 175/2021 on the amendment of some normative acts, the obligation of the controller to notify the NCPDP of personal data processing operations has been excluded, as well as it was established the obligation for the controller to carry out an data protection impact assessment, if the data processing is likely to result in an increased risk to the rights and freedoms of individuals, including the obligation to designate a data protection officer.

Consistently, Article 1 of the Law No. 133/2011 on personal data protection states that its purpose 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 inviolability of intimate, family and private life.

The possession and use of video means and/or the processing of personal data through them must be compatible with and appropriate to the tasks and duties of the controller and may take place only for the purpose of ensuring the security of persons and property, the security and protection of property, buildings, assets and materials under a special regime, while complying with the obligations of the entity as a controller, as laid down by law and the security measures adopted for personal data protection, the protection of privacy, legitimate interests and the safeguarding of the fundamental rights of data subjects.

On the same dimension of approach, we draw attention to the fact that the installation of a video surveillance system that could collect voice (audio recording) will affect the right to privacy of employees and visitors of personal data controllers or other persons who fall within the range of their capture for the following reasons:

a. *According to Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interference or attacks.*

b. *Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter - ECHR) states that everyone has the right to respect for his private and family life, his home and his correspondence.*

c. *Article 7 of the Charter of Fundamental Rights of the European Union regulates respect for private and intimate life. At the same time, Article 8 of the Charter states that everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly, for the purposes specified and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*

d. *The Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereinafter - Convention No 108) applies to all cases of data processing in the public and private sectors and protects the individual against abuses that may accompany the processing of personal data.*

e. *Further, recital 84 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27.04.2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter - GDPR) provides that [... where personal data processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for carrying out a data protection impact assessment assessing, in particular, the origin, nature, specificity and gravity of that risk ...].*

f. In addition, we refer to the following reasoning mentioned in ***Opinion No 2/2017 on data processing at work, adopted on 08.05.2017 by the Article 29 Data Protection Working Party*** *(available at: https://ec.europa.eu/newsroom/article29/items/610169/en), according to which "modern technologies allow employees to be tracked over time, from one workplace to another and in their homes, through many different devices, such as, smart phones, desktop computers, tablets, vehicles and wearable devices. If there are no limits on processing, and if the processing is not transparent, there is a high risk that the legitimate interest of employers in improving the efficiency and protection of companies' assets will turn into unwarranted and intrusive monitoring. [...] In addition, due to the capabilities of such technologies, employees may not know what personal data are being processed and for what purposes, while at the same time they may not even be aware of the existence of the monitoring technology itself".*

g. ***Point 129 of Guideline No 3/2019 on data processing by video-surveillance means****, approved at the Plenary Meeting of the European Data Protection Board (available at: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019 processing-personal-data-through-video_en) states that, "when selecting technical solutions, the controller should also consider privacy-friendly technologies, as they enhance security. Some examples of such technologies are systems that allow masking or distortion of areas irrelevant to surveillance or the removal of images of third parties from the recording when video recordings are made available to data subjects. On the other hand, selected solutions should not offer functions that are not needed (e.g. unlimited camera movement, magnification capability, radio transmission, analytics and audio recording). Functions that are offered but not needed should be disabled."*

h. *Article 28 of the Constitution of the Republic of Moldova provides that the State shall respect and protect private, family and private life. At the same time, Art. 54 para. (2) and (4) of the Constitution of the Republic of Moldova stipulates that the exercise of rights and freedoms may not be subject to restrictions other than those provided for by law, which correspond to the unanimously recognised norms of international law and are necessary in the interests of national security, territorial integrity, economic well-being of the country, public order, for the prevention of mass disturbances and crimes, for the protection of the rights, freedoms and dignity of other persons, for preventing the disclosure of confidential information or for guaranteeing the authority and impartiality of justice. The restriction must be proportionate to the situation giving rise to it and may not affect the existence of the right or freedom.*

i. *Consistently, we emphasize that the controller has the obligation to respect and ensure the implementation of the provisions of Art. 4, 5, 23 - 25, 29 para. (1) and 30 par. (1) of the Law no. 133/2011. Based on the above provisions, the processing of the personal data category such as voice (audio recording) by means of a video surveillance system and the use of handheld/mobile devices by the controller are excessive in relation to the purposes of personal data processing*

considering that they represent a greater interference into the privacy of the monitored persons, namely, the employees and visitors of the public and/or private entity, which involves the recorded and reproducible documentation of the conduct of employees at work and/or visitors.

j. *In this context we underline that the case law of the European Court of Human Rights (hereafter - the Court) has examined numerous situations where data protection issues have arisen through the prism of video surveillance:*

- In the Niemietz v. Germany case of 16.12.1992 (available at: https://www.echr.coe.int/Documents/FS_Workplace_surveillance_RON.pdf.), the Court held that Article 8 of the ECHR offers protection to a person not only in his private circle but also during and in the course of his professional activity;
- In the case of S. and M. Marper v. United Kingdom of 04.12.2008 (available at: https://www.echr.coe.int/Documents/FS_Workplace_surveillance_RON.pdf, the Court found that interference with respect for the right to privacy must be proportionate to the purpose of personal data processing;
- In the case Antović and Mirković v. Montenegro of 28.11.2017 (available at: https://www.echr.coe.int/Documents/FS_Workplace_surveillance_RON.pdf), the Court found that "video surveillance at the workplace constitutes an invasion of the employee's (teacher's) privacy, since university lecture halls are the places where teachers work, where they not only teach but also interact with students, establishing relationships and building their social identity";
- In the case Allan v. United Kingdom of 05.11.2002 (available at: https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001140543&filename=CASE%20OF%20ALLEN%20v.%20THE%20UNITED20KINGDOM%20%20%5BRomanian%20Translation%5D%20by%20the%20COE%20Human%20Rights%20

Trust%20Fund.pdf&logEvent=False), since at that time there was no legal system regulating police use of secret recording devices, the interference was not in accordance with the law. The Court found that the use of audio and video recording devices in the plaintiff's cell, in the prison visiting area and in the vicinity of another prisoner infringed the plaintiff's right to privacy.

k. We also bring into focus the case law of other personal data protection authorities regarding non-compliant processing of personal data by means of video surveillance, such as:

- Administrative fine of 72,000 EUR imposed by the Finnish Data Protection Authority against the company "Taksi Helsinki Oy" (available at: https://datepersonale.md/buletin-informativ-nr-5/) for processing personal data of its drivers, staff and customers with a surveillance system, which records both video and audio, which was not in line with the GDPR principle of data minimisation.
- A fine of 2,000 EUR imposed by the Swedish Data Protection Authority on a Homeowners' Association (available at: https://datepersonale.md/amenda-de-2-mii-de-euro-aplicata-de-catre-autoritatea-suedeza-pentru-protectia-datelor-pentru-supravegherea-video-si-audio/) that placed four cameras in the apartment block (one at the main entrance to the staircase, two in the staircase area and one in the storage area) processing both images and sounds.

At the same time, it was held that for the capture of images, through sound recording, it is necessary to demonstrate an objective reason justifying an additional intrusion into the privacy of individuals through the processing of personal data and through audio, not only video monitoring. This means that any homeowners' association, if it wants to record sounds via an audio/video camera in addition to filming, must ensure that there are additional justifiable reasons for this. If the objectives pursued could only be achieved by capturing images, then audio recording is not justified.

- The National Supervisory Authority for Personal Data Processing in Romania has issued two warnings and two fines of 5,000 EUR to Entirely Shipping &Trading S.R.L. (available at:https://www.dataprotection.ro/?page=O_noua_sanctiune_pentru_incalcarea_RGPD_2020_3&lang=ro) for violating the provisions of Article 5 para. (1) (a), (b), (c) and (e), 6, 7, 9, 12 and 13 of the GDPR. As a result of the investigation, the following was found:

a) the controller has not demonstrated a justified legitimate interest in the video surveillance system installed on its premises overriding the interests or fundamental rights and freedoms of the data subjects, has not demonstrated that the trade union or, where appropriate, the employees' representatives were consulted prior to the introduction of the monitoring systems, and that other less intrusive ways and means of achieving the employer's aim have not previously proved effective.

b) the controller has not demonstrated the existence of adequate data protection policies and the implementation of appropriate technical and organisational measures to ensure a level of security appropriate to this risk;

c) the processing of biometric data through the access control system was not collected for purposes that were adequate, relevant and limited to what was necessary in relation to the purposes for which they were processed;

d) the controller has not carried out a data protection impact assessment.

At the same time, we inform that the NCPDP has examined cases concerning the legality of personal data processing by means of video surveillance system, also making audio recordings. In this context, during the examination of a petition filed by a data subject, the NCPDP issued a decision finding a violation of the provisions of Article 4 para. (1) (a), (b), (c), Art. 5 para. (1) of the Law No. 133/2011 regarding personal data processing of the complaint, in connection with the collection/recording of the voice of the data subject, without his consent, by means of the video surveillance camera, installed on an electric pole, which included both the property of the video surveillance system manager and a portion of the area not belonging to the latter, without identifying the determined, explicit and legitimate purpose, the causal link between the purpose and the complaint's processed data, the proportionality, fairness and consistency with the legal rules in the field of personal data protection. Therefore, taking into account the above, the NCPDP held that before installing a video surveillance system, the data controller must always critically examine whether this measure is, firstly, adequate to achieve the intended purpose and, secondly, proportionate and necessary for its purposes, in relation to the interests or fundamental rights and freedoms of the data subject. Therefore, the audiovisual recording by the data controller in question, by means of the video surveillance camera, without the consent of the data subject, constituted an excessive and

disproportionate measure in relation to the stated purpose, in this case, ensuring the security of property.

Thus, based on the above, we note that any natural or legal person, by public law, or by private law, is entitled to own and use video means provided that the requirements of the legislation on personal data protection are met, namely: ensuring the basic conditions for the processing of personal data; data protection impact assessment, where the processing is likely to result in an increased risk to the rights and freedoms of individuals; designate the data protection officer; realising the rights of personal data subjects; organisational and technical measures necessary to ensure the confidentiality and security of personal data.

➢ *Recommendations for video surveillance installation service providers to provide advice to end-users when installing video surveillance systems*

The collection of images capturing natural persons, by means of a video surveillance system both in cases where they record and in cases where real-time transmission takes place, constitutes a form of processing of personal data within the meaning of Article 3 of the Law No. 133/2011 on personal data protection.

In this context, we note that any natural or legal person, by public law, or by private law, who, individually or jointly with others, establishes the purpose of personal data processing of to be a specific, explicit one, consisting in the need to ensure the security of persons, premises and/or property, as well as the (automated) means of personal data processing by means of video surveillance devices, obtains the status of personal data controller.

For example, controller status is attributed to the following entities:

- A condominium co-owners' association (hereafter – A.C.C) decided to ensure the security of the building by installing a video surveillance system;
- A company owning a private car park decided to install a video surveillance system to prevent theft from its customers' cars;
- A medical institution has decided to ensure the security of goods and persons by installing a video surveillance system in its corridors and staircases.

In view of ensuring the security of persons, premises and/or property, as well as the costs of installing video surveillance systems, many controllers use the services provided by economic agents, where by the services they offer, should know and inform their customers (beneficiaries) about the rules for processing personal data by means of video surveillance systems, provided for by the Law No. 133/2011, before providing services for the installation of video surveillance systems, as follows:

General requirements for controllers who have decided to install video surveillance systems

Video surveillance means are used with a legal basis for personal data processing and a well-defined purpose.

Access to video images is achieved through encryption devices or, if this is not possible, multi-factor authentication, not just passwords.

The use of hidden or concealed video surveillance means is prohibited, except for the cases expressly provided for by law.

Restricting unauthorised third-party access to data obtained through the video surveillance system.

Data storage equipment is located in a separate, fully secure place.

It is recommended that the storage period for processed video images to be a maximum of 30 days. It is forbidden to keep the images for a period exceeding the period set for the purpose, except for the situations expressly regulated by law or in duly justified cases.

The icon shall be displayed in visible places where the cameras are located and it shall contain information on: contact details of the data controller; purpose, legal basis of the processing; recipients of the data collected; storage period; transfer of data; rights of the data subject and how to exercise them.

It is not recommended that the pictogram contains the contact details of economic agents providing services for the installation of video surveillance systems, as the subjects concerned will classify the entity indicated on the pictogram as a personal data controller.

Controllers and/or processors *(e.g. the company maintaining the video surveillance system*) comply with security and confidentiality measures in accordance with Art. 29 and Art. 30 of the Law No. 133/2011.

The personal data controller and the processor shall designate a data protection officer, taking into account the provisions of Art. 25 of the Law No. 133/2011.

Where the purpose of personal data processing is *the systematic, large-scale monitoring of a publicly accessible area*, a personal data protection impact assessment shall be carried out.

It is recommended that the opinion of the data protection officer to be sought when conducting the data protection impact assessment.

Aspects of video surveillance on the area of private property (apartment, house, household yard)

The personal data processing by means of a video surveillance system, used exclusively for personal or family needs, **is exempted from the applicability of the Law No. 133/2011** (Art. 2 para. (4) let. c)). In this situation, the processing in question may only take place if the video cameras are positioned in such a way that the angle of capture of **the video images exclusively encompasses the area held by title of ownership or use**, where **the personal data processing is deemed to take place for personal or family needs**, and if **the rights of the subjects whose data are processed through this system are not affected.**

Video devices shall be positioned in such a way that the angle of capture of the video images encompasses the area of the property or use.

It is not recommended that video devices are directly aimed at the adjacent public area *(e.g. building, street, pavement and other parts of the public road*) or the adjacent private area, which does not belong to the controller with private property and/or use rights (*e.g. yard, windows of buildings or neighbor's garage*). In these situations, where the angle of capture of the video images cannot be changed, excessive areas shall be blurred so that the cameras capture exclusively the space owned by the owner or user, with the capture of adjacent public or private area being reduced to a minimum.

It is recommended that only one family member has access to data storage equipment and video images.

The written consent of the data subjects is required in case that the video cameras' capture angles include the private property of other people in the neighborhood (houses, neighbors' yards).

It is prohibited to publish on the Internet the images captured by means of video surveillance systems, as well as their disclosure to other persons, except to the law enforcement bodies, under the conditions of the legislation in the field of personal data protection.

Aspects of video surveillance by condominium co-owner associations (A.C.C)

The decision to install a video surveillance system within the A.C.C. shall be voted at the general assembly after meeting the conditions established by the Law No. 913/2000 of the condominium in the housing fund (in force during the reporting period, or, on January 29, 2023, the Law No. 187/2022 regarding the condominium entered into force), namely, with the vote of 2/3 of the total votes of the owners or at least by their simple majority, recorded in the minutes of the general assembly of A.C.C. members.

It is prohibited to point video devices directly at the *apartment doors of inhabitants/ neighbors,* to capture images from inside the homes of the data subjects.

Video cameras can be placed in the parking lot/parking spaces reserved exclusively for A.C.C. owners/members.

Cameras should not be placed in public areas: *sidewalks, driveways and other areas adjacent to parking lots.*

It is not recommended to install a video surveillance system that may collect the voice (audio recording) of data subjects, except as authorized by the law.

Data storage equipment must be located in the business office used by the A.C.C. management or in a separate and fully secured area.

The access to personal data processed by the video surveillance system shall be granted to a person designated by a decision of the general meeting of the A.C.C., with clear and precise written instructions on the principles of personal data processing.

The access to data storage equipment and video images is not recommended for all inhabitants.

Video surveillance of common areas in the condominium is allowed, such as: *the halls of the residential blocks, the access area in the block, the access to the elevator, the staircase leading to the first floor.*

Aspects of video surveillance by owners with common ownership in shares

It is only admitted to direct the video cameras towards the property forming the object of the joint ownership in shares on the basis of the majority consent of the subjects concerned, confirmed by a document to this effect.

It is forbidden to direct video surveillance means directly towards the adjacent public space (*e.g. adjacent rooms, street, pavement and other parts of the public road*) or the adjacent private space.

Access to the data processed by the video surveillance system shall be granted to a designated person within the joint ownership on the basis of a document and with clear and precise written instructions on the principles of data processing by the video surveillance system.

Aspects of video surveillance of legal person governed by public law, or by private law.

It is allowed to direct the cameras towards real estate belonging to the personal data controller with private ownership and/or right of use (*e.g. hallways, stairs, lift access, meeting rooms, indoor/outdoor parking*).

It is forbidden to point cameras directly at neighboring real estate (*e.g. windows, adjacent buildings, streets, pavements*). In these situations, if the angle of capture of the video images cannot be changed, excessive areas should be blurred so that they capture exclusively the space owned or used by the owner, with the capture of adjacent public or private space being reduced to a minimum.

It is not recommended to install a video surveillance system, which may collect the voice (audio recording) of data subjects, except for the cases authorized by law.

Video images filming the employees' entire workspace shall be blurred or the camera angles shall be redirected in such a way that the employees' workspace is not visible, in particular the employees' computing equipment, including their work devices (keyboards).

The access to the data processed by the video surveillance system shall be granted to authorised persons (*system administrator and management as well as representatives of the company maintaining the system (if applicable), as well as the system administrator*) and designated by the management of the data controller (*on the basis of the individual employment contract or order*).

The monitoring of areas commonly used for recovery and recreation activities, including sanitary groups, and places where individuals reasonably expect privacy is prohibited.

➢*Guidelines on Personal Data Protection Impact Assessment (DPIA)*

The personal data protection impact assessment is a process designed to describe the envisaged processing operations, to assess their necessity and proportionality and to contribute to the management of risks to the rights and freedoms of data subjects resulting from the personal data processing by assessing them and establishing measures to mitigate them.

The Data Protection Impact Assessment is an important tool for accountability as it helps personal data controllers not only to comply with the requirements of the Law 133/2011 on personal data protection, but also to demonstrate that adequate measures have been taken to ensure compliance with national as well as European legal provisions - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC.

In other words, data protection impact assessment is a process for **strengthening/building** and demonstrating compliance. A data protection impact assessment should ideally be carried out in the design phase of a new record-keeping/database system involving the personal data processing, and subsequently reviewed when the requirements of the record-keeping/database system and/or legal obligations change.

In order to ensure compliance with the Law No. 133/2011, where the processing is likely to result in an increased risk to the rights and freedoms of natural persons, the controller is responsible for conducting a data protection impact assessment to determine/estimate, in particular, the origin, nature, specificity/particularity and severity of that risk.

It is particularly relevant to carry out a data protection impact assessment when a new personal data processing technology is introduced and if the data protection impact assessment has not been previously carried out by the controller or if it becomes necessary in view of the time that has passed since the initial processing. In such cases, the controller must carry out a data protection impact assessment prior to the processing in order to evaluate/assess the likelihood and severity of the risk, taking into account the nature, purpose, context, objectives of the processing and sources of risk. This data protection impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged to mitigate this risk in order to ensure the personal data protection and to demonstrate the compliance of the personal data processing of with applicable law.

Where a data protection impact assessment indicates that personal data processing operations involve an increased risk which the controller cannot manage by appropriate measures, taking into account available technology and implementation costs, prior consultation with the National Centre for Personal Data Protection is required prior to processing.

Given the extensive and voluminous nature of the guide, the full text cannot be included in this report, or can be viewed by visiting the following link:

https://datepersonale.md/wp-content/uploads/2022/12/Ghid-privind-evaluarea-impactului-asupra protec%C8%9Biei-datelor-2-1.pdf

During 2022, the NCPDP also addressed other important issues to ensure that society is informed in order to prevent the unlawful processing of personal data. In this regard, in the context of the continued identification of practices of limiting access to information with unfounded invocation of personal data protection legislation, the Authority presented the following considerations:

The NCPDP has repeatedly highlighted the problem of abusing the legal provisions in the field of personal data protection, especially by representatives of public authorities, when allegedly arguing the refusal to provide information requested in order to realize the right of access to information.

In particular, when requests for access to information, submitted on the basis of the Law on Access to Information, concern (but are not limited to those indicated below) statistical data, confirmation/denial of the occurrence of certain events, names of enterprises/economic agents, state budget figures/expenditure, etc., data which do not or cannot lead to the identification of a personal data subject, the provisions of the Law on personal data protection of cannot be invoked as a reason for not providing the information.

Such situations are regrettable, or they affect the field of personal data protection both in terms of image and applicability, generating misinterpretations of legal norms in the field and unfounded insinuations aimed at hindering access to information.

In this context, in order to 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 personal data processing, including by ensuring a balance between the legal provisions related to the rights of access to information and the personal data protection, the NCPDP has developed and posted on its official website, https://datepersonale.md/, *Guidelines on access to information through personal data protection legislation*.

In addition, in the context of the publication of the above-mentioned communication, taking into account the reaction of some media institutions, which highlighted the fact of misinterpretation of the message conveyed, the NCPDP wished to state the following reasoning:

The message aimed to facilitate the right of access to information and to prevent the use of abusive practices, in particular by representatives of public authorities, to limit the right of access to information by unfoundedly invoking personal data protection legislation.

It was reiterated that the NCPDP does not intend to restrict the right of access to information or create the conditions for such restrictions. On the contrary, the NCPDP has called on all information providers containing personal data not to restrict access to information by using the field of personal data protection as an unfounded cover.

The guidelines on access to information through personal data protection legislation are of a general advisory/guidance nature and are addressed to both information providers and information seekers, in the public and private sector, without being addressed specifically to media representatives.

It should be emphasised that the position set out in the above mentioned document incorporates recommendations, which may constitute a point of reference for decision making by personal data controllers, but does not constitute a binding solution for them, since in the view of the

decision-making autonomy of the information provider and in the view of the principle of accountability of the personal data controller, they are to decide independently and individually on the provision or refusal to provide the information requested by natural or legal persons, or, under the Access to Information Law, if a person considers that his or her rights or interests have been infringed, he or she may challenge the actions or inactions of the information provider in court.

Moreover, despite what has been invoked in the public space by media representatives, it will be pointed out that the guidelines refer to the following quote:

"... As indicated above, following from the provisions of Art. 8 of the Law on Access to Information, access to information containing personal data is to be carried out in compliance with the principles laid down in Art. 4 of the Law on personal data protection. In this regard, the applicant for such information with limited accessibility shall indicate in his request for access, in the light of Art. 4 and Art. 5 or Art. 10 (if the journalistic purpose is invoked) of the Law No. 133 of 08.07.2011 on personal data protection...".

"Therefore, if the controller determines that the requested information represents an enhanced interest or even that there is a public interest in the information being known, the provisions of Art. 10 of the Law on personal data protection will be applied."

The current wording of Article 10 of the law in question states that the provisions of Art. 5, 6 and 8 do not apply where the processing of personal data is carried out solely for journalistic, artistic or literary purposes, if it relates to data which have been voluntarily and manifestly made public by the subject of the personal data or to data which are closely linked to the public person's status of the subject of the personal data or to the public nature of the facts in which he or she is involved, in accordance with the Freedom of Expression Law.

Respectively, the law does not provide for exceptions to the other legal provisions, including Art. 4, Art. 29 and Art. 30, to be respected by media representatives, but the personal data requested must correspond to the stated purpose, as well as being adequate, relevant and non-excessive in relation to that purpose, ensuring the confidentiality and security of the data that have become known to them, arising from the need to ensure a fair balance between the right to personal data protection and the right of society to information/right of access to information.

Thus, in order not to perceive both the field of personal data protection and the Personal Data Protection Authority as alleged instruments for creating impediments to the realization of the right of access to information by media representatives, the NCPDP expressed its openness and readiness to discuss the issues that were apparently misperceived from the documents posted on its website and to come up with clarifications in this regard.

CHAPTER VI

ACTIVITY OF SURVEILLANCE OF PERSONAL DATA PROCESSING

Completion of the notification activity of the NCPDP regarding the processing of personal data *(registration of controllers and personal data filing systems in the Register of evidence of personal data controllers)*

Following the publication in the Official Gazette of the Republic of Moldova of the Law No. 175/2021 on the amendment of some normative acts, amendments were made including to the Law No. 133/2011 on personal data protection, which directly concerns the activity of the NCPDP, thus being repealed from para. (1) of Art. 20 (b), (f) and (p), as well as amended let. (h) of the same paragraph. Art. 23 - 25 have also been amended and Art. 28 of the Law repealed.

The above-mentioned provisions, in the old wording, stipulated the requirements for compliance with the notification and authorisation procedure for personal data processing operations carried out by data controllers. In this respect, the powers of the supervisory body to receive and analyse notifications from data controllers and to issue a decision on whether or not to authorise the processing of personal data were excluded.

The fundamental change is that data controllers no longer have to submit a prior notification or prior authorisation request to process personal data. Instead, they will have to verify the lawfulness of the processing themselves and implement adequate safeguards to protect personal data. The effectiveness of the measures taken will be monitored by the NCPDP.

Accordingly, it should be noted that the Law No. 175/2021 has come with new legal obligations in terms of ensuring compliance of the processing of personal data by controllers, namely:

- Conducting the data protection impact assessment;
- Prior consultation;
- Designation of the data protection officer.

In this context, it should be noted that during the years 2012-2021, when the Register of evidence of personal data controllers was operational, the NCPDP examined **8848** notifications submitted by data controllers, and a total of **3479** data controllers and **6026** personal data filing systems were registered, while **2823** filing systems were refused registration.

These figures denote the fact (highlighted including in recital 89 of the General Data Protection Regulation 2016/679) that the general obligation to notify the processing of personal data to the supervisory authority has generated administrative and financial tasks, but has not always contributed to improving personal data protection. Therefore, such general undifferentiated notification obligations needed to be repealed and replaced by effective procedures and mechanisms that focus instead on those types of processing operations likely to generate a high risk to the rights and freedoms of natural persons themselves by their nature, scope, context and purposes.

However, it should be noted that due to the notification procedure, data controllers, especially those who process large volumes of personal data, including special categories of data, have carried out a series of actions in the context of compliance with the process of personal data processing to the principles of personal data protection, being:

- identified and regulated personal data filing systems;
- established the organizational and technical measures necessary for the personal data protection;
- designated personal data officers responsible for the data security policy, as well as for the filing systems managed by the data controller, etc.

At the same time, it should be noted that, regrettably, the changes brought by the Law No. 175/2021 in the field of personal data protection did not establish the obligation to keep records of personal data processing activities, provided by Art. 30 of the General Data Protection Regulation 2016/679, by which the European legislator replaced the notification process.

Additionally, in the context of the intervention of the changes mentioned above, it should be noted that, according to Art. XVIII para. 7 of the Law No. 175/2021, Art. 28 (*entitled "Register of evidence of personal data controllers")* of the Law No. 133/2011 on personal data protection was repealed, in which order, according to Art. XXXI para. (2) of the above-mentioned law, within 60 days from the date of entry into force of the mentioned law, NCPDP was to ensure the liquidation of the Register of evidence of personal data controllers by the irreversible destruction of documents and information stored on paper and those stored electronically.

In this context, we point out that the establishment and functioning of the Register of evidence of personal data controllers has been regulated by means of normative acts adopted by the Government, namely: Government Decision No 883 of 25 November 2011 on the approval of the technical concept of the automated information system "State Register of personal data controllers" and Government Decision No. 296 of 15 May 2012 on the approval of the Regulation of the Register of evidence of personal data controllers.

Consequently, in accordance with the provisions of Art. 18 para. (1) of the Law No 71/2007 on registers, the decision on the liquidation of the state register shall be adopted by the public authority that established the register. According to para. (3) of the same article, the decision on the liquidation of the register shall stipulate the manner of transmission of data and documents to the archive or the manner and deadlines for the destruction of data and documents, the normative acts and agreements to be amended or repealed, the manner of informing the data register providers and data register recipients, including other provisions determining the manner and conditions of the liquidation of the register.

In addition to the above, it was considered necessary to adopt a Government Decision on the liquidation of the Register of evidence of data controllers, which would describe in detail how to liquidate the Register by irreversibly destroying the documents and information stored on paper and those stored in electronic format, and to repeal the Government Decisions on the approval of the technical concept and regulation of the Register concerned.

Thus, on April 29, 2022, was published the Government Decision No. 282/2022 regarding the liquidation of the Register of evidence of personal data controllers and the repeal of some Government decisions, according to which **the documents and information stored on paper and those stored in electronic format were irreversibly destroyed**.

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

One of the objectives of the NCPDP is to ensure the fundamental rights and freedoms of natural persons in the field of personal data protection through prevention (support, advice, education and training).

Within this objective, the NCPDP carries out activities related to the implementation of the Law on personal data protection. Thus, the NCPDP provides advice to public authorities, provides support to the private sector, including by training employees, carrying out information activities, etc. This also includes the active implementation of new changes to the law, guided by the idea of "*First we recommend*", followed by controls and sanctions as appropriate.

As mentioned above in the content of this report, starting January 10, 2022, the obligation of the controller and the processor to appoint a personal data officer, in the cases provided for by Art. 25 of the Law on personal data protection. The role of personal data officer is to assist the controller or the processor to monitor internally the compliance.

In this context, we note that, according to para. (1) let. (a) of the same article, the controller and the processor shall designate a data protection officer whenever processing is carried out by a public authority or institution, except for the courts acting in their judicial role.

At the same time, according to Art. 25^1 para. (2) of the Law No. 133/2011, the controller and the processor shall support the data protection officer in the performance of the tasks referred to in Art. 25^2, providing him with the necessary resources for the performance of those tasks, for maintaining his professional knowledge, as well as access to personal data and processing operations. At the same time, according to para. (3), the data protection officer shall be directly subordinate to the highest level of management of the controller or processor.

In addition, it should be noted that the controller or processor is obliged to publish the contact details of the data protection officer and communicate them to the NCPDP, thus, by 31 December 2022, approximately 84 notifications were received regarding the designation of personal data protection officers, of which only 7 from central/local public authorities, in which order the NCPDP has placed on its website notices drawing the attention of controllers and processors to the obligation to designate the personal data protection officer.

At the same time, messages to this effect were sent during the consultations offered by the NCPDP to the controllers regarding the request for support in order to comply with the legal provisions in the field of personal data protection.

With regard to the conduct of a data protection impact assessment or prior consultation, which is mandatory insofar as the situation falls under the circumstances covered by Art. 23 and 24 of the Law on personal data protection, the NCPDP provided advisory support in 11 cases.

Additionally, in the context of compliance of data controllers with the new obligations: data protection impact assessment, designation of data protection officer, establishment of new requirements in the context of cross-border transmission of personal data, the NCPDP has developed and published on the website under the section **Legislation/Decisions/NCPDP Instructions/Decisions/Orders** a number of normative acts, which specify certain aspects for data controllers such as:

1. Decision on the approval of the list of States which ensure an adequate level of personal data protection.

By the Law No. 175/2021 on amending some normative acts, amendments were also made to Art. 32 "*Cross-border transmission of personal data*" of the Law No. 133/2011 on personal data protection.

As a result of the amendments made to the normative act, new conditions have been established under which the cross-border transmission of personal data to member states of the European Economic Area, to states which ensure an adequate level of personal data protection and to states which do not ensure an adequate level of personal data protection may take place and the authorisation of the cross-border transfer of personal data to another state by the NCPDP is no longer required.

Thus, according to para. (3) of this article, the NCPDP shall approve, by decision, the list of states ensuring an adequate level of data protection, taking into account: the international treaties on the personal data protection to which they are party; the existence and compatibility of data protection legislation; the competences and cooperation with the supervisory body for data processing, as well as other relevant aspects of the legal regime for the protection of personal data. The NCPDP takes into account the decisions adopted by the European Commission on the states that ensure an adequate level of personal data protection.

In view of the above-mentioned reasoning, the NCPDP by Decision No. 23 of 17 March 2022 approved the list of countries ensuring an adequate level of data protection as follows: *Andorra; Argentina; Canada; Faroe Islands; Guernsey; State of Israel; Isle of Man; Japan; Jersey; New Zealand; Republic of Korea; Switzerland; Uruguay; United Kingdom of Great Britain and Northern Ireland.*

2. Order on the approval of the Standard Contract for the cross-border transmission of personal data to states that do not ensure an adequate level of personal data protection.

According to para. (5), let. i) of Art. 32 of the Law No. 133/2011, the transmission of personal data to states that do not ensure an adequate level of protection may take place if the processing takes place under the standard contract for the cross-border transmission of personal data, drawn up and approved by the NCPDP, concluded by the data controller.

In this context, in order to meet the requirements of the Law on personal data protection, Order No. 33 of 22 April 2022 approved the Standard Contract for the cross-border transmission of personal data to states that do not ensure an adequate level of personal data protection.

The purpose of the Standard Contract is to ensure compliance with the requirements of the Law 133/2011 in the case of cross-border transmission of personal data to countries that do not ensure an adequate level of personal data protection.

At the same time, the role of the Standard Contract is to establish appropriate technical and organisational measures, including to ensure enforceable rights of personal data subjects

and effective remedies in relation to cross-border transmissions of data from controllers to controllers, from controllers to processors and/or from processors to controllers.

3. Order approving the list of types of processing operations subject to the requirement to carry out a personal data protection impact assessment.

The new amendments to Art. 23 of the Law No. 133/2011 on the personal data protection establish the obligation for data controllers to carry out a data protection impact assessment if certain criteria set out in paragraph 1of the same article are met.

Thus, depending on the nature, scope, context and purposes of the data processing, where a type of processing, in particular that based on the use of new technologies, is likely to result in an increased risk to the rights and freedoms of individuals, the controller shall, prior to the processing, data protection impact assessment envisaged on the protection of personal data. A single assessment may address a set of similar processing operations that present similar increased risks. Art. 23, para. (3) of the Law No. 133/2011 provides for cases regarding data protection impact assessment.

The data protection impact assessment is a new tool, taken over from Art. 35 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, with the same approach and purpose of **making controllers accountable for determining the appropriate measures to be taken to demonstrate that the personal data processing complies with the law.**

When assessing whether planned processing operations require a personal data protection impact assessment pursuant to Art. 23 of the Law No. 133/2011, the controller shall use the nine criteria reflected in the List of types of processing operations subject to the requirement to carry out a personal data protection impact assessment, in the development of which the guidance of the Guidance on Data Protection Impact Assessment (DPIA) and determining whether a processing operation is "likely to result in a high risk" within the meaning of Regulation 2016/679, as revised and adopted on 4 October 2017 by the Art. 29 Data Protection Working Party (Working Document No. 248), has been taken into account.

The list of types of processing operations subject to the requirement to carry out a personal data protection impact assessment is based on the provisions of Art. 23, para. (3) of the Law No. 133/2011 and contains certain types of processing operations as well as examples of personal data processing.

Thus, the list expressly, but not exhaustively, provides for operations for which an impact assessment is required, namely:

1. Processing of personal data for the purpose of a systematic and comprehensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and which forms the basis for automated decisions which produce legal effects concerning the natural person or which affect him or her to a substantial extent;

2. Processing, on a large scale, of categories of data which relate to the disclosure of racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, as well as the processing of genetic data, biometric data for the unique identification of a natural person, data concerning health or data concerning sex life or sexual orientation, criminal convictions and offences of a natural person;
3. Processing of personal data for the purpose of systematic, large-scale monitoring of a publicly accessible area;
4. Large-scale processing of personal data of vulnerable persons (such as asylum seekers, the elderly, patients, minors, persons subject to a legal protection order and employees) by automated means for systematic monitoring and/or recording of behavior, including for the purposes of advertising, marketing and publicity.
5. Large-scale personal data processing through the innovative use or implementation of new technologies, in particular where such operations limit the ability of individuals to exercise their rights;
6. Large-scale processing of data generated by sensor devices transmitting data over the Internet or by other means;
7. Large-scale and/or systematic processing of traffic and/or location data of natural persons where the processing is not necessary for the performance of a service requested by the data subject.

We would like to point out that the list of examples accompanying personal data processing operations is not limited to those included in the table in the Annex to the Order, but is intended to guide the controller in identifying personal data processing operations requiring a data protection impact assessment.

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

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

In this context, the NCPDP dynamically analyses the statistics of accesses made in 2022 by users of the Ministry of Internal Affairs, the National Anti-Corruption Centre, the General Prosecutor's Office, the National Integrity Authority, the Ministry of Defense, the Customs Service, the State Tax Service, the entities identified with the highest number of accesses of personal data performed. The information in the following table is based on data provided by the Public Services Agency and the e-Governance 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			
	through SIC "Access-Web" and COI			via the interoperability platform (MConnect)
	2020	2021	2022	2022
Ministry of Internal Affairs	11213170	13259515	22446877	15429
Intelligence and Security Service	65180	69196	70184	43080
National Anticorruption Center	86891	74493	75486	10468
General Prosecutor's Office	19985	22405	30797	6
Customs Service	12381	14063	17715	6
Ministry of Defence	1002	503	727	115301
National Integrity Authority	17217	18823	19127	11759
State Tax Service	3535927	3007799	4071998	9566872

According to the table, a large part of the accesses performed by the entities concerned continue to be carried out via the SIC "Access-Web" and COI, platforms managed by the Public Services Agency.

Thus, it will be noted that, in most cases, access to personal data by means of this technology does not meet the requirements of ensuring the security of personal data in relation to their processing in automated information systems and does not ensure the identification by name of the users who have carried out data access operations and who are obliged to justify the purpose and legal basis of these operations.

In this context, the NCPDP during 2022 requested the involvement of the e-Governance Agency, taking into account its competences provided by the Law No. 142/2018 on data exchange and interoperability by undertaking the necessary actions to ensure the compliance of all processing/accessing operations of personal data stored in state information resources, by admitting the access and use of this information exclusively through methods appropriate to the requirements of security and confidentiality, informing the NCPDP on the actions taken in this regard.

As a result, the P.I. ,,e-Governance Agency" has communicated that it will strengthen its efforts to ensure effective communication with the entities concerned and will take appropriate measures to resolve the contracts of data accessing institutions through COI technology and to ensure access through the Interoperability Platform (MConnect), as provided for in Art. 6 para. (3) of the Law No. 142/2018 on data exchange and interoperability and Point 4 of Government Decision No. 211/2019 on the Interoperability Platform (MConnect).

At the same time, during the reference period, in the framework of the examination of complaints concerning the processing of personal data through access to registers/information systems managed by the Public Services Agency, in particular related to the e-Cadastre information portal and the SIC "Web Access", the NCPDP found: tendency to use the access credentials (username and password) of a single authorized user account by several employees of the beneficiary entity; possession/use of username and password by third parties; non-updating of the list of users after their departure or after change of job or function in the entity; failure to include in user lists the user's personal data (IDNP, contact number or address); failure to inform the Public Services Agency of the change of the administrator responsible for access to the above-mentioned information portals indicated in the user list; failure to update user passwords, etc.

These actions have created the premises for the finding of violation of the provisions of the Law on personal data protection, as well as non-compliance with the provisions of the contracts concluded by the Public Services Agency, related to granting access to the state information registers managed.

Thus, the NCPDP intervened with the Public Services Agency to review/update the contracts concluded in the context of granting access to the registers/information systems managed by the Public Services Agency, in particular the lists of authorised users, as well as to reassess and grant access to the registers/information systems managed by the Public Services Agency only through the electronic governmental authentication and access control service (MPass).

As a result, the Public Services Agency (PSA) communicated about the implementation of the governmental electronic authentication and access control service (MPass) for external users in relation to the automated access SIC "Access-Web", the revision of the contracts in this respect by concluding additional agreements, as well as the initiation of certain actions in order to implement the governmental authentication and access control service (MPass) as a single mode of access of the authorized user to all information resources/systems managed by the PSA.

At the same time, in order to assess the situation regarding the implementation of the data subject's right to information, the NCPDP requested from the Public Services Agency and the e-Governance Agency information on the number of data subjects' addresses/requests submitted in 2022, aimed at requesting information on operations to access personal data concerning them from state registers/information systems. According to the information provided, it has been established that data subjects, during 2022, addressed more often the Public Services Agency, **392** requests, compared to **48** requests to the e-Governance Agency.

In this context, it should be mentioned that the data subject has access to the Citizen's Government Portal (MCabinet) offered by the e-Governance Agency through which he/she can view the history of access to his/her personal data by public authorities and institutions and other natural and legal persons, including private law entities. The portal provides 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 obliged to enter information about data access, including the data exchange process via the MConnect platform.

CHAPTER VII

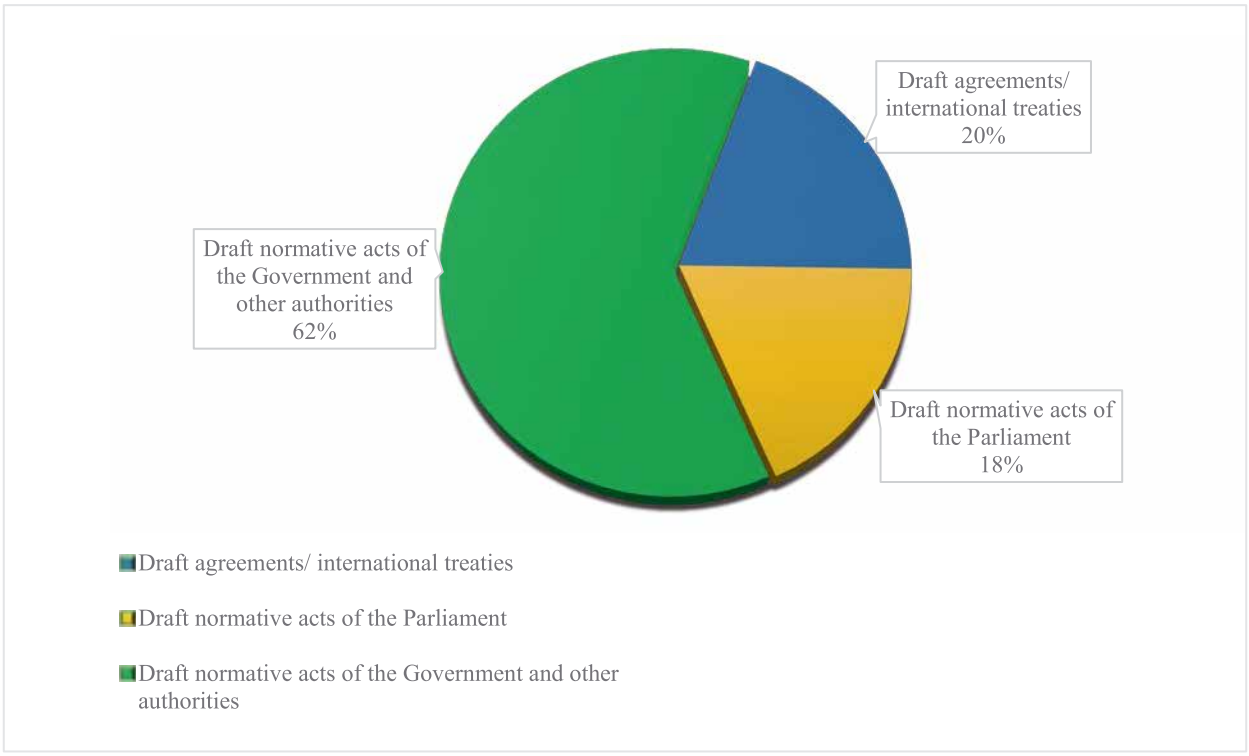
ENDORSEMENT AND DEVELOPMENT OF DRAFT NORMATIVE ACTS

According to Art. 32 para. (2) of the Law No. 100/2017 on normative acts, the draft normative acts that fall within the competence of the NCPDP are submitted for endorsement.

In this regard, during the year 2022, **127** national draft normative acts/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, of which:

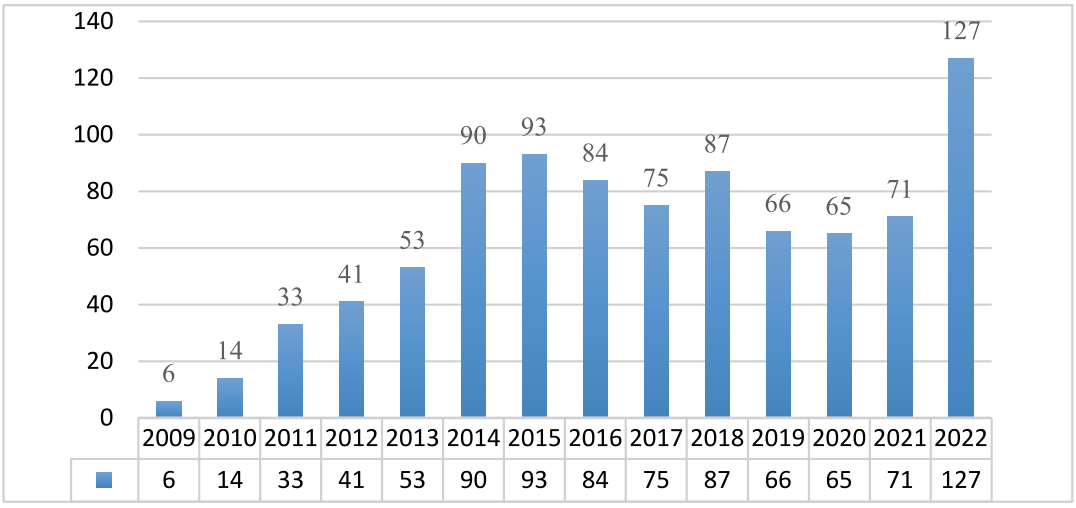
- **25** draft agreements / international treaties;
- **23** draft normative acts amending laws, codes;
- **79** draft normative acts of the Government and other authorities.

Percentage of opinions provided by the NCPDP in 2022



Therefore, on most of the drafts sent for endorsement, the NCPDP, in its capacity as personal data protection authority, considered it necessary to complete, amend or revise the respective texts, presenting a series of recommendations and proposals in order to adjust/conform some provisions of the respective drafts to the principles and conditions of personal data processing, in order to ensure respect for the rights of personal data subjects.

Dynamics of drafts submitted for approval 2009-2022

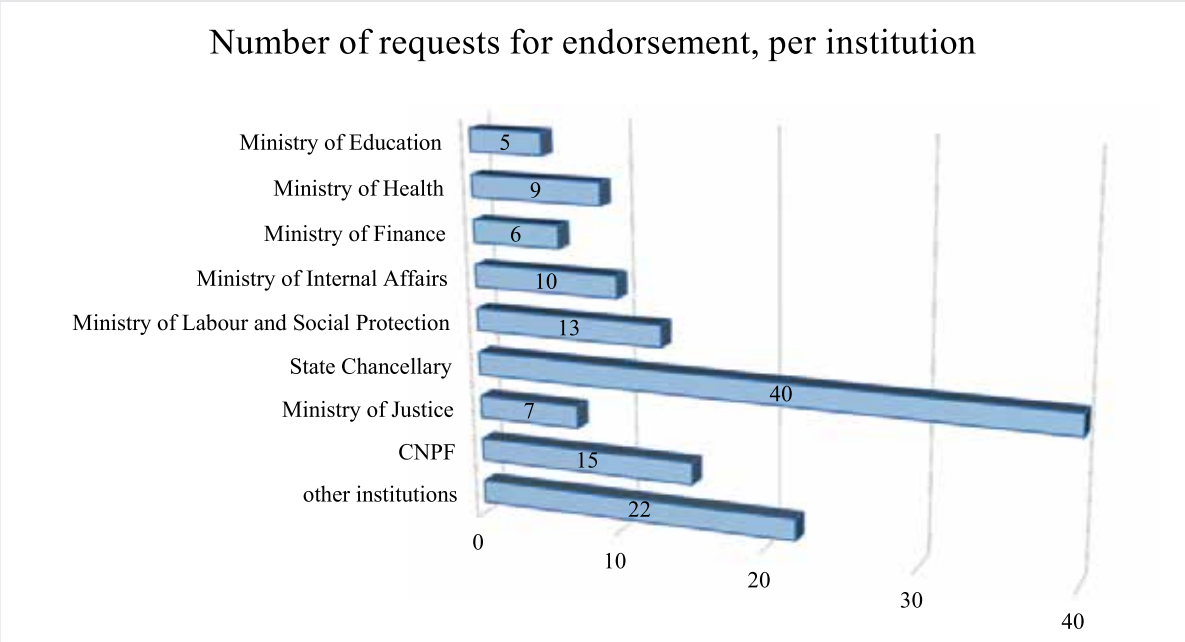


Separately, we present below the most relevant draft normative acts endorsed, as follows:

- *the draft Government Decision for the approval of the Regulation on the examination procedure for obtaining the right to drive vehicles, issuing and validity of the driving licence;*
- *the draft law on the amendment of the Law on the National Financial Market Commission;*
- *the draft decision on the approval of the Concept of the Information System "Civil Status Acts";*
- *the draft decision on the approval of the Concept of the Information System "UAHELP";*
- *the draft decision on the establishment of the Information System for the Surveillance of Communicable Diseases and Public Health Events;*
- *the draft decision on the approval of the Concept of the Information System "Energy Vulnerability";*
- *the draft decision on the approval of the Concept of the Information System "Recruitment and Evaluation of Human Resources in the Internal Affairs System" and the Regulation on the organisation and functioning of the Information System "Recruitment and Evaluation of Human Resources in the Internal Affairs System";*
- *the draft decision on the organisation and conduct of the population and housing census in 2024;*
- *the draft rules on reporting to the P.I."Public Audit Supervisory Board" on breaches of regulations in the field of audit of financial situations;*
- *the draft decision on the approval of the Concept of the Unified Information System "e-Admission" in higher education;*
- *the draft of the Government Decision "On the approval of the Development Strategy of the National Statistical System for the period 2022-2030";*
- *the draft law on Human Biological Bank;*
- *the draft decision regarding the approval of the draft law on the amendment of some normative acts (stimulation of electronic commerce);*

- *the draft decision for the approval of the Concept of the Informational System for the management of the authorization of economic agent and the Regulation on the way of keeping the State Register of the authorization of authorized economic agent formed by the Informational System for the management of the authorization of economic agent;*
- *draft decision on granting temporary protection;*
- *the draft Guidelines on how to depersonalize administrative acts in the State Register of Local Acts;*
- *draft Government Decision "On the approval of the Concept of the Information System "Demographic and Social Statistics";*
- *the draft Memorandum of Understanding between the Diplomatic Security Service of the United States of America and the Ministry of Internal Affairs of the Republic of Moldova as amended;*
- *the draft decision on the approval of the rules of conducting of unmanned aircraft;*
- *the draft decision approving the Regulation on the Automated Information System "Register of Electoral Officials";*
- *the set of materials on the initiation of negotiations and approval of the signing of the Agreement between the Republic of Moldova and the International Committee of the Red Cross;*
- *the draft decision on the approval of the Integrated State Border Management Programme for 2022-2025;*
- *the draft Government Decision on the approval of the Concept of the Information System "State Register of Law Units";*
- *the draft "Agreement in the field of social security between the Republic of Moldova and the Swiss Confederation".*

The number of requests for endorsement received by the NCPDP in 2022



Below, for information, we present the most important opinions issued by the NCPDP on draft normative acts:

1. The Ministry of Labour and Social Protection requested the NCPDP to examine the draft decision on the approval of the "*Child Protection Information System Concept*".

The NCPDP positively assessed the implementation of an information system in the field of child protection, designed in accordance with the legislation in force, being an integral part of the information and telecommunications component of the e-governance infrastructure of the Republic of Moldova.

At the same time, analysing the content of the Concept it was not identified the term storage/ archiving of personal data, in which context it was mentioned that:

- according to Art. 4 para. (1) let. e) of the Law No.133/2011 on personal data protection, *personal data must be stored in a form which permits the identification of the personal data subjects for a period not exceeding the time necessary to achieve the purposes for which they are collected and further processed*;

- according to Art. 11 para. (3) of the same legislative act, at the end of the personal data processing operations, *if the subject data has not given his consent to another destination or to further processing, personal data shall be: destroyed; transferred to another controller, provided that the initial controller ensures that further processing is for purposes similar to those for which the initial processing was carried out; rendered anonymous and stored exclusively for statistical, historical or scientific research purposes;*

In this context, it was necessary to mention in the content of the draft Concept the provisions on the concrete period of retention of personal data and the way to delete them from the mentioned System.

In Chapter VIII of the draft Concept, referring to personal data protection, only a paragraph with general provisions has been included in the part dealing with the collection, processing, storage and transmission of personal data.

Thus, it was proposed to divide the chapter into two parts: ***21.1 Aspects on information security and 21.2 Personal data protection.***

At point 21.2, it was recommended to add the following content:

"Personal data protection"

a) under the terms of this Concept, the possessors/holders/recorders will process only strictly necessary personal data, not excessive for the predetermined purpose, according to the powers assigned, respecting the principles established by the legislation on the personal data protection;

b) when the processing of personal data, the possessors/holders will ensure organizational measures to protect personal data against destruction, alteration, blocking, copying, disclosure, and against other unlawful forms of processing, that shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data processed.

c) in case of security incidents, the possessors/holders will take necessary measures to detect the source of the incident, they will analyze it and remove the causes of the security incident by informing the National Center for Personal Data the Protection of the Republic of Moldova;

d) within the personal data processing operations carried out according to this Regulation, the possessors/holders shall ensure compliance with the rights of the personal data subjects.

Taking into account the above, the NCPDP recommended the operation of the additions that must be made to the project, with the submission for repeated approval of the draft.

Following the definition of the draft, the proposals submitted by the NCPDP were accepted.

2. The Ministry of Health requested the NCPDP to review the draft law on the Human Biological Bank and, based on the functional powers, the following were communicated:

The analysis of the draft revealed that through the proposed regulations personal data will be processed regarding the state of health of the data subjects, in which order attention has been drawn to the fact that they are part of the special category of personal data, which, by their nature, are particularly sensitive in terms of fundamental rights and freedoms and require specific protection, because the context of their processing could generate considerable risks to fundamental rights and freedoms.

With reference to the content of the draft, it was recommended to include in Art. 5 provisions to ensure appropriate guarantees, in accordance with the provisions of Art. 29 and Art. 30 of the Law on personal data protection, by obliging biobanks to establish appropriate measures to ensure the security, confidentiality and integrity of personal data processed within the personal data filing systems, as follows:

"Biobank ensures the security and confidentiality of personal data, by applying the necessary organizational and technical measures for the personal data protection against destruction, modification, blocking, copying, spreading, as well as against other illegal actions, measures designed to ensure a level of security appropriate in terms of the risks presented by the processing and the nature of the processed data.

In the case when there will be a breach of the security of personal data, the biobank has the obligation to take the necessary measures to detect the source of the incident, carry out its analysis and remove the causes of the security incident."

Likewise, it was determined that according to Art. 4 of the draft, the biobank is a public institution with or without the status of a legal person, a fact that attests to different approaches and statutes assigned to biobanks, and in such conditions uncertainties are created also in the part related to the establishment of legal liability of biobanks, under the conditions of Art. 29 of the draft.

With reference to the provisions stipulated in Art. 6 of the draft, it was considered necessary to clarify the relationships and tasks between the research biobank and the biobank.

According to the provisions of Art. 6 para. (2) let. c) of the draft, the research biobank maintains and develops the biobank registers, provisions that do not justify the right of the research biobank to administer the biobank registers, which implies providing access to the data contained in the biobank registers. However, the biobank is a separate entity from the research bank and is qualified as a data controller which, in the sense of Art. 3 of the Law 133/2011, establishes the purposes and means of personal data processing expressly provided by the legislation in force. Moreover, in the context of the prenotated notion, the biobank should have the capacity of a legal person.

In the part concerning the consent offered to become a biospecimen donor, the NCPDP considered it relevant to complete Art. 14 para. (4) with new provisions for expressing an informed consent of the data subject, in the following order:

"Before a person donates biospecimens with their use for corrective, diagnostic and therapeutic purposes, the doctor provides him with written information regarding:

1) purposes, content and duration of the diagnostic or therapeutic research project;

2) possible risks;

3) the right to freely express consent and to withdraw it at any time;

4) the possibility of conducting research outside the Republic of Moldova."

Also here it is necessary to specify that the donor is to be informed about the fact that the biospecimens, in accordance with the rules stipulated in the project, can be used by the biobank for 3 distinct purposes, namely: **either for research purposes, or for diagnosis, or for therapeutic purpose**, or, each purpose is to be elucidated separately/individualized from the start, when the donor expresses his consent.

Moreover, for the clarity and predictability of the legal rule, it would be appropriate for these 3 types of determined purposes to be defined in Art. 2 of the draft.

At the same time, it was noted that Art. 14 para. (5) of the draft contains general regulations regarding the preservation of the consent of the donor of biospecimens, generally lacking the rules regarding the term of preservation of personal data recorded in the biobank registers.

In this context it was mentioned that, according to Art. 4 para. (1) let. e) of the Law on personal data protection, the personal data that are the subject of processing must be stored in a form that allows the identification of the subjects of the personal data for a period that will not exceed the duration necessary to achieve the purposes for which they are collected and subsequently processed.

At the same time, according to Art. 11 of the law mentioned above, the conditions and terms of storage of personal data are established by legislation taking into account the provisions of Art. 4 para. (1) let. e). At the end of the storage period, personal data will be destroyed in the manner established by law. The personal data from the state registers, from the date of termination of their use, may remain in storage receiving the status of archive document.

At the end of the personal data processing operations, if the subject of these data has not given consent for another destination or for further processing, they will be:

a) destroyed;

b) transferred to another controller, provided that the original controller guarantees that further processing shall be carried out for purposes similar to those for which the data initially have been processed;

c) transformed into anonymous data and stored exclusively for statistical, historical or scientific research purposes.

Starting from the mentioned provisions, in order to comply with the principles of personal data protection, it was recommended to evaluate and establish a concrete term for keeping this data, as well as the procedure for destroying/archiving/transmitting personal data after the purpose for which they were collected/processed has been fulfilled.

It was also specified that the provision of Art. 16 para. (1) of the draft has a general and ambiguous character, in which order it was recommended that the article or the draft be completed with rules that would establish the tasks and obligations of the biobank. Additionally, the draft should be supplemented with rules that would more clearly and thoroughly regulate aspects of the requirements for the organized collection of human biospecimens/samples and associated data.

With reference to the relations between biobanks and third parties, regulated in Art. 18 para. (6) and Art. 21 of the draft, it was noted that they also involve cross-border transfers of personal data.

Attention was drawn to the fact that, in the case of cross-border transfer of personal data to other states, the controllers must take into account the conditions provided in Art. 32 of the Law on personal data protection, in which it was recommended to identify the legal basis on the basis of which the cross-border transfer of personal data will be carried out.

As a rule, in situations of calling on the services of medical institutions/laboratories located in another state, the exported medical material, as well as the corresponding personal data, are depersonalized by the data controller.

According to Art. 3 of the Law No. 133/2011 depersonalisation of data represents the modification of personal data so that the details of personal or material circumstances no longer allow their attribution to an identified or identifiable natural person or allow attribution only under the conditions of an investigation that requires disproportionate time, means and labour force. Therefore, they will not be considered personal data and do not fall under data protection legislation. However, in case of doubt, the data subject must be fully informed and his consent must be obtained before any transmission of personal data.

It was found that, according to Art. 23 of the project, the biobank obtains the approval of the national authority for personal data protection of the code generation method.

In this line of ideas, starting from the competences of the NCPDP stipulated in Art. 20 of the Law on personal data protection, it was proposed to amend the rule so that the NCPDP provides consultancy in order to establish a compliant mechanism for assigning/allocating the codification, through the lens of respecting the guarantees of personal data protection and the rights of data subjects, or, the norm of Art. 23 of the draft, establishes an improper NCPDP competence, which exceeds the powers and tasks stipulated by the Law on personal data protection.

3. The Ministry of Economy submitted to the NCPDP the request for examination of the draft decision regarding the approval of the draft law for the modification of some normative acts (*stimulation of electronic commerce*).

With reference to Art. XVI of the draft law, by which it was intended to amend the Law No. 133/2011 on personal data protection, which will provide the right of subcontracting by authorized persons to another authorized person in the process of personal data processing, it was specified that these provisions are partially taken from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Thus, it was emphasized that the amendments submitted to the Law No. 133/2011 on personal data protection, through the draft law, will in no way align national legislation with European standards in the field of personal data protection and will not provide an adequate level of protection of the rights of data subjects, or even if, apparently, some provisions are taken from the General Data Protection Regulation, they are not sufficient to create the necessary conditions for the compliant processing of personal data, other situations that require intervention remain uncovered/unregulated.

The NCPDP mentioned that as long as the General Data Protection Regulation is not transposed into national legislation, it will not provide sufficient guarantees for personal data protection and the rights of data subjects.

In the light of the above, NCPDP considered it necessary that the changes to the regulatory framework occur with the adoption of the new legislative package in the field of personal data protection, which is being examined within the working group created by the Ministry of Justice and is to eliminate the discrepancy between the national legal framework in the field of personal data protection and existing regulations at European level.

However, in the situation where the proposed amendments to Art. XVI of the daft will be supported, it was mentioned that these rules are not complete and do not regulate the establishment of the obligations and individualized liability of authorized persons in relation to the controller, as stated in the provisions of the General Regulation on Data Protection.

As a result, the provisions formulated in Art. 30 of the Law No. 133/2011 are to be supplemented with the following legal provisions, which correspond to para. (4) and para. (9) of Art. 28 of the General Data Protection Regulation:

- *"Where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in paragraph 3 shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of this Regulation. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.*
- *The contract or the other legal act referred to in paragraphs 3 and 4 shall be in writing, including in electronic form."*

4. The National Bureau of Statistics requested approval of the *draft decision regarding the approval of the draft law on the population and housing census* and, based on its functional powers, NCPDP communicated the following:

According to Art. 10 para. (1) let. j) from the draft law on the population and housing census, the National Bureau of Statistics is responsible for organizing and carrying out the census, including the attribution to establish, regulate and develop information systems necessary for the collection, processing and validation of data, ensuring data confidentiality and protection against unauthorized or illegal processing and against accidental loss, destruction or damage through the technical, organizational and administrative measures implemented.

Subsequently, Art. 15 para. (4) of the draft states that the possessors and holders of administrative and private data are obliged to transmit individual data free of charge, including personal data from registers, information systems, personal data filing systems, managed as the owner or holder, such as, but not limited to:

a) Automated Information System State Register of the Population;

b) Real estate Register;

c) Integrated Information System of the Border Police;

d) Educational Management Information System;

e) State Register of individual records in the public social insurance system;

f) The information systems of the National Medical Insurance Company;

g) Register of electoral officials;

h) Data from the private information resources of service providers and public utility providers (water, landline and mobile telephony, gas, electricity and thermal energy, etc.).

Consequently, it was mentioned that according to para. (1) of the same article it is specified that the *NBS has the right to access*, extract and process for the purposes of the census personal data from administrative and private data sources about the characteristics mentioned in Art. 13 para. (1).

At the same time, paragraph (4) stipulates that the possessors and holders of administrative and private data are obliged *to transmit individual data free of charge, including personal data from registers, information systems, personal data record systems* [...], without being granted some NBS rights to directly access the targeted systems.

In this context, in order to avoid the dual interpretation of the mentioned norms, it was proposed in Art. 15 para. (1) of the draft, the completion of the rule, after the words "*personal data*" with the words "*transmitted by owners and holders*".

At the same time, Art. 15 para. (6) of the draft mentions that the list of categories of individual data, including personal data, at the level of individual registration, stored and processed by the data sources mentioned in para. (4) and (5), the format and deadlines for their transmission are determined by the NBS.

In this context, we mention that the technical concept of the automated information system of the National Bureau of Statistics, approved by Government Decision No. 856 of September 21, 2010, regulates the following aspects:

- Point 3 establishes that as a component part of the electronic government, SIA NBS is integrated with other informational systems with which the National Bureau of Statistics interacts for the exercise of its obligations.
- Point 5 states that the informational space of SIA NBS represents the set of the following informational resources: a) statistical registers; b) statistical data, which can be: primary statistical data, validated statistical data, aggregated statistical data, published statistical data.
- Point 6 stipulates that SIA NBS is intended to ensure the collection, processing, storage and dissemination of statistical information by developing, adapting and implementing

the statistics production model, based on processes and the standardized model of the information flow, to create a management mechanism of the main statistical processes and associated sub-processes, to monitor technological processes, intermediate and final results, to allow users free, convenient and interactive access to public statistical information resources.

- Point 11 establishes the basic functions of SIA BNS, in particular: data entry; forming the system database, updating and archiving data; providing users with relevant statistical information; ensuring information security at all stages of collection, storage, processing and presentation; ensuring interconnection with other state information systems.
- Point 13 lists the main data providers for SIA BNS. It is to be mentioned that the respective point includes the fact that the list of information presented and the list of suppliers is stipulated in the program of statistical works, approved annually by the Government.

Taking into account the provisions mentioned above, in Art. 15 para. (6) of the draft, it was proposed to replace the words "*are determined by the NBS*" with the words "*approved by the Government, at the proposal of the NBS*".

Subsequently, Art. 16 para. (7) of the draft mentions that "*the process of pseudonymization consists in assigning a unique statistical identifier for personal data (state identification number (IDNP), first name, last name)*".

The NCPDP informed that, according to the definitions stipulated in Art. 3 of the Law No. 133/2011 on personal data protection, *depersonalisation of data represents the modification of personal data so that the details of personal or material circumstances no longer allow their attribution to an identified or identifiable natural person or allow attribution only under the conditions of an investigation that requires disproportionate expenditures of time, means and labour force.*

Moreover, according to Art. 5 para. (5) let. f) from the registered law, the consent of the data subject is not required in cases where the processing is necessary for statistical, historical or scientific research purposes, provided that the personal data remain anonymous throughout the processing.

Additional, Art. 31 of the same normative act states that, for statistical, historical, scientific, sociological, medical research, legal documentation purposes, the controller depersonalizes personal data by removing from them the part that allows the identification of the natural person, turning them into anonymous data, which cannot be associated with an identified or identifiable person. In case of depersonalization, the confidentiality regime established for the respective data is cancelled.

At the same time, the European practice was also highlighted, exposed in Regulation 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 (GDPR), which states that data protection principles should apply to any information relating to an identified or identifiable natural person. *Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.* In order to determine whether a natural person is identifiable, all means, such as individuation, which either the controller or another person is reasonably likely to use for the purpose of identification should be taken into account, directly or indirectly, of the respective natural person. In order to determine whether it is reasonably likely that

means of identifying the natural person will be used, all objective factors such as the costs and time required for identification should be considered, taking into account both the technology available at the time processing, as well as technological development. *The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.* (Recital 26 GDPR).

In this sense, in order to align the draft law with the principles of personal data protection established in the Law on personal data protection, in Art. 18 of the draft law, it was proposed to replace the word *"pseudonymized"* with the phrase "*depersonalized*", or, otherwise, the author of the draft law should revise the term of storage set out in Art. 18 para. (1) in accordance with the provisions of Art. 11 paragraph (3) from the Law No. 133/2011 on personal data protection which states that at *the end of the personal data processing operations, if the subject of these data has not given consent for another destination or for further processing, they will be:* destroyed; transferred to another controller, provided that the initial controller guarantees that the subsequent processing has similar purposes to those in which the initial processing was done; *transformed into anonymous data and stored exclusively for statistical, historical or scientific research purposes.*

Last but not least, it was noted that according to Art. 18 para. (2) of the draft, "*the term of storage of the data collected on paper is 3 years from the dissemination of the final results of the census, after which they are sent for recycling (irreversible destruction) in accordance with the compliance and security requirements that are imposed to be applied in the case of this information with limited accessibility".*

Thus, it was recommended to the author of the draft law to review the 3-year term of storage of data collected on paper from the dissemination of the final results of the census as being excessively long. In this context, it was recommended to take into account the normative acts in the field from Romania, which provided for a much shorter term in this sense.

At the same time, it was noted that in the content of Art. 20 para. (2) in the draft it is mentioned that when processing personal data for the purposes of the census, *the right of access, the right to rectification/intervention, the restriction of processing and the opposition* of data subjects, provided by the legislation on personal data protection, *rights that do not correspond to those provided by the Law No. 133/2011 on personal data protection.*

Thus, it was recommended to replace the words *"right of access, right of rectification/intervention, restriction of processing and opposition"* with the words "*right of access to personal data, right of intervention on personal data and right of opposition of the personal data subject".*

Therefore, the revision of the draft decision regarding the approval of the draft law on the population and housing census was requested in the light of those indicated above.

5. The Ministry of Labor and Social Protection requested the examination of the draft decision *regarding the approval of the Information System Concept "UAHELP"* and, based on its functional competences, NCPDP communicated the following:

First of all, it was noted that the draft decision proposed not only the approval of the Concept of the "UAHELP" Information System, but also the approval of the Regulation on the way

of organization and operation of the "UAHELP" Information System, in which order it was recommended to revise the name of the draftdecision to correspond to the object of the regulation.

At the same time, it was mentioned that following the analysis of the "UAHELP" Information System Concept draft, it was established that in point 9 of Chapter II the phrase "Law No. 133/2011 on personal data protection" is provided for twice both in subpt. 7, as well as in subpt. 11. In this sense, it was proposed to remove the given error.

It was also noted that, according to Art. 3 of the Law on personal data protection, personal data is any information relating to an identified or identifiable natural person (personal data subject). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Thus, in point 27 of Chapter V of the draft Regulation on the way of organization and operation of the "UAHELP" Information System, the NCPDP noted the need to change the phrase "*except for data with limited access in the field of personal data*" with the phrase "*except for personal data*". However, access to personal data itself must be limited, in order to prevent non-compliant processing thereof.

In the same vein, the NCPDP noted the need to change the phrase "*data with limited access*" from point 28 of the same chapter with the phrase *"personal data"*.

Following the analysis of the Concept and Regulation of the Information System "UAHELP", the retention period was not retained, as well as the procedure for deleting/erasing the personal data included in this system when the retention period expires.

Art.11 para. (1) of the Law on personal data protection provides that the conditions and terms for storing personal data are established by legislation, taking into account the provisions of Art. 4 para. (1) let. e). Upon expiration of the storage period, personal data shall be destroyed in the manner established by law.

Thus, as a result of the above, it was proposed to the author of the draft decision regarding the approval of the Concept of the Information System "UAHELP" to complete it with a new point that will provide for the retention period of personal data and the procedure for their erasure/ deletion.

Consequently, for information purposes, it was mentioned that, by the Law No. 175/2021 for the amendment of some normative acts, amendments were made to the Law No. 133/2011 on personal data protection, establishing the obligation of the personal data controller to carry out the data protection impact assessment, in the event that data processing may generate an increased risk for the rights and freedoms of individuals, as well as designation of a data protection officers, according to Art. 23-25 of the registered normative act.

Thus, taking into account the provisions of Art. 23 para. (6) of the Law 133/2011, if the types of personal data processing, regulated by the Information System Concept "UAHELP", are likely to generate an increased risk for the rights and freedoms of individuals, resulting at least from the fact of processing at large scale of personal data, it is necessary for the Ministry of Labour and Social Protection, as owner and holder of the Information System "UAHELP", to assess the data protection impact assessment in the context of the adoption of the respective normative act.

CHAPTER VIII

INTERNATIONAL COOPERATION

Cooperation, both at European and international level, is a strategic aspect that requires involvement in all the initiatives that are under development.

The strengthening of international cooperation in 2022 was materialized through the active participation of the NCPDP representatives at the plenary meetings of the European Data Protection Board (EDPB) and of the Council of Europe. It is worth mentioning that since 2017 the Republic of Moldova has been a member observer within the EDPB.

In 2022, international meetings and conferences were held both online and in person.

Plenary meetings of the European Data Protection Board

During 2022, the NCPDP representatives participated in 9 plenary meetings, which took place online and four with physical presence - in Brussels. In the Plenary meetings of the European Data Protection Board, a number of important documents were adopted, including:

- Guidelines 06/2022 on the practical implementation of amicable settlements;
- Guidelines 02/2022 on the application of Article 60 GDPR;
- Guidelines 04/2021 on Codes of Conduct as tools for transfers;
- Guidelines 01/2021 on Examples regarding Personal Data Breach Notification;
- Statement 04/2022 on the design choices for a digital euro from the privacy and data protection perspective;
- Statement 03/2022 on the European Police Cooperation Code.

The importance of these meetings is reflected in the attempt to develop mechanisms for international cooperation in order to facilitate the effective enforcement of personal data protection legislation. Also, the provision of international mutual assistance in the implementation of personal data protection legislation, including by notification, assistance with investigations and the exchange of information, subject to adequate safeguards for the protection of personal data and other fundamental rights and freedoms.

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 2021, the NCPDP's management participated in 2 meetings of the Bureau of the Convention Committee 108 and 1 plenary meeting of the Consultative Committee of the Convention 108.

In the meetings was discussed about the activity regarding Convention 108+ the current situation; digital identity, inter-state data exchange for anti-money laundering/combating the financing of terrorism and tax purposes, interpretation of Article 11 of the modernised Convention 108, contractual clauses in the context of cross-border data flows, cooperation with the Council of Europe and other entities, etc. All these topics included in the Committee's 2022-2025 work program will be further developed in 2023. The Committee also elected its new Bureau as follows Chair: Elsa Mein, 1st Vice President: Caroline Gloor Scheidegger, 2nd Vice President: Awa Ndiaye and four members: Roxana Legezynska, Pablo Manuel Mateos Gascueña, Anamarija Mladinić and Gonzalo Sosa.

At the same time, we mention that, of the 46 member states of the Council of Europe and 9 non-member states (total of 55 states), the Protocol amending the Convention 108 for the

protection of individuals with regard to automatic processing of personal data was signed by 43 states from the total number and ratified by 20. In this context, it should be mentioned that, on December 22, 2022, the President of the Republic of Moldova signed Decree No. 757 approving the signing of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, orderliness in which the NCPDP requested the Ministry of Foreign Affairs and European Integration to grant Ambassador Daniela Cujbă, Permanent Representative of the Republic of Moldova to the Council of Europe, full powers to sign the respective Protocol.

Implementation the provisions of the RM – EU Association Agreement

On 19-20 October 2022 in Brussels, Belgium, the Deputy Director of the NCPDP, participated in the meeting of the RM – EU Subcommittee on Freedom, Security and Justice.

The main topics discussed in the meeting were: developments in personal data protection, justice sector reform, preventing and combating organised crime, corruption and other illegal activities, money laundering and terrorist financing.

In the meeting was also presented the main developments in the above-mentioned areas since the last meeting held online on 12-13 October 2021.

At the meeting participated the representatives of several Moldovan authorities, such as: the National Anti-Corruption Centre; the General Prosecutor's Office; the National Integrity Authority; the Ministry of Internal Affairs; the National Institute of Justice; the Service for Preventing and Combating Money Laundering.

Cooperation with European data protection authorities and national institutions in the field of personal data protection

On May 18-20, 2022 the representatives of the NCPDP attended the 30th Spring Conference of European Data Protection Authorities which took place in Cavtat, Croatia.

This year's Spring Conference was hosted by the Croatian Personal Data Protection Agency (AZOP) fostering practical collaboration and exchange of best practice between members, with 40 countries attending the event.

The agenda of the event included topical issues in the field of personal data protection, such as Convention 108+, mutual assistance and global convergence, data protection in ECHR case law: latest developments.

The event also featured panel discussions on the latest developments and challenges in cross-border data transfers, foresight, innovation and technology monitoring, hosted by European Data Protection Supervisor as well as raising awareness activities and implementation of the EU funded projects in EU and non-EU countries, etc.

Member authorities adopted a Resolution on the need for a prompt ratification of the "Convention 108+", the modernised version of Convention 108. The Resolution calls upon the governments of the member states of the Council of Europe, the governments of third countries to the Council of Europe, the European Union and International Organisations to speed up the signature and ratification of Convention 108+.

The event was attended by the representatives of the Central and Eastern European Data Protection Authorities, the Council of Europe, the European Data Protection Board, the European Data Protection Supervisor, where they had an extraordinary and unique opportunity to discuss best practices and strategies, including their own foresight function, data transfers and cross-border enforcement.

On 18-19 November 2022, the representatives of the NCPDP participated in the European Case Handling Workshop 2022, held in Tbilisi, Georgia.

The event focused on actual issues in the field of personal data protection and privacy, in particular such as:

– The steps taken by employees of the authorities in investigations;

– Social data protection, guidelines and exceptions in national legislation;

– International transfers of personal data;

– Personal data and artificial intelligence;

– Main challenges faced by data supervisory authorities, etc.

Attending the event, the representatives of the NCPDP addressed the topic – "*The experience of the Republic of Moldova and the methodology of examining the complaints having children as data subjects*".

The invitation to participate in the Workshop came from the Personal Data Protection Service of Georgia, which has been carrying out the control of the lawfulness of personal data processing since 2013. The event brought together around 50 participants from 26 European countries.

In order to provide mutual assistance, including through the exchange of best practices, by sharing expertise, with other supervisory authorities to ensure the consistency of the application of legal provisions in the field of personal data protection, the NCPDP and Personal Data Protection Office of Poland signed a Collaboration Agreement in the field of personal data protection.

The Agreement was signed by the Director of the NCPDP, Ms Victoria Muntean and President of the Personal Data Protection Office, Mr Jan Nowak.

The Agreement provides for the development of cooperation relations between the two institutions in terms of achieving constant progress in the field of personal data protection and the promotion of good practices that will create favorable conditions for ensuring effective protection of personal data of Poland's and Moldova's citizens, which is significant in the context of the recent granting of the status of EU candidate country of the Republic of Moldova.

The NCPDP states that the agreement is aimed at various activities that will encourage the exchange of information on the application of European laws, regulations, standards and recommendations in the field of personal data protection, as well as the organization of activities focused on promoting the protection of privacy and personal data protection, cooperation in order to organize projects of common interest for both institutions at regional and national level, etc.

In order to strengthen the field of personal data protection and its promotion in all sectors of the society's activity, an important role belongs to cooperation with various entities, in which order:

On 25 May 2022, was signed the Cooperation Agreement between the NCPDP and the Academy of Public Administration. The Agreement was signed by the Director of the NCPDP, Victoria MUNTEAN and the Rector of the Academy, Oleg BALAN. The aim of the Agreement is to strengthen the functional capacities of the institutions and human resources able to contribute to the development of staff's professional skills and to the strengthening of institutional integrity.

On 28 June 2022, within the Conference in the field of personal data protection a collaboration Agreement was signed between NCPDP and National Association of ICT Companies ATIC, which aims to implement national legislation and to apply the European standards in the field of personal data protection, as well as the joint organization of various events, conferences, workshops in order to promote the field of personal data protection.

We remind that the NCPDP has concluded another 17 national collaboration agreements with institutions from different fields of activity, as well as 9 international collaboration agreements with the Personal Data Protection Authorities from countries such as Romania, Ukraine, Georgia, Italy, Hungary, Latvia, Malta.

Projects carried out with the support of the European Union

In 2022, the NCPDP applied, won and benefited of support from the ***TAIEX project Technical Assistance and Information Exchange Instrument*** in the organization of national conferences, study visits and expert missions for the public sector, namely:

National Conference "Challenges of international data transfers from the perspective of the Convention 108+ and GDPR

On January 28, the NCPDP in collaboration with TAIEX project experts organizes the National Conference ***"Challenges of international data transfers from the perspective of the Convention 108+ and GDPR",*** held online. The aim of the Conference is to present information, examples of good practices and innovative solutions on raising awareness and informing the public sector about the challenges of cross-border data transfer. Personal data protection experts from Italy, Germany, Austria and the representatives of European Commission conducted the workshop. Amongst the topics addressed by the experts are: cross-border transfers of personal data from the perspective of Convention 108+ and global trends, overview of the grounds for the cross-border transfers of personal data under the GDPR and the type of safeguards needed, challenges of cross-border data transfers from the perspective of the EU supervisory authorities, cross-border data transfers in the area of law enforcement cooperation, General information on the concept of adequacy and Substantive and procedural aspects of adequacy decisions. About 70 representatives of the public sector attend the event.

Study visit "Data Protection Impact Assessment and the role of the Data Protection Officer"

From 26 to 28 September, the representatives of the NCPDP are conducting a study visit ***"Data Protection Impact Assessment and the role of the Data Protection Officer".*** The Italian Data Protection Authority (Garante per la Protezione dei Dati Personali) hosted the event.

The aim of the study visit was to take over the best legal and operational practices by the NCPDP on Data Protection Impact Assessment (DPIA) mechanisms, processing operations requiring a DPIA, as well as the role of the Data Protection Officer (DPO) within companies/state institutions that are personal data controllers. During the event, the aspects related to processing operations requiring such an assessment; the role of the DPO; data breach risks, transfer of personal data to third countries, as well as an exchange of information, knowledge and experience provided by Telecom Italia S.P.A.

Expert mission "Processing of personal data for statistical purposes"

In July 2022, the NCPDP applied and obtained support from the EU TAIEX project in organizing the Expert Mission ***"Personal data processing for statistical purposes"***. As the requirements of the public sector for reliable statistics on the analysis and understanding of contemporary society become a pressing need, the development of accurate statistics on the collection of the most detailed information possible and the processing of this information using automated data processing technologies and guaranteeing the anonymity of data subjects, increases considerably. The expert mission aims to strengthen the knowledge and skills of representatives of public institutions on personal data processing for statistical purposes. The main objective of the experts' mission is to present the European legal and operational best practices on the mechanisms of processing and storage of personal data for statistical purposes by the National Bureau of Statistics, data exchange between the institutions and the NBS, as well as the regulations related to the security of these data.

At the same time, the expert mission involves the training of the staff from the public authorities such as: NCPDP; National Bureau of Statistics; General Inspectorate of Border Police; Public Service Agency; e-Governance Agency; Ministry of Internal Affairs; Ministry of Health; State Chancellery; State Tax Service; Customs Service.

The event will be organized in early 2023, based on the availability of EU experts.

National Conference „Data Protection Impact Assessment and the role of the Data Protection Officer"

In September, the NCPDP applied and obtained support from the EU TAIEX project in organizing the national conference ***„Data Protection Impact Assessment and the role of the Data Protection Officer".*** Current aspirations to digitize society, as well as the rapid technological developments widely used by both EU and other countries, underline the urgent need for personal data protection - a right guaranteed by both the instruments of the European Union and the instruments of the Council of Europe. The collection, storage and use of personal data at an unprecedented level exposes the data subjects whose data is processed to certain risks. These risks range from discrimination, identity theft or fraud, financial loss, damage to the reputation, etc.

A Data Protection Impact Assessment (DPIA) in this case is more than necessary, as it describes a process designed to identify the risks arising from the processing of personal data, to minimise these risks as much as possible and to detect them as early as possible.

The objective of the conference is to inform and take over the best legal and operational practices by the representatives of public institutions, on Data Protection Impact Assessment mechanisms, processing operations requiring a DPIA, as well as the role of the Data Protection Officer (DPO) within companies/state institutions the main activities of which consist of processing operations which, by their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale as well as the processing of special categories of data. At the same time, during the conference, representatives of public institutions will be trained, such as: Parliament of the Republic of Moldova, State Chancellery, General Prosecutor's Office, National Anticorruption Center, National Bank of Moldova, Competition Council, National Commission for Financial Markets, National Agency for Energy Regulation, National Integrity Authority, Central Electoral Commission, etc.

The event will be organized during 2023, based on the availability of EU experts.

CHAPTER IX
AWARENESS AND TRAINING ACTIVITIES

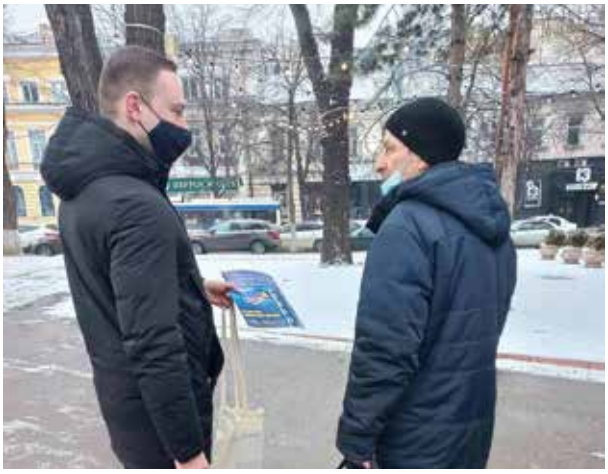
Despite the continuing COVID-19 pandemic, during 2022, the NCPDP was able to make significant progress on awareness and training activities. Trainings were conducted in online, hybrid, as well as physical presence at the entities' premises. In this regard, the NCPDP managed in 2022 to train all local public authorities (LPAs) in the districts of the Republic. Trainings were also organized for central public authorities at the initiative of or in collaboration with the NCPDP.

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

Raising awareness actions

Thus, during the year 2022, 5 activities were organized to inform and raise awareness of citizens and the school community regarding the field of personal data protection, as follows:

- On January 26, 2022, the *"Protect personal data"* street action was held, organized by NCPDP representatives in the context of celebrating European Data Protection Day. In this context, a few employees of NCPDP distributed to passers-by, near the Cathedral Square, information materials, raising awareness among citizens about the concept of personal data, the rights of personal data subjects, security and confidentiality measures when processing data. At the same time, they were informed about the possible situations in which personal data are not processed in accordance with the provisions of national legislation in this field, providing them with practical guidance and recommendations that should be undertaken in such situations.



- On 15 April, the NCPDP launched the information and awareness campaign for school communities with the generic: "*Personal data protection and the safety of children in the online environment*". The first training course was organized at the Public Institution High School "Onisifor Ghibu" in Chisinau, the target audience being the students of the 4th class. The aim of the information and awareness campaign for school communities is to provide high visibility on personal data protection and child safety online, at local and national level, by promoting empowerment and best practice for intervention and support. Later, on May 6, two more training sessions were organized in the same educational institution.

The topics addressed in the training were: *general notions on personal data; the correct use of photos/videos online; risks and threats online; communication on social networks.*

• On 10 July, the NCPDP celebrated 14 years of activity. On this occasion, the institution organized several activities dedicated to the field of personal data protection. Among the activities is the street action organized on July 11 with the generic: "14 years since the foundation of the NCPDP". The street action was organised near the Cathedral Square. Its purpose was to disseminate useful information regarding the field of personal data protection to passers-by, to inform and encourage the citizens of the Republic of Moldova to pay more attention to that field.

- On December 7, the NCPDP organized a workshop for pupils of the 5th-6th grades of IPLT "Gheorghe Asachi" mun. Chişinău.

The aim of the workshop was to promote among students the culture of personal data protection and to encourage respect for private life, especially in the online environment.

Also, during 2022, NCPDP developed and published on the official website www.datepersonale.md, 105 announcements, as well as 26 announcements regarding vacant public positions. In the same way, the authority has developed and published information newsletters with reference to statistical information regarding the activity of the NCPDP, as well as other useful information at the national and international level in the field of personal data protection.

At the same time, there was a growing interest of citizens towards the activity of the National Authority for Personal Data Protection, which can also be deduced from the environment of social networks. In context, the official Facebook page – www.facebook.com/NCPDP registered around 3028 followers and the website https://datepersonale.md/ registered 41281 visitors.

Training activities

During the reference period, the NCPDP continued educational-preventive actions to encourage personal data controllers to implement the principles of personal data processing (the principle of minimization, the principle of legality, fairness and transparency, the principle of purpose-related limitation, the principle of accuracy, the principle of storage limitation, the principle of integrity and confidentiality, the principle of responsibility). In the same context, the awareness of the public about the importance of individual's protection in relation to personal data processing is an immense value. The increase in people's perception and awareness of the importance of personal data protection will also influence the increase in the competitiveness of enterprises, the economic, social and cultural development of the country.

The activity of providing methodological and advisory support from the NCPDP in the context of implementing national legislation on data protection, including cases related to the data protection impact assessment, as well as the implementation of data security measures, targeted a significant number of public and private controllers, with actions and measures necessary to be implemented in this regard explained and clarified. It should be emphasized that, during the post-pandemic period, data controllers still prefer to obtain remote consultations, and therefore, consultations were mostly provided through phone calls in **1105** cases and through email in **101** cases.

In addition, **38** training sessions were organized for data controllers (mostly public authorities) to comply with the legal provisions in the field of personal data protection, where the trained individuals were familiarized with general aspects related to personal data protection, new obligations stipulated by the legislation, and obtained practical solutions for different cases they faced in the context of personal data processing. Approximately **2862** participants attended the training sessions. The topic of the training course was ***"Requirements, principles and new trends in the field of personal data protection***". The main topics covered in the training were the following aspects***:*** legal grounds for personal data processing; processing of special categories of personal data; filming and transmission of district council meetings, depersonalization of data in the State Local Documents Registry; designation of DPO; function and tasks of DPO.

- Thus, in the first half of 2022, **12** trainings were organized in which participated approximately **515** representatives of local public authorities (LPA) as follows:

- On January 27th - Ialoveni District Council;
- On February 4th- Telenești District Council;
- On February 11th - Edineț District Council;
- On February 25th - Drochia District Council;
- On March 11th- Dondușeni District Council;
- On March 25th - Soroca District Council;
- On April 8th - Bălți Municipal Council;
- On April 19th - Rezina District Council;
- On May 6th - Florești District Council;
- On May 20th - Sîngerei District Council;
- On June 3rd - Ungheni District Council;
- On June 17th - Călărași District Council.

The training courses were organized at the initiative of the NCPDP and were held in a hybrid format with online and offline sessions.

• During the reporting period, NCPDP also organized trainings for **1860** representatives from central public authorities, as follows: Customs Service, State Fiscal Service, National Agency for Food Safety, Secretariat of the Parliament of the Republic of Moldova, National Bank of Moldova, for 25 audiences of the Academy of Public Administration and 100 employees of Mobiasbanca (OTP Bank). The trainings were organized in a hybrid format.

- In the second half of 2022, NCPDP representatives continued the training process for APL representatives as follows:

- On July 15th - Nisporeni District Council;
- On July 20th - General Directorate of Youth Education and Sport;
- On August 4th- Strășeni District Council;
- On August 19 th - Hîncești District Council;
- On September 2nd- Anenii Noi District Council;
- On September 22th - Leova District Council;
- On October 11th, the Cimișlia District Council;
- On October 27th, the Soldănești District Council;
- On November 4th, the Cantemir District Council;
- On November 18th, Ocnița District Council;
- On November 25th, the Ștefan Vodă District Council;
- On December 2nd - Basarabeasca District Council;
- On December 9th, the Criuleni and Dubăsari District Councils;
- On December 20th, Taraclia District Council.

In this regard, trainers from NCPDP instructed approximately **487** representatives from representatives from the LPAs mentioned above. Thus, this year, NCPDP managed to train representatives of local public authorities from all districts of the country.

CHAPTER X

MANAGERIAL ACTIVITY OF THE NCPDP

Human resource management

Human resources represent one of the most valuable and strategic investments of an institution, through which its basic objectives and tasks are achieved, and the promotion and implementation of an effective human resources management ensures the achievement of strategic objectives.

In the reporting year, the organizational chart and organizational structure of the personal data protection authority did not undergo changes.

According to the Staff List and the Staffing Scheme, the following categories of functions are included in the NCPDP:

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

The staff limit of the authority is **45** positions. At the beginning of the reporting period, NCPDP had a staff of **39** employees, and at the end of the period, there were **32** employees working in the institution. During 2022, 13 employees resigned from NCPDP, while 6 new employees were hired, including 4 through a competitive recruitment process and 2 through transfer. It should also be mentioned that during 2022, 2 persons were reappointed to their previous public positions, which they held before suspending their employment contracts due to taking partially paid leave for child care until the age of 3. So, at the end of the reporting year, the employment rate of functions within NCPDP was approximately 71%, being with 18% lower than in 2021.

Within the National Authority for Personal Data Protection, an equality policy is applied in the recruitment and management of human resources, thus, the gender ratios representing: 72% (23) – women, 28% (9) – men. However, there is a preponderance of female employees over male employees. The share of women is higher than that of men in both executive and management positions.

In the age structure, the trend of recent years is maintained regarding the inclusion of people aged between 35-45 years, having the largest share - 37.5% of the total number, as well as those aged 25-35 (32, 5% of the total).

So, in the table below shows the proportion of the NCPDP employees by age and gender in positions of public dignity, management and executive positions.

Center staff by age and gender categories

Year 2022	Total effective persons		Functions of office holders		Public management positions		Public execution functions		Auxiliary staff	
	Women	Men	Women	Men	Women	Men	Women	Men	Women	Men
Number of persons	**23**	**9**	**2**	**-**	**9**	**2**	**12**	**6**	**-**	**1**
• < 25 years old	3	1	-	-	-	-	3	1	-	-
• 25-35 years old	7	3	-	-	2	-	5	3	-	-
• 35-45 years old	10	2	1	-	5	2	4	-	-	-
• 45-55 years old	2	1	1	-	1	-	-	1	-	-
• 55-63 years old	-	1	-	-	-	-	-	1	-	-
• 63 years old <	1	1	-	-	1	-	-	-	-	1

In the reporting year, a considerable decrease can be observed regarding the occupation rate of functions/positions, decreasing by approximately 18 percentage points compared to the level recorded in the previous year. This phenomen takes place under the conditions of a low salary in relation to the specifics and volume of work assigned to NCPDP employees.

Degree of employment with staff in the period 2018-2022

Year	Approved units	Effectively, employees	Share, %
2018	45	32	71
2019	45	33	73
2020	45	35	78
2021	45	39	89
2022	***45***	***32***	***71***

The recruitment policy of the NCPDP focuses on a well-defined process, which aims to ensure the optimal staffing needs, based on the principles of open competition, transparency, equal opportunity and professional merit.

In the year 2022, the National Authority for Personal Data Protection faced a considerable reduction in the workforce, compared to the previous reporting years, which conditioned the involvement of the authority in a continuous process of recruitment and selection for employment the vacant positions put up for competition to ensure their proper institutional functioning.

Thus, during 2022, were organized and developed 5 competitions to fill 7 vacant public positions, where 34 candidate files were submitted and accepted, approximately 3 times less than in 2021.

As a result of the competitions held, only 4 people were hired, 2 of whom were debutant civil servants.

It should be noted that 2 competitions have been extended countless times, for example, for the position of state inspector in the Conformity Department - 7 times, and for the position of state inspector in Prevention, Surveillance and Evidence Department 5 times.

Another way of occupying public positions in 2022 within the NCPDP was the transfer from other public authorities, such as from the Ministry of Finance and from the Cricova local Council, Chisinau municipality.

A personnel procedure used in the activity of the NCPDP is the interim provision of vacant or temporarily vacant public management positions. Thus, during the reporting period, 3 civil servants temporarily exercised public management functions of important subdivisions.

At the same time, during 2022, 8 employees were promoted to higher positions, of which 2 were in management positions.

As in 2021, NCPDP faces an exaggerated fluctuation of human resources (about 37%) and a large number of vacant and temporarily vacant positions (about 13 positions).

Staff turnover:

Within the NCPDP, the phenomenon of turnover is at a very high level. This fact increases the risk of the impossibility of carrying out the institution's activity and is determined by the deficiencies in the payroll legislation. Thus, the reference salary of NCPDP employees is approximately 30% lower compared to the salary granted by other entities in the budget sector with similar control activities.

In this context, there is an essential increase in the share of staff with seniority within the NCPDP between 1 and 2 years (41%), which generates the risk of loss of institutional memory.

Thus, after a good professional training and assimilation of the knowledge, work skills necessary to carry out the activity, the employees decide to go to other public authorities for a more attractive salary package.

The procedure for selecting and hiring new staff is onerous and complicated due to the lack of competent and experienced specialists in the field of personal data protection, and the high degree of staff turnover leads to the destabilization of the good performance of the authority's activity and the loss of institutional memory.

Professional training

In order to strengthen the institutional NCPDP tends to ensure continuous professional development for the institution's employees. Training activities of various types and forms are organized in order to deepen and update knowledge, develop skills and model the skills/ behaviours necessary for the effective exercise of job duties.

In this sense, the annual professional development plan was elaborated based on individual professional development needs, according to which, NCPDP employees participated in 6 internal training courses and 15 external training courses. During the reporting period, 45 NCPDP employees benefited from training.

The professional training of employees was carried out mainly at the Academy of Public Administration. At the same time, NCPDP employees also participated in training programs

provided by the Center for Information Technologies in Finance, the National Anticorruption Center, the Ministry of Internal Affairs, etc.

An essential role in the professional development of the institution's employees was played by the exchange of experience with representatives of similar authorities from other countries in order to take over good practices in the field. Thus, 8 employees of NCPDP participated in 2 study visits, one of which was organized in Rome, Italy, in the context of the data protection impact assessment and the role of DPO, and the second – in Tbilisi, Georgia in the context of the European Case Handling Workshop 2022 (ECHW 2022).

Motivation of the staff

It is also necessary to emphasize the stimulating aspect of NCPDP employees in the form of diplomas of honour and thanks, granted by the order of Director on the occasion of professional holiday ***"Civil Servant's Day"*** for the effective exercise of their duties, the manifestation of the spirit of initiative, as well as a sign of high appreciation of contribution made in the field of personal data protection.

Among other achievements in this chapter is the awarding of the Government Diploma to a leading civil servant for prodigious and irreproachable activity in the public service.

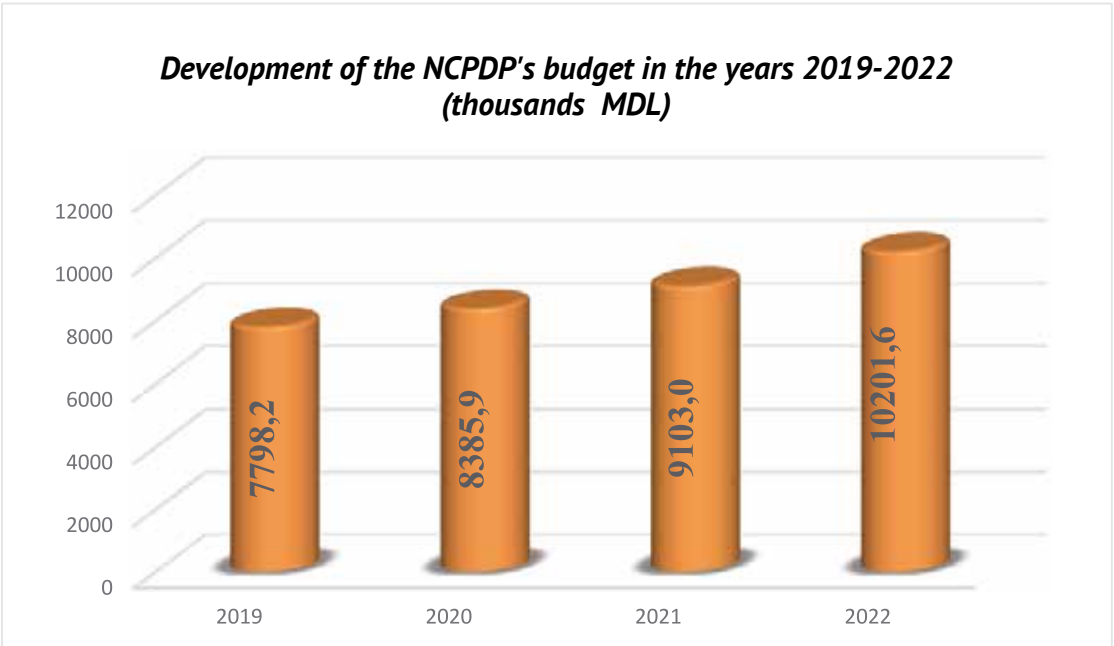
In conclusion, to this chapter, we emphasize that NCPDP, permanently, emphasizes the provision of human resources, the professional development of employees, the motivation and maintenance of staff to ensure the efficiency of managerial processes.

Economic and financial activity

The NCPDP is fully financed from the state budget and has its own budget which is managed independently in accordance with the legal provisions.

The budget of the NCPDP is approved annually pursuant to Art. 19 of the Law No. 133/2011 on personal data protection.

Development of the NCPDP's budget in the years 2019-2022 (thousands MDL)



According to the data of the Report on the budget's implementation in the reporting period, the summary expenditure amounted to 9,137.5 thousand MDL, having the level of execution compared to the specified plan 89.57%.

The distribution of allocations by categories of expenditure was made on the basis of the approved resource framework and in accordance with the needs of the NCPDP for basic activities.

Execution of spending in 2022 *(thousand MDL)*

Indicators	Aproved	Specified	Executed	Executed versus specified (%)
Staff expenditure	7 842,6	7 940,6	7 504,5	94,51
Goods and Services	1 199,1	1 349,1	889,1	65,90
Social benefits	120,0	201,0	159,9	79,58
Non-financial assets, including:	710,9	710,9	584,0	82,14
– *Fixed assets*	385,9	385,9	313,6	81,26
– *Stocks of circulating materials*	325,0	325,0	270,4	83,19
TOTAL	**9 872,6**	**10 201,6**	**9 137,5**	**89,57**

Thus, in the "*expenditure*" compartment, the amount of **9 161,7** thousand MDL was approved, the amount specified was **9 490,7** thousand MDL During the year **8 553,5** thousand MDL were spent.

In the distribution of expendure, the largest share is held by the expenditure for labour remuneration and social benefits/indemnities, where allocations in the amount of 7 962,6 thousand MDL were initially approved, the amount specified was 8 141,6 thousand MDL and the amount executed during the reporting period was 7 664,4 thousand MDL. This reflects the payment of the annual bonus to employees of the NCPDP for the results of work in 2022, social benefits/indemnities, as well as the payment of the one-time payment of exceptional character, according to the Law No.260/2022 on the amendment of the Law on the State Budget for 2022 No.205/2021.

The budget specified in the chapter "*goods and services*" amounted to 1 349.1 thousand MDL, the largest share being in "information services", with a level of execution of 889.1 thousand MDL, forming an unspent balance of 460.0 thousand MDL. This unspent fund was influenced by the amendments made by the Law No. 175/2021 for the amendment of some normative acts, in force since 10 January 2022, which excluded the obligation of personal data controllers to notify the NCPDP, as well as repealed Art. 28 of the Law No. 133/2011 on the personal data protection and stipulated the liquidation of the Register of evidence personal data controllers by irreversibly destroying the documents and information stored both on paper and in electronic format, in accordance with the legal provisions.

With reference to the chapter "*non-financial assets*" we mention that the approved amount, as well as the specified one, amounted to 710.9 thousand MDL.

As a result, during the reporting period, allocations to the chapter "*non-financial assets*" in the total amount of 583.9 thousand MDL were spent in order to ensure optimal conditions for the proper performance of the activity.

In accordance with the provisions of the Law on Public Finance and Fiscal Responsibility No. 181/2014 and the Law on Public Procurement No. 131/2015, 49 low-value contracts for the purchase of goods and services were concluded during the reporting period in order to implement the procurement plan.

In the process of applying the public procurement procedure, factors such as the timeliness of the expenditure and the lowest price criterion were taken into account together with established technical requirements.

All procurement contracts concluded to meet the needs of the NCPDP were executed on time. There were no disputes over the execution of the contracts concerned.

Activity of the Internal Audit Service

The Internal Audit Service is the subdivision of the NCPDP, that ensures the fulfilment of the mission and core functions in the following areas

- *carrying out audit missions;*
- *evaluating the internal management control system.*

The mission of the Internal Audit Service is to perform internal audit assignments, provide advice to ensure the effectiveness of the internal managerial control system, provide recommendations for enhancement and contribute to improving the work of the NCPDP.

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

The Internal Audit Service carried out its work in accordance with the Internal Audit Work Plan for 2022, carrying out the **2** planned audit missions.

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

- *execution of the NCPDP budget for 2021;*
- *Verification of the compliance of personal data processing based on complaints of personal data subjects.*

The internal audit reports have been submitted to the Director of the NCPDP and the operational managers of the audited subdivisions for taking action, according to the competencies.

During 2022, in the process of monitoring by the Internal Audit Service Service of the execution of the aspects mentioned in the audit reports, **11** audit recommendations were implemented, including from the audit mission at the end of 2021.

The degree of implementation of 5 recommendations from 2 audit missions on which the implementation deadline has passed, was 100%.

The implementation of **6** recommendations from the last audit mission, with a reporting deadline of March 2023, is in process.

The monitoring of the implementation of the recommendations is kept under constant review.

The assessment of the Annual Report on Internal Managerial Control (CIM), for the year 2021, has been carried out within the deadline with the preparation and presentation to the management of the Authority.

As a result of the assessment of the report on the CIM, as well as internal training on the given area, with the aim of developing and improving the CIM system, in the subdivisions of the NCPDP in the last year of activity several basic processes were identified and described.

At the same time, 3 new Regulations were drafted/updated and approved within the institution in order to implement the proposals and objections presented in the process of assessing the internal managerial control system:

- *Regulation on the legal regime of conflicts of interest within the NCPDP;*
- *Regulation on integrity warnings, procedures for examination and internal reporting of disclosure of illegal practices within the NCPDP;*
- *Regulation on the inventory and management of sensitive functions in the NCPDP.*

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

At the same time, during 2022, in more than 80 cases, advice and guidance was provided to the authority's staff on public internal financial control.

The procedure for risk management in the NCPDP is approved. Risks are updated and assessed according to the approved objectives and activity actions. The risk management control measures ensure an acceptable level appropriate to the risk tolerance.

Monitoring of control measures within the Authority's subdivisions is carried out regularly, depending on the type of risk, with appropriate reporting.

For the implementation of the Annual Staff Training Plan, the Internal Audit Service has developed instructional-methodological material and has conducted the internal training session on the implementation and development of the Internal Managerial Control System CIM).

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

PROBLEMS AND OBJECTIVES IN THE ACTIVITY OF THE NCPDP

The concerns that hamper the activity of the National Authority for Personal Data Protection, which were reflected earlier over several reporting periods, show their practically unchanged nature over the years that generate increasingly accentuated impediments both in the institutional and organisational activity, as well in the advancement of the field of data protection at the national level. Or, taking into account the fact that solving the urgent problems faced by the NCPDP, mostly exceeds the limit of competence of this authority, it becomes even more difficult overcome/achieve them.

Thus, the harmonisation of national legal framework with the community acquis remains top priority for the field of personal data protection at the national level. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, as well as Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, are the reference documents for achieving the priority.

It should be noted, that the NCPDP together with European experts have developed the draft laws related to the adjustment of the national legal framework to the European legislation. The legislative projects were voted by the Moldovan Parliament in the first reading on 30 November 2018.

In the period after the vote in the first reading, the NCPDP made considerable efforts to improve the mentioned draft laws.

Thus, Parliamentary Commission "Committee for national security, defence and public order" of the Parliament of the Republic of Moldova created the Interinstitutional-working group for further analysis of the relevant draft laws during 2021 in order to finalise the abovementioned draft laws for the second reading. In the framework of this initiative, a number of notes and proposals for adjustments to these drafts were submitted by e-Governance Agency, the private sector (European Business Association, American Chamber of Commerce in Moldova, Moldovan Banks Association, National Association of ICT Companies), as well as by the contracted independent experts. The aim of the draft laws was the accurate and comprehensive transposition of the EU regulations on data protection. The proposals were taken into account by NCPDP as author of the drafts that were analysed and submitted.

In addition, the analysis of the draft laws on the personal data protection and on the National Centre for Personal Data Protection of the Republic of Moldova was carried out among with the proposed amendments after these drafts' approval in the first reading by the Moldovan Parliament during 2021 within the framework of the EU-funded project "*Support for structured*

policy dialogue, coordination of the implementation of the Association Agreement and enhancement of the legal approximation process for the Republic of Moldova". The analysis was carried out by European experts in the data protection field, as well as working meetings were organised during which these draft laws were further discussed with representatives of the Economic Council to the Prime Minister of the Republic of Moldova and civil society.

Subsequently, an interinstitutional working group was established on the platform of the Ministry of Justice at the initiative of the NCPDP in the summer of 2022. This group was ready for a further draft law analysis and finalisation/development that will ensure the alignment of national legislation with the latest EU data protection standards.

As for the work basis or analysis, the draft normative acts were taken in the working group. These draft laws were adopted by the Parliament of the Republic of Moldova in the first reading in 2018, as well as they were supplemented with all the proposals accumulated or announced later in 2019-2021.

It is worth noting that the representatives of the abovementioned working group prepared the referred drafts for the analysis and the review by the end of 2022. Regrettably, the activity of the working group has stagnated up to the time of present report drafting, and not even half of the draft law on personal data protection has been analysed for reasons not attributable to the NCPDP.

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

It is worth mentioning that the Republic of Moldova currently has a major lack of regulations that resonate with the regulations provided by European law on the personal data protection, as well as provide secure protection for individuals with regard to the personal data processing and respect for the right to inviolability of privacy. In this regard, it is necessary for the Republic of Moldova to harmonise its national legal framework with the European provisions on the personal data protection, namely the provisions of Regulation (EU) 2016/679 and Directive (EU) 2016/680.

The process of legislation harmonization is essential to maintain an upward trend in personal data protection and to ensure that the rights of personal data subjects are genuinely respected. Furthermore, this harmonization promotes a legally secure environment for personal data controllers.

It is noteworthy that the implementation of new regulations at national level in the personal data protection field will contribute to the fulfilment of the commitments undertaken by the Republic of Moldova in relation to the European Union and, likewise, to the recognition of the adequate level of personal data protection in the Republic of Moldova, which will generate a wide range of benefits such as increasing the trustworthiness of the state, strengthening the economic strategy, developing the business environment, attracting investment etc.

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

However, in view of the fact that the specific nature and volume of the activities in which the employees of the NCPDP are involved have increased considerably in recent years, it is crucial and mandatory to strengthen and ensure the efficient functioning of the supervisory authority for the compliance of personal data processing.

In order to ensure the independent exercise of their powers, employees of the NCPDP must be adequately remunerated in the same way as other employees of independent institutions and have a salary equal to that existing in the authorities falling within the scope of activity of the NCPDP, subject to verification by the NCPDP of the lawfulness of the processing of personal data.

To address the current institutional crisis, the NCPDP has submitted multiple requests over the years to the Ministry of Finance, the Parliament of the Republic of Moldova and the Prime Minister of the Republic of Moldova for the salaries increase of its employees. However, these requests were not considered in the drafting of the Laws on State Budget for years 2020, 2021, 2022 and 2023.

We emphasize that, according to the levers of competence regulated by the relevant legislative acts, the NCPDP is vested with supervisory powers in the segment of personal data processing such as under:

- actions related to the prevention and investigation of offences, enforcement of sentences, and other activities in criminal or misdemeanour proceedings under the law;
- processing of personal data related to health status, DNA data, dactyloscopic data and other sensitive information carried out in automated form (e.g., databases/information systems) and/or manually;
- actions related to the use of video media in public and private spaces, where the expanding and rapid development of technologies in this field may potentially violate the fundamental rights and freedoms of individuals;
- verification of suitable technical and organizational measures to protect the security of services provided by electronic communications service providers;
- verification of the legality of posting, publishing, and disseminating personal data online;
- operations related to accessing, viewing and using personal data stored in various automated and/or manual filing systems.

It is important to note that the competences of the NCPDP have a broad scope since all data controllers process personal data, whether in the public or private sector, by natural persons and by legal persons. In practice, the processing of personal data is becoming increasingly complex and diversified, including the use of innovative methods and possibilities.

It should be noted that the low salary level for the NCPDP's employees creates a severe chain problem, namely, high staff turnover, which significantly disrupts the work of the NCPDP. In this regard, we note that in recent years the NCPDP has faced severe staff fluctuation.

Thus, during 2021, 12 persons resigned, and during 2022 - 13 persons, 10 of whom each year from the subdivisions carrying out the core functions of the NCPDP, engaged in carrying out investigations/controls on the compliance of personal data processing and in prevention/ monitoring actions.

It is worth noting that the majority of employees who resigned between 2020 and 2022 left to work in other public authorities where the salary is more attractive, such as the National Integrity Authority, National Anticorruption Centre, Customs Service etc. However, it is important to emphasize that the high staff turnover is ultimately caused by the low level of salaries, which does not reflect the complexity and volume of activities carried out by the NCPDP.

The figures mentioned above may seem insignificant in the case of institutions with a large number of employees, but in relation to the number of NCPDP personnel (45 units, according to the staff limit) the number of resignations is dramatic (20 people resigned during the 2021-2022 period), especially those involved in conducting investigations/activities of the authority's core functioning (27 existing units, according to the staff status, and 17 employees were working at the end of the reporting period). This reality is even more concerning in the context of the lack of qualified specialists in the personal data protection field, as a new employee requires a period of professional education/training in the field of more than a year. As a result of recruiting new employees, NCPDP invests financial, logistical and human resources, which are not subsequently justified due to the significant fluctuation of employees.

Over the past few years, several recruitment competitions have been held to fill vacancies in the NCPDP. However, these competitions have not been successful in producing suitable candidates due to the unattractive salary offered by the NCPDP. In some cases, even after being offered employment, candidates have refused to take up the positions due to the low salary.

Moreover, the NCPDP is unable to recruit and retain qualified specialists in the field of information technologies due to the same reason of unattractive salary levels. IT specialists of the data protection field are essential to the work of the authority, as they require advanced knowledge and skills to meet the current challenges.

It should be pointed out that most employees of the NCPDP tend to be employed by public authorities with a much higher salary level than the Data Protection Authority.

Failure to address the issue of increasing NCPDP employee remuneration will result in a number of negative consequences, including decreased employee motivation, increased staff turnover, an expansion of job responsibilities for remaining employees due to a lack of personnel, a negative impact on the emotional well-being of employees, destabilization of existing employment relationships, a weakening of the institution's capacity, loss of institutional memory, and the inability of the NCPDP to fulfil legal obligations and respond to requests etc.

In light of the above, it is imperative to remedy the institutional crisis within NCPDP through legislative measures that guarantee an adequate level of remuneration for the employees of the institution in question. Otherwise, the process of exercising the powers of the NCPDP to guarantee and protect the right to inviolability of privacy and the right to personal data protection of the citizens of the Republic of Moldova, a right that concerns absolutely all citizens, regardless of social status, function, political affiliation, etc., is seriously disrupted.

Carrying out a synthesis of problems faced by the NCPDP **-** legal, institutional, perception and applicability issues, which require urgent solutions in order to overcome the stagnation in the

field of personal data protection at national level and which are, for the most part, reflected in detail in the content of this report, are the following:

- ✓ ***disparity between the national legal framework in the field of personal data protection and the new regulations existing at European level***;
- ✓ ***discriminatory salary level of the civil servants within the NCPDP*** as compared to the one provided to other supervisory bodies, with similar status, and taking into account the specific activities that undoubtedly presume the personal data processing, are subject to verification of legality of data processing by the NCPDP;
- ✓ ***staff turnover*** and insufficiency/lack at national level of qualified specialists in personal data protection field;
- ✓ ***the small number of employees in relation to the increasing workload***, especially in the basic subdivisions of the authority: the General Department for Surveillance and Conformity, the Legal Department, especially in the context in which the same employees examine complaints, participate in the drafting and approval of draft normative acts, carry out controls/investigations of the compliance of personal data processing, carry out the duties of ascertaining agent, participate as trainers in trainings, represent NCPDP in courts in administrative litigation and contravention procedure, without being created / assured and reliable institutional mechanisms for carrying out the prescribed tasks;
- ✓ ***the lack of adequate safeguards for the NCPDP staff*** with regard to the risks arising from the control activity and interference by certain legal bodies subject to control by the NCPDP with the aim of intimidating the NCPDP employees by fabricating files;
- ✓ ***the inefficiency and insufficiency of the coercive levers for the unlawful processing of personal data,*** the reason being the double, contradictory and susceptible character of the procedures for examining the findings resulting from the checking lawfulness of personal data processing, manifested by doubling examination in court, in the same period, the same documents and findings issued by the NCPDP, both in administrative litigations and in contravention procedure(detailed information reflected in the chapter representation in court);
- ✓ ***abusive use, in particular by representatives of public authorities, of the legal provisions in the field of personal data protection,*** the alleged argumentation of the refusal to present the requested information through the realization of the right of access to information***;***
- ✓ ***the huge number of personal data access operations stored in state automated information resources, with the use of SIC "Access-Web" and COI, which creates difficulties in identifying the user who accessed the personal data and, respectively, the purpose and legal basis of the access,*** **or, where appropriate, the need to ensure the granting of access to the registers / the fyling systems managed by the Public Services Agency only through the governmental electronic authentication and access control service (MPass).**

The Center's objectives for 2023 - essentially to undertake the necessary actions to address the concerns highlighted above. Thus, the basic objectives outlined for the immediate period ahead, but not limited to those described below, will focus on ensuring:

- ✓ ***compliance of the national legal framework in the field of personal data protection with the new regulations at European level,*** by approving by the Parliament of the Republic of

Moldova in final reading two draft laws: on personal data protection and on the National Center for Personal Data Protection.

- ✓ ***the salary increase of the NCPDP staff,*** linked to that provided for other control bodies of similar status, which, having regard to the specific nature of the activity, are subject to verification of data processing legality by the NCPDP;
- ✓ ***increase of the staff limit*** of the National Authority for the control of personal data processing, ***in relation to the workload and competencies assigned to the NCPDP***;
- ✓ further fulfilling of the Action Plan for the implementation of the Association Agreement Republic of Moldova – European Union;
- ✓ continuation and enhancement of actions to ***raise awareness of the importance of personal data protection***, both from the point of view of respecting the rights of the data subjects and from the perspective of ensuring the implementation of the obligations related to the personal data controllers;
- ✓ contributing ***to raising the level of correct interpretation and compliance with the legal provisions in the field of personal data protection*** by the actors involved in personal data processing, including by ensuring the balance between the legal provisions related to the rights of access to information, the freedom of expression and the personal data protection;
- ✓ raising awareness of development partners in carrying out joint projects, in order to ensure the adequate level of personal data protection in the Republic of Moldova.