08.06.2018

**Conclusions about the survey for**

**National Centre for Personal Data Protection**

Survey for National Centre for Personal Data Protection (NCPDP) was completed by 18 respondents. In NCPDP work 30 employees.

**Personal data, principles relating to processing of personal data,**

**legal basis for personal data processing**

*What are the personal data in your opinion? Please mark the data what are personal data*: *[..]*

**Conclusion:** On the first question was only one wrong answer. 55,6% of NCPDP employees checked this wrong answer as correct (that street`s name is personal data).

*Do you process personal data and what kind of personal data do you process?*

Most of NCPDP employees (94, 4%) mentioned that they process personal data. They point out in the survey that they process such personal data: first name, last name, personal identification number, address, medical data, bank data, all mentioned, including data from the ID, home address, health status, ethnicity, telephone number, civil status, medical data, criminal record, data on family members, sex, date and place of birth, citizenship, signature and e-mail, data in the civil status documents, data in the driving license, data in the certificate of registration, administrative offence sanctions, social security number, mandatory health insurance number, telephone/fax, mobile phone, address (home/residence), e-mail, genetic data, biometric or anthropometric data, dactyloscopic data, occupation, position, training, personal identification number, family situation, military situation, economic or financial situation, data on property, banking data/preferences/behaviour, image, voice, geolocation/traffic data, physical characteristics, health data, beliefs: ethnic, political, racial, religious. Daily processing (within the meaning of the definition "data processing" provided by Article 3 of the Law on personal data protection) personal data in the most varied fields of life: work, studies and other activities, including categories the data specified in the question, even special data. However, this processing is exempted from the provisions of the law on the protection of personal data under paragraph (4) Article 2 of the Law on the personal data protection, special category personal data, Facebook nickname, digital signature.

*Please mark the legal basis for the data processing [..]*

Various answers were given to this question. For instance, only 22,2% of NCPDP employees marked that legal basis for the personal data processing is person`s vital interests; 55,6% - person`s consent; 38,9% - controller`s legitimate interests; 33,3% - agreement between person and controller.

Majority of NCPDP employees marked correct that the legal bases for the data processing are legislative acts – 88,9%; governmental authority tasks, duties – 77,8%.

*What kind of data purposes do you have? Please, specify each of them.*

The NCPDP employees indicated such personal data purposes:

“Reply to a letter; the purpose of protection of rights, the purpose of executing the duties of the service. Job description. The purpose depends on the specific case. Execution of a contract to which the data subject is a party or for taking action prior to the conclusion of the contract at its request; fulfilment of a controller’s obligation under law; protecting the life, physical integrity or health of the data subject; the performance of tasks of public interest or resulting from the exercise of the powers of public authority delegated to the controller or third party to whom the personal data are disclosed; the legitimate interest of the controller or the third party to whom the personal data are disclosed, provided that such interest does not prejudice the interests or the fundamental rights and freedoms of the subject matter of personal data; Statistical, historical or scientific research purposes, provided that personal data remain anonymous throughout the processing. Filing of complaint. The purpose must be determined, explicit and legitimate. The enumeration of "every" purpose for which data will be processed is a utopia, as it is not possible to give exhaustive indication of the purpose for which the data will be processed, as the data is processed in any field. Ex: There are various purposes in the relationship between traders, such as contract execution, debt recovery, marketing, etc. Examining a complaint, establishing identity, possibly the guilt. Under law. Information notes, competitions, tenders. I do not know. To identify the person, inform the person, summons, etc. Duty related. Keeping state registers, performing justice, population records or civil status records, human resources, electoral records, etc. Keeping state registers, responding to complaints, requests, etc. Personal. Organization of service trips.”

*Do you have the personal data processing which is based on person’s consent? If you have, please specify the personal data processing.*

66,6% of NCPDP employees point out that they process the personal data based on person`s consent; 33,7% point out that they don’t process the personal data based on person`s consent.

*Please mark the personal data protection principles [..]*

NCPDP employees marked correct answers about data protection principles but also 88,9% of NCPDP employees marked one wrong answer that personal data protection principle is personal data should be processed in public registers.

*How long do you process the personal data? Please, specify the period for which the personal data is stored, or if that is not possible, specify the criteria used to determine that period. If you have more than one data processing, specify the period of processing for all data processing.*

NCPDP employees point out such answers about storage periods: 7 years, to achieve the purpose, completion of the verification, until reaching the purpose, the processing time differs on a case-by-case basis, depending on the complexity of the case, the managed material and the time needed to settle the case (1 month, 5 months, 1 year), until reaching the purpose of personal data processing, I process personal data until the purpose is reached. Some data is stored for personal or family interest for an indefinite period. Until final settlement of the complaint case. I do not keep processed personal data. Until the purpose is reached. Unlimited storage term. For the period set by the legislation. Criteria - reaching the purpose for which the data was collected.

**Conclusion:**

1. From given answers the expert concludes that NCPDP employees understand what in practise mean personal data, distinguish common category of data and sensitive personal data. Also they process the personal data what they need for their duties. NCPDP employees don’t need education about definition of personal data.
2. Part of NCPDP employees does not understand what are the legal basis for personal data processing. To create an understanding and a common interpretation what are the legal basis of the data processing, there is a need for a training about legal basis of the data processing, explaining the differences among these legal bases. Some respondents answered that NCPDP process personal data based on person`s consent. It is unclear when for what activities of the Center this legal basis is used. So there is a need to have trainings about data subject`s consent and differences between the controller`s legal obligation and performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
3. Part of NCPDP employees have an understanding about what is purpose of the personal data processing, they can separate purposes.

For NCPDP employees who have recently been recruited training about the purposes for personal data processing when they fulfil their duties shall to be performed. The topic about the purposes could be included to the training program about the data processing principles. Implementation of general personal data protection principles have to be explained using certain practical examples.

1. NCPDP employees know storage limitation principle but don’t know how long they can storage personal data when they fulfil their duties. Question about personal data storage is connected with archive issues and rules in the other legislative acts. Principle of personal data storage limitation have to be included in the training program. NCPDP like other controllers should storage personal data for fixed period what is written in legislative act. If there are no legislative acts, controllers have to create internal procedure where the storage period is notified.

**Data subject rights**

*Do you obtain personal data from another sources, for example, from another institution, private companies, government authorities, information system etc.? Please specify them.*

NCPDP employees point out that they got personal data from NGOs, Ministries, from individual. Institutions that are eventually concerned during the verification. Depends on the context. LLCs, state authorities. Automated Information system “Register of personal data controllers”, public authorities, private companies, etc. State institutions, private entities, mass-media. Public authorities, information systems (state registers). Online, phone. Not yet part of my job. I do not know. Query. From people, other institutions. Prosecutor's Office, criminal prosecution bodies. Private companies, state authorities, information system. Facebook. No.

*If you inform person before the data processing or when you obtain personal data, please, specify information what you provide the person.*

The NCPDP employees on this question answered: The right of opposition. Is informed that the document contains personal data, and further processing only according to the Law. That it is processed or that it will eventually be processed. No, because it is related to the fulfilment of a work duty, according to the law. That his/her personal data is to be processed and he/she has rights according to the law on the personal data protection, as stipulated in art. 12-18. Purpose of processing. The data categories, their sources of origin and the purpose/legal grounds. No. Preventive notice about the purpose for which data processing takes place. I don’t know. Your data was collected for your employment purposes. Example: the phone call is being recorded. Established in art. 12 of the Law on personal data protection. Data.

*Do you profile personal data? If yes, please specify cases.*

NCPDP employees pointed out that four of them profile personal data. Also answered - No. Not in materialized or automated form. Abstractly, by addressing the question, each person projects the psychological/social/ professional profile of a person, according to the information at his/ her disposal (this largely being personal data). I don’t know.

*Please specify data subject’s rights?*

NCPDP gave such answers: the existence of rights of access to data, data interference and opposition, as well as the conditions under which they can be exercised; c) if the answers to the questions with which the data are collected are mandatory or voluntary, as well as the possible consequences of the refusal to answer. (2) Where personal data is not collected directly from the data subject, the controller or processor is obliged, at the time of data collection or, if it is intended to be disclosed to third parties, at the latest, first disclosure to provide the subject of personal data with information on the categories of data to be collected or disclosed - processing of personal data is done for statistical, historical or scientific research purposes; the provision of information is impossible or involves a disproportionate effort to the legitimate interest that might be harmed, - the registration or disclosure of personal data is expressly provided for by law. the right to oppose, access, modify data.

Right of access, intervention, opposition, not to be subject to an individual decision, to notify the court. The right of access to data, the right to oppose, the right not to be subject to an individual decision. Information on the subject of personal data, the right to access personal data, the right to interference with personal data, the right to object to the subject of personal data, the right to access to justice in the event of breach. Information, Opportunity, Access, Rectification, Data Clearing, Intervention. Chapter III of Law No.133. Information, access, intervention, opposition, an individual decision. Information, access, intervention, opposition, not to be subject to an individual decision. Law 133 on the protection of personal data. The right to respect for privacy, the right to be informed about data processing, the right to be forgotten. Do not know. The right to information. The right of access to personal data, the right to interfere with personal data, the right of opposition of the subject, the right not to be subject to an individual decision.

• According to the provisions of art. 12-18 of the Law on Personal Data Protection no.133 of 08.07.2011, the subject of personal data has the right to information, the right of access to personal data, interference with personal data, the right to object to personal data, the right not to be the subject of an individual decision, the right of access to justice. For the purpose of exercising these rights, the subject is to address via a written request to the personal data controller and/or the processor. Right of access, information, deletion, rectification, opposition

**Conclusion**

From these answers the expert concludes that NCPDP employees have different approach for implementation of providing information for data subject.

Trainings about data subject`s information when NCPDP employees obtain the personal data from the data subject and when from other source have to be provided. This training should be focused on the theory and the practical issues how to inform data subjects about their rights in correct and transparent form, including information about others rights of data subject - right to access, right to rectification, right to erasure, right to restriction of processing, right to data portability, right to object, right no to be subject to a decision on automated processing, including profiling. In the expert`s opinion NCPDP should be an example for others how to implement data subject`s rights in practise. NCPDP process its employee’s personal data and should respect requirements for the data processing also for this activity.

**NCPDP competence**

*Did you notify the processing of personal data in the National Centre for Personal Data Protection accordance with Law on Personal Data Protection?*

61,1% of NCPDP employees answered no, 27,8% - yes, 11,1% - I don’t know.

*Please, highlight the duties of the National Centre for Personal Data Protection* – 44,4% of NCPDP employees point out that NCPDP duty is to impose fines for data protection breaches; 77,8% - to advise persons in personal data protection field; 94,4% - to advise controllers; 61,1% - to develop laws; 22,2% to carry out investigations on public authorities; 100% - to inform the society about importance of data protection; 0% - to arrest persons who illegally process personal data.

Survey was a question about NCPDP role, 11,1% thinks that NCPDP should be advisory institution (gives advice to the controllers); 5,6% - punishing institution (imposes administrative fines for data protection breaches); 44,4% - preventive institution (explains to controllers and data subjects how to process the personal data) and 38,9% gave other answer - Center, it is an autonomous, independent and impartial public authority in relation other public authorities, individuals and legal entities, exercising the attributions given to it by law and impartial on the protection of personal data. 1,2,3. Authority verifying the legality of personal data processing. The control body in the field of data processing. Institution. Answers a), b) and c)

In the survey was the question about NCPDP status, all NCPDP employers answered that NCPDP should be independent institution.

*For what purpose does the NCPDP use the register of the controller?*

NCPDP gave such answers: For data protection purposes. Verification. Records of the controllers and personal data categories being processed, filing systems in management. Purpose of protecting personal data. In order to achieve the policy of ensuring an adequate level of protection of personal data. For recording and filings. Probably the Controllers Register' (plural) \_ probably as a measure of education and awareness. It is in fact not worth keeping such a register. Record of authorized controllers, informing citizens. Legal. In order to keep a record of existing personal data controllers. do not know. In order to see if it is registered as a personal data controller. The purpose of ensuring transparency and the purpose of ensuring the registration as a data controller. The registration of personal data controllers and the registration and filing systems managed by them. To help make data controllers comply with the provisions of law 13

*Should the requirements for the registration of personal data processing, as well as the amount of information to be provided be the same for the private and state sectors?*

55,6% of NCPDP employees point out yes, 44,4 % - no.

*Do the areas that pose a high risk for a person in the process of personal data processing should be registered in the register of the controller?*

88,9% of NCPDP employees point out – yes, 11,1 %- no.

*List the areas in which the data processing, in your opinion, is considered as a high risk to the rights and freedoms of data subject?*

NCPDP employees point out such answers: Education, services. Courts, journalists, TV stations. All areas that do not have security policy. Police, banking, financial, medical, online environment. Special categories of personal data, minors. Medical, Police, Digital. Police, fiscal, medical, banking, national security. Banking, law enforcement, private sector. Politics, marketing/advertising, etc. Health, financial situation, banking, the social networks, in the areas referred to in Article 24 of the Law on personal data protection. Medical. Profiling, processing of special categories of personal data.

*What actions does the NCPDP perform to perform a prior checking?*

NCPDP employees gave such answers: do not know (2). Issues certain queries to the institutions, bodies or entities concerned or which may relate to the case under examination. Examines accumulated material. Actions provided by Article 24 of the Law 133. If the Center finds that the notice under review requires prior checking, i.e. it falls under one of the provisions of paragraph 2 art. 23 of the Law on personal data protection, then this verification will be done within 5 days. The time limit for examining the notification contained in the pre-verification compartment is reviewed for up to 45 days, with the possibility of extending for a further 45 days; those provided by art. 24 of the Law on personal data protection. Verify the legality of data processing by controllers who get registered as such. Request information; control; checking the controller if it complies with all legal requirements. Center’s notification; provided in the Law on personal data protection and the Regulation of the Register of Personal Data Controllers, approved by the Government Decision no. 296 of May 15, 2012.

*NCPDP starts investigation on the basis of (choose several answers):* 94,4% of NCPDP employees point out - complaint made by a data subject, 33,3% - prior checking; 77,8% - NCPDP own initiative;

*NCPDP in the process of investigation can apply the following legal obligations for the controller (choose several answers): 88,9% -* to impose a temporary or definitive limitation including a ban on processing; 77,8% - to order a rectification or deletion of personal data of processing; 38,9% - to impose a fine; other -Issues the offence report; Within the investigation the Center request relevant data and materials on the case, and the processing ban (suspension, destruction ban etc) may be enforced by the Center’s decision.

*Does the NCPDP provide consultations for the public sector before public institutions begin develop a database/information system/register and while it is in progress?*

77,8% of NCPDP employees answered - Yes; 22,2% - no.

*Indicate institutions which have similar rules (legal regulation) on personal data protection (choose several answers)*: 55,6 % of NCPDP employees point put private companies; 72,2% - tax institution; 38,9% - Parliament; 66,7% - Court; 5,6% - Moldovan orthodox church; 72,2% - Police; 55,6% - Ministry of Agriculture; 66,7% - Ministry of Justice; 11,1% - Privesc.eu.

**Conclusion**

1. The expert concludes that NCPDP should have information about their duties according to GDPR. The training should provide information about an idea of records of processing activities, what does it mean, what information this records should contain, when controller has to make this records, when NCPDP has the right to ask for it. If it is possible training should provide some ideas how to make this records of processing activities.

Also the training should have the information about the data protection impact assessment, meaning of this assessment, when this assessment controller have to make, when NCPDP has to ask for it, examples how to make this impact assessment.

The experts suppose that NCPDP should have the training about a high risk data processing, what data processing activities could be considered as a high risk processing, how to understand that data processing will bhave a high risk. Such training is needed because GDPR doesn’t have rules for registration controllers and their data processing. GDPR has rules about records of processing activities what should be done by controllers. GDPR prescribes that controller shall make impact assessment for high risk processing and make prior consultation with data protection authority. It would be necessary to provide trainings on procedure of prior consultations and scope of impact assessment. It is new duty for all supervisory institutions. The training should provide information about the meaning of this prior consultation, when this prior consultation is obliged, how to organize this prior consultation.

1. The expert considers that the training should provide information about supervision, how to make supervision more effective. It could be done through exchange of experience between NCPDP and an expert.
2. One of the main thing on what NCPDP should have to work is prevention and monitoring of the personal data processing. GDPR makes supervisory institution more proactive authority, but not punishing authority. The training should focus on monitoring on the personal data processing, how to make monitoring process more effective and how to organize prevention in a way that in the future there are less offenses.

**Transfers of personal data to another institution, other countries**

**or international organisations**

*Do you transfer the data to other public or private institutions? If yes, please specify the recipients or categories of recipients (for example, law enforcement agencies, courts, public registers, ministries, private companies etc.) for the personal data. If you have more than one data processing purpose, specify the recipients or categories for the recipients for each personal data processing.*

NCPD employees indicated that they transfer the personal data to Central Public Administration, NGOs. City halls, microfinance organizations, law firms, Ministry of Economy and Infrastructure, Local District Councils, Union Fenosa, Local Public Administration. Authorities or entities that are concerned in complaints, notifications of the data subject. Courts, companies, ministries. Public authorities, data subjects, their representatives. State bodies in the judiciary and executive branch, private entities, individuals. Please note that the definition of the recipient within the meaning of Art. 3 of the Personal Data Protection Law stipulates that the bodies in the field of defence, criminal prosecution and courts are not recipients of personal data. Law enforcement agencies, judicial authorities, other public authorities. Social Security Office, Mandatory Health Insurance Office, Tax Authority etc. State authorities. Judicial institutions, etc. Ministries, international organizations.

*What requirements should be complied to transfer data to other countries and EU Member States?*

NCPDP gave such answers: the legal framework; be a state-level data protection authority, the data security policy should be adequate; verify the purpose and legal basis, the level of protection of the personal data in the countries to be transmitted, etc.; the protection level and guarantees of the state where the data is transmitted - if it is party to Convention 108

Appropriate level of data protection. Framework established in the field. Party to the Convention Bilateral treaties, special laws in other situations provided by Article 32 of the Law 133; If the transfer takes place in EU Member States, there is a list with adequacy decision. If the transfer takes place in other non-EU states, then an adequate level of protection must be ensured and a contract should be submitted in case of transfer. Another State is to guarantee an adequate level of protection for DPA. The provisions of art. 32 of the Law. State party to Convention 108, national law and the establishment of a DPA authority. International treaties, contract execution, etc. Compliance with applicable legislation; be protected. The EU Member State must be a member of Convention 108. Transmitting personal data to states that provide or do not provide an adequate level of protection; consent of the data subject, etc. Those established by art. 32 of the Law on the protection of personal data. EU. The existence of data protection legislation (2) the existence of a DPA.

**Conclusion**

1. From the answers of this question the expert considers that NCPDP employees understand what the recipients are. The expert considers that NCPDP don`t need training about recipients. But the expert doesn’t have answer on question`s part about purposes for the personal data transfer. That`s why the training should include information about a requirements for the data transfer within public authorities (legal basis, purpose, types of the personal data or categories etc). If personal data is transferred between Moldavian institutions, there should be an agreement about the personal data processing between /among institutions. The training should have information about the agreement content.
2. The training should provide the requirements when personal data could be transferred to another country or international organisation.

**NCPDP internal procedures**

*In survey were questions about internal procedures for receiving visitors and providing consultation.*

NCPDP has internal procedure for receiving visitors and providing consultation but doesn’t have consulting hours for visitors.

94,4% of NCPDP employees would like consulting hours. If in NCPDP would be consulting hours, it will better organize NCPDP employees work.

*Does the NCPDP develop guidelines in any areas of personal data processing? In case of a positive answer indicate an area in which guidelines are developed.*

NCPDP employees point out that NCPDP has written guidelines for law enforcement agencies, education, healthcare, research.

*Should the NCPDP publish anonymised NCPDP decisions to inform the public about the most common offences in personal data processing?*

83,3% of NCPDP employees point out that it will be a good idea how to inform society about the data protection rules and violations.

*Has the NCPDP developed an internal procedure to perform a prior checking?*

77,9% of NCPDP employees answered yes, 22,2% - no.

*Does the NCPDP have a specific internal procedure for processing a data subject’s application/complaint?*

94,1% of NCPDP employees answered – yes, 5,9% - no,

*How does the NCPDP verify the identity of the person who submitted the application/complaint?*

NCPDP gave such answers: are not checked, just the signature. Sometimes cannot be verified. Identity is not verified. Based on the identification data stipulated in the complaint. Indicating the data in the complaint, name, surname, e-mail address, home address, handwritten signature/ electronic signature. Currently it is not possible. Only in some cases by hearing/contacting the person; by phone, by inviting to an interview, etc. Call the phone number written in the request. I do not know. Summoning the person concerned to give explanation. According to the citizen's identity card. According to the provisions of the Law on Complaints. Public sources. By submitting an official document certifying the identity of the data subject.

*Should the NCPDP have to verify the identity of the person being provided with the telephone consultation? In the case of a positive answer, please describe the arrangement.*

44,4% of NCPDP employees answered – yes, 55,6% - no.

Submitting the report. In case of reasonable doubt by summoning to the Center and hearing the person in order to establish the correct identity. Requesting the person to report to the Centre; whom am I speaking to, if it is you, please report to the Center. By corroborating data from the Population Register with the information provided by the subject.

**Conclusion**

The expert concludes that NCPDP has some internal procedures, but it could be elaborated according to the new draft law. From the answers the expert concludes that there are no internal procedures how to organize visit hours for the visitors, how to verify the identity of the person being provided with the telephone consultation, how to verify the identity of the person who submitted the application/complaint, procedures of complains handling and prevention and monitoring procedures. The training shall provide tools how to organize NCPDP work more effective and how to deal with visitors, complainers and how to identify persons when it is necessary.