Draft

PARLIAMENT OF THE REPUBLIC OF MOLDOVA

LAW

for approving the National Development Strategy of the Personal Data Protection domain for the years 2013-2018 and the Action Plan for its implementation

The Parliament passes the present ordinary law.

Art.1. – To approve:

The National Development Strategy of the Personal Data Protection domain for the years 2013-2018, according to Annex No. 1;

The Action Plan for the implementation of the National Development Strategy of the Personal Data Protection domain for the years 2013-2018, according to Annex No. 2.

Art.2. – The Government shall adjust the national programs and action plans to the objectives and priorities set forth in the above-mentioned Strategy.

Art. 3. – The National Center for Personal Data Protection shall monitor the implementation of the Strategy and shall submit annual activity reports to the relevant parliamentary committee, covering information about the carrying out of the activities set in the Action Plan.

President of the Parliament **Igor CORMAN**

No.229, Chisinau, 10th of October 2013

Annex No. 1

NATIONAL DEVELOPMENT STRATEGY
of the Personal Data Protection domain
for the years 2013-2018

Introduction

The National Development Strategy for the development of the field of Personal Data Protection Development for the years 2013-2018 (hereinafter referred to as the Strategy) is the main policy document tackling the problems existing in the field of personal data protection, identifying the tools to settle these problems, and analyzing the impact on individuals, in particular, and on the State, in general.

The respective document sets forth the mid-term objectives and tasks to ensure an adequate level of personal data protection, by consolidating the dialogue with the interested stakeholders from the public and private sectors to increase the awareness about the need to implement personal data protection measures, by raising the awareness of individuals about the rights they have as personal data subjects, including through development and enhancement of the legal, institutional, and social frameworks necessary to harness the potential benefits.

The Strategy sets forth the following priority development directions:

a) strengthening the adequate legal, institutional, and social frameworks to ensure protection of individuals' fundamental rights and freedoms related to personal data processing, especially the right to inviolability of intimate, family, and private life, enshrined in the Article 28 of the Constitution of the Republic of Moldova;

b) establishing the necessary mechanisms to enforce the Law no. 133 of 8th of July 2011 on Personal Data Protection and for controllers and other processors to implement the provisions of this legislative act;

c) raising awareness among the personal data subjects about the rights they have and the existing tools to take decisions about the use and disclosure of personal data related to them;

d) institutional strengthening of the National Center for Personal Data Protection of the Republic of Moldova (hereinafter referred to as the Center), empowered with duties to control the compliance of personal data processing with the legal requirements so as to ensure the functionality, independency and impartiality of this national authority.

The existing normative and policy frameworks, as well as the European best practices and the specific peculiarities of the field of personal data protection in the Republic of Moldova were taken into account while developing the respective Strategy.

At the same time, were taken into account the conclusions and recommendations formulated by the European experts in the "Personal Data Protection in the context of the Visa Liberalization Regime Dialogue and Negotiations of the Future European Union – Republic of Moldova Association Agreement" Study, as well as within the European Union – Republic of Moldova Cooperation Project "Support to the Government of the Republic of Moldova in the field of anticorruption, reform of the Ministry of Internal Affairs, including the police and per-

sonal data protection" (MIAPAC).

The gradual implementation of the activities included in the Strategy will contribute to the establishment of a solid and coherent framework to guarantee individuals' right to personal data protection, ensuring the increase of confidence for online services, which is an essential criterion to harness the digital economy potential, leading thus to fostering economic growth and intensification of cross-border exchange of personal data.

The Strategy shall use the notions defined in the Law No. 133 of July 08, 2011 on Personal Data Protection, the Requirements for ensuring personal data security when such data are processed in personal data information systems, approved by the Government Decision No. 1123 of December 14, 2010, and the Regulation of the Register of Evidence of the Personal Data Controllers, approved by the Government Decision No. 296 of May 15, 2012.

Chapter I
Current situation, definition of problems and general trends

Section 1. Current situation

The European integration aspirations of the Republic of Moldova have determined the country to initiate the harmonization of the legislation regulating personal data protection field with the European acquis, in order to ensure a level of protection and enforcement of the subjects' rights to processing of personal data related to them, equivalent to the one existing in the European Union.

Nevertheless, the current situation is characterized by a set of complicated evolutions, partially unconsolidated progresses in the day-to-day practice, missing institutional and normative framework for the sector, and confusions related to the exercise of duties referring to personal data protection.

Although, currently, the national legal framework related to the field of personal data protection is in line with the European Union standards, the legislation harmonization should be a continuous process, so as to cope with the permanent changes generated by the evolutions in the area of reference.

At the moment, in spite of the existing normative framework, every personal data controller sets its own security policy (or, in general, neglects this compartment), which, in majority of cases, does not respond to some simple exigencies, hence inducing the danger of unauthorized access to personal data filing systems, illegal operations for such data processing, and breach of data confidentiality principles.

Actually, there is a considerable number of entities processing personal data (controllers or processors) who do not know the legal framework regulating the respective area, as well as the obligation to ensure confidentiality and security of processed personal data.

Individuals are daily exposed to situations when banks, tourism agencies, medical institutions, telephone and internet services' providers, etc., widely use personal data, frequently abusing the volume and the categories of data to be collected and breaching flagrantly the rights set forth in the Law on Personal Data Protection. Personal data subjects are not informed thoroughly so as to fully understand the purpose for which the data are collected and the reasons for which the personal data are to be processed. A special case would be the pro-

cessing of personal data referring to minors.

Although, the European Union has a much more advanced level of personal data protection than the Republic of Moldova, the conclusions of some studies and reports on personal data protection at the European level reveal that problems also exist in Europe and they have to be settled and considered.

Hence, according to the Euro-Barometer No. 359[1], carried out in 2011, when asking about the attitudes towards data protection and electronic identity, 3 out of 4 Europeans disclose personal data in their day-to-day activity, but they are really concerned with the way in which entities, search engines, and social media use their personal data.

According to the survey, 62% of the EU citizens disclose minimum of requested information so as to protect their identity, while 75% wish to have the possibility to erase at any moment any personal data existing on-line – the so-called "right to be forgotten"; 60% of those who use internet buy and sell things online and use social media sites.

People disclose personal data, including biographic information (almost 90%), social information (almost 50%) and sensitive information (almost 10%) on these sites; 70% of the EU citizens have stated that they are concerned with the way in which entities use their data and consider it to be a partial control over their personal data; 74% wish to specifically give the consent before their personal data are collected and processed in the internet.

The most frequently expressed concerns by the EU citizens are related to fraud in case of online purchases (aspect mentioned by 55% of respondents), use of information without their knowledge on the social media sites (44%), and communication of the respective data towards entities without their consent (43%). At the same time, 42% of the EU citizens use the existing tools and strategies to limit the number of unwanted messages, and 23% of them modify the security settings of the browser they use.

According to the carried out survey, about 6 out of 10 internet users consult the online confidentiality statements (58%), but not all of them understand its content. In total, 62% of users do not understand, do not read or cannot find such confidentiality statements, or just ignore them. Whenever users read such statements, they are cautious about their personal data.

Another important study revealing the problems in this field is be the Academic Study "Data Protection Practice" carried out in Germany's business environment[2]. It was implemented by the 2B Advice GmbH in collaboration with the Dortmund Technical University from Germany in 2012.

Hence, the study reveals that the majority of persons responsible for personal data protection within the company do not have enough time to carry out the duties they ought to, and the reporting to managers is not regular. The study shows that 60% of company employees, most frequently, commit breaches when processing personal data, and the most frequent victim would be the client; 50% of most frequent cases leading to violation of personal data protection principles in the company are due to negligence, and 51% of violation cases are not registered and sanctioned appropriately.

At the same time, some concerns and fears were identified within the Moldovan mod-

1 http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.
2 http://www.2b-advice.com/ws/LLC-en/Study-Data-Protection-Practice-2012

ern society as well. For instance, during the talk-show Vox Publika broadcasted on February 6, 2012 in relation to "Free to choose on the Internet"[3], participants have stated that Internet is a huge technological development of humanity, but the way in which it is used is very dangerous. Using anonymity veil, people frequently are not accountable for what they do in the virtual space, and forget that these technologies give the possibility to follow and control the person, that is why all these processes should be regulated at the national level. As a result of the televoting, only 48% of respondents said that Internet use is actually a danger.

Section 2. Defining problems

At the national level, during the Center's activities were identified, a number of breaches of personal data processing principles, such as:

a) illegal processing of special categories of personal data by granting unrestricted access and disclosing such data to the general public, as well as by collecting an excessive volume of personal data as compared to the reasons for which such data are processed subsequently;

b) non-observance of the confidentiality and security regime for personal data processing when databases with personal data are exchanged illegally among controllers, for such purposes as direct marketing, with no prior consent of such data subjects;

c) abusive and unauthorized access to the main state information resources by public and private legal entities, including by law enforcement entities with no legal basis and justified reasons.

The detailed information regarding the dynamics registered for consulting the State Register of Population is presented in Table No. 1, and it becomes obvious that the use of one of the most important state information resource, which covers a huge volume of personal data for the purpose of efficient management of public duties, has stopped to be uncontrolled – for instance to find out the birthday of an acquaintance or for other reasons of personal interest, and in some cases the number of accesses and extraction of personal data has dropped by 90%.

Table No. 1

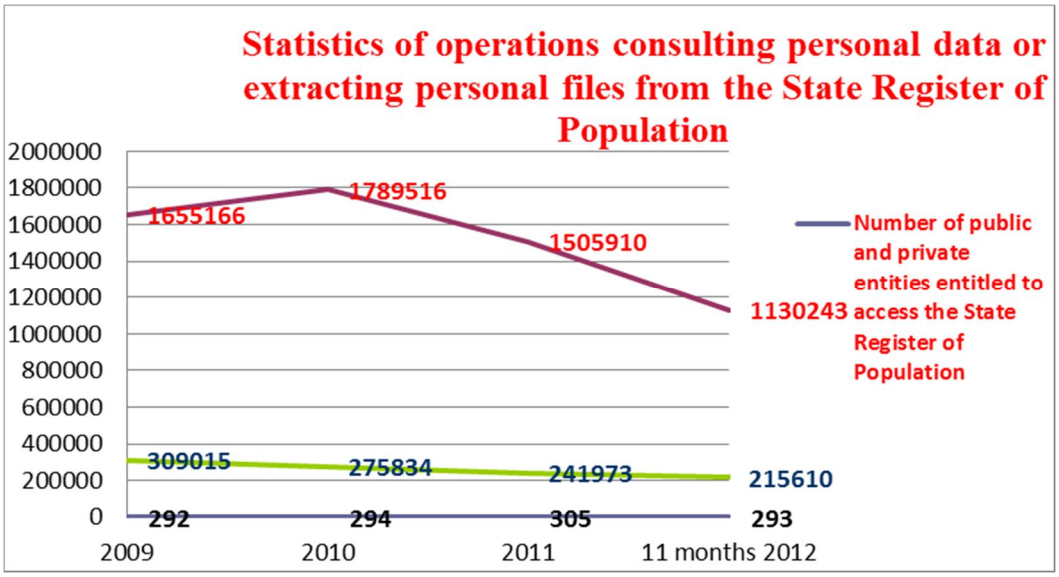
Entity	**2009**		**2010**		**2011**		**11 months of 2012**	
	consulting data	**extracting personal file**	**consulting data**	**extracting personal file**	**consulting data**	**extracting personal file**	**consulting data**	**extracting personal file**
General Prosecutor Office, together with territorial offices	**89199**	**14691**	**75520**	**12796**	**52353**	**11076**	**33006**	**8414**
Ministry of Internal Affairs , together with territo-	**725550**	**204587**	**671396**	**179211**	**546296**	**166271**	**439816**	**164893**

3 http://www.publika.md/editie/_1361_1100991.html.

rial subdivisions								
Ministry of Defense	**1032**	**0**	**2194**	**0**	**478**	**0**	**127**	**0**
National Anticorruption Center, Together with territorial subdivisions	**137632**	**9730**	**214735**	**15171**	**166348**	**14936**	**84056**	**6532**
Customs Service	**15989**	**2661**	**19081**	**3082**	**13422**	**2317**	**4985**	**1335**
Security and Intelligence Service	**82257**	**24951**	**129341**	**30304**	**74505**	**20006**	**26020**	**11605**
Judges of all levels	**1178**	**74**	**1383**	**55**	**1042**	**215**	**556**	**144**
Court of Accounts	**1900**	**110**	**2174**	**273**	**370**	**106**	**124**	**36**
State Protection and Guard Service	**11611**	**1884**	**16254**	**1706**	**12896**	**1028**	**4339**	**820**
Mayors' and praetors' offices	**17919**	**0**	**49613**	**0**	**23362**	**0**	**4596**	**0**
Department of Penitentiary Institutions	**6847**	**921**	**4294**	**417**	**2723**	**346**	**800**	**204**

Generally speaking, taking into account the information presented in Table No. 2, it becomes obvious that there is a sharp decrease of the number of operations referring to consulting the personal data stored in the State Register of Population. Hence, in 2010 a number of 1789516 data consulting operations were registered, while in the 11 months of 2012, only 1130243 such operations were registered - over 650 thousand fewer operations or a drop by 30%;

Table No. 2



d) breach of the right to information of the individuals and access to information regarding the operations related to their personal data processing, as well as the abusive and unjustified extension of the period set for applying exceptions and restrictions as compared to the moment when the subject has the real possibility to exercise his/her right to access – the period exceeding the limit necessary to achieve the goal of not damaging the efficiency of the set action or objective while exercising the legal competences of public authorities;

e) breach of personal data protection principles in case of minors' data through disclosure of children's personal data by media outlets, medical workers, and teaching staff during personalized interviews taken within medical or educational institutions and referring to very sensitive topics. The cases of news disseminated in mass-media about children's health status, shooting and taking photos of minor patients, as well as the personalized interviews taken within medical institutions with medical workers' involvement, represent a serious breach of private and intimate life, as well as of personal data protection principles, in spite of the fact that processing of minors' personal data is a very sensitive aspect, as the mere fact that a child already is a vulnerable element and he should be compensated by an adequate level of safety and security;

f) controllers' failure to update the processed personal data, which, in majority of cases, implies damages, including material damages for a specific individual. Sometimes, such inactions lead to cases when individuals cannot conclude a passport whenever the information, for instance, from the State Register of Population is not updated by prosecutors, judges or bailiffs, and hence the individuals have to go and bring documentary evidence themselves, etc.;

g) failure to include in the work contracts the obligation for employers to not disclose personal data to controllers and processors, including after the termination of the contractual relations;

h) processing of personal data for reasons which are incompatible with the grounds they were initially collected for – the case when data are collected by different entities in relation to voters when electoral lists are made public, and which afterwards are organized and systematized in databases, in contradiction with the provisions set in the Article 40 of the Electoral Code.

There is also a series of factors determining frequent breaches of personal data processing security and confidentiality regime by the personal data controllers or processors, such as:

1) missing policy on personal data security, which would be approved at the level of the public or private entity, and which would be adjusted to its needs and corroborated with the risks implied by personal data processing operations in relation to the rights of such data holders;

2) failure to use special technical protection means, software, licensed programs, and antivirus soft for organizing the system for security control of softs meant to process personal data;

3) sending personal data via unsecured channels;

4) no persons responsible for protecting personal data;

5) missing internal audit for information systems with personal data;

6) no regulations on deadlines for storing information containing personal data;

7) cross-border transfer of personal data without Center's authorization, etc.

Moreover, it was found out that the information collected and managed by the public sector for public services' provision reasons, is frequently redundant: it is not archived in the format which would ensure information security and confidentiality, the access to information is not registered in the adequate way, as frequently neither the reasons or the legal bases for personal data consulting operations are not known, and the regulations on ensuring confidentiality for the information provided by business environment and the individuals' right to protect their personal data are frequently not observed.

And finally, the small number of employees and the austere budget of the Center do not allow developing big-scale projects which would contribute to promoting this personal data protection area, raising people's awareness about the need, importance, and benefits of personal data protection, as well as increasing the level of personal data holders' knowledge about the ways to control the personal data referring to them.

Section 3. General trends

Currently, advanced technologies allow private entities and public authorities using personal data at a very wide scale, and people make their personal information public without fully understanding the involved risks.

In this context, building confidence for online environment is essential for the economic development of the country. Because of lack of trust, consumers hesitate to buy online, to pay invoices or to accept new services, including e-governance public services. If this lack of trust is not tackled, it will continue hinder the development of new technologies, and would be an obstacle for the economic growth, impeding the public sector to enjoy the potential benefits of its services' digitization.

To settle the above-mentioned problems, it is important to have a set of objectives, priority fields of action, and measures to come up with a strategic vision for developing the field of personal data protection. To implement this goal, it is necessary to have the involvement and supported efforts of all interested stakeholders. The concrete action plans, as well as a more solid and coherent framework for protection of personal data in the Republic of Moldova, together with a more rigorous enforcement of rules in the respective area, would allow the digital economy and society to actually get developed, facilitating individuals' control over their own personal data and enhancing legal and practical security for economic entities and public authorities, hence determining the promotion of personal data protection culture within

public and private institutions, which will finally contribute to a better governance.

In a modern world, the concepts of "private life" and "personal data protection" are rapidly evolving, just like the factors which could endanger such data security. Hence, modern information technologies have provided the possibilities and the capacities to collect and process easily and efficiently a huge volume of personal data. Highly appreciating the numerous advantages of these technologies, nevertheless it should be recognized that in case of incorrect use, they can cause serious consequences.

Moreover, during the Center's activity, it was found out that the central public administration authorities have over 70 departmental automated information systems, which use sector databanks and databases, classifiers, registers, and standards developed over a number of years. In majority of cases, the data held by some authorities are accessed and consulted by other authorities only for the purpose of reading or validating the respective data, without any possibility to operate automated rectifications. The exchange of data carried out among the state institutions are based on ad-hoc relations, bilateral arrangements concluded just for one specific project or reason, hence only technologies available at a certain moment are used, and their implementation does not always meet the relevant standards.

At the current moment, the area of information technologies and communications (ITC) provides extraordinary possibilities for automated processing of personal data related to almost every aspect of our life, the way we work, rest, network and study, in general, they are considered to be essential for the nowadays information economy and for the society, as a whole.

At the same time, the development of technologies, communication systems, information systems, and of a huge number of personal data filing systems collected for different reasons, the high development level of social media, internet and other communication forms, without a concomitant assurance of some minimum security requirements, have generated the unauthorized and unmonitored access to personal data. This fact implies the need to develop a policy document in this area, which would provide for concrete actions to secure protection of individuals' fundamental rights and freedoms related to personal data processing.

The strategic program for technological upgrade of the governance (e-Transformation), approved via the Government Decision No. 710 dated September 20, 2011 (hereinafter referred to as the Strategic Program), reveals that IT resources' use in public administration is rather sporadic and lacks coordination, hence decreased governance efficiency and agility. However, this Strategic Program suggests making governance more efficient by ensuring the interoperability of IT systems, as well as by consolidating and reusing IT resources, interacting on a joint technologic platform. People should provide the public authorities with personal data just one time, while the public authorities should reuse these data for provision of requested services.

Additionally, starting with 2012, activities were initiated to develop a common technological platform in the Republic of Moldova, M-cloud, based on cloud-computing, for all the central public administration entities, which will host the information systems serving as basis for public services, in a secure way and with no additional expenses. Nevertheless, the insufficient information about the processing operations used by a cloud-computing provider represents a challenge for the personal data controllers, as well as for the personal data subjects, whenever they might be not aware of the possible threats and risks, and thus might be unable to adopt adequate measures to protect personal data.

In this context, even as a result of undertaking some correct assessments and applying some necessary security measures, a certain risk still persists for the automated processing of personal data, but the enforcement of some adequate protection measures, which would lead to risks' minimizing, is both possible and necessary.

The eventual abuses and breaches of the security regime for personal data processing might undermine users' level of confidence in the information society and the benefits it may bring. That is why the field of personal data protection is one of the key elements for business success. The personal data protection field is outlined as a priority field at the national and European levels, as it is an area of horizontal regulation, which is of interest for other vertical regulation areas in all the activity sectors of a democratic society.

At the same time, as the situation related to protection of individuals' fundamental rights and freedoms related to personal data processing has a direct impact on the State's credibility and capacity to implement an efficient internal and external policy in human rights' area, the operations of processed personal data disclosure by the authorities from the administrative districts on the left bank of the Dniester River, will be performed only when the Center will have the possibility to carry out an effective control over the conformity of such data processing, in line with the provisions set in the Law No. 133 dated July 08, 2011 on Personal Data Protection and the Requirements for ensuring personal data security when being processed in the personal data information systems, approved via the Government Decision No. 1123 dated December 14, 2010.

The analysis of the current situation points out the strengths, weaknesses, opportunities, and threats of the personal data protection area, related to the internal and external factors. The results of the analysis are reflected in the following SWOT Matrix.

SWOT Matrix

Strengths	***Weaknesses***
1. Law No. 133 dated July 8, 2011 on Personal Data Protection is fully harmonized with the provisions of the Directive 95/46/EC of the European Parliament and Council dated October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 2. Creation of the Automated Information System "State Register of Evidence of the Personal Data Controllers" ensures the possibility to notify them about the establishment of registers, databases, information and statistical systems, which are storing and processing personal data automatically or manually, ensuring as well the public nature of the system in online format. 3. Presence and active participation within the European Neighborhood Policy, international and regional cooperation with similar authorities and organizations of personal	1. Low level of individuals' awareness and information about their rights as personal data subjects; 2. Failure of some controllers to implement the requirements set for ensuring personal data security when processing data within information systems of personal data. 3. Lack of coordination and collaboration between the public authorities and the Center in order to set and implement information systems, which would ensure an adequate level of personal data protection. 4. Low level of awareness among the public and private entities about the position and the role of the Center while supervising the assurance of an adequate level of personal data protection. 5. Costs and insufficiency of the necessary technical equipment and licensed software for the personal data controllers so as to ensure an adequate security level, in line with the EU

data protection control from the European Union for transfer of good practices and coherent implementation of European policies of personal data protection in the national context. 4. The personnel of the Center is well-trained as a result of the experience exchange with the EU Member States and taking over good practices in the area of personal data protection.	norms and requirements.
Opportunities 1. Consolidation of administrative and institutional capacities of the Center to use the funds of the European Union and other external donors. 2. Assurance of an adequate level of personal data protection as a tool for the Republic of Moldova to achieve economic benefits. 3. Saving time, financial and human resources of the Center and personal data controllers based on the notification through the Automated Information System "Register of Evidence of the Personal Data Controllers". 4. Improvement of the communication with the civil society and general public by maintaining a well-organized, updated, and accessible official web page of the Center. 5. Establishment and consolidation of partnerships between public authorities and civil society, including non-governmental organizations.	***Threats*** 1. Opportunities and benefits associated with the ITC area development involve risks, especially in relation to personal data protection and confidentiality assurance, because these technologies frequently lead to proliferation, in many cases imperceptible, by the data subjects of huge volumes of collected, organized, adjusted, transferred information, hence increasing the risks related to such data processing. 2. Insufficient financial resources for carrying out the planned actions. 3. Permanent turnover of qualified personnel. 4. Low level of awareness among the personal data controllers of the need to implement and develop information technologies by ensuring confidentiality and security of the personal data processing.

Chapter II
Vision, general and specific objectives of the Strategy

Section 1. Strategic vision

Strategic vision: a society in which personal data protection is guaranteed, the controllers ensure the enforcement of the confidentiality and security principles within personal data processing, and data subjects know about their rights, and there is a mechanism for such rights' effective exercise.

This Strategy aims to have a complex, multidisciplinary, and well-balanced approach to the problems related to personal data protection field, based on a high level of interdepartmental, interdisciplinary and intersectoral cooperation at all the levels, meant to consolidate and mainstream the personal data protection in all the activity sectors of the society, at a national level.

The personal data controllers, the processors mandated by both controllers and the general public should acknowledge that the National Center for Personal Data Protection is the

autonomous public authority supervising the legality of personal data processing, having trained personnel for taking prompt decisions for the purpose of achieving the set objectives.

The efficient protection of personal data needs not only consolidation of the framework for data subjects to exercise their rights and the controllers to fulfill their obligations when processing personal data and deciding upon the outputs of personal data processing, but also skills to monitor and ensure the compliance of personal data processing with protection norms, including sanctions for breach of legislation.

Section 2. General and specific objectives of the Strategy

General objective

The general objective of the Strategy is to ensure an adequate level of personal data protection in the Republic of Moldova, which would be in line with the European standards and would ensure the rule of law, and would contribute to increasing data subjects' confidence that the personal data processing by different entities does not aim to limit their private life and intimacy.

Currently, the need to ensure an adequate level of personal data protection is a binding commitment assumed by the Republic of Moldova when ratifying the Convention for the protection of individuals with regard to automatic processing of personal data, being a precondition for concluding and operating the Association Agreement with the European Union and the Cooperation Agreement with EUROJUST, the Operational Agreement with EUROPOL, and the Agreement for visa regime liberalization.

Specific objectives

Specific objective 1: To inform all the personal data controllers about their responsibilities, as well as about the need to protect the processed personal data, taking into account the most recent techniques in relation to the risks deriving from the personal data processing and nature of protected data.

Taking into consideration the trend to digitalize the public services in the Republic of Moldova, by creating information systems and administrating them in line with the e-Governance policies, reform recommendations of the European Union framework on personal data protection, the national normative framework regulating the information field, as well as in the context of the "Digital Moldova 2020" Strategy, this specific objective implies the establishment and development of the ITC field enshrining the principles of personal data protection and confidentiality in the entire life cycle of the technology, from the very first stage of the project until the operation, use, and elimination of such technology from the system (privacy by design).

For instance, the health sector is increasingly based on the ITC infrastructure determining centralized storage of medical information of the patients. Hence, the enforcement of the given principle in the health sector would need the adequacy assessment of the different measures, as well as the possibility to reduce to minimum the stored data at the central level or to limit them to one index, by using some encoding tools, strict provision of access rights based on the principle of knowing the minimum necessary, and making data anonymous as soon as they are not necessary, as well as by ensuring the right to be left alone, etc.

Priority measures:

a) to carry out studies and analyses in different sectors and fields so as to identify the issues related to the personal data processing operations;

b) to develop guidelines for personal data processing in different sectors, especially: in police activity, medical, educational, electoral, communication, financial-banking areas, and other;

c) to develop cooperation relations with the personal data controllers and their processors by: signing collaboration agreements; initiating joint projects in personal data protection field; training; consultation; endorsement of draft normative acts, etc.;

d) to promote the obligation to get registered in the Register of Evidence of the Personal Data Controllers, as well as to encourage and support the personal data controllers in developing codes of professional conduct in relation to personal data processing;

e) to monitor the control over the organizational and technical procedures necessary to ensure an adequate level of personal data protection by the controllers and other entities involved in personal data processing.

Specific objective 2: To raise awareness of the general public about the rights they have in relation to processing of personal data.

The increase of awareness and perception levels among the individuals about the importance of personal data protection would also influence the increase of companies' competiveness, and growth of the country's economic, social, and cultural development.

Priority measures:

a) to actively involve the representatives of civil society, educational authorities, and mass-media, by signing cooperation agreements with the faculties of law, journalism, political science, information technology, medicine etc., as well as by training the journalists about the principles of personal data protection in the Republic of Moldova and European Union so as to inform the public about the importance of the personal data field;

b) to create a sustainable system for continuous training of pupils, teaching staff (professors) from primary and secondary education, and public service employees about the principles of personal data protection;

c) to promote the concepts of "private life" and "protection of personal data", including the importance, advantages, and benefits resulting from protecting individuals' fundamental rights and freedoms in relation to personal data processing, including public opinion awareness;

d) to increase the level of public perception and awareness among individuals about the field and importance of personal data protection, so as to increase companies' competitiveness, and country's economic, social, and cultural development;

e) to ensure individuals' right to information in relation to the personal data protection; it is essential for the persons to be informed in a transparent way by the data controllers about the way in which the personal data are collected and processed, by whom, for what reasons, for how long, and which are the practical methods and procedures for exercising the rights set forth in the Law on Personal Data Protection;

f) to clarify the mechanism for collecting the explicit consent via any appropriate method, which would allow free, specific, and informed manifestation of the given person's will.

To carry out these measures, it is important to take into account the ways which would allow the person to manifest his/her consent either through a statement or through a clear act, ensuring that the individual is conscious of the fact that he/she consents for the personal data to be processed, including by checking a small box when visiting an internet site or via any other statement or action clearly indicating that the given person accepts the processing of his/her personal data.

Hence, the absence of an answer or an action should not be perceived as consent. The consent should refer to all the processing activities carried out for the same purpose(s). If the consent of a given person should be given as a result of an electronic request, this should be clear and concise, without perturbing uselessly the service for which the consent is granted.

Specific objective 3: To build the administrative and institutional capacities of the National Center for Personal Data Protection of the Republic of Moldova.

After the European experts have assessed the progress registered by the Republic of Moldova in legislation harmonization with the European Union standards in personal data protection field, it was concluded that most of the achievements were obtained over the past years. Nevertheless, some systemic (not legislative) drawbacks still may be identified, as well as gaps related to optimizing the operation of the respective area as a whole.

At the same time, the improvement and harmonization of the legislation on personal data protection is a continuous process, due to the complexity of the field, and its interconnection with the different sectors at the national and international levels.

It is also worth mentioning the process of adjusting the national normative framework to the changes or obligations assumed by the Republic of Moldova as a result of signing political or economic bilateral agreements related to personal data protection. In the context of the international evolutions over the last years, especially of the economic globalization and European Union's extension, it became extremely important to create and maintain a cooperation environment among the authorities supervising personal data protection, as well as between such authorities and international institutions specialized in the field. Special attention should be paid to cooperation in personal data protection field with the EU member states and candidate states, which benefit from assistance projects in the context of the Association Agreement with the European Union.

Priority measures:

a) to continue the improvement and harmonization of the normative framework related to personal data protection and regulating the rights, duties, and competences of the Center;

b) to train the personnel of the Center on a continuous basis so as to increase the level of professionalism and competence in the field of personal data protection;

c) to develop the infrastructure of the Center by endowing it with equipment, IT technical means, necessary information systems, etc.;

d) to consolidate the collaboration relations with the authorities supervising the personal data protection field from European countries, in the context of ensuring exchange of experience, organization of workshops, trainings, study visits, seminars, international conferences in the domain, which would contribute to promoting the image of the Center and of the country, as a whole;

e) to develop international, regional, and bilateral cooperation in the field of personal data protection.

Chapter III
Financial sources

The financial sources necessary for the implementation of the Strategy shall include:

a) allocations from the state budget for the involved public authorities, according to their competence, for the implementation of the Strategy's objectives in line with the sector activity plans;

b) internal and external means provided by donors, including donations and sponsorships provided according to the legislation in force;

c) other sources not prohibited by the law.

For some of the actions, it is possible to estimate correctly the necessary financial means at the stage of proposals' submission. In other cases, the financial costs represent some approximate estimations, directly depending on the de-facto circumstances, such as the size of the personal data controller, the implementation level of the technical and organizational measures necessary for ensuring the personal data security, confidentiality, and integrity, the risks derived from the personal data processing operations for the right to private life, etc., but the correct identification of the financing volume is not possible due to justified reasons.

Chapter IV
Implementation, monitoring, and evaluation of the Strategy

Section 1. Implementation

For the purpose of achieving the objectives, and producing the expected results, the Strategy shall be implemented through clear mechanisms, the implementation progress being monitored, and the successes and/or failures being pointed out as a result of an ample evaluation.

The implementation of the Strategy shall be carried out by transposing the action plan, and every activity will differ depending on the type of necessary measures set separately for every action priority.

In this respect, for:

a) regulatory measures – mixed working groups will be set, covering representatives of the responsible institutions indicated in the action plan; experts from civil society shall be invited to attend the meetings of these working groups on binding basis;

b) technical measures – procurements shall be carried out for equipment, software, and infrastructure endowment;

c) financial measures – budgetary and extra-budgetary means shall be allocated; upon need, the means provided by the technical assistance programs will be used as well;

d) administrative-institutional measures – concrete actions will be undertaken by the administration so as to consolidate the operation of the National Authority for supervising personal data protection (modifying the staffing plans, creating new structures, and increasing the number of employees in the existing bodies, developing the organizational charts and job descriptions, recruiting personnel, and adopting department acts);

e) training measures – initial and continuous trainings shall be carried out;

f) analysis measures – assessment and analysis activities shall be undertaken by some independent experts and/or experts from within the institution;

g) public communication measures – public actions shall be implemented to raise awareness of the general public and some target groups, at the national and international levels.

Section 2. Monitoring

The monitoring of the Strategy and Action Plan shall be carried out by organizing the operative exchange of information and assessing the implementation stage.

The Strategy monitoring activities shall be carried out during the entire period of implementation and shall include collecting, processing, and analyzing monitoring data, identify-

ing the errors or the unforeseen effects, as well as the eventual rectifications of the content and form of planned measures and activities.

The institutions mentioned in the Strategy's Action Plan shall submit annually, by January 05, progress reports on results obtained from undertaking prescribed actions, which will serve as basis for the National Center for Personal Data Protection of the Republic of Moldova to develop consolidated monitoring reports.

The progress reports will reflect the results registered at the respective stage of Strategy's implementation – the achievement level of the general goal and specific objectives, the fulfillment of the planned activities, the attainment of performance indicators specific for every activity, and formulation of proposals to improve and correct the planned measures. In case of unfulfilled activities – the reasons for such failures or partial fulfillment shall be exposed and efficient measures will be suggested to implement the general goal of the Strategy.

At the same time, the control over the present Strategy implementation monitoring shall be carried out by the relevant Parliamentary Committee, as well as by the interested stakeholders of the civil society.

In this respect, the Center shall support periodical public information campaigns about the progress registered in the implementation of the Strategy.

Section 3. Evaluation

The evaluation of the Strategy implementation shall include the analysis of the way in which the Strategy is implemented and how efficient this modality is; this will also serve as means for contributing to the improvement of the personal data protection policy.

The evaluation report shall be developed annually by the National Center for Personal Data Protection of the Republic of Moldova, with the support of interested development partners, as well as of the civil society representatives, the results being provided to the Parliament and general public for information.

The final evaluation shall be carried out by the end of 2018 and will provide a clear image of how the objectives proposed by the Strategy were achieved. The conclusions expressed in the final evaluation report shall identify the priority problems existing in the country in relation to "personal data protection", specifying the objectives and the activity directions for such objectives' implementation in a new policy document.

The final evaluation report shall be developed with the involvement and assistance of experts – organizations or individuals, which did not participate directly in the development, as well as foreign specialists and international organizations.

Annex No. 2

ACTION PLAN
for implementing the National Strategy for Personal Data Protection Development during 2013-2018

No.	Actions	Performance indicators	Deadlines	Responsible	Finance source
1	**2**	**3**	**4**	**5**	**6**
GENERAL GOAL: To ensure an adequate level of personal data protection in the Republic of Moldova					
Specific objective 1. To inform all personal data controllers about their responsibilities, as well as about the need to protect the processed personal data, taking into account the most recent techniques in relation to the risks deriving from the personal data processing and nature of protected data.					
1.1.	Carrying out sector studies to provide the personal data providers with the necessary guidelines to adjust the personal data processing to the provisions set in the Law on Personal Data Protection	Number of carried out studies, annually	2014	National Center for Personal Data Protection with the support of the institutions active in the field (from different sectors)	Budget of the National Center for Personal Data Protection /sources allocated by development partners

1.2.	Development and promotion of guidelines on processing personal data in different sectors, especially: in police activity, medical, educational, electoral, communication, financial-banking sectors, etc.	Developed guidelines, published on the web-site of the Center and sending them to concerned target-groups	2014	National Center for Personal Data Protection in collaboration with the personal data controllers	Budget of the National Center for Personal Data Protection /sources allocated by development partners
1.3.	Development of cooperation relations between the Center and the personal data controllers and processors so as to conclude cooperation agreements, to initiate some joint projects in the area of personal data protection	Number of concluded agreements, initiated projects and successfully fulfilled projects, annually	2018	National Center for Personal Data Protection in collaboration with the personal data controllers	Budget of the National Center for Personal Data Protection /sources allocated by development partners

1.4.	Involvement of professional organizations of judges, bailiffs, lawyers, notaries, banks, press, trade-unions, IT, etc. to promote the registration in the Register of Personal Data Controllers, as well as to develop the codes of professional conduct which would include provisions related to personal data protection or completing the codes with such rules	Number of meetings, seminars, round tables organized annually, number of provided consultations, number of codes of developed or completed codes of conduct, number of personal data controllers registered in the Register of Personal Data Controllers	2018	National Center for Personal Data Protection in collaboration with the development partners	The budget of the concerned institution / sources allocated by development partners

1.5.	Covering in the media the cases with special resonance and the violations admitted by the public and private law entities when processing personal data	Number of cases covered in the media, annually	2018	National Center for Personal Data Protection in collaboration with the development partners	Budget of the concerned institution / sources allocated by the development partners
1.6.	Provision of assistance to public and private institutions, which are established as personal data controllers so as to ensure the observance of the organizational and technical procedures for personal data protection	Number of notifications about personal data processing submitted to the Center annually	2018	National Center for Personal Data Protection	Budget of the National Center for Personal Data Protection /sources allocate by development partners
1.7.	Provision of assistance to personal data controllers to develop the confidentiality statements, as a contractual clause or being inserted in the job description, mentioning about the civil, contravention, or criminal liability for violation of such statement for the persons who participate in the personal data processing process.	Number of consultations provided annually	2018	National Center for Personal Data Protection in collaboration with the personal data controllers	Budget of the National Center for Personal Data Protection / sources allocated by development partners

1.8.	Revision of the categories and volume of personal data processed by controllers	Minimizing the number of categories of processed personal data.	2014	National Center for Personal Data Protection in collaboration with the public authorities and institutions subordinated to them	Budget of concerned institution / sources allocated by development partners
1.9.	Provision of methodological assistance to subdivisions / persons responsible for personal data protection established within the personal data controllers	Number of requests examined annually (written or verbal), submitted by the subdivisions of personal data protection	2018	National Center for Personal Data Protection	Budget of the National Center for Personal Data Protection / sources allocated by development partners
1.10.	Ensuring transparency and accessibility in relation to personal data processing and the modality for concerned persons to exercise their rights, especially the possibility to verify the category and the volume of personal data collected and processed by the state authorities, as well as such data use for other purposes than the ones they actually were initially provided for by the data-holders	Annually developed information material and posted through official web-pages, within official premises	2018	Public authorities in collaboration with the subordinated institutions, National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners

1.11.	Tackling the principles of personal data protection, starting with the development of information systems and record-keeping systems meant for automated processing of personal data (privacy by design)	Principles of personal data protection integrated in the technical concepts of the systems meant for automated processing of personal data	2018	National Center for Personal Data Protection in collaboration with the personal data controllers	Budget of concerned institution / sources allocated by development partners
1.12.	Coverage in the media, promotion, and monitoring the observance of the obligation to notify and register the personal data controllers, databases, information systems and IT systems storing and processing personal data, automatically or manually, as well as the observance of the principle of transparency in the activity of data processing	Number of media coverage actions and number of promotions organized and carried out annually; Number of notifications, controllers, databases, information systems, and IT systems storing and processing personal data automatically or manually, which are registered annually	2018	National Center for Personal Data Protection in collaboration with the personal data controllers	Budget of the National Center for Personal Data Protection / sources allocated by development partners

Specific Objective 2. To raise awareness of the general public about the rights they have in relation to processing of personal data.					
2.1.	Active involvement of the representatives of civil society, authorities from education and mass-media field in raising awareness of the persons about the concepts of "private life", "personal data", the benefits resulting from personal data protection, the negative consequences which may occur when the regime of personal data processing confidentiality and security is not respected, as well as the role of personal data protection in the economic, social, and cultural development of the country	Number of seminars, trainings, round tables, workshops organized annually for different categories of personal data controllers Number of specialists trained annually Number of information materials developed and distributed annually	2018	National Center for Personal Data Protection in collaboration with the central public administration authorities, local public authorities, as well as in cooperation with other entities	Budget of the National Center for Personal Data Protection / sources allocated by development partners

2.2.	Organization of training courses for journalists related to the need to ensure a balance between the right to freedom of expression and the right to private life	Number of sessions organized annually and number of course beneficiaries	2018	National Center for Personal Data Protection	Budget of the National Center for Personal Data Protection / sources allocated by development partners
2.3.	Organization of the contest among journalists for the best expression of the need to respect the area of personal data protection, the problems related to non-observance of the principles of personal data protection, as well as the dissemination of articles referring to this area	Number of participants in the contest, number of materials developed by journalists and submitted annually to the contest	2018	National Center for Personal Data Protection	Budget of the National Center for Personal Data Protection / sources allocated by development partners
2.4.	Signing the collaboration agreements with the Ministry of Education so as to create a sustainable system for continuous training of pupils and teaching staff	Signed agreement	2013	National Center for Personal Data Protection, Ministry of Education	Budget of the concerned institution / sources allocated by development partners

2.5.	Introduction in the national school curriculum of a course/discipline related to protection of personal data	Course/discipline included in the curriculum	2014	Ministry of Education in collaboration with the National Center for Personal Data Protection, higher education institutions	Budget of the concerned institution /sources allocated by development partners
2.6.	Organization of activities to raise awareness among the pupils about the importance of personal data protection	Number of organized activities and number of pupils trained annually	2018	Ministry of Education jointly with the educational institutions, as well as in collaboration with the National Center for Personal Data Protection	Budget of the concerned institution /sources allocated by development partners
2.7.	Celebration on the 28th of January of the Personal Data Protection Day within the educational institutions	Number of pupils lyceum pupils, and students who have participated in the event, annually	2018	Ministry of Education jointly with the educational institutions	Budget of the concerned institution / sources allocated by development partners
2.8.	Signature of collaboration agreements with the pre-university educational institutions and universities to train teaching staff and students in the area of personal data protection	Number of agreements concluded and number of teachers who attended the courses	2015	National Center for Personal Data Protection in collaboration with the pre-university institutions, universities	Budget of the concerned institution / sources allocated by development

					partners
2.9.	Organization of contests for children related to different topics on personal data protection	Number of contests organized annually	2018	Ministry of Education in collaboration with the National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners
2.10.	Creation of a sustainable system for training the employees from the public service and the employees from other institutions about the principles of personal data protection	Number of courses organized annually; number of persons / institutions trained annually	2018	National Center for personal Data Protection in collaboration with the Academy of Public Administration under the President of the Republic of Moldova jointly with the State Chancellery	Budget of the concerned institution / sources allocated by development partners
2.11.	Elaboration and dissemination of brochures, leaflets, information newsletters regarding the importance of personal data protection, as well as regarding the negative effects of violation of principles to protect personal data	Number of information material developed and disseminated annually	2018	National Center for Personal Data Protection in collaboration with development partners	Budget of the concerned institution / sources allocated by development partners

2.12.	Organization of conferences focused on the need to observe the principles of personal data protection	Number of conferences held annually	2018	National Center for Personal Data Protection in collaboration with development partners	Budget of the concerned institution / sources allocated by development partners
2.13.	Organization and implementation of national events dedicated to the Personal Data Protection Day	Events organized at the national level, annually	2018	National Center for Personal Data Protection in collaboration with development partners	Budget of the concerned institution / sources allocated by development partners
2.14.	Creation of some clear mechanisms to collect the explicit consent, either through a statement or via a clear personal act, ensuring that the individual is conscious that he/she consents for his/her personal data to be processed	Created mechanisms	2018	Public authorities in collaboration with the National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners
Specific Objective 3. To build the administrative and institutional capacities of the National Center for Personal Data Protection of the Republic of Moldova					
3.1.	Analysis of how the decisions issued by the Center during the controls un-	Problems and deficiencies	2018	National Center for Personal Data Pro-	Budget of the concerned

	dertaken to identify the problems and emerged deficiencies are executed	identified annually		tection	institution / sources allocated by development partners
3.2.	Analysis of claims and complaints submitted to the Center so as to identify the problem and the necessary actions to be undertaken to improve the situation in relation to persons' protection as related to personal data processing, as well as the protection of the right to intimate, family, and private life	Proposals for identifying the necessary actions to be undertaken	2018	National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners
3.3.	Analysis of the problems emerged during the registration of the personal data controllers, databases, information systems, and IT systems in which personal data are stored and processed in the Register of Personal Data Controllers, so as to identify the eventual deficiencies and the needs to adjust the registration procedures	Identified deficiencies and the adjusted registration procedures	2018	National Center for Personal Data Protection jointly with the personal data controllers	Budget of the concerned institution / sources allocated by development partners

3.4.	Identification of eventual normative drawbacks in the implementation of the Law on Personal Data Protection and Requirements for ensuring the personal data security when such data are processed in the information systems with personal data	Number of proposals to eliminate the identified drawbacks	2018	National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners
3.5.	Evaluation of needs to adjust the national normative framework to the Directives and Recommendations of the European Union and Council of Europe	Developed final evaluation report, formulated proposals	2015	National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners
3.6.	Revision and endorsement of the sectoral normative framework in line with the principles of personal data protection	Number of annually endorsed normative acts, number of proposals to complete or modify such acts	2018	National Center for Personal Data Protection, public authorities	Budget of the concerned institution / sources allocated by development partners

3.7.	Revision of the national legislation in the area of electronic communication for the implementation into the national legal system of the specific rules of the European acquis for the telecommunication sector referring to the processing of personal data and protection of confidentiality in the electronic communication sector	Amended normative framework	2014	Ministry of Information Technologies and Communication, National Agency for Regulation in Electronic Communication and Information Technology, National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners
3.8.	Continuous training, exchange of experience with similar European institutions, participation in seminars, trainings, study visits, workshops, and international conferences	Number of professionally trained officials, annually	2018	National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners
3.9.	Ensuring the participation in international forums of the national authorities supervising personal data protection, so as to promote the image of the Center and that of the country, and active participation in the development of the normative framework regulating the area of personal data protection.	Number of annual participations in international forums	2018	National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners

3.10.	Updating the design of the Center's official page so as to ensure an interactive platform for informing the society about the activity of the national control authority	Updated design of the official page	2014	National Center for Personal Data Protection	Budget of the concerned institution/ sources allocated by development partners
3.11.	Ensuring the information of the public about the problems identified during the control of how the legislation is respected in relation to personal data protection	Information and updated published on the Center's web-page	2018	National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners
3.12.	Completing the staffing of the Center and revising the number of employees in relation to the volumes of performed activities	Staffing plan completed 100%. Proposals to modify the staffing number in relation to the volume of performed activities	2015	National Center for Personal Data Protection	Budget of the concerned institution / sources allocated by development partners
3.13.	Participation in the negotiation of the Cooperation Agreement between the Republic of Moldova and Eurojust	Signed cooperation agreement	2014	General Prosecutor Office, National Center for Personal Data Protection, Ministry of Justice, Ministry of Foreign	Budget of the concerned institution / sources allocated by development

				Affairs and Europe-an Integration	partners
3.14.	Provision of assistance to the Ministry of Internal Affairs to initiate negotia-tion and to negotiate the Operational Agreement of Cooperation between the Republic of Moldova and Europol	Signed cooperation agreement	2014	Ministry of Interior, National Center for Personal Data Pro-tection, Ministry of Foreign Affairs and European Integra-tion	Budget of the concerned institution / sources allo-cated by de-velopment partners