CZU: 342.721:004.056.5(478):339.924

INSTRUCȚIUNI PENTRU ÎMBUNĂTĂȚAREA MECANISMELOR STRATEGICE DE SECURITATE ȘI PROPRIETARE A DATELOR PERSONALE ÎN MOLDOVA ÎN CONTEXTUL DE ȚARĂ CANDITAT ITS LA UE

DIRECTIONS FOR IMPROVING STRATEGIC MECHANISMS OF PERSONAL DATA SECURITY AND OWNERSHIP IN MOLDOVA IN THE CONTEXT OF ITS EU CANDIDACY

LISNIC Alexei
Universitatea de Stat dn Moldova
E-mail: alexei.lisnic@gmail.com

Introduction. *Moldova is facing a critical moment regarding its strategic mechanisms of personal data security and ownership. Its current capacity to ensure the aggregated anonymization systems and processes harmonized with the new European Law Enforcement Directive, which redefines the data protection regulatory architecture for both EU and non-EU countries, will greatly impact its future in the EU. Data protection has become a core element of trust and a painful stake in the competition between greenfield newcomers and industrialized incumbents currently seeking to benefit from the tightly regulated European digital market and its two billion-strong pool of personal data in the coming years. Beyond personal data, the country is also competing to join the European value space where human rights, including data self-determination fundamental rights, are built-in features, defining both public digital services and the regulatory framework.*

Privatizing data protection and personal data treatment transparency can give Moldova a competitive edge in the EU or make it fall to the side of UDG-ridden quasi-European outer rings. To make their case and leave an indelible positive mark in their current regulatory nurture phase, both the national data protection regulator and the representing Data Owners' Association have to propose and implement a pan-European level innovation and protection roadmap. Increased field application of these skill-evidencing competitive tools also allows our national vendor — the most personal data-empowered citizenry — to be favorably positioned regarding any bilateral investment and travel data agreement with the European Union or one of its Member States to facilitate acquiring substantial infusions, access to the European personal data-rich market, granting a visa-free regime for nationals, and finding a safe haven for personal data transfer abroad. Last but not least, meeting these regulatory requirements turns Moldova into a policy-accepting European millionaire and a polity-adroit millionaire-maker of personal wealth.

Background and rationale Abstract Over the past 10 years, society's vulnerabilities regarding data protection have received heightened attention across various countries. The Republic of Moldova is no exception. Transparency reports show that a relatively high number of official requests for the disclosure of personal data emanate from Moldovan authorities. It is suspected that personal data obtained via these requests are sometimes used to intimidate or harass citizens, especially when investigations of human rights violations are lacking in various sectors of public administration. On the other hand, it is revealed that Moldova issued an astonishingly high number of mobile interception warrants between 2006 and 2007—some without proper judicial oversight.

In 2003, the State Chancellery justified the need for data protection legislation based on state and civil society requests and on the impact of data protection and privacy on the process of democratization, market development, and European integration. This raised serious concerns in European circles given the wider European community's preoccupation with data protection and privacy. Proof of Moldova's serious lack of commitment to data protection reform appeared in 2007, when a thematic report was published in this direction. Over the subsequent years, international projects implemented in Moldova aimed to support the further adoption of a legislative framework in this area. These efforts to provide a solid basis for upgrading data protection legislation became a top priority for Moldova as part of its European Neighbourhood Policy Action Plan. At present, the growing technological need for data protection reform is accelerating given the advanced process of digitalization of administration, as well as economic development, law enforcement, the judiciary, the medical system, and everyday life. Moldovan people living in either the country or abroad are becoming vulnerable to poor data protection legislation. This vulnerability could have a significant impact on the prospect of Moldova's future embedding within the European Union. The whole issue of European integration has and will have a significant impact on personal data governance. The unnecessary long-term delay of any comprehensive data protection reform constitutes an anticipated legislative breach that could automatically remove Moldova from the "EU potential candidate" category due to the amplification of the created legislative and psychic inconvenience. The legal functioning of individual governance from a data protection perspective will increase confidence in general citizens and attract direct long-term investors as a predictable and secure governance model. Given these peculiarities, we believe that we are addressing a high-priority scientific assessment, which overall falls within the general scope of our research, as the overall data protection legislation is of significant scientific, economic, and social applicability and provides an ensured comprehensive personal data strategy for internal and cross-border governance in Moldova.

Research aim and objectives. The aim of the study is to develop strategic recommendations for improving the mechanisms of ensuring personal data protection and ownership in the Republic of Moldova. In order to reach the aim, the following objectives have been set: - Analyzing the current state of the art of data protection law, including recent legislation and law enforcement mechanisms; - Exploring the lack of effectiveness of legislation, institutions, and their involvement in the strategic setting of personal data protection, including the deliberate and actual cases; - Reviewing the best practices and lessons learned; - Formalizing possible courses of action for policymakers in the Republic of Moldova, including more sustainable solutions, and setting recommendations considered to be strategic in terms of personal data protection and ownership issues. Context: It is generally accepted that data protection is considered the international gold standard for data governance, characterized by a globally successful data protection framework that has set much of the current global data protection agenda. Therefore, aligning personal data processing standards and the effectiveness of the legal framework with the provisions and requirements would significantly contribute to achieving sustainable economic and social progress in the Republic of Moldova.

Personal data security and ownership: key concepts. Personal data protection refers to any operation or set of operations that includes the collection, recording, organization, storage, adaptation, or alteration of personal data. There cannot be privacy without data protection, and the two share a complementarity, even a dialectical relationship. Clearly, these two rights—privacy and data protection—are closely connected and intertwined in today's digitized world. Data ownership

in its widest sense can be described as the legal right to determine what happens to data about you. There is a debate as to whether individuals can be the owners of a right in personal data, given that some decisions cannot be entirely free.

With the spread of global communication networks, personal data has become the defining feature of the modern information society. It is often said that in the age of big data, information is the currency of a digital society. A more descriptive view suggests that personal data, being the cornerstone of big data, is the valuable asset of digital technologies. This data includes personal and social virtual profiles, documents, photos, markup of preferences on social networks, data from purchase history, as well as from mobile phone registration. The complexity and large amount of intermingled personal data accessed from different sources turn the data into probabilistic personal orientation data. The challenge that has to be met is to define to what level an individual can be a data processor extracting logical formulas from data processed by data mining, while respecting the data subject's privacy. Data protection refers to any operation or set of operations that includes the collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data.

Definitions and scope. Directions for Improving Strategic Mechanisms of Personal Data Security and Ownership. The core device for this investigation is personal data security and ownership. Personal data includes information on persons, which identifies them directly or indirectly, as well as their characteristics, features, and behavior. Analyzed extensively in the legal literature, personal data definitions and interpretations are broad and flexible. The universal concepts and practical definitions can be provided by the latest international sources in the fields of human rights and business. During this regulation, the concept of personal data refers to any information related to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

This covering also emphasizes the mandatory relations between the data subject, the data controller, and the data processor. Thus, as the data subject has rights concerning their personal data, the data controller and data processor are held accountable to exercise their professional activities. As we can see from such a general legal perspective, personal data have been an important issue of law reform all over the world, including for the business community during the application of these principles. This is because these principles as global best practices reflect very well the international human rights standards in a unique personal data system where personal data is closely linked to private and family life, home, and personal relations. The personal data system includes additional high legal requirements such as the right of persons to move and reside freely all around the world.

Importance in the digital age. Personal data security and privacy have always been important, although their relevance has significantly increased in the digital age. Presently, a huge amount of personal data is being generated – an estimated 64.2 zettabytes in 2021, and it will rise to as much as 180 zettabytes by 2025. The ways of using personal data are also expanding, especially for data profiling and segmentation driven by artificial intelligence. Such development has opened up multiple commercial opportunities, among other benefits. All these conditions put enormous pressure on personal data security.

Inadequate protection of personal data gives rise to several risks, such as identity theft or financial fraud. If banks, for instance, are not able to reliably and certainly know who their clients are and who uses their services, fraud and other financial crimes will skyrocket, meaning steeper insurance costs that will be recuperated through higher banking service fees. Another risk is privacy intrusions: if people's private information is used in a way that is concerning and becomes publicly known, users will be far less likely to engage in online or digital services. Fundamental actions towards this include securing an institution's cybersecurity, with surveys showing that online consumers rank fear of cybersecurity failures near the top as an obstacle to purchasing goods and services. This loss of trust has been picked up as a major issue for the European Union and digital service providers: a significant percentage of data subjects are concerned about how their personal information is being used, and a notable percentage of global digital users express concern that advanced technologies are slowly eroding their privacy.

Current state of personal data security and ownership in moldova. The following section assesses the current legislative framework and other mechanisms that regulate privacy as personal data ownership and protection in Moldova. The existing legal framework has already incorporated necessary legislation to grant the provisions imposing the basic requirements on state actors and data subjects. In brief, the current legislative framework is appropriate in terms of defining several criteria to provide personal data protection; nevertheless, Moldova has also failed to adopt several necessary legislative provisions. Because of that, Moldova is facing the main weakness in the legislative field and protection mechanisms. This political deficiency in enforcing the Moldovan state to adopt all the necessary instruments for individual data ownership and to secure Moldovan society has deteriorated the state of personal data security in Moldova.

The legal acts dealing with personal data protection and privacy as the ownership of individual data contain many weaknesses regarding their provisions in order to protect individuals' personal information. Consequently, in response to the public, the Moldovan authorities enacted new laws to protect personal data, which are fully in line with the international and European Union data protection standards set out in the official documents and legal acts. Meanwhile, concerning the regulatory and legal level, the operational part was weakened due to the absence of a management authority with the power to enforce this law or to monitor the level of compliance of operators with these regulations. Furthermore, there is an ineffective or inefficient status of the existing self-regulatory mechanisms for data protection, and thus, it cannot provide law enforcement when personal data owners' rights are violated. As known, according to the legal documentation, only the National Data Protection Authority is legally empowered to ensure that personal data protection laws are followed in Moldova as required. If a relevant authority were created with the purpose of enforcing the protection law and monitoring its fulfillment, it would be possible to offer better perspectives on personal data protection in Moldova. Finally, the internal intelligence agents experience challenges in ensuring that all European personal data ownership protection requirements are reflected in the activities of the information holders, as well as in law enforcement and implementation in Moldova.

Legislative Framework. A significant determinant impact on the strategic mechanisms of both personal data security and ownership is exercised by the legislative environment in the area. A number of acts have been recognized as the legislative basis in the area of protection of individuals with regard to the processing of personal data as well as the rules related to the free movement of personal data. It makes provisions on legal acts that are included in the national legal corpus. At the European level, in the list of acts of secondary character that are included in the second part, the

provisions of the European Convention on the Protection of Human Rights and Fundamental Freedoms and other international documents enshrining human rights are included.

The basis of the legal framework in the Republic of Moldova is constituted by the Constitution of the Republic of Moldova of July 29, 1994. At the level of laws, three acts on data protection issues have been elaborated. Their character is direct, in the sense that they establish principled and practical rules and measures of legal order, which have an obligatory character and include a complex of norms. The acts are oriented to a specific object being appellative. In the Republic of Moldova, a series of normative acts regulating legal relationships in the field of protection of personal data have been issued relatively recently. However, in some areas of personal data security and ownership, these remain virtually unregulated by national law. For their further development, the already existing laws and regulations should be revised or new ones adopted. The new regulations entail a set of new challenges that need to be addressed.

Enforcement mechanisms. Based on the new legal provisions in this area, the main actors in enforcing the mechanisms of personal data security are presented. The capacity and conditions of these institutions to enforce the requirements of the data protection legislative framework are discussed. In particular, the effectiveness of the enforcement is directly connected to the level of penalty, its predictability, and enforcement.

Enforcement Mechanisms. The active cooperation, involvement of stakeholders, data controllers, and their data processors, and applying the legislation are the main roles of the national supervisory authority. Among the most important limitations in the activity of the enforcing institution are the resources, lack of expertise in data protection methodologies and the legislative field, and the presence of a small effective sanction as the main intervention means for abuse prevention. In Moldova, the level of penalty as a means of dissuasion is relatively low; it fluctuates between 2,000 and 4,000 euros for the failure of the obligation between the data subject and the personal data holder, up to 10,000 to 20,000 euros in case of violation of the obligations by not ensuring adequate security measures.

To ensure compliance with the national legal framework and align with European practice, it is necessary to place the concept of personal data security within the national public policy agenda and identify specific instruments capable of ensuring the necessary framework for personal data security. The imposition of restrictions on owners regarding the processing and security of personal data within information systems cannot make sense if no mechanisms for administrative, financial, material, and other enforcement of the legal provisions are established, while ensuring the security of personal data. Although the law enforcement means used by public authorities to apply some legal norms are multiple, in contemporary society, depending on the regulated field, conviction, public censure, compensation, and the provision of dissuasive penalties by restricting personal profit are feasible in the data security field. The first legal means could be effective only under the condition that persons privy to harm are aware of their rights and have trust in institutional mechanisms such as the supervisory authority and the courts tasked with ensuring compliance with the personal data security requirements.

Challenges and vulnerabilities in moldova's data security landscape. The current Moldovan data security environment is beset with various challenges from several angles. One set of concerns denotes limitations in technological infrastructure. The insufficiency of cybersecurity investments earmarked for telecommunications or internet infrastructure from the state or businesses entails that maintained technology infrastructures could remain outdated or slow, having a major impact on Moldova's technical aptitude for facing various associated challenges.

Insufficient investments might also limit the capacity of sectoral businesses in ICT, especially communication operators, to implement cutting-edge cybersecurity measures, thereby reducing Moldova's overall ability for data security. Cybersecurity initiatives have been identified that can poorly align sectoral priorities and national interests. For instance, limited capacities could hamper the swift transition to advanced telecommunications forms that use encrypted data security, which thereby require updating supplementary technical settings associated with legal interception.

Data breaches, hacking, and related phishing attacks are commonly brought up regarding threats that could affect enterprises or government agencies. A data breach is rather generic in the sense that it can affect a wide range of services. There might be many more indicators for predicting these breaches and related figures of their victims, but identifying potential spread is particularly important for personal data, which are so important to us. If our personal data falls into the hands of others, there is a risk. As people frequently interact, so do their personal data with different sectors of the economy, and the potential consequences of such interactions should be noted and addressed. Large-scale central databases with personal data, such as on ID cards, can be of significant interest to fraudsters. Attacks and malware encryption can easily wipe out all necessary information and make it difficult to restore. The outbreak of targeted ransomware attacks corresponds seamlessly with Moldova's data theft and ransomware trends too. Healthcare, financial institutions, and governments have the highest risks. An infringement of personal data protection rights with real or potential negative ramifications that affect the economic, physical, psychological, and professional status of a person, or that hinder the exercise of civil liberties and the rights of individuals, is unacceptable. There must be concrete and fast actions and attitudes in this regard. The subject of personal data should be established as a unified strategy and pragmatic plan to ensure data security and both permissions and restrictions for data-related entities.

Technological challenges. There are specific technological factors that are impeding the elimination of the digital divide in Moldova and the conclusion of personal data in the country. Many businesses need to develop and grow in an adequate technical infrastructure like the internet and software and hardware solutions to address security issues. Some of the first registered servers and software solutions in Moldova, installed early on after Moldova became a country and during the transition to democracy, are now outdated and actually contain vulnerabilities. Depending on their settlement and warranty, they may impose a financial burden and block physical fittings and software components. This creates vulnerabilities in the data and needs modernization to regulate both technology and the prominent tools that cover every size and the new requirements, as well as the volume and structure of the data collected. A situation like this is being reported in both the public and private sectors.

The bulk of transactions and digital public benefits requirements are being fulfilled. Therefore, these technological features enable digital rights to be enjoyed and act as checks and controls in the secure processing of personal data and access to information. As the costs of technology controls decrease, regulators must work to annul the contrasts, maintain industry growth, and manage the side changes. Another circumstance that needs to be underscored regarding that report is the speed of technological shifts. Because new technology statistics yield results and demonstrations more rapidly than legislation can keep up with its demands, this extends the implementation of new cases and the emerging sectors of the economy and the labor market. All this has to be emphasized because it is crucial for the private sector to rely on the public to develop devices as countries align with regulations in processing under law. Overall, understanding

technological challenges yields a clearer understanding of the essence of problems in the field of data protection.

Cybersecurity threats. The number of threats to personal data of citizens and other residents of the Republic of Moldova increases. Office automation solutions enable not only an increase in efficiency and improvement in the quality of services but also the employment of economies of scale. The use of correct private and public advanced encryption tools can make illegal access impossible. The encryption of personal, work, and defense data ensured reliable protection against unauthorized access on network-connected IT equipment.

The fungible software is designed to cause personal data destruction, internet banking, social theft, ransomware, or espionage. Such attacks not only distort reality by inciting lies and rumors, but they also present a serious menace against freedom of the media and the credibility and reliability of media organizations, whose activity is solely based on truthful information. Trust in digital services and fully protecting one's privacy harms cybersecurity, with threats being the most common, including malware, web-based, mobile, and email-based phishing. Despite the advantages, these technologies also create new cybersecurity challenges. In most cases, organizations, including public servants, are not well-resourced or simply are not aware of the risks facing them. A number of threats may compromise personal data security, such as failure, malicious, voluntary, and forced, on the part of individual end users. A similar role is played by the positive impact of information and communication technologies. Proactive measures to prevent such threats must be efficiently taken consistently.

Best practices and case studies from eu countries. The European Union has been at the forefront of many data protection developments. Each EU Member State has its particularities in terms of data protection, privacy law, and framework, and this has translated into many best practices and case studies on how data protection regulation mechanisms could be improved. There are more and more reasons why EU best practices and case studies in data protection can be thought of as exemplary for those who have the desire to accept the EU way of data protection and privacy. Many national case studies from European countries regarding data protection and privacy can be found in best practice documents published by the relevant agency.

Under the project "Assessment of the Respect for the Right to the Protection of Personal Data in the Republic of Moldova," conducted in Moldova within the project "Enhancing Data Protection in the Republic of Moldova," cases from the national practices of several EU Member States were considered as examples. Some countries with effective data protection laws and frameworks were chosen based on the attention that could be given to Moldova's example, given its proximity to the Union and EU candidacy, as well as many interconnections and harmonization of legislation with that of the EU. The general focus was on rendering copies of the various personal data protection systems of the EU Member States closely according to the situation in the Republic of Moldova, including from the standpoint of EU norms and standards.

Data protection regulations. One of the tools for ensuring personal data security is the establishment of data protection regulations. The data protection legal framework is sound and is working effectively in most EU countries. It is based on the data protection principles that are mostly identical or very close to those established by previous directives. These principles have proved to be efficient. They include the principle of data minimization, the principle of purpose specification, the principle of reliability control and verified correctness, the principles of responsible and accountable processing, and that of transparency, the principle of data quality, the principle of providing remedies in case of legal breach, and of effective enforcement measures.

The most important data protection regulation that entered into force in the EU is the General Data Protection Regulation, adopted and coming into effect on a specific date. It is based on previous directives but includes strict rules for processing non-sensitive data, such as re-obtaining consent when being used for different purposes than initially established. Furthermore, it has the capacity to sanction companies and individuals in respect of all its provisions with significant fines. Many provisions are considered the gold standard, and this regulation is used by other countries as a source of inspiration in preparing new data protection regulations. There are many provisions and regulations included in this regulation, and as such, there are rules and regulations that countries must abide by. Moldovan data protection law is more than 20 years old. It does not guarantee a level of protection for individuals, and it does not have a sanctions policy that would deter illegal processing. That is why the framework law is to be brought "to teeth." It is necessary to modernize this law, but on the basis of a "data protection strategy," bearing in mind several coordinates.

Innovative technologies. Innovative technologies play an essential role in enhancing the security of personal data and data ownership. EU Member States are continuously working on the development of ecosystems for this purpose, involving emerging technologies such as artificial intelligence, blockchain, and encryption. The use of the above-mentioned innovative technologies could compensate for the risks associated with both data breaches and cyber threats. The security feature of AI is already being used to reduce cyber threats and attacks.

Blockchain allows for a distributed ledger that stores the data in blocks and has already been used as a distributed system for publishing expenditures in order to increase transparency. It has been used to secure electronic voting and to secure large databases of citizens. The security feature of encryption is being used for secure communication, such as the use of virtual private network connections, and for securing files, for example, with encrypted email used by EU Member States. The European Development Fund for projects and Technical Assistance has built a number of innovative mechanisms to ensure transparency and efficiency. Subsequently, these innovative technologies will be developed at the national level in the Southern Neighbourhood and used in innovative projects to enhance data security in the EU neighbourhood. It is advisable for Moldova to consider these innovative technologies and success stories as the development of a new regulatory ecosystem that needs to be compatible with current and future EU data protection legislation. By considering the use of these innovative technologies, Moldovan stakeholders could understand what kind of decentralization in the supported activities involving data governance would be more efficient and secure in the area of personal data and data ownership.

Trategic directions for enchasing personal data security in moldova. In terms of the gaps identified in the analysis of personal data security mechanisms, a set of recommendations for action to address the identified needs of the strategic directions that contribute to the improvement of the personal data security mechanism in the country is shown in the list below: policies are necessary. Depending on the proposed strategic directions, a series of actions are proposed that are important to be taken. The promotion of best practices in personal data protection involves collaboration between government, industry, and other relevant stakeholders in civil society.

At present, a number of public authorities have increased expertise in the collection, verification, processing, and maintenance of personal data for the performance of their duties, with specialized structures in charge of special forms being in the conditions of regulating activities for the applied informatics and information systems. Some staff have a Data Protection Officer who collaborates effectively with project teams and is responsible for implementation and monitoring.

At the same time, it is proposed to improve the training of other employees in the field of data protection. Public authorities must treat electronic data with the protection of the confidential information they contain so that at any time, when data is not in the public domain, we can rely on the principles of availability and integrity. The achieved security level of critical resources is necessary in the following areas: strengthening technical measures to manage and protect personal data in situations of agency management, improvement of the legal framework, and development of the existing potential in education and training. There is a need to promote a campaign to inform citizens about the right of ownership of data that circulate in the information society. The introduction of this right must be fully aligned with the European and national standards of data protection, ensuring the possibility of exercising it. Thus, for the provision of adequate strategies and practices in the field, it is necessary to develop skills among several categories of national actors. The strategic actions proposed are immediate and sustainable since the field of data protection is in continuous development. The section of the needs analysis referred to the first two categories presented, while the following chapter addresses the strengthening of the capacity of the staff, which will have to be adapted to the practical dimensions specific to public administration.

Policy recommendations. The analysis presented above reveals several dimensions of personal data insecurity and the inadequacy of either existing mechanisms or their implementation in the case of Moldova. While enumerating the existing gaps and deficiencies, the narrative also proposed logical connections of what could or should be done to address them. These are:

1. Legislative changes are needed to ratify and implement more comprehensive and clearer personal data standards. This standard should be aligned with current requirements and some of the best developing national practices. 2. Changes are also required to make greater efforts to provide appropriate personal data collection and storage standards before laws and concurrent rights are ratified. This corresponds to another best practice from a much earlier adopter in the area of the integrator - the provision of a law in this respect as the first one from 1973. 3. It is also required to review the mechanisms of the law on personal data control and to identify deficiencies and causes that have generated the deficiencies in enforcing the law by the competent bodies. 4. Relevant data protection legislation consolidates and harmonizes practices and activities of different sectors in the country, as well as relations with foreign nations. It can also be used as an instrument for improving the standard of Moldovan data storage policies for both for-profit entities and the public sector.

Solid efforts are required to strengthen enforcement for strategies set by private and public actors due to the inefficiency of the legislated mechanisms in data defense.

The inadequacies of the Moldovan data protection infrastructure require a more institutional approach oriented towards the delivery and adoption of personal data protection standards. The responsibilities of a relevant legal body have been performed previously by the CICFP, but mainly in confidential data safety. The novelty of a consistent and extensive approach in addressing data information systems requires a detailed analysis of the causes of poor implementation.

The current enforcement agency, the National Center for Personal Data Protection, established in 2009, has been the authority responsible for data protection. The enhancement of enforcement mechanisms and the improvement of existing capacities are imperative in the short term. Once improved, the national legislative framework and the compliance with data protection standards will offer the necessary foundation for obtaining a safe level.

At the same time, for the Moldovan framework to work effectively, much larger contributions are required in identifying technical and human resources, including the clarification of a framework and the use of the latest technology meant to guard the right to private life. The

development of public-private partnerships is urgent. The modernization of personal data storage and management standards must also be accomplished through substantial technological investments.

Capacity building initiatives. Capacity building initiatives can encompass a range of measures—training, knowledge-sharing programs, workshops, technical assistance, policy dialogues, think tanks, and awareness-raising activities. For a long time, efforts have been made to ensure as much as possible of these activities, such as the annual national workshops with the participation of representatives from local authorities and state services, meetings held by participants in the personal data protection school, and other workshops, round tables, and events. An important issue in this context is the organization of training programs, seminars, and workshops in the field of protection of personal data for a wide range of stakeholders (public authorities and institutions, businesses, media, civil society, and the public).

Partnerships can be established with international organizations that can provide training and awareness experience in the field of data protection and privacy. Several awareness events should be organized, targeted at notifying citizens of their rights and obligations in the field of personal data protection. In the field of education, the adaptation of existing school subjects or the development of new curricular subjects can be carried out that will provide students with fundamental knowledge on "Digital Culture and Personal Data Protection." At all levels of education, round tables, contests, workshops, and events in partnership with specialized institutions should be organized to inform students and teachers about the importance of protecting personal data and privacy. Protecting and engaging all stakeholders in this area is important for developing a data protection culture. Starting from a better understanding and implementation of measured data protection, they can aid in the effective management of personal data and help generate confidence among citizens. The main problem of data protection and privacy on the internet is that authorities have outdated knowledge and do not understand how the current processes work. The National Regulatory Authority must undertake efforts to improve this situation as soon as possible and set programs for training and upgrading businesses in the private and governmental sectors as a matter of urgency.

The role of the european union in moldova's data security landscape. Currently, a standardized attitude to data security is practiced within the Association Agreement so that the cooperation between the Republic of Moldova and the European Union is a reference point for this research topic. The fundamental explanation of why the collaboration with the EU in the matter of personal data protection is considered a handy affair for the Republic of Moldova, irrespective of the actualities that are of institutional, financial, or merely technical nature, lies in the drawer of genetic underpinnings. As a rule, concerning its potential candidate countries, the European Union has been promoting its standards, whether it be the adoption of a specific regulation, a universal treaty, or a considerable amount of directives, standards, and good practices, which give the candidate country a comprehensive, sincere, deep, and broad set of tasks and recommendations for the prospective reforms.

"Aligning the national legal and institutional frameworks with the directives of the European Union in the sphere of personal data protection" is an important aspect of the Europeanization of the legislation and the actual practice in the sphere of personal data protection, which would increase the confidence of the EU Member States in the inhabitants of the Republic of Moldova, as future guests of the EU. Collaboration and partial parallel policy lines, which were located within the Europeanization frame, created a consensus towards a very simple and specific coherence of the

domestic legislation and its regulators with the international acquis communautaire, which is in force for the member states of the European Union. The list of additional tasks concerned the changed arrangements within the governmental environment of the ministries after signing the AA, which will eventually lead to a more specific and operational approach. There was also a shift in the principal methodologies the EU had been offering to Moldova towards more practical and personal normative regimes for handling personal data within member states, which is in the direct area of professional competence of the practitioners. In that sense, the EU has succeeded in creating the first three channels for beginning to draft and discuss a comprehensive and practical model of securing personal data on the move in the Republic of Moldova.

Eu data protection standards. Data protection in the European Union is underpinned by the provisions of the General Data Protection Regulation. It applies principles concerning data quality and fairness. It also requires data to be processed for legitimate purposes only and to be protected to the highest possible standards. Its data protection principles can be helpful in forming a common understanding of personal data protection in European countries. It can also be helpful in the calibration of new data protection legislation leading to the Consumer Protection Law harmonization with the GDPR. Many of these principles are also foreseen in Convention No. 108 on the protection of individuals with regard to the automatic processing of personal data. It is deservedly noted that full compliance with such high international standards will be a strong argument for the European Union when making decisions on Moldova's application for accession.

A number of EU and EU candidate partners, including Moldova, adopted a rights-based data protection approach. In the laws of these countries, there are several provisions related to data subjects' rights to access their personal data; to challenge the accuracy of their personal data where undertaken by the data controller; to request the locking, deletion, and destruction of their personal data; to file legal appeals if their requests are not satisfied; and to receive compensation if there is mismanagement of their personal data. Moldova should inform the public about such European requirements, in particular, Moldovan businesses that process personal data of citizens of the member states of the European Union. Also, it is very important to inaugurate a large-scale training program for business representatives. The GDPR will enter into force in Moldova at the regional level. Therefore, representatives of the supervisory authorities and the business community should be aware of these standards before the GDPR enters into force. Therefore, the importance of raising awareness and education among the business community should be specially highlighted. It will be necessary to periodically check the adaptation of the domestic legal framework to the relevant legislation, as the legislation will evolve and will facilitate Moldova's accession to the European Union.

Collaboration opportunities. On the collaboration opportunities to enhance personal data security in line with the exercised functions, first attention should be turned to technical assistance and capacity building. Ideally, the support should equip its technical support and advice in managing the process of alignment to the acquis in all topic areas and head several comprehensive projects, which would promote personal data protection as well. Initially, the support might focus on sharing best practices, knowledge, and lessons learned by the Member States and the respective agencies. Taking into account the political stage of the Moldovan-EU talks, one could explore opportunities for the development with relevant institutions of bilateral Moldova-EU 'small projects' to build some common foundation in order to promote future alignment with standards.

Regarding the mainstream aspect of personal data protection, there might be a particularly strong interest in further investments and capacity building to ensure effective regulatory

governance. These investments would benefit the Moldovan data protection system and also facilitate the exercised functions as the two are seen as interlinked. For this reason alone, there are significant relations to be drawn from a partnership between these lines and training, technical assistance, or knowledge contributions from other acceded and candidate countries on regulatory governance and how to build a regulatory framework. Joint initiatives to foster a data protection culture would be among the first steps to be undertaken once regulatory frameworks are in place, meaning they are also an immediate topic area where collaboration could start. Awareness, citizens' education, and participation programs can indeed be of mutual benefit to enhance mutual learning and to promote the strategic development of approaches to data governance that are based on trust. Moreover, a joint initiative on strategic exercises can promote trust and increase awareness about data protection responsibilities.

Conclusion and future outlook. In this paper, we have attempted to analyze the legal and strategic aspects of ensuring the security and ownership of personal data of citizens of the Republic of Moldova as part of European integration. The present level of harmonization of the given principles with EU law has been demonstrated, and a list of priority statutory changes necessary to improve their legal framework for effective approximation has been formulated. Also, we formulated priority strategic goals in the field of ensuring the security and ownership of personal data in the context of European integration, analyzed the level of their development, and recommended a set of measures for their implementation.

The obtained results have practical importance for Moldovan society and civil service institutions from the perspective that the identified problems still need to be solved within the current association process in order to jointly create an effective mechanism for ensuring the security and ownership of personal data, which could serve as a reliable basis for building relationships with the EU in the field of protection of the fundamental rights of citizens.

Summary of findings. The present cases act as an attempt to give the example of potentially dangerous goods when applied and used, namely personal data, if the field of strategy is not well employed. The cases are intended to raise awareness about the importance of personal data security and ownership in light of the upcoming candidature of Moldova to the EU and suggest improvement directions. Thus, its main contribution consists of the identification of the issues in this context and recommendations in order to ensure that Moldova could harness the EU opportunities in this respect. The employed methods include an analysis of personal data protection components and the strategy-governance-performance trio. It is organized into sections that provide the context and the role of strategies in personal data security and ownership, their linkage to candidacy to the EU, the strategy concepts and tools, the case studies from the Republic of Moldova that illustrate particular issues, and finally recommendations based on the findings.

Implications for moldova’s eucandidacy. The need for harmonizing Moldovan legal provisions with the EU legal framework as a precondition to Moldova's EU candidacy has been mentioned. The current study highlights the importance of EU membership for Moldova in an area that is of increasing importance for both individual countries and as a whole for the EU and Moldova in particular. Personal data in the digital era are essential for Moldova's economic welfare, as it functions as an indispensable fuel for innovation. Safe and fair access to data should be considered in principle as part of the broader set of norms, rules, and values that are key for Moldova's functioning. However, personal data-oriented regulation in Moldova does not provide enough mechanisms for its full conceptual implementation in the form of personal data ownership and security enhancement. This chapter focuses on considering improved legal mechanisms for

enhancing the security and ownership of personal data in the context of EU rules, as one of the necessary directions and commitments needed to be taken and implemented by Moldova in order to get closer to a candidate for obtaining an EU membership perspective. We intend to define what the implications of the proposed modernization of legal mechanisms for personal data security and ownership would be on the status of Moldova as an EU candidate, providing in this way an alternative approach to the official developments, which might lead to upgraded political dialogue between Moldova and the EU itself. The chapter concludes by outlining the main findings and providing implications together with the broader questions arising from the practiced question.