REPORT

OF

THE INFORMATION AND DATA PROTECTION

COMMISSIONER'S OFFICE

in the framework of

Resolution dated 21/05/2020 of the Parliament of the Republic of Albania "On evaluation of the activity of the Information and Data Protection Commissioner for the year 2019"

Tirana, on 28/12/2020

TABLE OF CONTENTS

A. GLOSSARY	
State database	The organized collection of information, stored in electronic form, where its processing and updating are carried out through a computer system, as part of fulfilling the legal obligations of the administrative institution.
EU	European Union
Controller	Any natural or legal person, public authority, agency or any other body which, alone or jointly, determines the purposes and means of processing of personal data in compliance with the laws and applicable secondary legislation, responsible for the fulfillment of obligations defined in this law.
Law on the Protection of Personal Data	Law No. 9887, dated 10/03/2008 "*On the protection of personal data*" as amended.
Log	Abbreviated note containing the needed data to ensure that such data can be used to guarantee the monitoring, investigation and solution to any security problem.
Processor	Any natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Controller.
Resolution of the Parliament	Resolution of the Parliament of the Republic of Albania, dated 21/05/2020, "*On evaluation of the activity of the Information and Personal Data Protection Commissioner for the year 2019*"
Information Security Management System (ISMS)	The Information Security Management System for the protection of personal data, provided under Instruction no. 47 and Instruction no. 48 of the Commissioner
Data Subject	Any natural person whose personal data are being processed
ICT	Information and Communication Technology
Instruction no. 19	Instruction no. 19, dated 03/08/2012 of the Information and Data Protection Commissioner "*On the regulation of relations between Controller and Processor in cases of delegation of data processing and the use of a standard contract in cases of delegation*", as amended.
Instruction no. 47	Instruction no. 47, dated 14/09/2018, of the Information and Data Protection Commissioner "*On determining*

	rules for safeguarding personal data processed by large processing entities"
Instruction no. 48	Instruction no. 48, dated 14/09/2018, of the Information and Data Protection Commissioner "*On Certification of information security management systems, personal data and their protection*"
Instruction no. 49	Instruction no. 49, dated 02/03/2012 of the Information and Data Protection Commissioner, "*On the protection of personal health data*"
Commissioner's Office	Office of the Information and Data Protection Commissioner

B. REPORT

This Report is prepared in accordance with paragraph 2, Article 30 of the Law "On the Protection of Personal Data", as well as the tasks assigned to the Commissioner's Office based on the Resolution of the Parliament.

The aim of this Report is to convey to the attention of the Parliament, the findings and recommendations of the Commissioner's Office on the supervision areas defined as special tasks by the resolution.

The findings and recommendations according to this Report are part of the ongoing commitments of the Commissioner's Office regarding the monitoring and supervision of compliance with the legislation for the protection of personal data by the Controllers, *inter alia*, in the Information and Communication Technology sectors, as well as in sectors where sensitive data is processed, such as the health care sector.

The duration of the conducted inspections and controls for the purposes of this Report has been dictated, among other things, by the circumstances and difficulties created by the COVID-19 pandemic.

Therefore, the Commissioner's Office reserves the right to further report to the Parliament on other developments, circumstances and/or situations that may be verified in the future in relation to the scope of this Report, in accordance with paragraph 2, Article 30 of the Law "On Personal Data Protection".

The report is prepared in two parts as follows:

- *Part 1 - Data processing in the Information and Communication Technology sector.*
- *Part 2 - Data processing in the health care sector.*

Part 1 presents the findings and recommendations of the Commissioner's Office regarding data processing in the public sector of Information and Communication Technology.

Part 2 presents the findings and recommendations regarding the public and private health care sectors.

The reasons for including the private sector in this part of the Report are related to the situation caused by COVID-19 and, consequently, to the importance that this sector assumes within its obligations to coordinate with public health care institutions their efforts and commitments to prevent and cope with the consequences brought by the pandemic.

PART 1 - Data processing in the ICT sector

I. Introduction

The provision of *online* public services through ICT platforms has been accompanied by an increase in the processing of personal data by public authorities, due to the ease of citizens' access to public services thanks to such platforms.

Consequently, the Commissioner's Office has continuously found an increasing processing of personal data by public Controllers (institutions and/or companies with state capital) through the ICT systems.

The spread of the COVID-19 pandemic and its serious consequences on the health and life of citizens have caused the provision of public services through ICT platforms to be not one of the options for accessing public services alongside physical offices, but almost the only one option for this purpose.

E-Albania, the unique government portal, which is administered and maintained by the National Agency for Information Society (NAIS) has played a key and particularly important role in this aspect.

Thus, ICT platforms are currently and, in all likelihood, will continue to be in the future, a necessity and a reasonable solution for citizens to access services.

On the other hand, the citizens, in addition to being guaranteed the right to access public services, must also be guaranteed the inviolability of their rights to protect their personal data and private life when using ICT platforms for receiving public services.

This means the obligation of public Controllers to pay special attention to taking technical-organizational measures and creating the necessary conditions for guaranteeing the safety and protection of citizens' personal data, as well as, along with it, the preservation of confidentiality pursuant to the provisions of articles 27 and 28 of the Law "On the Protection of Personal Data", as well as the provisions of the Commissioner's by-laws.

Therefore, monitoring and supervising the processing of personal data in the ICT sector has been at the center of the priorities of the Commissioner's Office for the year 2020.

Throughout the activity of the Commissioner's Office, in particular during the period of the state of natural disaster declared due to the COVID-19 pandemic, and following, there have been observed a series of complaints from the citizens regarding issues related to the processing of personal data through network platforms.

On the other hand, the Commissioner's Office has provided continuous assistance for a series of legal and sub-legal acts, submitted for consideration by the Council of Ministers, Ministries, and/or various government agencies.

It is worth mentioning, in this aspect, the draft law "*On the creation of the state database "e-Albania"- Unique Government Portal*" and on the approval of the rules "*On the operation of the Single Point of Contact*", the draft law "*On the central register of bank accounts*", the draft decision on the approval in principle of the treaty "On the exchange of data for the verification of asset declarations", etc.

As mentioned above, in implementation of the tasks assigned by the Parliament based on its resolutions, in addition to its regulatory, sensitizing and orienting commitment, the Commissioner's Office has developed a campaign of inspections and supervisory visits to Public Controllers in the Information Technology and Communication sector, the summarized results of which are presented in this part of the Report.

II. Facts and circumstances related to the supervision

Pursuant to the Resolution of the Parliament, as well as the powers and legal obligations provided under the Law "On Personal Data Protection", the Commissioner's Office has been entrusted with the task of supervising, *inter alia*, online and ICT platforms, as well as with submitting a detailed report on the state of personal data protection.

In this context, upon letter with protocol no. 669, dated 10/06/2020, with subject "*Request for information in the framework of identification and analysis of databases and online platforms in the administration and use of public institutions*", the Commissioner's Office has addressed to 82 public Controllers (institutions of public administration and commercial companies with state capital), requesting information regarding the following:

(i) Number of databases and *online* platforms/systems in administration and use;

(ii) The legal basis for the creation and operation of databases, as well as *online* platforms/systems;

(iii) Specification of access level to databases, as well as *online* platforms/systems. The number of employees with an access to them, as well as their position in the institution by task/function;

(iv) The traceability of processing actions in order to document interventions and other actions (creation, modification, destruction, storage/backup, etc.) in databases, as well as online platforms/systems.

Only 68 public authorities responded to the above request.

Furthermore, upon Order no. 91, dated 09/06/2020 of the Commissioner, a special working group has been set up, consisting of lawyers and ICT experts, to carry out some inspections and supervisory visits to certain public Controllers.

The selection of Controllers for this purpose was based, mainly, on the group of those who did not respond to letter with protocol no. 669, dated 10/06/2020, as well as, first of all, based on the importance that the activity of the said Controllers bears in relation to the provision of public services and, consequently, on the high volume and frequency of personal data processing.

Methodologically, the working group, when conducting its inspections and supervisory visits, has focused on verifying the compliance of Public Controllers with the principles and legal criteria of processing personal data, respecting the data subject rights, as well as on the special measures taken by such Controllers to ensure the security and confidentiality of personal data, with a special focus on Information Security Management Systems (ISMS) for the protection of personal data, regulated by Instructions no. 47 and 48 of the Commissioner.

In order to identify the factual situation beyond the declarations made by the institutions, the Commissioner's Office, taking into consideration, inter alia, factors such as the nature of the public service offered by the relevant authority and the risk level in the protection of personal data, took the procedural steps to supervise the processes of personal data processing in the below mentioned Controllers:

i. National Agency for Information Society (NAIS);

ii. State Cadastre Agency (SCA);

iii. Albanian Post SHA;

iv. National Business Center (NBC);

v. Agency for the Delivery of Integrated Services Albania (ADISA)

vi. General Directorate of State Police (GDoSP)

vii. General Directorate for the Prevention of Money Laundering (GDPML)

viii. General Directorate of Taxation (GDoT)

ix. General Directorate of Prisons (GDoP)

The inspections and verifications related to the observance of the legislation for the protection of personal data were carried out during October - November 2020, by reviewing the documentation made available at the request of the inspectors of the Commissioner's Office, as well as through site inspection in the above mentioned entities.

III. Legal basis

Inspections and supervisory visits conducted by the Commissioner's Office, in implementation of the powers defined under articles 31 and 32 of the Law “On the Protection of Personal Data”, focused on the verification of compliance with the legal principles and criteria for the processing of personal data, as well as the verification of technical and organizational measures for the prevention of illegal dissemination of the subject data in accordance with articles 5, 6, 12 - 15, 18 - 20, 27 and 28 of the said law.

Furthermore, in addition to the above-mentioned provisions of the law, the working group is also based on the binding provisions of the by-laws issued by the Commissioner, including in particular Instruction no. 19, 47 and 48 of the Commissioner determining the Controllers’ obligations regarding the relations with the respective Processors, as well as for the creation, maintenance and administration of the Information Security Management System (ISMS) for the protection of personal data.

Namely, Article 5 and 6 of the Law “On the Protection of Personal Data” specify the legal principles and criteria on which the processing of personal data is based, such as the principle of lawful basis of data processing, the principle of sufficiency, processing based on the consent of the data subject, for the fulfillment of a legal task by the Controller, etc.

Furthermore, Controllers are obliged to respect the data subject rights defined under Chapter IV of the Law "On the Protection of Personal Data" which include, but are not limited to, the right of access to data, the right to request the blocking, correction and erasure of personal data, as well as obligations for information before the start and/or after the change of the state of data processing sanctioned under Article 18 of the law.

In addition to that, depending on the nature of their activity, part or all of the data processing process may be delegated to third parties. An example of this is the interaction of public institutions with *e-Albania* through which they offer their services to citizens.

At the core of this interaction is the data processing that the Controllers in question carry out through "e-Albania" - the unique government portal, which entails the obligation of the parties to standardize their Controller-Processor relation through special agreements provided under Article 20 of the Law "On the Protection of Personal Data" and Instruction no. 19 of the Commissioner.

In addition to the above, Controllers are obliged to take technical and organizational measures to ensure the security of personal data and maintain their confidentiality in accordance with article 27 and 28 of the Law "On the Protection of Personal Data".

These articles foresee the obligation of each Controller to protect personal data from illegal, accidental destruction, accidental loss, to protect access or dissemination by unauthorized persons, especially when data processing takes place in the network (through ICT platforms), as well as from any other illegal form of processing.

In implementation of this obligation, in order to explain and elaborate the provisions of Article 27 of the Law "On the Protection of Personal Data", the Commissioner has drafted and approved Instruction no. 47.

This instruction foresees the obligation of all Controllers – who engage more than 6 people for the processing of personal data – to create, administer and maintain the Information Security Management System (ISMS) for the protection of personal data.

ISMS is based on the identification, analysis and mitigation of risks to the security of personal data taking into account ICT systems for data processing, manual forms of processing, physical security of environments, personnel and equipment, as well as defined in ICT standards as follows"

(i) "*Confidentiality*", ensuring that personal data are accessible only to authorized persons;

(ii) "*Integrity*", ensuring that the data are accurate, complete and that they stick to the their processing methods;

(iii) "*Availability*", ensuring authorized user access to data and processing systems;

(iv) "*Confidentiality*", guaranteeing that every activity/action on the data, of ICT systems and personnel used for their processing is traceable and controllable.

Moreover, it is necessary for ISMS to include a set of binding rules and documents for Controllers, such as Personal Data Impact Analysis, Information Security Policy, Data

Archiving System Control, etc., as well as physical security of premises, personnel and ICT equipment (platforms).

Further, the Controllers must take measures for the training of employees who have access to and process personal data, in accordance with the legislation in force for the protection of personal data.

Controllers have the obligation to create, administer and maintain the ISMS for the protection of personal data, based on the requirements of the ISO/IEC 27001 standard, provided under Article 5 of Instruction no. 48.

Also, Instruction no. 48 provides the possibility of Controllers for ISMS certification, for compliance purposes with the above-mentioned standard, by accredited and authorized bodies according to the provisions of this instruction.

It is worth noting that the certification mechanism is an innovation introduced within the General Data Protection Regulation (GDPR) of the EU, which the Commissioner's Office has "transposed" (in a non-binding way), with the assistance of the counterpart authorities of the EU, in the provisions of Directive no. 48.

In addition to the technical and organizational guarantees that precondition the Controllers, as well as the positive reputational effects it carries for the latter, the certification mechanism also aims to encourage Controllers take self-regulatory measures for guaranteeing the security and confidentiality of personal data.

IV. Problems identified

The problems identified in the framework of the inspections and supervisory visits carried out by the Commissioner's Office working group in the public authorities listed under Chapter II above, are presented, for the purposes of this Report, in two main respects:

(i) In terms of compliance with the obligations arising from the legal framework for the protection of personal data, which includes the verification of compliance with the legal principles and processing criteria, compliance with data subject rights, Controller-Processor relation, etc.; and

(ii) In terms of technical and organizational measures, in particular, based on the existence of the ISMS in each Controller that is subject to control.

IV.1 National Agency for Information Society (NAIS)

NAIS is the central institution responsible, among other things, for the implementation of policies and strategies, for the development of the information society sector; it is a coordinating regulatory authority, responsible for state databases, as well as providing centralized services through ICT for electronic governance, for state, citizen, and business administration.

NAIS administers every ICT system and infrastructure for institutions and state administration bodies under the responsibility of the Council of Ministers, according to

Decision no. 673, dated 22/11/2017 “On the Reorganization of the National Agency for Information Society”, as amended.

Based on the conducted verifications, it was established that NAIS has adopted a specific regulation for privacy policies, which is also published on the institution's official website.

Having reviewed the regulation, it results that such regulation provides the principles of data processing, as well as data subject rights, organizational security measures, the right to complain, etc.

However, it is noted that this regulation does not include all personal data processing processes carried out by NAIS, limiting, in this way, the data subject right to be informed about the categories of personal data that are processed and the purpose of the processing.

NAIS turns out to have delegated the physical security service of the premises to a private entity (Processor). After examining this contract, it has been noted a lack of data protection rules for this processing process, as well as shortcomings regarding the elements, obligations and legal guarantees required by the provisions under Article 20 of the Law “On the Protection of Personal Data.

NAIS has adopted the ISMS system as per the information security standard ISO/IEC 27001.

Based on the review of the documents, which are part of this system, it results that the procedures and policies for information security are determined in relation to access management, asset use, human resources management, system capacity management, incident management, continuity of information security, etc.

However, it is noted that in this institution, the organizational structure lacks an independent function to monitor and continuously improve the implemented system.

The mission of this information security organizational structure should be to design, implement and maintain an information security program that protects NAIS systems, services and data against unauthorized use, disclosure, modification, damage and loss.

The importance of a proactive and unbiased team is a key factor for carrying out processes for ensuring information security in relation to management, instructions, coordination and operational functions, as well as for defining policies/regulations for monitoring and managing information security.

This role is important to periodically monitor the ISMS effectiveness by analyzing the progress achieved and proposing further improvements.

Continuous improvement is a key aspect of the ISMS in the effort to achieve and maintain the confidentiality, integrity, availability and reliability of information security and should be an integrated part of the objectives of public Controllers.

Analyzing the importance of NAIS as the central institution responsible for the infrastructure of electronic government services, the establishment of an independent and qualified structure according to information security standards plays an important role in the personal data security and efficiency of ISMS.

With the pace of innovation and technology progress, it is essential to develop competencies, especially for ICT specialists, according to ISO/IEC 27001 security standards, to have the professional knowledge for the administration of the systems in use.

Taking into consideration the critical infrastructures in management, the Commissioner's Office assesses that this institution should pay great attention to the continuous monitoring of systems, infrastructures and services offered through the government platform GG (Government Gateway), Cloud services and infrastructure public key (PKI).

Also, the disaster recovery strategy, as well as the plans determining business continuity in case of failure, must be in accordance with the permitted norms of safety distances and be periodically tested for all their components.

IV.2 State Cadastre Agency (SCA)

SCA is a public legal entity under the Prime Minister responsible for providing cadastral services, based on the provisions of Law 111/2018 "On Cadastre".

SCA has approved a series of regulatory acts which provide general and declarative obligations to maintain confidentiality, such as the ethical code of the institution, the internal regulation, as well as the regulation for guaranteeing the security of the electronic register of immovable properties.

However, in the above acts, there are no specific norms that regulate the storage, protection and security of personal data of data subjects during the processing that this Controller conducts in fulfilling his legal tasks.

Specifically, SCA has drafted a regulation "*On guaranteeing the security of the electronic register of immovable properties (ALBSReP)*", which specifies general rules and procedures to ensure the protection of confidentiality, integrity and availability of information in ALBSReP.

On the other hand, based on the control exercised, it results that there is a marked lack of monitoring of information security processes by the ICT department.

Furthermore, a lack of a strategy has been noticed for ISMS in accordance with the provisions of Instruction no. 47 which consists of the implementation, monitoring and continuous improvement of the ISMS, guaranteeing the protection of information through a centralized and standardized management system.

User creation and termination is done according to registration forms upon approval, but a user's lifecycle, updates and devices (assets) are not continuously monitored by the ICT department.

It was found that users are not categorized for access depending on the functions they perform. In some cases the users and devices (assets) are not centrally managed in *Active Directory* (AD). This violates the data integrity that is processed and memorized in the fulfillment of the functional tasks of this institution.

IV.3 Albanian Post SHA

Albanian Post SHA is responsible for providing the state mail service in the Republic of Albania.

This Controller has drafted and approved a specific regulation for the storage, processing, protection and security of personal data, which is also published on the company's website, accessible to website visitors.

The regulation includes, in a general framework, the processing processes carried out by Albanian Post SHA, the principles and criteria of processing, data subject rights such as the right to access, the right to correction or erasure, security measures, as well as organizational functions between internal structures.

In addition to that, Albanian Post SHA has drafted and approved a regulation for the use of electronic mail and some procedures related to the operation of information security processes.

This entity manages and monitors users with centralized systems, ensuring the integrity of the data being processed.

It has designed and implements procedures for business continuity and tests them on a regular basis through contracts with suppliers.

However, standardized processes related to asset management, information security incidents, as well as a continuous monitoring and improvement plan of ISMS in this institution, in accordance with the ISO/IEC 27001 standard, have not been identified.

Implementation of an ISMS in accordance with the above-mentioned standard will ensure protection from risks that may affect the confidentiality, integrity or availability of personal data.

With the pace of innovation and technology progress, it is essential to develop competencies, especially for ICT specialists, according to the ISO/IEC 27001 security standard to have the professional knowledge of systems administration.

In addition to specific programs for the ICT staff, continuous awareness programs for the latter should also be designed, taking into consideration the advancement of technology, cyber attacks and legislative updates in force.

IV.4 National Business Center (NBC)

The National Business Center (NBC) is the responsible institution for maintaining and administering the commercial register and register of licenses in the Republic of Albania.

NBC has drafted and approved a specific regulation for the storage, processing, protection and security of personal data in 2018.

The regulation includes, in a general framework, the processing processes conducted by this Controller, the processing principles and criteria, data subject rights, division of processing processes into relevant organizational units, physical security of the environments whereby the processing take place and a provision for IT security.

Moreover, NBC has drafted and approved the ICT regulation, dated 11/11/2020, in which the principles and rules of information security are laid out.

This regulation sets out the responsibilities for actions related to security in order to maintain the integrity, availability and confidentiality of NBC's information assets.

However, there is no strategy in place for monitoring on a regular basis the ISMS effectiveness as per ISO/IEC 27001 standard, for analyzing the progress achieved and proposing further improvements.

This factor is important for meeting information security requirements and personal data protection.

In addition to specific programs for the ICT staff, continuous awareness programs for the latter should also be designed, taking into consideration the advancement of technology, cyber attacks and legislative updates in force.

IV.5 Agency for the Delivery of Integrated Services Albania (ADISA)

ADISA is the institution responsible for providing public services to natural and legal persons through service desks, one-stop-shop desks and integrated public services desks.

Upon Decision no. 7, dated 09/05/2019 of the Governing Council, ADISA has adopted the regulation for the protection of personal data, which provides the observance of the processing principles and criteria, data subject rights, separation of processing processes into the relevant organizational units, etc. in the processing processes conducted by ADISA.

However, the inspection conducted at ADISA found that the number of services offered to citizens in physical desks has been significantly reduced, because the services are offered through e-Albania - the unique government service portal.

The desks in the local government units mainly serve to provide assistance to citizens in accessing e-Albania - the unique government service portal.

On the other hand, it resulted that ADISA did not have any regulations and procedures in place for ICT platform governance, ICT operation management, as well as systems and information security.

A lack of strategy or plan for information security in accordance with the provisions of Instruction no. 47 has also been found.

This process is conducted by the ICT structure under NAIS, which operates according to the processes defined in the work regulations of this institution.

User and utilized devices are managed in a non-centralized way, posing, thus, a great risk for the protection of personal data.

Ongoing staff awareness programs should be designed, taking into consideration the advancement of technology, cyber attacks and applicable legislative updates.

IV.6 General Directorate of State Police (GDoSP)

There is an increased attention of the GDoSP in the framework of implementation of legal obligations in the field of personal data protection, this as a result of the commitments this institution has with its EU counterpart institutions and beyond which impose a strict respect of the rules related to the protection of personal data that constitute the basis of any cooperation in the police field.

Organizational and technical procedures, as well as measures for the protection of personal data are defined under the Regulation "On the protection of personal data and their security in the State Police", approved by Order no. 330, dated 04/07/2011 of the Minister of the Interior.

Access to the GDoSP systems is organized at two levels: specifically, at database administrator level and user level as per the respective roles and responsibilities.

One of the most important systems in administering this Controller is the Total Information Management System (TIMS) which manages the entry-exits of data subjects from the Republic of Albania. This IT system is built and technically maintained by the Directorate of Information Technology under the Controller.

During the inspection, the Commissioner's Office found that during data processing in the TIMS system, the GDoSp applies, inter alia, the provisions of the regulation "On the protection of personal data and their security in the State Police".

The aforementioned regulation provides the technical and organizational measures for the processing and security of personal data administered by the State Police in accordance with Article 27 of the Law "On the Protection of Personal Data". The provided technical and organizational measures are of a satisfactory level.

However, in order for these measures to be as effective as possible, it is necessary to align them with the ISMS elements pursuant to Instruction no. 47 of the Commissioner.

The inspection has identified the existence of several cooperation agreements such as "On the granting of the right to use the total information management system (TIMS) of the State Police", entered by and between the Directorate of State Police and several institutions such as the General Prosecution Office, General Directorate of Customs, General Directorate of Taxation, State Intelligence Service and General Directorate for the Prevention of Money Laundering.

Through these agreements, the institutions in question are allowed to access personal data of Albanian citizens through the TIMS system. Such agreements include the conditions, obligations and administrative and criminal liability of the authorized persons to access the system for maintaining confidentiality and not disseminating information.

In this context, the Commissioner's Office deems necessary for the GDoSP, in any case, to carry out the Impact Analysis on Personal Data (as an important element of ISMS), appraising in advance the risk of the provided access and the processing processes.

Furthermore, it is necessary that the agreements reflect the necessary elements provided under Article 20 of the Law "On the Protection of Personal Data" and Instruction no. 19, as long as the institutions that have access to TIMS are considered processors.

The Commissioner's Office, upon Recommendation no. 32, dated 23/12/2016, assigned a series of tasks to the GDoSP regarding the security of data protection in the TIMS system.

In this context, it was found that technical measures have been taken regarding the traceability of actions in TIMS, increasing the term from 6 months to 2 years. However, it is necessary for this to also be reflected in the internal regulatory acts that are mandatory for every user.

The terms for subject data storage in the TIMS system is provided by the Order of the General Director of State Police no. 245, dated 16/03/2016 "On the terms of personal data storage in the State Police electronic systems for purposes of prevention, investigation, detection and prosecution of criminal offenses".

In this context, the inspection found non-implementation of the terms provided under Instruction no. 17, dated 11/05/2012 "On determining the storage term of personal data processed in electronic systems by State Police bodies for the purposes of prevention, investigation, detection and prosecution of criminal offenses", approved by the Commissioner's Office, which also extends its effects in all electronic systems administered by State Police bodies.

GDoSP has drafted and approved procedures and regulations for ensuring data and information security. Responsibilities are laid out in the work procedures and the process for creating, updating and closing users in critical systems is structured.

GDoSP has set up monitoring processes for users and their access, and has started their auditing. Secure infrastructures have been set up in GDoSP which interact with secure communication channels between its collaborators and the internal infrastructure.

However, the partial implementation of the ISMS does not provide sufficient security for the protection of personal data.

The effort to achieve and maintain the confidentiality, integrity, availability and reliability of information security should be an integrated part of the GDoSP objectives.

Therefore, the Log generation process (Audit Log and Operating System Log) monitoring should be improved.

Support systems and infrastructures for Logs generation must be built according to detective and evidentiary security controls. Traceability in critical systems is a key factor to detect and identify unauthorized access or data modification in a database. The operating system logs must contain the necessary information to ensure that such information can be used to guarantee monitoring and detection, and, therefore, the solution to any security problems.

Security log analysis should be performed on a regular basis considering the impact that critical systems and infrastructures have on personal data.

IV.7 General Directorate for the Prevention of Money Laundering (GDPML)

GDPML is an institution under the Ministry of Finance and serves as a specialized financial unit for the prevention and fight against money laundering and terrorist financing.

The Commissioner's Office, within the framework of identifying the processing processes, the categories of personal data subjects, personal data categories and technical organizational and legal measures to ensure the security and confidentiality of such data, has analyzed the specific legal basis regulating the activity of this Controller and provides the rules for administering and creating the database administered by this institution.

Article 16 of Law no. 9917, dated 19/05/2008 "On the prevention of money laundering and terrorism financing" as amended, provides concrete measures for data storage terms which refer only to reporting entities.

The Commissioner's Office appraises that even though the general elements on the security of personal data, access level and traceability of actions are important and are also reflected in the obligations that the institution has as a public controller, it is necessary to take measures also within the implementation of other specific elements that originate from the Law "On the Protection of Personal Data", as well as the by-laws adopted in its implementation.

Such measures should reflect the personal data subject rights, Controller's obligations, data protection principles (in particular the data storage term), the provision of guarantees on the data system security in accordance with Instruction no. 47, as well as must be applicable to every processing process conducted by GDPML.

GDPML has drafted and approved procedures and regulations to guarantee data and information security, in which responsibilities are defined and processes are structured for access management and monitoring, asset management, incident management, human resources management, system capacity management, incident management, information transmission security, business continuity.

The operating systems and infrastructures of this institution are centrally managed, both for users and assets, which ensures the integrity of the data being processed.

Furthermore, even though general policies and procedures that partially cover information security have been drafted, it was found that there is a lack of a strategy for the ISMS implementation in all its security elements in accordance with Instruction no. 47 of the Commissioner.

IV.8 Central Tax Administration Office (CTAO)

CTAO is an institution under the Minister responsible for Finance and its main mission is to collect tax revenues by implementing the tax legislation uniformly in order to finance the Albanian state budget.

CTAO has drafted a series of regulatory acts which include provisions on maintaining confidentiality.

However, no specific norms have been found that regulate the storage, protection and security of personal data during the processing processes that the institution conducts in fulfilling its functional tasks.

CTAO has adopted a regulation for information security which lays out the general rules for information security and responsibilities for actions related to information security in CTAO.

Based on this regulation, several policies and procedures have been drafted for the purpose of information security.

However, no standardized and periodic monitoring processes have been established according to the regulations designed for the protection of assets and information, for maintaining data integrity and for data availability and confidentiality.

Therefore, the continuous audit of the network and the systems in use must be a documented and continuous process for the fulfillment of the information security objective and the protection of personal data.

The continuous review and updating of applicable rules and policies regarding security and privacy must respond to the technological innovation pace and to the legislation in force.

IV.9 General Directorate of Prisons (GDoP)

The GDoP administers and uses, among others, the "Penitentiary System Information Management Database" (MISP) and the "Penalty Evidence Program Database" (CEP).

Their organization, administration and operation is regulated by specific regulations approved by the General Director of Prisons.

Based on the analysis of such regulations, the Commissioner's Office deems that, despite serious efforts within the framework of fulfilling the security standards, the foreseen measures do not fully implement the personal data security elements in accordance with Instruction no. 47.

Based on the analysis of the delegation contract for the creation and maintenance of the application for the convicts and personnel files which the Controller has signed with a union of economic operators (in the capacity of Processor), there are observed deficiencies in addressing the elements, obligations and legal guarantees as per Article 20 of the Law "On the Protection of Personal Data" and Instruction no. 19 of the Commissioner.

GDoP has drafted and implements rules regarding information security, the infrastructure and systems it uses. Such rules are also reflected in the maintenance contracts that the institution has with the main suppliers for the systems and physical maintenance of the premises.

Access and responsibilities by administrative structure functions are well defined and structured in the work processes.

Moreover, interaction with external systems takes place under secure and monitored communication channels.

However, taking into account the fact that GDoP processes and transfers sensitive data, continuous monitoring of all critical infrastructures should be improved, with periodic audit procedures for analyzing the operating system logs.

Managers play a key role in ensuring awareness of information security and confidentiality throughout the institution and in developing a "security culture", designing ongoing staff awareness programs based on the importance of personal data being processed and to their classification.

V. Conclusions and Recommendations

Based on the entire supervision process, it results that in most of the public Controllers the regulatory aspect of personal data protection during processing through information technology is separated from the rules regarding other data processing processes.

In this context, state administration institutions that process personal data must concretely foresee all processing processes in decent regulatory acts that guarantee storage, security, and protection of personal data of data subjects in compliance with obligation under Article 27 of the Law "On the Protection of Personal Data".

The Commissioner's Office deems that the problems identified in these public institutions are related to the lack of legal and technical knowledge and awareness of the obligations provided under the legislation for the protection of personal data.

As for the contractual relations that public institutions (in the capacity of Controller) enter with third parties (in the capacity of Processor) for the delegation of various services, where in essence personal data processing is involved, there are deficiencies in addressing elements, obligations and legal guarantees sanctioned under Article 20 of the Law "On the Protection of Personal Data" and Instruction no. 19 of the Commissioner.

The Commissioner's Office recommends that in the future, public institutions when drafting contracts with third parties should include the elements of Article 20 of the Law "On the Protection of Personal Data" and Instruction no. 19.

The Commissioner's Office has found that the Controllers have drafted and approved internal regulatory acts on personal data protection, but such acts contain general regulations on personal data management and data subject confidentiality, there are no regular details on the appropriate and applicable technical-organizational measures to guarantee the protection of personal and sensitive data, the lawfulness of data processing, measures to guarantee the traceability and control of the actions of the persons/personnel who had and/or has access to such data, as well as their disposal method when their processing purpose has been fulfilled.

Especially in relation to granting access to personal data, we find the opportunity to note again our continuous capacity as a supervisory authority that such action/processing, even when authorized by law, does not necessarily and always imply a direct and unrestricted access to the required data.

Granting a direct and unrestricted access to personal data, despite the fact that it may in principle be authorized by law, may lead to data processing in excess of the purpose of the activity and/or the task for which the law authorizes a Controller (authority/institution)

designated to have access to personal data administered by another Controller (authority/institution) and vice-versa.

For this reason, in order to ensure compliance with the principle of lawfulness of processing, defined under letter “a”, paragraph 1, article 5 of the Law “On the Protection of Personal Data” and, therefore, to prevent possible security breaches and data confidentiality as a result of possible excessive processing (exceeding the purpose), as required by the provisions of articles 27 and 28 of this law, as well as Instruction no. 47 of the Commissioner, it is imperative that Controllers take concrete measures (i) to ensure the traceability of access to data, as well as (ii) to determine the access level in accordance with the legal provisions that authorize it - in full alignment with the scope and purpose of the activity of the Controller (authority/institution) who is granted such access.

As above, the Commissioner's Office advises the Controllers to take immediate initiatives to first identify all the processing processes and then adapt the existing regulations or draft internal regulations that foresee concrete technical organizational measures in reference and implementation of article 27 and 28 of the Law “On the Protection of Personal Data”, and by-laws approved by the Commissioner's Office in various sectors.

In this context, a more serious commitment from such institutions is necessary in terms of training employees who have access to personal data and supervise processing, as well as in terms of consolidating practices and specific legislation that regulates their activity.

Furthermore, it remains a task for the Controllers to consider and respect, in accordance with the provisions of letter “a”, paragraph 1, article 31 of the Law “On the Protection of Personal Data”, the fiscal responsibility of the Commissioner's Office for providing opinions related to draft laws and by-laws on personal data, as well as in particular on projects that are planned, undertaken and/or required to be implemented by the Controllers (either alone or in cooperation with others). We emphasize that in the recent past there have been cases of projects implemented by central institutions which exercise vital functions for the state (such as budget management and public finance management), and result in violation of the provisions of the legislation in force for protection of personal data.

In addition to that, of fundamental importance is the need to modernize the infrastructure and regulatory acts related to the systems and Databases.

In this context, the Commissioner's Office deems that continuous efforts are needed in terms of guaranteeing the technical and organizational security of data, as well as the creation, maintenance and administration of ISMS in accordance with the binding provisions of Instruction no. 47 of the Commissioner.

Most of the Controllers have not implemented the necessary mechanisms for the controls and monitoring of ICT activities in order to develop, operate, manage and maintain them.

The audit findings indicate that there are difficulties in managing information technology resources. The ICT activity management is not sufficiently based on appropriate policies, procedures and operational processes for information security.

The absence of a strategy or plan for the implementation of the ISMS that includes all the components of a complete system for managing information security in accordance with the provisions of the above-mentioned guidelines was found.

In addition to the lack of a strategy for the ISMS which consists of its implementation, monitoring and continuous improvement, there is a lack of an independent structure to perform this function. This role is important to monitor, on a regular basis, the ISMS effectiveness, analyze the progress achieved and propose further improvements.

Continuous improvement is a key aspect of the ISMS in the effort to achieve and maintain the confidentiality, integrity, availability and reliability of information security and should be an integrated part of public Controllers' objectives.

In particular, with regards to ISMS, the Commissioner's Office recommends the following:

(i) Drafting of the ISMS strategy based on the principles of ICT security (confidentiality, integrity, availability, reliability) according to the ISO/IEC 27001 standard;

(ii) Establishment of the monitoring structures for ISMSs and continuous improvement of security objectives;

(iii) Continuous staff training on international standards (in particular ISO/IEC 27001) of information security and privacy;

(iv) Continuous design and monitoring of network security and data encryption during their transfer in all channels (*HTTPS, IPSec, TLS, PPTP, SSH*);

(v) Establishment of a complete register of ICT equipment (assets) in use, analyzing the importance of personal data that such assets store and process.

Centralization of all assets through which personal data processing and their periodic monitoring is conducted, as well as the implementation and monitoring of policies for the installation, access and updating of equipment (assets) through which personal data processing is conducted;

(vi) Implementation of policies for (physical and technical) inspections and restriction of users as per the work needs, as well as periodic system and network audit based on access matrix. Use of Multifactor Authentication (MFA) in critical structures and those containing sensitive data;

(vii) Control through regular scans of critical infrastructure;

(viii) Implementation of a plan for the continuity of information security (disaster recovery plan) and periodic testing of all its components;

(ix) Appraisal of ISMS compliance with ISO/IEC 27001 standard as per Instruction no. 48 of the Commissioner through periodic audit and the certification mechanism for such purpose.

PART 2 - Data processing in the health care sector

I. Introduction

Personal data processing in the health sector has occupied a special place in the entire activity of the Commissioner's Office for 2020.

In this context, the Commissioner's Office has paid increased attention to this sector, either at the regulatory aspect, or within the framework of its field monitoring and supervisory activity.

In terms of the regulatory point of view, the Commissioner's Office has drafted and published several acts with a binding character, as well as guidelines, related to the processing of health data.

The most important, in this aspect, is Instruction no. 49, dated 02/03/2020 "On the protection of personal health data" (hereinafter referred to as "Instruction no. 49)", which also represents an improving intervention of the Commissioner's Office in the health sector, as it abrogates the two previous applicable instructions, specifically, Instruction no. 5, dated 26/05/2010 "On the fundamental rules regarding the protection of personal data in the health care system" and Instruction no. 23, dated 20/11/2012 "On the processing of personal data in the health sector".

The purpose of this instruction, which entered into force on 05/03/2020, after its publication in the Official Gazette, is to regulate the processing of personal data related to health, aiming at the respect of the fundamental rights and freedoms of every individual, in particular, the right to privacy and personal data protection.

Instruction no. 49 is binding and applicable to all (public and private) Controllers operating in the health care system.

As noted from its publication date in the Official Gazette, Instruction no. 49 entered into force before the announcement by the Council of Ministers of the state of emergency at national level, due to the spread of the COVID-19 pandemic, which fortunately made it possible to address in advance the situation of personal data processing during the pandemic period which still continues.

Furthermore, following with special care the personal data processing activities in the health sector, inter alia, within the framework of measures to cope with and prevent the further spread of COVID-19, the Commissioner's Office has prepared and published 3 guidelines with a general character, as well as some specific ones (including here that of health), based on the provisions of the legislation in force for the protection of personal data, as well as in full harmony with the practice followed in EU countries and beyond.

The publication of the above-mentioned guidelines aimed to direct and guide the health sector Controllers in addressing as correctly as possible the obligations stemming from the legislation for the protection of personal data, as well as at the same time to eliminate as much as possible the uncertainties that arose in the context of respecting human rights in general, dealing with an unpredictable situation like the COVID-19 pandemic.

The Commissioner's Office has considered such an intervention as a priority, among other things, with the aim of orienting the law enforcement authorities, through the guidelines in question, in relation to the measures of surveillance and epidemiological investigation of COVID-19 that the latter have taken (on the basis of legislation for the prevention of infections and infectious diseases), which, of course, entail the processing of personal and sensitive (health) data of persons infected with and/or exposed to COVID-19.

As above, dictated also by the situation we are going through, as well as, especially, by the tasks assigned based on the Resolution of the Parliament, in addition to its regulatory, sensitizing and orienting commitment, the Commissioner's Office has developed a campaign of inspections in the public and private Controllers, in the health care sector, the summarized results of which are presented in this part of the Report.

II. Facts and circumstances related to supervision

Every public and private Controller in the Republic of Albania, during the exercise of its activity, is obliged to act in accordance with the provisions of the Law "On the Protection of Personal Data", as well as the by-laws issued by the Commissioner in its implementation.

The situation caused by the COVID-19 pandemic does not constitute a legal reason for the restriction and failure to respect the right of every citizen to the protection of his/her personal data and, consequently, for the failure to respect his private life, which altogether constitute a category of personal rights protected by the Constitution (Article 35).

Particularly important, in this context, is the processing of data related to citizens' health, especially data related to infection by COVID-19, as well as other diseases which, in combination with it, can seriously threaten health and/or the lives of citizens.

This information constitutes sensitive data with reference to paragraph 4, article 3 of the Law "On the Protection of Personal Data" and their processing is specifically regulated by article 7 of this law, in alignment with its articles 5 and 6.

Events such as the spread of COVID-19, which pose serious threats to the health and lives of citizens, require special control measures or contact tracing measures in a coordinated manner, to identify persons who may be infected or exposed to the risk of infection.

Furthermore, within the framework of the measures against the pandemic, the bodies engaged in the fight against it may find it mandatory or necessary to internationally transfer data to different countries and/or international organizations (such as WHO) for statistical, scientific and/or for the purposes of their more specialized analysis.

The Commissioner's Office deems that personal data processing and, in particular, those related to the health of data subjects, is extremely important for the protection of health and public interest in the situation in which the country currently finds itself.

In these conditions, in addition to gathering and storing personal data, the need for increased transmission and exchange of such data between each Controller and law enforcement institution within the framework of the measures against the COVID-19 virus is found reasonable in principle. Such processing processes, in any case, must be preceded by appropriate technical-organizational measures to ensure data security and maintain confidentiality in accordance with article 27 and 28 of the Law, as well as Instruction no. 47 of the Commissioner, which, as explained in Part I of this Report, is particularly important in this respect.

The Commissioner's Office has found, throughout this period, a growing concern in data subjects regarding the lawfulness of personal data processing, as well as for the security and their confidentiality by the health care sector operators.

This concern is found either in the context of complaints submitted by data subjects to the Commissioner's Office or in indications published in various media, related to allegations of illegal dissemination of personal data, especially health data related to infected patients with COVID-19.

In all cases, the Commissioner's Office has proceeded in a legal way, and at the same time, it has reacted publicly through the preparation and publication of 3 guidelines dedicated to the pandemic situation, as well as through press releases where it has drawn the attention of the Controllers in question to act in accordance with the legislation in force for the protection of personal data.

More specifically, for the aforementioned reasons, the Commissioner's Office, within November, has conducted a group of administrative investigations in the public and private Controllers of the sector - despite the increased risk of possible infection with COVID-19 during the administrative investigations.

For this purpose, the following subjects have been the object of investigation and supervision.

(i) ***In the public sector***

- Institute of Public Health
- Health Care Services Operator
- Tirana Local Health Care Unit
- Health Center of Specialties no. 1

(ii) ***In the private sector***

- American Hospital;
- “Intermedica Center” Clinic
- “Pegasus Med” Clinic
- “Salus” Hospital

III. Legal basis

Pursuant to the powers sanctioned under article 31 and 32 of the Law, as mentioned above, the Commissioner's Office has conducted a number of administrative inspections with the aim of supervising the Controllers' processing activities in the public and private health sectors, with an emphasis on verifying compliance with the principles and legal criteria provided under article 5, 6 and 7 of the Law, as well as verifying the technical and organizational measures to prevent the illegal dissemination of personal and sensitive data of patients in accordance with article 27 and 28 of the Law.

In this context, in addition to the aforementioned provisions of the law, the inspections are also based on the binding provisions of the legal acts issued by the Commissioner's Office in implementation of the Law, including, here, but not limited to the provisions of Instructions no. 47, 48 and 49 of the Commissioner.

Whereas, a general description of the main obligations arising from Instructions no. 47 and 48 is presented in Part I of this Report, below are summarized the main obligations arising from Instruction no. 49:

- Health data must be processed in a transparent, legal and fair manner, collected for clear, specific and legitimate purposes and must not be processed contrary to such purposes.
- Health data processing must be proportionate and necessary in relation to the intended legitimate purpose and must be carried out only based on the law or upon consent of the data subject.
- During health data processing, Controllers must take appropriate security measures that should anticipate the latest technological developments, the sensitive nature of health data and the potential risk assessment in order to prevent risks such as unauthorized access to data, destruction, loss, use, non-use, inability to access data.
- Health professionals in the various health care sectors must be subject to the rules on maintaining confidentiality.
- The Controller must inform data subjects about the processing of their health-related data regarding the identity, processing purpose, duration, category of recipient, possibility of objection and provision of conditions to exercise the rights. Information should be understandable and easily accessible.
- Health data storage term is determined in accordance with the specific legislation and the legislation for the protection of personal data.
- Data processed manually or electronically after term expiry are destroyed or anonymised so that individuals are not identified or made identifiable.
- Public and private Controllers and processors of medical records must, in accordance with data protection legislation, draft appropriate internal regulations that reflect the principles in the specific legislation.

IV. Problems identified

IV.1 Public sector

The main purpose of the inspection in the public sector was to monitor compliance with the legislation for the protection of personal data in the context of data processing of persons infected with COVID-19 and/or exposed to this virus.

Controllers, subject to inspection, process sensitive personal (health) data, manually and electronically to fulfill the duties and functions provided under Law 15/2016 "On the Prevention of Infections and Infectious Diseases", as well as in accordance with the provisions of other binding sectoral legislation.

Specifically, based on the conducted verifications, it results that, within the epidemiological investigation, the Controllers collect, among other things, data such as "name, surname, gender, age, address, telephone number, etc.", as well as perform the anonymization of first and last name on the swab sample used for COVID-19 testing, assigning a code to enable later identification of the patient.

Based on the field verifications, it results that the Controllers in question communicate the patient personal data through staff personal e-mails, as well through the "*WhatsApp*" application. Therefore, it turns out that these Controllers have formed close communication groups on "WhatsApp", in which positive cases with COVID-19 are continuously reported.

Moreover, this form of communication (WhatsApp) is also used to inform patients.

In addition, it is observed that the participation and frequency of data communication related to COVID-19 patients and/or those exposed to it, is extremely high. This has also resulted in leakage (illegal dissemination) of personal data of COVID-19 patients and/or persons exposed to it.

As an example would be a situation reported to the Commissioner's Office on the allegation of illegal dissemination of the list of COVID-19 patients in the Durrës Local Health Care Unit (LHCU). After the Commissioner's Office verifications, officially confirmed by the Durrës LHCU, it has been found that the list of infected patients with COVID-19 is transferred via *WhatsApp*, inter alia, in communications with 18 (eighteen) family physicians, etc..

As mentioned above, during the inspections conducted in the public sector, major problems were found in terms of compliance with the legislation for the protection of personal data by the Controller subject to the inspection.

Data security level is particularly problematic as a result of the lack of the necessary technical-organizational measures as provided under the provisions of the legislation in force.

Below you may find a summary of the main issues:

(i) There is a lack of clear rules for guaranteeing the protection, processing, storage and security of personal data, in order to determine the organizational and technical procedures related to measures for the protection of personal data.

Certain controllers turn out to have standard regulations regarding the processing of personal data, but insufficient and inappropriate to address the requirements of the legislation in force in the field of protection of patient personal data;

Based on article 2, Instruction no. 49, Controllers are obliged to take appropriate security measures which must anticipate the latest technological developments, the sensitive nature of health related data and potential risk assessment in order to prevent risks such as access to unauthorized access to data, destruction, loss, use, non-use, impossibility of accessing them.

As above, a complete lack of regulations regarding the access level to sensitive data (especially of COVID-19 patients) is found.

Such deficiency makes it impossible to track and investigate cases of leakage of patient lists, since, as noted above, the large number of participants in *WhatsApp* communications, as well as their high frequency, makes this impossible (as was the case of Durrës LHCU).

We clarify that determining the access levels and traceability of persons engaged in the processing of personal data that may have been distributed illegally, helps to prevent them in other cases to punish offenders, as well as to guarantee the right of personal data subjects to seek compensation from the latter (in the sense of articles 17 and 28 of the Law "On the Protection of Personal Data").

(ii) Every element of the necessary infrastructure for the establishment, maintenance and administration of ISMS for the protection of personal data, provided under Instruction no. 47, is absent.

In addition, no training has been conducted with the relevant personnel regarding compliance with the legislation in force in the field of personal data protection. Based on Instruction no. 47, this training takes place, at least, 1 (one) time a year;

(iii) There is no informing of data subjects regarding the duration of their data processing, the right to request, as the case may be, access, correction, erasure, etc., as well as any other element of mandatory informing for the Controllers based on Article 18 of the Law "On the Protection of Personal Data".

Moreover, data subjects are not provided with any information regarding the duration of their data processing, as well as regarding the destruction/erasure of data at the end of the relevant processing period;

(iv) Controllers do not have concrete arrangements in place for personal data management and confidentiality maintenance of the data subjects who use the official websites, thus not informing the data subjects who visit this site about the data processing methods, the security measures, maintenance of confidentiality, data subject rights and the Controller's obligations within the framework of privacy protection;

(v) Failure to comply with the obligation to notify and update personal data whenever different categories or quantities of it are processed, in order to enable data subjects to be informed about any processing of their personal data and, thus, to exercise the rights expressly granted by Chapter IV of the Law "On the Protection of Personal Data".

IV.2 Private Sector

The inspections conducted in the private sector have had a more general focus compared to the public sector, thus not only focusing on the processing activity within the services they offer for testing COVID-19 suspects.

Thus, the conducted inspections' goal has been to verify the compliance of these Controllers with the obligations stemming from the legislation for the protection of personal data.

In this sector, there is a greater commitment to address the general requirements of the legislation for the protection of personal data, as well as in terms of guaranteeing the respect of the personal data subject rights.

Furthermore, it is observed that Controllers in this sector are oriented towards taking technical and organizational measures to guarantee the security of personal data they process.

However, even in this sector, the measures taken in the field of data security are extremely far from the standard level imposed by Instructions no. 47, 48 and 49 of the Commissioner.

The main findings regarding the state of personal data processing in the private sector are listed below:

(i) Based on the conducted verifications, it results that the Controllers process data such as "*name, surname, gender, age, address, phone number, health data*, etc".

They inform data subjects regarding the processing of personal/sensitive data, however this information needs to be detailed to specify, among other things, in accordance with Article 18 of the Law "On the Protection of Personal Data" which personal data are mandatory to submit and which are voluntary, the purpose and methods of data processing, security measures, data subject rights and Controller obligations.

In addition, in many cases, data subjects are not informed about personal data recipients in cases of data dissemination and transfer, as well as the "Privacy Policy" on the relevant websites do not provide the necessary elements for information, pursuant to article 18 of the Law "On the Protection of Personal Data".

(ii) In many cases, it results that Controllers have not provided any term for the storage of personal/sensitive patient data that are processed, contrary to letter "d", paragraph 1, article 5 of the Law "On the Protection of Personal Data", as well as article 5 of Instruction no. 49. There are also cases of data processing (storage) exceeding the purpose of processing contrary to the principles of personal data protection sanctioned under letter "c", paragraph 1, article 5 and the legal criteria sanctioned under article 6 of the Law;

(iii) Efforts are made to regulate the delegation of personal data processing through delegation contracts provided under Article 20 of the Law "On the Protection of Personal Data" and Instruction no. 19. However, in the vast majority of cases, such binding contractual instruments only formally contain the standard obligations of the law, without concretely specifying the delegation level, processing type, duration, etc.

What is most important, there is no concrete measure or effort by these Controllers regarding the verification and assurance that the processors contracted to process the their patients' personal data (especially sensitive ones) have taken technical-organizational measures to protect the said data from any unauthorized processing, including, but not limited to, their destruction, loss, illegal dissemination or damage;

Nevertheless, there have also been cases where the processing delegation has not been conducted based on a delegation agreement according to Instruction no. 19.

(iv) Controllers have general arrangements, in writing, about personal data management and confidentiality maintenance of data subjects, but not rightfully detailed about the appropriate and applicable technical-organizational measures to guarantee the protection of personal and sensitive data, the criteria for the lawfulness of patient data processing, the measures to guarantee traceability and control of the actions of the persons/personnel who had and/or have access to such data, as well as for data disposal method when the purpose of their processing has been fulfilled;

(v) No Controller has fulfilled the obligations related to the establishment, administration and maintenance of the information security management system (ISMS) about the protection of personal data, provided under Instruction no. 47, in alignment with the standard provided under Instruction no. 48.

In addition, in most cases, the Controllers do not appear to have taken measures for the mandatory training of employees who have access to and process personal data, on the applicable legislation for the protection of personal data as per the provisions of Instruction no. 47.

V. Conclusions and Recommendations

The Commissioner's Office emphasizes that a serious and rigorous commitment from the Controllers' side in the health care sector is needed to guarantee the respect of the personal data subject rights, as well as, technical and organizational measures are immediately needed to guarantee the security and confidentiality of personal data, in accordance with Instructions no. 47, 48 and 49 of the Commissioner.

In this context, due to their capacity as large Controllers/Processors, as well as due to the nature of the activity they carry out, which requires increased technical and organizational measures to guarantee the security of personal data, the health care sector Controllers must not only create, maintain and administer ISMS in accordance with the mandatory provisions of Instruction no. 47, but they should also consider this essential issue a priority for ensuring the security of their patients' personal data.

For this purpose, the Commissioner's Office recommends the Controllers of this sector to consider undertaking self-regulatory commitments on the ISMS existence, even through the ISMS certification mechanism.

In addition, there is a general lack of knowledge in all levels of this sector regarding the obligations stemming from the legislation for the protection of personal data.

Therefore, this is not only an obligation, but, first of all, it is for the benefit of the Controllers themselves to carry out and document the continuous training of the relevant personnel (actively involved in the processing of personal data) about the principles, criteria and the obligations to be respected and fulfilled within the legislation for the protection of personal data.

Based on the findings presented in this report, in addition to the individual administrative proceedings, the Commissioner's Office will come up with a unifying sectoral recommendation to point out and guide these Controllers more concretely about the shortcomings and their obligations to address them in accordance with the provisions of the legal and sub-legal acts of the Commissioner, as well as continue their strict monitoring even in the future.