Policy for establishing a personal data protection system in the Institute for Accreditation of the Republic of North Macedonia

Basic provisions

The Policy for establishing a personal data protection system (hereinafter: **The Policy)** is the starting point and framework document in the establishing of the system for technical and organizational measures for personal data protection at the Institute for Accreditation of the Republic of North Macedonia (IARNM), (hereinafter**: IARNM or Controller).**

The Policy is a document that sets the principles and guidelines for achieving confidentiality, integrity and availability of personal data in accordance with the Law on Personal Data Protection (hereinafter: The Law) as well as the relevant bylaws, i.e. Rulebooks and other positive legislation of the sector (Law on Accreditation).

In order to achieve its goals, the IARNM implements procedures, guidelines and standards in accordance with the assessment of the level of risks in the processing of personal data.

IARNM as a Controller, and through a continuous system for monitoring the risks in the operation proposes measures for updating this Policy and the appropriate procedures and guidelines in order to increase the level of security or reduce threats to personal data security and integrity, confidentiality and availability of the personal data.

Any information such as personal data relating to an identified natural person or an identifiable natural person (personal data subject) needs to be adequately protected, regardless of the form or means through which it is transmitted or stored. Therefore, the scope of application of this Policy is in all processes and organizational parts of the IARNM.

Application

The provisions of this Policy shall apply to:

- fully and partially automated processing of personal data;
- other processing of the personal data that are part of an existing collection of personal data or are intended to be part of a collection of personal data.

Definitions

- **Personal data** means any information relating to an identified natural person or an identifiable natural person (personal data subject), and an identifiable natural person is a person whose identity can be established directly or indirectly, separately on the basis of an identifier such as name and surname, personal identification number of the citizen, location information,

online identifier, or on the basis of one or more characteristics specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- **Information** means a basic tool that should be adequately protected regardless of the form (written, spoken, printed or electronic);
- **Information System Security** is defined as the provision of the following basic principles:
  - **Confidentiality**: The information is available only to those who have authorized access to it;
  - **Integrity**: Protection of the accuracy and consistency of information and processing methods;
  - **Availability:** The authorized users have access to the data and the relevant IT systems, when there is a business need for it;
  - **Credibility:** Confirmation and reliability of the activities related to the access to and the use of the information;
  - **Accountability:** The responsibility for activities related to the use and the access to data is univocally established and clearly defined.
- **Information Technology - IT or Information Communication Technology - ICT**, covers information - communication assets (applications and infrastructure) which is used for collection, processing, distribution and/or storage of information in digital form;
- **Information System**, means a system of information - communication assets, human resources and processes used for collecting, processing, distribution and/or storage of information in digital form;
- **System Administrator (Information System Administrator)** means an expert in the field of information and communication, employed by the IARNM or externally engaged legal or natural person, who takes care of the functionality of the information system in terms of ensuring the integrity and security of data, the application for access to data and technical equipment that is in function of the information system, as well as for ensuring confidentiality and data protection;
- **Personal Data Protection Officer** means an authorized person from the Controller who is responsible for the implementation and coordination of the activities and the processes necessary for compliance with the Law on Personal Data Protection;
- **Personal data processing** means any operation or set of operations performed on personal data or group of personal data, automatically or otherwise, such as: collection, recording, organizing, structuring, storing, adjusting or changing, withdrawing, consulting, inspecting, using, disclosure through transmission, publication or otherwise making available, harmonizing or combining, limiting, deleting or destroying;
- **Restriction of personal data processing** means marking the personal data that are stored, in order to limit their processing in the future;
- **Profiling** means any form of automatic processing of personal data, which consists of the use of personal data for the assessment of certain personal aspects related to the natural person, and especially for the analysis or prediction of aspects related to the performance of professional duties of that natural person, his/her economic status, health, personal preferences, interests, confidentiality, behaviour, location or movement;

- **Pseudonymisation** means the processing of personal data in such a way that personal data can no longer be linked to a particular personal data subject without the use of additional information, provided that such additional information is stored separately and is subject to technical and organizational measures that will ensure that personal data are not linked to an identified natural person or an identifiable natural person;
- **Collection of personal data** means a structured set of personal data available in accordance with specific criteria, whether centralized, decentralized or distributed on a functional or geographical basis;
- **Controller** means a natural person or legal person, body of state power, state body or legal person established by the state for exercising public authority, agency or other body, which independently or together with others determines the goals and the manner of processing personal data, and when the goals and the manner of processing the personal data is determined by law, the same law determines the controller or the special criteria for its determination;
- **Personal data collection processor** means a natural person or legal person, body of state authority, state body or legal person established by the state for exercising public authority, agency or other body that processes personal data on behalf of the controller;
- **User** means a natural or legal person, body of state authority, state body or legal entity established by the state to exercise public authority, agency or other body to which personal data are disclosed, whether it is a third party or not. However, the state authorities and state bodies to which personal data are disclosed in a special investigation in accordance with the law, are not considered users, and the processing of these data by these authorities must be in accordance with the applicable rules for protection of personal data according to the purposes of that processing;
- **Third party means** any natural or legal person, body of state authority, state body or legal person established by the state to exercise public authority, agency or other body, which is not a personal data subject, controller, processor or a person, who under the direct authorization of the controller or processor is authorized to process the data;
- **Consent** of the personal data subject means any freely given, specific, informed and unambiguous stated will of the personal data subject, through a statement or clear affirmative action, clear by which he or she, signifies agreement to the processing of personal data relating to him or her;
- **Personal data breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- **Special categories of personal data** mean personal data revealing racial or ethnic origin, political views, religious or philosophical beliefs or membership in trade unions, as well as genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Organizational set-up and responsibilities

The Controller has established an appropriate organizational structure to support the Law on Personal Data Protection (LPDP) as well as the relevant Rulebooks, whereby the decisive role for their application in accordance with the Law has certainly the Personal Data Protection Officer.

The Controller has appointed an authorized person for personal data protection - as an external Personal Data Protection Officer.

IARNM as **personal data collection controller** determines the goals and the manner of processing the personal data and is responsible for harmonizing its operation with the Law on Personal Data as well as the relevant external and internal regulations arising from it.

Personal data collection processor means a natural person or legal person that processes personal data on behalf of the IARNM as a Controller. The IARNM in relation to its employees is in the capacity of a processor in accordance with the Law.

Personal Data Protection Officer (hereinafter: PDPO) and his/her deputies (if appointed) as authorized persons for personal data protection will be appointed by the Director as the sole managing body of the IARNM.

The PDPO is the key figure through which the IARNM as Controller ensures and demonstrates compliance with personal data protection regulations. In this regard, the PDPO has a strategic and independent position to achieve more efficient performance of this function and a higher degree of personal data protection. The PDPO monitors compliance with the Law and the regulations adopted on the basis of the Law regarding the processing of personal data, as well as with the internal regulations for personal data protection and the documentation of technical and organizational measures for ensuring confidentiality and protection of personal data processing.

The main responsibilities and tasks of the PDPO in the IARNM are:

- participates in the decision-making related to the processing of personal data, as well as in the realization of the rights of the personal data subjects,
- monitors the compliance with the Law and the regulations adopted on the basis of the Law regarding the processing of personal data, as well as with the internal regulations for personal data protection and the documentation for technical and organizational measures for ensuring confidentiality and protection of personal data processing.
- prepares the internal regulations for personal data protection and the necessary documentation for the organizational and technical measures for ensuring confidentiality and protection of personal data,
- coordinates the control of the procedures and instructions determined by the internal regulations which refer to the personal data,
- proposes training of the employees regarding the personal data protection
- participates in the decision-making related to the processing of personal data, as well as in the realization of the rights of the personal data subjects,
- coordinates the control of the procedures and the guidelines determined in the internal regulations for personal data protection and in the documentation for the technical and organizational measures for ensuring secrecy and protection of the personal data processing,
- coordinates the work of the Deputy Officers (if appointed),
- adopts the work program of the PDPO,
- Submits the Annual Report of the undertaken activities to the Director,
- Participates in meetings, collegiums, projects, meetings and communication where the subject of processing or discussion are the personal data, i.e. processing thereof

- participates and is a member of working groups, commissions and other bodies in the IARNM, as well as in domestic and international associations and organizations in the field of personal data protection,
- proposes participation in trainings for the officer and employees who process personal data.

- **IARNM Management as a Controller**- represented by the Director of the IARNM provides adequate organizational set-up and allocation of appropriate resources for efficient management of the protection process and compliance with the Law on Personal Data Protection.
- **Managers** - The heads of the respective organizational units and the members of the working bodies in the IARSM have responsibilities in the process of personal data protection, as follows:
  - They are responsible for the collections of personal data kept in their organizational units (Sector/Unit, or working body) if such collections are established;
  - Implementation and maintenance of controls which refer to their scope of work, and are related to the process of personal data protection;
  - They cooperate with the Personal Data Protection Officer in determining the risks and defining the measures and controls for personal data protection
  - They harmonize the processes and the internal documentation in accordance with the recommendations of the Personal Data Officer, i.e. the provisions of the Law on Personal Data Protection.
  - They inform the Personal Data Protection Officer for request and realization of public procurement in which the personal data are involved.
  - When preparing bylaws in the field of electronic communications where there would be processing of personal data they must consult and seek confirmation from the PDPO.

System of controls for personal data protection

The security of personal data is an issue that goes far beyond the simple application of appropriate technical and organizational measures. Security is a prerequisite for achieving compliance with all other principles of personal data processing.
The controller establishes a system of organizational and technical measures in accordance with the Rulebook on security of personal data processing and the Rulebook on the manner of breach of the security of personal data and other legislation in the field of personal data protection and best practices and established standards. These measures provide an adequately high level of data protection and information and data processing infrastructure, including personal data.

The security of personal data is ensured by fulfilling the following principles:

- **Confidentiality**: The data is available only to those who have authorized access to it;
- **Integrity**: Protection of the accuracy and consistency of data and processing methods;
- **Availability:** The authorized users have access to the data and the relevant IT systems, when there is a business need for it;
- **Non-repudiation:** Confirmation and non-repudiation of the activities related to the access to and the use of information;

- **Accountability:** The responsibility for activities related to the use and the access to data is univocally established and clearly defined.

The protection of personal data with the Controller is based on the following basic principles:

- Assessment of the level of risk, for which there is an appropriate Methodology for assessment of the impact of personal data protection in the IARNM,
- The IARNM as Controller in the determination and assessment of risk (risk management) shall take into account the risks associated with the processing, in particular the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of personal data;
- Appropriate documentation structure consisting of Policies, procedures, guidelines and other internal acts - which define the processes and responsibilities in the process of implementation and control of technical and organizational measures for personal data protection.
- Implementation of a system of controls which are divided into:
  - Physical controls, which serve to ensure adequate physical security of personal data and information means (servers, network devices). Examples of physical controls include the use of uninterruptible power supplies (e.g. UPS), security services, video surveillance of the Controller's facilities, sensors and alarms, and similar measures to control physical access and to protect the resources and the means used for processing, transfer and storage of personal data.
  - Technical controls are controls that are embedded in the information means, i.e. the application software, network - communication equipment and the associated devices that are used for collecting, processing, transmission and/or storage of personal data.
  - The administrative controls include the establishment of procedures and guidelines for authorizing the users (employees, third parties) who have access to the personal data and the necessary authorization to carry out their business processes.
- Application of the principle of personal data protection according to the principle by default and by design - according to this principle the Controller IARNM implements appropriate technical and organizational measures that will ensure that by default (default) processes only those personal data that are necessary to achieve on the purpose of the specific processing. This means that with the implemented measures the Controller processes only the minimum amount of personal data, in the range that is necessary to fulfil the purpose of the specific processing.

General principles for personal data processing

The protection of the personal data is one of the fundamental rights and freedoms of the citizens guaranteed by the Constitution of the Republic of North Macedonia and the European, i.e. international Conventions. This especially implies the right to privacy regarding the processing of personal data.

Pursuant to the Law on Personal Data Protection (Law on Personal Data Protection) and the European General Data Protection Regulation-GDPR, eight principles of data protection have been established as fundamental values:

- The personal data are collected and processed on a legal basis, in a transparent manner (prior information) and in compliance with the rules for processing special categories of personal data (personal data revealing racial or ethnic origin, political affiliation, religious or philosophical affiliations, membership in trade unions and data concerning health or data concerning sexual orientation).
- The personal data are processed in accordance with the law, to a sufficient extent and in a transparent manner in relation to the personal data subject ("legality, fairness and transparency"),
- The personal data are collected for specific, clear and legitimate purposes and will not be processed in a way that is not in accordance with those purposes prescribed by the Law on Electronic Communications
- The personal data are appropriate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("minimum amount of data");
- the personal data are accurate and up-to-date, and all appropriate measures will be taken for timely deletion or correction of the data that are inaccurate or incomplete, taking into account the purposes for which they were processed ("accuracy"),
- The personal data are stored in a form that allows the identification of personal data subjects, no longer than is necessary for the purposes for which personal data are processed. The personal data can be stored longer than their storage deadline if they are processed for statistical purposes, preparation of reports, fulfilment of legal obligations of the Controller, and by applying appropriate technical and organizational measures in accordance with this law, to protect the rights and freedoms of the personal data subject ("limitation of the storage period"),
- The personal data are processed in a manner that ensures an adequate level of security, including protection against unauthorized or unlawful processing, as well as their accidental loss, destruction or damage, by applying appropriate technical or organizational measures ("integrity and confidentiality").
- The personal data shall not be transferred to a country or territory outside the European Union or the European Economic Community unless that country or territory provides an adequate level of protection of the rights and freedoms of the subjects with regard to the processing of personal data.

In order to achieve these basic goals, the Controller develops and maintains a system of internal controls, in accordance with the Law on Personal Data Protection, as well as the relevant best practices and standards, as described in the Rulebook on security of personal data processing in the IARNM.

The processing of personal data in the IARNM is legal, because it is performed on the basis of the Law on Personal Data Protection, bylaws adopted by the Personal Data Protection Agency in which the provisions of appropriate departmental legislation relevant to the operation of the Controller of national and international character are implemented, fair and it takes place in a transparent manner in relation to the personal data subject.

Personal Data Protection Impact Assessment (PDPIA)

When using new technologies for some type of processing, according to the nature, scope, context and objectives of the processing, it is likely to cause a high risk to the rights and freedoms of individuals before processing is performed, IARNM as Controller performs impact assessment of the envisaged processing operations in relation to the protection of personal data. One estimate can refer to a series of similar processing operations, which pose similarly high risks. Personal Data Protection Impact Assessment as a tool defined in the Personal Data Protection Impact Assessment Methodology is used by the IARNM as a Controller in order to identify and address any problems with the processing of personal data that may occur during developing new products or services, or undertaking new activities involving the processing of personal data. The measures for protection of personal data in the IARNM are implemented on the basis of a previously conducted risk assessment.

The Personal Data Protection Impact Assessment must be performed before starting the processing of personal data using new technologies, and processing that may have a high risk for the rights and freedoms of the natural persons.

Transfer of personal data to third countries

The IARNM, in its capacity of Controller, is obliged to inform the Personal Data Protection Agency about the transfer of personal data of subjects it processes in case they are transferred to the countries of the European Union or the European Economic Community.

In case the transfer of personal data needs to be done to a country that is not a member of the European Union or the European Economic Community, i.e. the transfer takes place in third countries or international institutions or organizations, the prior consent of the Personal Data Protection Agency of personal data before the transfer itself. The request for obtaining a transfer approval is submitted 15 days before the day of starting the transfer of personal data, and the Personal Data Protection Agency submits a response within 90 days from the day of submitting the data.

In case the third country or international organization to which the personal data are to be transferred provides an appropriate degree of protection of the personal data, the IARNM in its capacity of Controller may transfer the personal data on the basis of an eligibility decision made by the Personal Data Protection Agency.

Basically, IARNM can perform the transfer of personal data to other countries when:

- the transfer is necessary for conducting a business or other activity for which the personal data subject has given explicit consent,
- protection of the life or essential interests of the personal data subject,
- others reasons determined by law, to the extent provided by the Law.

The IARNM, as the Personal Data Controller, has established rules and principles for the transfer of personal data, in accordance with the relevant legislation contained in the Rulebook for the transfer of the personal data of the IARNM.

Video surveillance

Video surveillance in the IARNM can be performed:
- in order to ensure control over the entry and exit of the official premises only for security purposes and
- for the protection of property.

The process of establishing a video surveillance system and the measures taken and the responsibilities are defined in an appropriate Rulebook on video surveillance of the IARNM. The IARNM will issue an appropriate video surveillance notification that will enable the personal data subjects to get acquainted with the set-up, the obligations and the rights related to the installed video surveillance system. Access to the relevant regulations with the necessary data can be achieved through the website and by scanning the code that is placed on the notification.

The recordings made in the process of the video surveillance recording will be kept until the reasons for their purpose determined in the bylaws are met, but, generally, no longer than 30 days, unless another law stipulates a longer period which contains protective measures and other measures for protection of the rights and freedoms of personal data subjects in accordance with the provisions of this Law.

Levels of security measures for personal data processing

Taking into account the nature, the scope, the context and the objectives of the processing, as well as the risks with different probability and seriousness for the rights and freedoms of the natural persons, the controller is obliged to apply an appropriate level of technical and organizational measures that will be proportional to the processing activities of the personal data.

The technical and the organizational measures applied by the IARNM can be classified into two levels:

- standard and

- high.

Standard level

The following levels of technical and organizational measures of standard level are applied in the IARNM:

- Physical security of servers and other equipment used for personal data processing;
- Appropriate methods for authentication and registration of users;
- Appropriate password management policies and rules;
- Securing servers and other equipment used for personal data processing;
- Automated logging out of the information system after a certain period of 15 minutes of inactivity and re-entering the username and password is necessary for reactivation of the system;

- Installed hardware/software security network barrier ("Firewall") and router between the information system and the Internet or any other form of external network, as a protection against unauthorized or malicious attempts to enter or system break-in;
- Effective and reliable anti-virus and anti-spyware information system protection, which will be constantly updated to prevent unknown and unplanned threats from new viruses and spyware;
- Effective and reliable anti-spam protection, which is constantly updated for preventive protection against spam;
- Connection of the information system (computers and servers) to the power network through a device for uninterruptible power supply;
- Provision of an appropriate separate location for storing backup copies of the personal data in a protected form;
- Provision of a disaster recovery location where the data are replicated from the servers of the primary location - IARNM in Skopje, which includes file server, e-mail server, web server, etc.;
- Process for effective detection and management of security incidents;
- Removable media management

High level

The following levels of technical and organizational measures of high level are applied in the IARNM:

- Password management - which refer to the protection and misuse of the password hashing system;
- Removable media management- by using appropriate protection methods (encryption) that ensure that data will not be readable by unauthorized persons, such as using a tool for encryption of disks on laptops;
- Information system testing - introduction of practice for regular independent and professional testing of data protection mechanisms and controls and cyber threats, such as ethical hacking;
- Transfer of personal data over an electronic communications network using appropriate encryption and protection methods.

Level of application

For all collections, the IARNM must apply technical and organizational measures that are classified at a standard level.

For the collections containing: special categories of personal data, personal data that are processed for the protection of the security and interests of the country, it is mandatory to apply technical and organizational measures that are classified at standard and high level.

For the documents that contain the personal identification number of the citizen, technical and organizational measures that are classified at standard and high level are applied obligatorily.

Legality of processing

Within the management of the personal data protection system in the IARNM as a Controller, and in accordance with its competencies and functions determined by the Law on Accreditation and other positive regulations, the following collections of personal data are established:

-Collection of personal data of employees and contractually engaged persons

-Collection of personal data of assessors and experts.

Annex 1 is an integral part of this Policy: Records of processing activities which list the conditions that determine the legality of the processing, the purposes of processing, the categories of the personal data that are subject to processing, the categories of the personal data subjects and the deadlines for storage of the personal data.

Final Provisions

The personal data protection policy is subject to regular reviews and updates in accordance with the changes in the organizational set-up, the technical infrastructure or new legal and/or regulatory requirements.

The Personal Data Protection Officer at least once a year prepares a Report to the Director of the IARNM on the compliance and adequacy of this Policy which is an integral part of the Annual Report of the PDPO.

This Policy shall enter into force and shall begin to apply on the day of its adoption.

Institute for Accreditation of
The Republic of North Macedonia

Director,
Slobodan Chokrevski, M.Sc.

Skopje, _____