REPUBLIKA E SHQIPËRISË

ENERGY REGULATORY AUTHORITY

BOARD

DECISION

No. 114, dated 19.05.2022

ON APPROVING THE REGULATION ON THE PROTECTION, PROCESSING, MAINTENANCE AND SAFETY OF PERSONAL DATA

Based on article 16, of Law no. 43/2015 "*On Power Sector*"; Law no. 988, dated 10.03.2008 "*On the Protection of Personal Data*", as amended; as well as article 16 of the "*Regulation for ERE Organization, Operation and Procedures*" approved with ERE Board Decision no. 96, dated 17.06.2016; ERE Board on their meeting dated 19.05.2022, after reviewing the report Protocol no. 668/9, dated 17.05.2022, prepared by the Legal Directory, "*On approving the Regulation on the protection, processing, maintenance and safety of personal data*",

Observed that:

- Pursuant to Law no. 9887, dated 10.03.2008 "On the Protection of Personal Data", as amended, public authorities have the obligation to provide public information, as well as the protection of personal data, according to the provisions of this law.

- Implementing the legal obligations of Law no. 9887, dated 10.03.2008, "On the protection of personal data", as amended, the Information and Data Protection Commissioner published the standard Regulation for approval by public authorities with the purpose of determining the organizational and technical procedures, the measures on the protection of personal data and safety and processing of personal data by public authorities.

- Based on articles 16 and 46 of Law no. 43/2015 "On Power Sector"; articles 20 and 41, point 1, letter "e" of Law no. 102/2015 "On Natural Gas Sector", ERE Board with decision no. 65, dated 26.03.2018, approved the "Rules on the protection of confidential information".

- Pursuant to the obligations arising from Law no. 9887, dated 10.03.2008 "On the protection of personal data", as amended, ERE adapted the standard Regulation drafted by the Information and Data Protection Commissioner (the Commissioner), maintaining the terminology and technical-organizational rules for the processing of public, sensitive and secret information, as defined in Law no. 9887/2008 and in the standard Regulation published by the Commissioner.

The regulation "On the protection, processing, maintenance and safety of personal data ", in ERE, sets out: General provisions, the object, the legal framework, the purpose, the definitions used in the regulation as well as the scope of its application based on the standard regulation of the Commissioner for approval by public authorities.

For all of the above mentioned, ERE Board,

Decided:

1. To approve the "Regulation on the protection, processing, maintenance and safety of personal data".
2. The Legal Directory is charged with issuing the necessary orders for the implementation of this regulation within 30 calendar days. The Legal Directory shall inform all organizational structures in ERE regarding ERE Board decision.

This decision enters immediately into force.

This decision is published on the Official Gazette.

ERE CHAIRMAN

Petrit AHMETI

ENERGY REGULATOR AUTHORITY

REGULATION

"ON THE PROTECTION, PROCESSING, MAINTENANCE AND SAFETY OF PERSONAL DATA"

CHAPTER I

GENERAL PROVISIONS

Article 1
Object

The object of this Regulation is to define the organizational and technical procedures, the measures for the protection of personal and safety of data, maintenance and administration of personal data from the structures of Energy Regulator Authority (as follows ERE).

Article 2
Legal basis

1. National acts:

   a. Albanian Constitution, articles 15-58;
   b. Law no. 43/2015 "On Power Sector", as amended, article 20 letter "f";
   c. Law no. 102/2015 "On Natural Gas Sector", as amended, article 20 and 41, point 1, letter "e";
   d. Law no. 9887, dated 10.03.2008, "On the Protection of Personal Data", as amended;
   e. The Orders, Instructions and the Decisions of the Commissioner for the Protection of Personal Data.
   f. Law no. 9154, dated 06.11.2003, "On the Archieves"
   g. Legal and by – legal organic acts for ERE organization and operation.
   h. Law no.119/2014 on the "Information Right".

2. International acts:

   a. Universal declaration of the human rights and freedom;
   b. Convention for the Protection of Human Rights and the Essential Freedoms, amended with Protocol no. 11, entered into force on 1 November 1998;
   c. Directives 2002/58/EC and 95/46/EC of the European Council and Parliament;
   d. Convention 108 of the European Council "On the protection of the individuals from Automatic Process of the Personal Data", ratified with Law no. 9288, dated 07.10.2004;
   e. Additional protocol of the Convention of the European Council "On the protection of individuals from the Automatic Process of the Personal Data, regarding the supervisory authorities and the cross-border movement of the Personal Data, ratified with Law no. 9287, dated 7.10.2004.

Article 3
Purpose

1. This regulation aims on defining the general principles and the organizational and technical measures for the protection, maintenance, safety and administration of the personal data and confidential information. This is applied for all the data processed by ERE in conformity with Law no. 9887, dated 10.03.2008, "On the Protection of Personal Data".

2. The process of the data shall be in conformity with the Constitution, the Law for the Protection of Personal Data, as well as the principles of Energy Regulator Authority which are transparency, non-discriminatory procedudres and the increase of competition on power and natural gas process, respecting the human rights and freedoms.

Article 4
Definitions

1. For the purpose of this Regulation, the terms shall have the meaning as follows:

   a. **"Inspector"** shall mean, or are the responsible persons from ERE which on its own or accompanied with others, in conformity with the laws and by-laws of the area, and the responses to comply with the obligations defined on Law no. 9887, dated 10.03.2008, "On the Protection of Personal Data".
   b. **"Processor"** shall mean or are ERE responsible persons, that process the data for the self – inspector.
   c. **"Receiver"** shall mean any natural, legal, public authority, agency or any other body to whom are issued the data of a third party or not.
   d. **"Entity of the data"** shall mean any natural person to whom are processed the personal data during the activity to comply with Law no. 9887, dated 10.03.2008, "On the Protection of Personal Data".
   e. **"Personal information"** shall mean any information regarding an identified/identifiable natural person. The elements with which it is realized the direct or partial identification of a person, are the identity numbers or other physical, psychological, economical, social, cultural etc other specific factors.
   f. **"Sensitive information**" shall mean any information of the personal data entity, regarding racial or ethnic origin, political thoughts, trade union membership religious or philosophical beliefs, criminal convictions, as well as data on health and sex life, etc.
   g. **"Process of personal data"** shall mean any action or group of actions, that are performed regarding the personal information, with automatic means or not, such as the collection, registration, organization, maintenance, adoption or amendment, return, consultation, utilization, transmission, distribution or otherwise, setting available, the extension or combination, photography, reflection, data input, completion, selection, block, exterioration or destruction, even if these are not registered on a data-base.

2. The other terms used to implement this Regulation, shall have the same meaning as on Law no. 9887, dated 10.03.2008 "On the Protection of Personal Data", as amended.

Article 5
Scope

This regulation shall be implemented for fully / partially personal data process, through automatic or other means that are maintained in an archieve system or aim to be part of the archieve system at ERE.

CHAPTER II
PROCESSING OF PERSONAL DATA

Article 6
Protection of personal data

Every ERE employee, that deals with the entities personal data, is obliged to implement the requirements of Articles 2 and 5 of Law no. 9887, dated 10.03.2008, "On the Protection of Personal Data", amended, as follows:

1. Respecting the principle for legal processing of personal data, respecting ang guaranteeing the essential hman rights and freedoms and especially, the right of maintaining the personal life;
2. Performance of the process in a fair and legal way;
3. Collection of personal data for specific purposes, legitimate and clearly specified and their processing regarding these purposes;
4. The data shall be processed and shall be sufficient, shall be connected with the process purpose and shall not exceed this purpose;
5. The data shall be factually accurate and when necessary, shall be updated and performance of any action to ensure that the incorrect and irregular data shall be deleted or amended;
6. The data shall be maintained in a form, that allows the identification of data entities for a period of time, but not longer than necessary for the purpose, for which they are collected or further processed.

Article 7
The processing purposes

Each ERE employee may use its personal data only to perform the obligations defined from Law no. 9887, dated 10.03.2008, "On the Protection of Personal Data" and in conformity with the legal and by-legal acts that regulate the processing approach of personal data.

Article 8
Criteria for the processing of personal data

1. ERE employees that process the personal data of the entities, shall be based on the criteria defined on Article 6 of Law no. 9887, dated 10.03.2008, "On the Protection of Personal Data".

2. The personal data are processed only to:
   a. protect the vital interests of the data entity;
   b. compliance of the legal obligation of the Inspector;

c. to perform the legal obligation with a public interest or exercising ERE competences or those of a third party, to which are shared the data;
d. to follow up the legitimate interests of the inspector, or a third party, to which are shared the data, except when these interests prevail over the interests for the fundamental rights and freedoms of the data entity.

Article 9
Processing of sensitive data

The processing of the sensitive data from any employee is performed in conformity with the criteria defined on Article 7 of Law no. 9887, dated 10.03.2008, "On the Protection of Personal Data", as amended.

Article 10
International transferring of the data

1. International transferring od the personal data from the Albanian government to the receiver the foreign state.

2. In case of performing the international personal data transferring, any ERE employee implements the provisions of Articles 8 and 9 of Law no. 9887, dated 10.03.2008, "On the Protection of Personal Data" and the by-laws issued implementing it, as well as the Instruction no..41, dated 13.6.2014 "On permitting certain categories of international transferring of personal data to a country that does not have an adequate level of personal data protection", the Instruction on international transferring of personal data as well as the Decision of the Commissioner for the Information Right and the Protection of Personal Data (KMDHP) no. 3, dated 20.ll.2012 "On defining the countries, with a sufficient level of protecting the personal data".

3. The data and information, may be communicated to homologous institutions of the other countries according to the cooperation agreement, on the condition that at the demanding country, these data and information shall be handled and maintained in conformity with the legislation for the protection of the data.

4. The data and information mentioned above, are handled only from respective authorities of the recipient country.

5. Data transferring which are "very secret" are not realized through electronic communication lines.

Article 11
Data processing with video surveillance system

1. ERE, shall proces the personal data, the images issued from the surveillance / registration cameras based on Article 6, point 1 of Law no. 9887, dated 10.03.2008, "On the Protection of Personal Data", as amended.
2. The set of the surveillance video system shall be to survey the entries and exits of people on ERE premises for the protection of people and property safety. These are the only environments that are surveilled by the surveillance – registration camera.
3. The positioning of the cameras is as such that it does not permit the registration of the images outside the environment of ERE premises, the entrance on private environments (sanitary, toilets).

4. The data collected through provided registrations, shall be used only for the investigation of an event that harms the investigator legal interests. In other cases, shall be used only for public important interest.
5. The data maintained in the surveillance system are maintained for a 2 months period and then they are deleted.

CHAPTER III
THE RIGHTS OF THE ENTITY DATA

Article 12
Implementation of the entity rights for the personal data

1. Share, or communication of personal data is performed in conformity with the purpose for which these data are collected.

2. Any person shall have the right to be informed with the personal data processed by a written request.

3. ERE, when processing the personal data or confidential information, implementing Law no. 9887, dated 10.03.2008 "On the Protection of Personal Data", as amended, shall respect these rights of the entities personal data or confidential information:
   a. the right for access;
   b. the right to require the correction or delete;
   c. automatic decision-taking;
   d. the right to object;
   e. the right to complaint;
   f. the right for damage compensation.

4. The request shall contain sufficient data to verify the identity of the applicant.

5. The inspector, within 30 days shall from receiving the request, shall inform the entity issuing the data or inform the entity the reasons for not giving the information.

Article 13
Request for information

1. The request for information may be issued:

   a. Byrom the person/entity itself;
   b. By the legal representative equipped with the respective authorization;
   c. Other persons that although they do not have direct interest, may evidence legal interest to be informed regarding these data and that are compatible with the purpose of collecting these data.

2. The response on each case shall be submitted at the address required from the applicant itself.

CHAPTER IV

SAFETY OF PERSONAL DATA

Article 14
Measures for the safety of data

1. ERE chairman through the orders and instructions shall define the structures or the authorized persons and the appropriate operational and technical measures to protect the personal data from illegal, accidental destruction, accidental loss, to protect access or the share by unauthorized persons, especially when data processing takes place on the network, as well as from any other illegal form of processing.

   The authorized persons and ERE structures shall take these specific safety measures:

   a. The chairman shall define the operations between the organizational units and the operators for using the data;
   b. The use of the data shall be on Chairman order or the order of authorized persons;
   c. The Chairman shall instruct the authorized persons, without exception, for the obligations that they have, regarding the Law on the protection of personal data and the internal regulation for the data protection, including the regulations for the safety of the data;
   d. Shall prohibit the entrance of unauthorized persons at the inspector or data processor environments;
   e. The access to the data and programs, shall be only from authorized representatives, shall be prohibited the entrance at the archieve devices and their usage from unauthorized persons;
   f. Shall register and document the modifications, corrections, deletions, transmissions and updates etc;
   g. Any time the ERE employees leave their working place, they shall close their computers, their closets, the safes and office, on which there are maintained the personal data;
   h. The employees shall not leave the office when there are unprotected data on their desk, and are at the presence of persons which are not employeed by ERE;
   i. Do not open on their computer the personal data, in the presence of an unauthorized person and especially in not public environments;
   j. They do not take out of the office, in any case, computers, laptops, flash drives or other devices that contain personal data and shall not leave them in unsafe places, without providing the delete or destruction of the data;
   k. The data shall be protected verifying the identity of the user and permiting access only to authorized individuals.
   l. The instructions to use the computer, shall be maintained in a way not to be accessible from unauthorized persons;
   m. Shall continuously perform the entry/exit procedure using personal passwords at the beginning and end of their access to the protected data, maintained on ERE data basis;
   n. The documented data shall not be used for other purposes, that are not in conformity with the collection purposes;
   o. Shall be prohibited the recognition or any data processing registered on the file for a different purpose from the right to discard or process the data. From this rule shall be excluded the case when the data shall be used for the prevention or prosecution of a criminal offence;
   p. Shall maintain the documentation of the data as long as necessary for the purpose of which is collected;
   q. The security level shall be appropriate with the nature of processing the personal data;

r. Shall respect the other legal and by – legal acts that define how shall be used the personal data.

Article 15
Protection of the environment

1. The environments on which shall be processed the personal data shall be protected by organizational, physical and technical measures to prevent the access of unauthorized persons to the environment and devices with which shall be processed the personal data. The implementation of safety measures shall be in conformity with the safety level of the administered data and information, as well as the risk level indicators that may come from the unauthorized exposure of maintained information.

2. At the environment where are processed the personal data are implemented these safety measures:

   a. It is prohibited the entrance of unauthorized persons;
   b. The persons that enter on these environments shall be equipped with the respective authorization;
   c. The entrance environments, shall be surveilled 24 hours by the cameras;
   d. Despite other protective measures and systems, are set the devices and electronic security systems (alarm systems, cameras, etc);
   e. The environments are equipped with iron closets, safe for the protection of the files from their damage, with lockers and keys and specific padlocks from those of ordinary usage ans shall be sealed with wax or plasticine;
   f. The doors shall be shielded and the windows reinforced with iron bars;
   g. Shall be provided continuous surveillance.

Article 16
Maintenance

1. At the environment of processing the protected (personal) data shall be permitted to stand:
   a. The employees of the institution, only if they are employeed on this environment or if their presence is essential to perform the work obligations;
   b. The employee of the system maintenance or of telecommunication devices is permitted to enter on these environments accompanied from the person appointed by the Director only if required from the Director/Chief Sector.

Article 17
Informing technology

ERE handles and accesses the electronic information as an internal issue. For this reason, ERE shall follow all the respective practices and procedures for the provision, maintenance and destruction of information in conformity with the effective legal provisions.

Article 18
The rights and obligations of the IT employee

1. The Information Technology employee in exercising his/her duty shall:
   a. Implement the effective legislation for personal data protection, confidentiality in communication, the human rights and freedoms;

b. Ensure the sources for using the electronic devices and electronic systems to assist the employees in completing their obligations;
c. Ensure that the configuration of all security devices is a confidential data only of the IT employee. The same rule is valid for the external and technical staff;
d. Shall take advices, including intensive trainings regarding the regulation and the use of the equipments;
e. Shall register the documentation, the modifications, corrections, deletions, transmissions, updates etc;
f. Shall set the options of the system and local computes in order the users shall not have full rights on the security softwares and antiviruses;
g. To ensure the maintenance of internet network operation and its efficiency increase, IT employee may monitor in conformity with the legal provisions:
   - the volume of Internet activity and the capacity of the system to provide its efficient operation;
   - the accessed webpages and the time spend time spent browsing them.

Article 19
Protection of electronic equipments

1. The electronic equipments to process the data and information at ERE are used only to perform the duties defined on the regulation. These devices are used only from ERE employees trained in advance for their usage. The training of the staff that deals with the automatic processing of the data shall be from the Directory of Finance and IT.

2. Regarding any error or defect on the systems/database of the institution shall be informed the system administrator, whom according to the request shall perform the respective regulation.

Article 20
Software protection

1. The programs for handling the data and information purchased or donated from different doners shall be managed by the IT Responsible Person, part of ERE structures. When the program designated for handling the data of ERE institution is established with the initiative of an ERE employee and this employee is not included on the development of the programmes organization and planning, before being included in the programme shall be approved by the ERE Secretary General and the IT responsible Person. After this approval the IT responsible person shall organize the installatio with the electronic devices.
2. For each program the IT responsible person / with the approval of the ERE Secretary General shall define:
   a. Who may delete, copy or amend it;
   b. Where shall be saved the copy of the program and who is responsible for keeping it updated.

2. The program purchased by the authorized person from ERE shall be equipped with the license for permitting ERE to install and use the planned programs for exercising ERE duties and competences.

Article 21
Passwords

1. Many applications and computer systems are password protected. For security reasons, these passwords must be changed from time to time (*every 3 months or every 6 months*). Some rules on the use and setting of passwords:

   a. The password for accessing technology and information resources (*ex. computer, etc*.) shall not be shared with other people inside or outside the organization. Employees are responsible for maintaining and not sharing this information.

   b. When setting a password, shall be a word or phrase that can be easily remembered, but not something that is easily identifiable, such as a name or address. It is recommended to use a strong password. A strong password is considered one that contains upper- and lower-case letters, numbers and punctuation characters.

Article 22
Monitoring and registration of access for the personal data

1. Access to data and information is subject to special security norms for maintaining the unachievability and for their update. The system is constructed in such a way that it verifies the user's identity. This requires the central server shall recognize each terminal operator and each user through specific programs. This system enables the continuous identification of the user at any time, on a certain terminal, workplace or other equipment for the period for which the specific data is stored.

2. Users shall familiarize themselves with the type of data in daily records and the maintenance time of these records.

3. Daily records are administered by the organizational unit of ERE general administration, responsible for data protection, which determines the daily records data content and the storage time of personal data. The maintenance period of the registration of the data or information is equal to the maintenance period of the written document containing this data or information. After this period, the data are archived or destroyed. Identification and registration of terminal operators and users is carried out using passwords for entering the database. Passwords are considered secret and personal.

4. Access to data and information shall be permitted or prevented with special electronic programs. The control and documentation of access to data and information is carried out by the persons responsible for data protection.

Article 23
Documents protection

The classified documents and other means of communication on which shall be carried the personal data, are marked with a type of secrecy and a specific level of confidentiality. The secrecy and the confidentiality level are defined in conformity with the effective normative acts.

Article 24

Secret documents

1. When there are documents that contain data considered “discreet” or “secret”, at the original document are defined the data regarding the number of copies made to the (written, printed, designed, dublicated) document and to whom these data are issued. Each copy shall have its record number.

2. If the material referred to in the preceding paragraph consists of several pages or is linked to other documents or has other component parts then each page shall be secured by a certain level of confidentiality or ensure that the pages and links are not removed or torn without a previous warning.

3. When sensitive and/or secret data are submitted on a screen, or on other media systems, the level of secrecy or confidentiality shall be indicated in each part (illustrations, pictures, previews, projections) of the presentation (submission).

Article 25
Maintenance of secret documents

1. The documents containing “discreet" or "secret" information shall be locked in technically secure iron units, or collected on a locked and sealed iron plate secured by a code, although they are directly controlled by an employee who needs relevant (certain) documents for his work.

2. The keys for these units shall be protected from the employee in close physical contact, on their places or envelopes sealed by the central office. The other keys shall be kept at the central office of the respective organizational unit directors. If one key is lost, then it shall be removed.

3. At the places where there are protected the documents refered on the above paragraph, shall enter only employees that use, protect or provide these documents.

Article 26
Document’s destruction

1. The destruction of the documents that contain sensitive data and/or “secret” data shall be from a commission, to guarantee that the confidential information shall not be disclosed and on each case shall be maintained a discretion minute.

2. The chairman shall define the commission and the way of destructing the secret documentation.

3. The commission of 3 persons shall be composed:
   a. the protocol -archieve employee;
   b. the representative from the Legal Issues Directory;
   c. the representative of the institution’s organization chart, which had or shall have access to the confidential documentation.

Article 27
Authorized person

ERE Chairman, with a secret Order, shall define the authorized employer/employee for processing the personal data or "secret" information. The order is issued in specific cases, or for a group of cases according to the nature processing needs.

Article 28
Unauthorized access to the personal or sensitive data

1. If discovering or disappear of materials containing personal or sensitive data, the person who has learned about this, is obliged to immediately inform the responsible person at ERE, and/or the chairman of ERE, who shall take the necessary measures to eliminate unfavourable consequences and to determine the circumstances that have influenced in the dislosure or disappearance of documents and confidential information.

2. The data for the disclosed documents, or their absence and the confidential information are registered in a minute.

Article 29
Dublicate of the programs

Duplicate programs with data that are used in case of natural disasters or in emergency situations or war shall be maintained in places or premises located outside the central office of the relevant organizational unit. The method of establishing, multiplying and storing these duplicates is determined separately for each document, in accordance with their maintenance and guarantee rules, established by the relevant organizational unit and with the rules applicable in the case of natural disasters.

CHAPTER V

ADMINISTRATIVE SANCTIONS

Article 30
Administrative measures

Any ERE employee who violates the duty to protect the personal data is responsible for breaking the discipline, the rules as well as the obligations on its work activity. If their actions do not constitute a criminal offence to them, shall be undertaken the administrative and disciplinary measures according to the effective normative act.

Article 31
Supervision of the measures and protection procedures

The supervision for the implementation of the rules for the protection of personal data to respect the safety norms, for the data protection authorized to their accidental or unauthorized destruction, as well as to the entrance, change and their unauthorized spread, is realized from responsible persons for the supervision and maintenance of the respective data.

CHAPTER VI
FINAL PROVISIONS

Article 32

Confidentiality of data processing

1. Any ERE employee that processes the data or is informed with the processed data shall not share the content of these data to other persons. He/she is obliged to maintain the confidentiality and reliability even after its function.

2. Any person that acts under the authority of the inspector, shall not process the personal data, to which he/she has access, without the authorization of the inspector, despite when obliged by the law

Article 33
Obligation for cooperation

ERE is aware for the obligation that they have regarding the Commissioner for the Information Right and the Protection of Personal Data and to ensure that all the information that it requires to complete the obligations, as well as the access to the computers system, archieve system, that perform the process of personal data and all of the documentation regarding their processing and transferring, for exercising the rights and obligations charged by the Law.

Article 34
Obligation for its implementation

1. All the legal acts of the Commissioner for the Information Right and for the Protection of the Personal Data are obligatory to be implemented by ERE.

2. Any employee that deals with the process of personal data is aware that the process of personal data, contrary to the requirements of Law "On the protection of personal data" shall compose an administrative offence and is punished with a fine.

Article 35
Sanctions

This regulation is part of the internal regulation and the failure to comply of its requirements shall constitute violation of the work discipline and is punished according to the effective legislation.

Article 37
Entry into force

This regulation enters into force after its publication in the Official Gazette.