ĐURO ĐAKOVIĆ
TERMOENERGETSKA
POSTROJENJA D.O.O.

Đuro Đaković Termoenergetska postrojenja d.o.o.

Dr. Mile Budaka 1
Slavonski Brod
Slavonski Brod, 24/05/2018

Title: **Data management policy**

Version: 01

Date: 24/05/2018

DATA MANAGEMENT POLICY

In accordance with the General Data Protection Regulation (GDPR EU 2016/679, hereinafter: the Regulation), the Law on the implementation of the General Data Protection Regulation (Official Gazette No. 42/2018) and other legal regulations, The Administration of Đuro Đaković Termoenergetska postrojenja d.o.o., Dr. Mile Budaka 1, Slavonski Brod (hereinafter: the Company), determines the attitude of the Company towards personal data, defines the rules, assigns responsibilities and provides full support to data management and protection of personal data. The personal data collected and processed by the Company is considered confidential information given to the Company by their subjects. This data is to be handled with special care and can be used only for the purposes for which it is collected.

COLLECTION AND PROCESSING

The collection of personal data can be conducted only in accordance with legal regulations and ethical principles. Personal data can be processed only when there is a clearly determined and documented legal basis for the processing or a basis in accordance with a contract agreement while all other types of personal data processing are permitted only with a clearly documented consent of the data subject or their power of attorney.

During the collection and processing of personal data, it is obligatory to abide by the principle according to which only the data indispensable for a specific processing can be collected. Any form of collection of unnecessary data is forbidden.

Before the collection of personal data, data subjects shall be given clear information on the purpose for which the collection is conducted, on the type of collection, type of processing in which the information in question will be used as well as on the possible third parties with access to it.

Any form of collection and processing of the information regarding a minor (16-18 years of age) will be handled with ultimate care and with the application of the highest ethical principles.

DATA SUBJECTS' RIGHTS

Data subjects shall have the right to access the information on the type of personal data that the Company has on them and the right to know for which purposes the information is used. The Company shall provide the data subjects with the possibility to correct false and to complete the incomplete personal data as well as the possibility to withhold the right to have their data processed in cases when the processing is conditioned by their consent. When a data subject withholds the right to have their information processed, they shall be informed on the possible consequences of the information being withheld, that is, on the possible deprivation of a certain right within the employment contract if the right in question is conditioned by the processing of personal data.

At the request of a data subject, personal data obtained through one's consent must be deleted (removed) from all information systems of the Company and the data systems held by third parties to which the Company allowed access.

A data subject has the right to have their data transferred. At the request of a data subject, their personal data must be delivered in electronic form.

RECORD KEEPING, SAFEKEEPING AND HANDLING

The Company is required to create and keep a register of types of personal data and types of processing conducted on the data and shall appoint a person responsible for the processing and the type of personal data collected. The person in charge is required to ensure the processing only of personal data obtained on a legal basis, through an appropriate permission or for business purposes.

When there is no legal basis for keeping certain personal data, it must be destroyed without delay. The Company is required to secure the data in an adequate manner.

Personal data can be sent to third countries only in accordance with legal regulations and if it is possible to ensure a certain level of security through appropriate legislation (Standard contractual clauses, Binding corporate rules).

INTEGRATED DATA PROTECTION

When designing information systems and arranging business processes which can in any way influence personal data security or data subjects' right to privacy, the Company shall assess their impact on data security and take appropriate measures of protection. If it is established that the measures of protection that have been implemented are not good enough, the Company shall consult the competent authority. All new processes and information systems within the Company shall be arranged in such a manner that they meet the requirements of this Policy.

MINIMIZING AND PROTECTING PERSONAL DATA

The Company shall collect and store personal data only to the extent which is necessary for the service rendered, employment contract, dispatch of workers and for the exercise of rights based on employment contract.

Data shall be stored in the smallest number of places possible and shall be adequately protected. The access to personal data can be allowed for business purposes exclusively.

It is forbidden to use personal data for development or testing of information technology systems. Whenever it is possible, personal data must be protected by encryption, pseudonymization or anonymization.

INCIDENT MANAGEMENT

The Company shall establish and maintain the procedures of action in case of an incident related to violation of personal data security both within the Company and with third parties who were allowed access to by Company or who allowed the Company to access personal data.

The Company shall establish and maintain the structure of responsibility for giving reports on incidents related to personal data security.

The Company shall design and maintain the measures intended for detection of unauthorized access to personal data or unauthorized disclosure of personal data kept in the information system.

In case of violation of personal data security, the Company shall without delay, not later than within 72 hours after the incident has been noticed, inform the competent authority. In case of unauthorized disclosure of personal data, the Company shall also inform the subjects whose data have been compromised, if that proves to be possible.

CERTIFICATION

The Company shall create and maintain a database management system in compliance with applicable standards of privacy protection and information security such as ISO 27001 whose compliance shall be proved by appropriate certification when it is possible.

EXCEPTIONS

In exceptional cases regarding personal data, the Data Protection Officer can approve a temporary action which does not comply with this Policy. The officer in charge of data security is required to keep records of such approvals, responsibilities and deadlines for the data to be adjusted and to inform the Administration about that.

RESPONSIBILITIES

All employees of the Company are required to follow the measures defined by this Policy as are all third parties who can access the data within the scope of cooperation with the Company.

The person responsible for data creation and maintenance and for the coordination of all activities regarding data management is Data Protection Officer. The officer is appointed by the Company Administration to whom they are directly responsible. The Data Protection Officer is especially responsible for the following:

- informing and counselling the data holder or the data processor as well as the employees processing personal data about their duties stated in the Regulation,
- monitoring the compliance with the Regulation and internal policies and other legislation connected with data protection,
- creating and maintaining personal data register,
- assigning responsibilities for data protection to employees and to third parties involved in the collection and the processing of personal data,
- raising awareness of and educating employees about data protection,
- implementing privacy protection into business processes and information systems,
- implementing privacy protection into audit procedures,
- counselling during the assessments of possible impacts on data protection,
- cooperating with supervisory authorities,
- monitoring the risk management process when personal data is processed,
- reporting to the Administration about the effectiveness of database management systems.

The IT Department is responsible for the formation and for the performance of technical inspections needed for the adjustment to the requirements of this Policy, especially for the following:

- identification and protection of personal data,
- mechanisms intended for the protection of data subjects' rights.

The Legal Department is responsible for the follow-up and the interpretation of regulations connected with data protection and the provision of legal support to data management system.

The Security Department is responsible for the supervision of the application of data protection measures and the provision of professional support to the data management system.

This Policy is revised at least once a year or after every change in the legal or the risk environment that might have an impact on its efficiency or application.

The follow-up on the application of the regulations stated by this Policy as well as the suggestions regarding the improvement and promotion of data protection system in the Company are duties of Data Protection Officer.

Slavonski Brod, 24/05/2018

On behalf of the Administration

Ivica Marić, CEO