WOMEN IN ENERGY ASSOCIATION

PRIVACY POLICY

2018

As a Managing Director of **Women in Energy Association** (hereinafter referred to as the 'Data Controller'), taking into account the provisions of *Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data (*hereinafter referred to as the '**GDPR**'), *the Fundamental Law of Hungary* and *Act CXII of 2011 on the right of informational self-determination and on freedom of information* (hereinafter referred to as '**Infotv**.' (the above mentioned legal provisions jointly referred to as the '**Legislation**'), hereby I set out the rules for the management and processing of personal data carried out by the organisational units of the Company in this Privacy Policy (hereafter referred to as the '**Policy**').

Section I.
General Provisions

The Purpose and Scope of the Policy

The purpose of the Policy is to determine the rights and obligations of the Data Controller and the Data Subject in the management and processing of the personal data of Data Subjects and the management of irregularities, and thereby to ensure that the requirements laid down in the Legislation are enforced.

The Data Controller is obliged to process personal data in accordance with the provisions of the Legislation, in particular, to prevent any unauthorised access to the data, unauthorised modification, transmission, disclosure, erasure or destruction of data, and to ensure, where necessary, their appropriate rectification and, upon the termination of the purpose of processing, their erasure.

The Scope of the Policy applies to the processing of personal data managed, processed by all organisational units of the Data Controller on the basis of all employee, client and partner contracts, hereinafter jointly referred to as **'Personal Data'**.

Section II.
Fundamental Concepts and Principles of Data Protection

1. Personal Data

1.1. For the purposes of this Policy the 'personal data' shall mean any information relating to an identified or identifiable natural person hereinafter referred to as the **'Data Subject'**); an identifiable natural person is one who can be identified, directly or indirectly, in particular, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

1.2. Personal data mean identifying and descriptive data.

1.2.1 Natural or artificial **identifying data** serve personalisation of the person concerned Natural identifying data are, in particular, the name, the mother's name, the place and date of birth, and the home address or the residential address of the data subject. Artificial identifying data are generated data based on mathematical or other algorithms, in particular, the tax payer identification number, identity card number, passport number, consumer number, etc.

1.2.2 **Descriptive data** mean any other data considered relevant for data processing (such as income data, qualification data, etc.). Descriptive data that are not connected with the Data Subject (such as statistical data) are not considered as personal data.

1.3. Sensitive Data mean data that relate to the racial origin, membership of a national or ethnic minority, political opinion or party affiliation, religion or beliefs, trade union membership, health status, harmful passion, sex orientation or criminal record. The Data Controller does not process any sensitive data.

2. Data Management and Data Processing

2.1. **Data Processing**: any operation or set of operations which is performed on personal data, such as collection, inclusion, recording, organisation, storage, alteration, use, transfer, disclosure, alignment or combination, blocking, erasure or destruction and prevention of the data re-use. The photographing, sound or picture recording are also considered as data processing.

2.2. **Data Controller**: natural or legal person, or organisation without legal personality, who or which determines the purposes of the processing of personal data; makes and executes decisions concerning data processing (including the means used) or ensures their execution by a data processor.

2.3. **Data Processor**: a natural or legal person or organisation without legal personality, who or which processes personal data on behalf of the controller, including the mandate under the provision of the law.

2.4. **Data processing**: the completion of technical tasks related to data management operations, regardless of the techniques and means used to carry out the operations, as well as of the place of application.

2.5. **Data Transfer:** the disclosure of data to a specific third party.

2.6. **Disclosure:** making any data accessible to anyone.

3. Purpose Limitation and Proportionality of Data Processing

3.1. Personal data can be processed only for a specific purpose, for the exercise of the right and the fulfillment of the obligation, to the extent and for such time as is necessary to attain it. If the purpose of data processing no longer exists or the processing of data is otherwise illegal, the data must be erased.

The processing and erasure of personal data recorded by the Data Controller are governed by the ***Information Security Procedure*** included in **Annex 4**. The erasure obligation with the statutory deadlines relates to data that have a statutory retention period, in particular, with regard to the length of time limitation of claims.

3.2. **Erasure**: making the data unidentifiable so that they cannot be restored at all. The facts related to the erasure or destruction of data shall be recorded.

4. Data Subject

4.1. Within the meaning of this Policy, Data Subjects are the following:
- Data Controller's employees!
- all natural persons acting on behalf of individuals and legal entities from whom the Data Controller purchases services, or who establish a contractual relationship with the Data Controller as agents, contractors, sponsors or suppliers (hereinafter referred to as the 'Partner').

4.2. Consent of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action (hereinafter referred to as the '**Statement**'), signifies agreement to the processing of personal data relating to him or her.

5. Filing System

Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

6. Personal Data Breach

A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed.

7. Third Party

A natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, data processor and persons who, under the direct authority of the data controller or processor, are authorised to process personal data. For this Policy, third parties are natural or legal persons other than the Data Subject and the Data Controller.

Section III.
Principles Relating to Processing of Personal Data

- Lawfulness, fairness, and transparency;
- Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);

- Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);
- Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy);
- Data shall be kept in a form which permits identification of the Data Subject for no longer than is necessary for the purposes for which the personal data are processed (storage limitation);
- Data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

Section IV
Data Processing

1. Rules for Data Processing

1.1. Personal data can be processed at the Data Controller if

a) the Data Subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the Data Subject is a party or to take steps at the request of the Data Subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the Data Controller is subject;

(f) processing is necessary for the legitimate interests pursued by the Data Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

1.2. The Data Subject shall be informed of the data processing through this privacy policy posted at the data Controller's website and, in case of a Partner Data Subject, by making available the ***Information on Privacy Rules*** according to ***Annex 2***.

1.3. At the Data Controller, only those persons are authorised to manage and process personal data for whom the management and processing of personal data are strictly necessary for the legal performance of their duties and their work. Employees engaged in data processing at the organisational units of the Data Controller are subject to confidentiality obligation in respect of the personal data they have access to. The detailed rules for processing the data and the penalties for violating them are contained in the Privacy Policy of the Data Controller.

1.4. Personal data that may be processed by the Data Controller for Partners, in the case of natural persons, include the name and, if necessary, a telephone number and an e-mail address, however, depending on the content of the relevant contract or service, other personal data may also be processed in accordance with the purpose limitation and data minimisation principle.

2. Records of Data Processing

2.1. Data processing carried out at the Data Controller takes place in the Data Controller's IT and other systems.

2.2. Where two or more Data Controllers jointly determine the purposes and means of processing, they shall be considered as joint controllers. The joint controllers shall in a transparent manner determine their respective responsibilities, in particular as regards their duties in connection with the exercising of the rights of the Data Subject, by means of an arrangement between them. The arrangement may designate a contact point for Data Subject. The arrangement shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the Data Subject. The essence of the arrangement shall be made available to the Data Subject. Irrespective of the terms of the arrangement, the Data Subject may exercise his or her rights in respect of and against each of the data controllers.

3. Rights of Data Subjects

3.1. The Data Subject may request information from the responsible administrator of the Data Controller about the processing of his or her personal data, such as his or her data managed by the Data Controller or processed by the Processor mandated by the Data Controller, the purpose, legal basis, duration of the data processing, activity of the Processor contiguous to data management, and who and for what purpose are receiving or have received the data. The Data Controller shall provide the requested information free of charge as soon as possible after the submission of the request, but at the latest within 30 days in writing, in a clearly understandable form.

3.2. In the event of refusal to give information, the Data Controller shall inform the Data Subject in writing under which provision of Infotv. the refusal is made. In the event of denial of information, the Data Controller shall inform the Data Subject about the possibility applying for a judicial remedy and to the National Authority for Data Protection and Freedom of Information (hereinafter referred to as the '**Authority**'). The Data Controller shall annually notify the Authority of any refused requests until 31 January of the year following the reference year.

3.2.1. In the event of a data change or incorrect recording of data, the Data Subject may request rectification of his or her processed data. Wrong data must be rectified by the Data Controller within 15 working days.

3.2.2. Except for statutory data processing, the Data Subject may request the erasure of his or her processed data without reasoning. The erasure must be completed immediately. The Data Controller may block personal data instead of erasing if so requested by the Data Subject, or if based on the information available it can be assumed that erasure could affect the legitimate interests of the Data Subject. Personal data blocked this way can only be processed as long as the purpose of data processing which prevented their erasure persists.

3.3. In the event of violation of his or her rights with regard to data processing, the Data Subject shall be able to lodge a complaint to the head of the relevant department or the Data Controller's executive director. In case of doubt, the Data Controller's executive director shall decide within the shortest possible time, but not later than 15 days after the submission of the complaint. If the Data Subject does not consider the decision to be satisfactory or thinks that his or her rights have been prejudiced with regard to the processing of his or her personal data, the Data Subject may contact the court within 30 days of the decision date or the last day of the deadline.

If according to the findings of the Data Controller, the Data Subject's objection is justified, it shall terminate all data processing operations, including data collection and transfer, shall erase the data and notify all those to whom any of these personal data had previously been transferred about the objection and the ensuing measures, upon which these recipients shall take measures regarding the enforcement of the objection.

3.4. The Data Controller shall not delete the data of the data subject if data processing has been prescribed by law. However, the personal data may not be transferred to the data recipient if the Data Controller agrees with the objection or if the court has found the objection justified. The Data Controller shall be liable for any damage caused to the Data Subject as a result of unlawful processing or by any breach of data security requirements. The Data Subject shall be liable for damage caused to the Data Controller by the Data Processor as well. The Data Controller shall be exempted from liability if it can prove that the damage was a result of obstacles outside the scope of data processing. No compensation shall be paid where the damage was a result of deliberate or gross negligent conduct of the Data Subject or the injured party.

3.5. Where processing is based on consent, the Data Controller shall be able to demonstrate that the Data Subject has consented to the processing of his or her personal data. If the Data Subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. The Data Subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the Data Subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

3.6. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of services, is conditional on consent to the processing of such personal data that are not necessary for the performance of that contract.

Section V.
Data Processing, Data Transfer, Combined Processing

1. Disclosures

Personal data may be disclosed to a third party by means of data transfer or disclosure.

2. Data Processing, Data Processing Contract

2.1. The Data Processor is responsible for the processing, alteration, erasure, transfer, and disclosure of personal data within the scope of its activities and within the framework set by the Data Controller.

2.2. The data processing organisation must conclude a contract in which the Data Processor agrees to process the data provided at its disposal only in order to meet the specified contractual objective, to commit itself to the confidential processing of the data, to comply with the provisions of the Legislation and to irreversibly erase the transferred data after reaching a contractual goal.

3. Combination of Data Transfer, Data Processing

3.1. Various data processing processes carried out at the Data Controller can be combined in the cases listed by the law. For protection electronically processed sets of data, the Data Controller ensures by means of an appropriate technical solution that the data stored in different records cannot be directly linked and assigned to the data subject unless permitted by law.

Both the transfer of personal data and the combination of data processing may be possible if the Data Subject has consented to it, or the data processing is required to perform a contract in which the Data Subject is one of the parties or is required to take action on the request of the Data Subject prior to the conclusion of the contract, also if the data processing is necessary for the fulfillment of the legal obligation relating to the Data Controller and if the data processing is necessary to enforce the legitimate interests of the Data Controller or Third Party, and otherwise the terms of data processing are met for each personal data.

The Data Controller shall, in the absence of any other legal basis, acquire the consent of the Data Subject in all cases to transfer his or her data for the processing.

4. Disclosure of Personal Data

Any disclosure of personal data processed by the Data Controller is prohibited unless it is ordered by law, or is expressly consented to by the Data Subject.

Section VI
Security of Personal Data

1. Data Security Regulations, Data Protection

1.1. Data security regulations and measures are designed to protect data and data carriers against corruption, damage, destruction, and unauthorised access.

1.2. The necessary measures should be taken to ensure the security of personal data whether manually processed or stored, archived and processed on the computer.

1.3. The data carriers, their movement, content, and use are governed by the ***Information Security Procedure*** included in ***Annex 4***.

Section VII
Certain Data Processing

Processing of Data Necessary for the Performance of Contracts Concluded with the Partners and Employees of the Data Controller, or for the Enforcement of the Legitimate Interests of the Data Controller or the Data Subject

1. Processing of Partners' Data

1.1. The principal purpose of processing of personal data of the natural person Partner or the representative of the legal person Partner in the partner relations of the Data Controller is to use the contract concluded with the Partner, to keep in touch in the performance of the contract, to pay off the services provided by the Partner and to enforce the performance guarantee claims.

1.2. The Data Controller's units process the Partners' data with the content shown in ***Partner Data Records*** in accordance with ***Annex 1/B***.

1.3. The processing of Partner Data Records is carried out on a computer. The Data Controller's cumulative Partner Database can be accessed by the relevant administrators via their personal computer used for working purposes. With the permission of the Managing Director of the Data Controller, the unit administrators or other rightsholders mandated by the Data Controller can only process and learn the data of their respective Partners.

2. Processing of Employee Data

2.1. Data Controller's units process the data of employees with the content shown in ***Employee Data Records*** in accordance with ***Annex 1/A***.

2.2. The personnel division also processes, based on the ***Employee Consent to Data Processing*** according to ***Annex 3,*** any data that are necessary for the purpose of completing the company signatures during the term of the employment relationship, or indispensable for the investigation and termination of occupational accidents, or entitle to some allowances, or which recording is justified and necessary on any other legal ground.

Section VIII
Control

1. Compliance with the provisions on data protection, in particular, the provisions of this Policy, is regularly monitored by the management of organisational units responsible for data management and data processing. In case of data processing incompatible (abnormal) with the provisions of this Policy, the head of the unit concerned shall immediately take action to terminate it and then prepare a report using the ***Report Template*** in accordance with ***Annex 4/A***. The Report is sent to the Managing Director of the Data Controller who decides on the necessary additional measures.

1.4. In case of infringement of the law or this Policy, the head of the unit shall immediately take action to eliminate the infringement. In the case of particularly serious misuse, the competent labour organization initiates disciplinary proceedings for liability determination.

1.5. The Managing Director of the Data Controller is entitled to have access to the processes of data processing, as well as the related records and reports, at all the organisational units of the Data Manager. The Managing Director can ask the unit leader and the staff for an oral or written explanation. The Managing Director is subject to confidentiality obligation in respect of the personal data he has access to.

1.5. In case of detection of unauthorised data management or processing, the head of the unit requests the data controller to terminate it. If necessary, he or she shall assist in restoring the lawful condition. The head of the unit is obliged to take the necessary action immediately and to inform of thin the Managing Director of the Data Controller in writing within three days. If the infringement can only be terminated by modifying the data processing process or the data protection activity, the head of the unit is required to initiate the development of appropriate modifications at the Data Controller for the violation status to be terminated as soon as possible and the data processing to be consistent with data processing and data protection goals. In case of doubt, the Managing Director of the Data Controller decides on the matter.

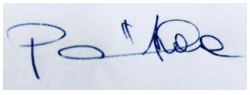
1.6. In the event that a change is made in the Legislation concerning this Policy or it is justified for any other reason, the Data Controller shall ensure that this Policy is amended accordingly.

<u>This Policy shall enter into force on 24 May 2018.</u>

Annexes:

- Annex 1/A: Employee Data Records
- Annex 1/B: Partner Data Records
- Annex 2: Information on Privacy Rules for Partner Data
- Annex 3: Employee Consent to Data Processing
- Annex 4: Information Security Procedure
- Annex 4/A Protocol on Anomalies Detected during Data Processing

Budapest, 24 May 2018.



Dr. Andrea Pánczél
Managing Director