SECURITY POLICY OF PERSONAL DATA PROCESSING

preamble:

Having regard to Regulation (EU) No. 679 of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation) and the obligations to provide guarantees, related in particular to the security, processing and transfer of personal data, WIND ENERGY SERVICE EAST EUROPE SRL (hereinafter referred to as "WESEE", a Romanian legal person, headquartered in Cluj-Napoca, 217 Calea Turzii str., ensures the security of the processed data by implementing appropriate technical and organizational measures to protect personal data, called the Security Policy of Processing Personal Data ("Security Policy")

The purpose of this Security Policy is to establish appropriate technical and organizational measures, the responsibilities of WESEE employees with personal data processing tasks and / or, where applicable, of WESEE persons empowered to fulfill their obligations to guarantee and protect rights and the fundamental freedoms of natural persons, in particular the right to intimate, family and private life, with regard to the processing of personal data.

Chapter I Principles for the processing of personal data

1.1. Correctness and legality

When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed legally and correctly.

1.2. Restriction to a particular purpose

Personal data may be processed only for the purpose defined before collecting the data and communicated to the data subject. Subsequent changes to the scope are possible only to a limited extent and require a solid foundation.

1.3. Transparency

The data subject should be informed of how his data is dealt with. In general, personal data must be collected directly from the person concerned. When data is collected, the data subject must either already know or be informed about: Data controller identity, purpose of data processing, third parties or categories of third parties to whom data may be transmitted.

1.4. Reducing data and minimizing data

Before processing personal data, you need to determine whether and to what extent processing of personal data is necessary to achieve the purpose for which it is performed. Where the goal permits and where the costs involved are proportionate to the objective, anonymous data should be used. Personal data can not be collected in advance and stored for future potential purposes, unless this is required or permitted by national law.

1.5. deleting

Personal data is not stored by WESEE for a longer period than is required. Once the legal or business process expires, it must be deleted. There may be situations in which legal interests oblige them to keep these data on pre-defined terms. In this case, the data must remain in the files until the legal obligations expire.

1.6. The accuracy and timeliness of the data

Personal data collected must be accurate, complete and, if necessary, updated. Permanent measures must be taken to ensure that inaccurate or incomplete data is deleted, corrected, supplemented or updated.

1.7. Privacy and data security

Within WESEE, personal data is considered to be confidential information and is protected by appropriate organizational and technical measures to prevent unauthorized access to, unauthorized processing, processing or distribution, accidental loss, alteration, destruction, erasure, or rectification of inaccurate or incomplete data for which they are collected and for which they will be further processed.

Chapter II Categories of data and purpose of using personal data

Personal data include name and surname identification, surname and forename of legal representatives, gender, date and place of birth, age, nationality, telephone / fax, home address / residence, e-mail address, the series and the identity / passport number, job, profession, training - diplomas - studies, banking data or the like that serve to identify you or the persons you represent or represent you.

WESEE will process data on the target person only to the extent that there is a purpose for that purpose. In working relationships, personal data can be processed if necessary to initiate, perform, and close the employment contract. When starting an employment relationship, the personal data of the applicants can be processed. When the candidate is rejected, his or her data must be deleted (according to the required retention period), unless the applicant has agreed that his or her data will remain in the file for a future selection process.

Employee personal data may be processed if a legitimate interest, legal interest (eg filing, enforcing or defending legal claims, recovering claims, etc.) is necessary.

Personal data of prospective customers, existing clients, and partners can be processed in order to conclude, execute and complete a contract. This includes consulting services for the partner if this is related to the contractual purpose.

WESEE may collect, use, process and provide your personal data for purposes such as advertising, marketing and advertising, statistics within the organization, organization of courses, seminars for its own employees or intragroup collaborators, delegations, conferences, fairs and other events, for educational purposes for the organization of professional training programs for their employees, for the issuance of any financial-accounting documents, the conclusion of contracts or other necessary documents in the WESEE activity.

Personal data are intended to be used by WESEE and are collected through the Human Resources Department and other designated persons on the grounds of European Union law and national law, which provides appropriate safeguards for the fundamental rights and interests of the data subject. Some of these data may be shared with WESEE partner companies and other WESEE partners in order to comply with their legal obligations.

If applicable, the collection and processing of personal data of minors the name and date of birth by WESEE will only be made with the explicit consent of parents employed by WESEE or other legal representatives for the purpose of granting personal deductions, , gifts, etc.

Chapter III General rules

The Security Policy sets out the technical and organizational measures implemented by WESEE to meet the confidentiality and security of processing obligations undertaken in the course of its business. Minimum security requirements include a set of technical measures,

IT, organizational, logistics and procedures to ensure a minimum level of security of processing.

In order to meet the legal requirements, WESEE has adopted appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, disclosure, unauthorized access, or any other form of illegal processing. oriented on certain directions of action:

- User authentication and authentication and type of access;
- Data collection and backup execution;
- Computers and access terminals;
- Electronic register for processing of personal data;
- Training personnel, using computers and printing.

Chapter IV Procedures

4.1. User authentication, authentication, and type of access

Computers, laptops, telephone equipment, e-mail addresses, intranet, and the internet together with internal applications are provided by the company for work-related tasks. They are a tool and a resource for the company. They can be used within the applicable legal regulations and the company's internal policies.

The user is the person acting under the authority of WESEE or the person authorized by WESEE, with a recognized right of access to personal databases.

In order to gain access to personal data, users must identify themselves by logging in to WESEE's computer systems by entering unique login data: username and password. Passwords are security strings that are appropriate in terms of length and composition, according to WESEE's IT security policy. When typing passwords, typed characters are not displayed clearly on the monitor. According to WESEE's IT security policy, passwords must be changed periodically.

WESEE has deployed a computer system that automatically refuses a user's access after three wrong password inputs. A user receiving access to the personal database is informed that he / she must maintain the confidentiality of the authentication data and respond in the same way to the operator. A procedure for administering and managing user accounts has also been implemented, with rules for granting and canceling rights and ways of accessing the user account.

Users can access only the personal data required to fulfill the service attributions assigned by WESEE, only those who have attributions in the job sheet and have signed the confidentiality agreement. For this, the types of access by functionality (administration, input, processing, rescue, etc.) and after actions on personal data (writing, reading, deleting) as well as procedures for these types of access are stable.

External service providers, personal data processing programmers have access to personal data on the basis of a confidentiality agreement strictly signed with WESEE, except where required, each operation being documented.

The IT Compartment has access to personal data to resolve incidents and problems in using computer systems.

Documents containing personal data of the type considered as special categories of data are kept in restricted access rooms and kept in cabinets and / or metal lockers provided with a locking system.

The operator has established strict ways of destroying personal data by effectively deleting the company's computers / servers in the case of electronic documents held in computer system and by the actual destruction of documents held in manual paper format.

Periodically, authenticated users are controlled by authenticated users and access types to detect malfunctions in the use of telecommunication systems, through which only the strictly necessary personal data will be transmitted.

4.2. Collect data and run backups

WESEE designates authorized users from human, operational, and IT departments for the collection, input and processing of personal data in a computer or manual system. Modification of personal data may only be made by authorized WESEE-designated users.

WESEE has taken steps to ensure that the information system records who has made the change, the date and time of the change, and maintains deleted or modified data.

Periodically, within the timeframe set by internal regulation, the IT Department performs back-up of personal databases for data recovery in the event of loss, destruction or malfunction of computer systems. The database saved by CD / DVD printing as well as by copying on USB sticks, memory cards

(backups) are stored in a safe box with restricted access, located in another room than the one in which make a backup copy.

4.3. Computers, laptops and access terminals

Computers, laptops and other access terminals are installed in lockable, lockable rooms. If the computers are open and do not act on them for 5 minutes, the session closes automatically.

Personal information databases open when unauthorized persons enter the room or approach the computer on which they are displayed are closed by users.

Servers hosting databases can only be accessed in a controlled manner based on access rights.

4.4. Electronic Register for Personal Data Processing

Any access to the personal database will be recorded in an electronic register for personal data processing in a form that the operator has established. The register shall contain the following information:

• user name / identification code;

• the name of the file you are accessing (the file);

• number of records made;

• type of access;

• the code of the executed operation or the program used;

• Date of access (year, month, day, hour, minute);

• Access time.

The operator is required to keep the Access Register for at least 3 years, constituting the test in the case of investigations. If investigations are prolonged, they will be kept until investigations and any actions related to them are completed. The register should make it possible to identify persons who have accessed personal data for no particular reason, for the purpose of applying sanctions or notifying the competent bodies.

4.5. Staff training, computer use and printing

Users who have access to their personal databases are trained on the provisions of the General Data Protection Regulation, the minimum security requirements for personal data processing, WESEE's IT security policy, and the importance of maintaining confidentiality and the risks involved in the processing of personal data.

To maintain the security of the processing of personal data (especially against computer viruses), WESEE has taken the following measures:

• Prohibiting the use by users of software that comes from unsafe sources;

• Restrict administrative rights on your computer, laptops, notebooks, and users are unable to install software without announcing the IT compartment;

• Licensed software is used;

• training users on WESEE's IT security policy and other general IT operating policies, including the threat of computer viruses;

• protecting computers, laptops with antivirus programs;

• monitor user activity and restrict access to printers; personal data will only be printed by the designated users and only for the purpose specified in these guidelines.

• Obligation for users to close their work session when leaving the workplace.

Chapter V Rights of persons whose personal data are collected and / or processed

The individuals concerned have certain established expense rights, regardless of whether the data are processed for the purpose of fulfilling a legal obligation or on the basis of the consent of the individual

5.1. The right to information

You have the right to obtain from WESEE, according to art. 13 and 14 GDPR at least the following information, unless you already have this information:

(a) the identity of the operator and his representative, if any;

b) the purpose of data processing;

c) additional information, such as: recipients or categories of data recipients; if the provision of all required data is mandatory and the consequences of the refusal to provide them; the existence of the rights provided for by this law for the data subject, in particular the right of access, data interference and opposition, and the conditions under which they may be exercised;

(d) any other information the provision of which is required by the supervisory authority's order, taking into account the specific nature of the processing.

5.2. Right of access to data

You also have the right to obtain from WESEE, according to art. art. 15 GDPR, upon request and free of charge for a request per year, confirmation that the data concerning you are processed by WESEE or not.

5.3 Right to interfere with data

At the same time, you have the right to obtain from the operator, according to art. 16 of the GDPR, upon request and free of charge, to rectify, update, block or delete data the processing of which is inconsistent with the law, in particular incomplete or inaccurate data.

5.4 Right of opposition

You have the right to oppose at any time the processing of personal data concerning you by WESEE, in accordance with art. 21 GDPR.

5.5 The right not to be subject to an individual decision

Another right you are entitled to is the right under art. 22 GDPR to request and obtain the withdrawal / cancellation / reassessment of any decision having legal effect on you, adopted solely on the basis of an automatic processing of personal data intended to evaluate some aspects of your personality, such as professional competence, credibility, behavior or other such issues, including the creation of profiles.

5.6 The Right to Appeate to Justice

At the same time, you have the right to appeal to the courts for the protection of any rights guaranteed by law that have been violated.

For the exercise of these rights, you may address us with a written, dated and signed request transmitted using the contact details indicated in Section 7 of this Security Policy.

Chapter VI Disclosure of personal data to third parties

Collected data are disclosed to third parties only if WESEE is under a legal obligation to do so. Any disclosure to third parties of other personal data will be made only with your consent to the data subject, expressed in advance.

Final provisions

If you wish to exercise your rights under the GDPR, for inquiries or questions about the Security Policy for Personal Data Processing, you may contact WESEE at the following e-mail address: data.protection@wesee.eu. com

If you believe that your rights have not been respected, you are not satisfied with the response to your request from the Data Protection Officer, or your request has not been properly and legally settled, you may contact the National Supervisory Authority of Personal Data Processing (ANSPDCP).

The present Security Policy for the Processing of Personal Data shall be supplemented with the Internal Regulation on the application of Regulation (EU) no. 679/2016 and the entire set of procedures approved by WESEE, including the WESEE IT Security Policy, and was adopted today, May 25, 2018.

ADMINISTRATOR,

[redacted]