ILMATAR GROUP
DATA PROTECTION AND INFORMATION SECURITY POLICY

ILMATAR OY, UNIONINKATU 30, 00100 HELSINKI, FINLAND
WWW.ILMATAR.FI

INDEX

1 INTRODUCTION

The primary objective of information security is to ensure the continuity of Ilmatar Energy Oy's and its subsidiaries (jointly hereinafter "Ilmatar") operations under all circumstances. Appropriate and effective information security enables the availability of ICT (Information and Communications Technology) solutions related to Ilmatar's activities, the integrity and confidentiality of data used in processes and services, under all circumstances and in all countries of operation. This policy provides the basis for ensuring the security of Ilmatar's information systems and data processing.

Data protection is a part of Ilmatar's compliance and risk management. The main objective of the Data Protection Policy is to define the principles, practices, and responsibilities for ensuring the lawful processing of personal data and a high level of data protection within Ilmatar. Data protection is closely linked to information security.

This policy describes Ilmatar's data protection and information security policy, including responsibilities and organization. This policy defines the basic requirements and provides the basis for the planning and implementation of activities under the policy. To support the implementation of the policy, more detailed guidance will also be developed in the different areas of data protection and information security.

Data protection and information security will be implemented and developed in a risk-based manner, using appropriate and cost-effective solutions. The appropriateness of the data protection and information security policy will be assessed annually by Ilmatar's Management Group.

2 DEFINITION AND OBJECTIVES OF INFORMATION SECURITY

Information security consists of responsibilities and practices related to data protection and information security, which aim to ensure that data, information systems and services are protected and secured in such a way that their confidentiality, integrity, and availability can be guaranteed and demonstrated.

- **Confidentiality**: Data, information systems and services are accessible only to those entitled to them and are not disclosed or otherwise made available to third parties without authorization.
- **Integrity**: Data, information systems and services are accurate and complete and have not been altered by intentional or unintentional technical or human intervention.
- **Availability**: Data, information systems and services are accessible, where necessary, without hindrance to those entitled to use them.

3 DEFINITION AND OBJECTIVES OF DATA PROTECTION

Data protection means the protection of privacy when processing personal data. The right to the protection of personal data is a fundamental right for everyone. This means that personal data must be processed fairly and always for a specific purpose and with the consent of the data subject or based on other legitimate grounds laid down by law. The protection of personal data also means that everyone has a guaranteed right of access to the data that has been collected about them and, where necessary, to have it amended or erased if it needs to be rectified.

Personal data are processed in accordance with the following data protection principles at all stages of the processing of personal data within Ilmatar:

- the processing of personal data is lawful, fair, and transparent for the data subject
- personal data are collected only to the extent necessary for the purposes for which they are processed
- personal data are collected and processed for specified, explicit and legitimate purposes
- personal data are processed confidentially and securely
- personal data are updated whenever necessary
- inaccurate and incorrect personal data are deleted or corrected without undue delay
- personal data are kept in a form which allows identification of data subjects for no longer than is necessary for the purposes for which the data are processed

Ilmatar privacy policy aligns with these principles and is visible to the public on Ilmatar homepage. The processing of the personal data of Ilmatar employees is detailed in specific process description that is made available for all employees.

4 DRIVERS OF DATA PROTECTION AND INFORMATION SECURITY

Ilmatar's data protection and information security is subject to and governed by general legal obligations and sector-specific specific legal obligations such as but not limited to Regulation on Wholesale Energy Market Integrity (Regulation (EU) No 1227/2011) (so called REMIT Regulation) and Regulation (EU) 543/2013) on Submission and Publication Data in Electricity Markets ((Regulation (EU) 543/2013) that regulate on the duty to publish inside information timely and efficiently and aim to guarantee that the secrecy of the information remains before publication and that no unauthorized access is enabled for such information. In addition, other guiding obligations, regulations, and guidelines, such as confidentiality agreements with suppliers. In addition, other guidelines related to data protection and information security will be followed where applicable.

The management of Ilmatar is responsible for steering the development of data protection and information security at a strategic level, together with those responsible for data protection and information security.

Ilmatar's legal department follows the applicable legislation and any changes thereto and informs the persons involved of any changes in the applicable laws regulating data protection and information security. Ilmatar's REMIT process is also frequently updated and audited.

5 IMPLEMENTING DATA PROTECTION AND INFORMATION SECURITY

5.1 RISK ASSESSMENT

Data protection and information security risks are regularly assessed and analyzed based on their business impact. Risk assessments should also be carried out during the configuration phase of new systems and when significant changes affecting business criticality occur.

5.2 DATA CLASSIFICATION AND HANDLING

Ilmatar classifies data based on its criticality and relation to insider trading regulations. Instructions and technical controls are in place to prevent misuse of such data. Data classification is the responsibility of the data owner.

5.3 HANDLING OF PERSONAL DATA

Ilmatar implements the principle of data protection by design and by default and integrates data protection principles and requirements into the processing of personal data at an early stage. Ilmatar's system and application development processes include steps to analyze the data protection requirements applicable to the purposes for which personal data are used. The applicable data protection requirements vary depending on the personal data collected and the purposes for which the data is used.

The above measures ensure that:

- only personal data that are necessary for the purpose of the processing are collected
- the data is not collected or stored in greater quantities or for longer than is necessary for the purposes for which it is processed
- personal data are not made available to an unlimited number of persons
- ensure the exercise of the rights of data subjects
- ensure the protection of personal data by appropriate security measures

In implementing data protection, Ilmatar aims to ensure compliance with the requirements of data protection legislation throughout the life cycle of the personal data processed. The technical implementation will be designed to reflect the level of risk involved in the processing. Based on the risk level, the appropriate management tools and security practices are selected to manage the risk level and achieve compliance.

Ilmatar, as controller, may outsource the processing of personal data to a contractor, a processor, for a part of the processing of personal data of its choice. Ilmatar shall only select as its contractors' processors that comply with good personal data processing practices through appropriate technical and organizational measures, meet the requirements of the GDPR (General Data Protection Regulation) and are able to ensure the exercise of the rights of the data subject. For procurements involving the processing of personal data, data protection considerations are already considered at the design stage of the procurement and included in the tender.

A written data processing agreement (DPA) is drawn up between Ilmatar and the specifically selected processor. According to the GDPR and national laws implementing the regulation, the DPA shall specify the subject matter, purpose, and duration of the processing of personal data and agree on the personal data to be processed. The content of the contract and its requirements must be defined as precisely as possible and shall be approved by Ilmatar's legel department.

5.4 DATA PROTECTION AND INFORMATION SECURITY REQUIREMENTS

Ilmatar's data protection and information security requirements are based on national, general, and industry-specific regulations, guidelines and standards governing and obliging data protection, information security, personal records, good information management and information quality. Changes in legislation and guidelines are considered in the development of Ilmatar's data protection and information security.

Ilmatar's security requirements define the minimum level of security required from contractors and other stakeholders having any access to Ilmatar data. The level of security compliance may be verified by audits where appropriate.

5.5 MAINTAINING DATA PROTECTION AND INFORMATION SECURITY SKILLS AND AWARENESS

Each employee of Ilmatar will be briefed on the location of the information security and data protection guidelines, the organization of information security and data protection, and will undergo training on information security and data protection basics in accordance with the induction policy. Ilmatar has a range of measures in place to maintain and improve employees' awareness of information security and data protection, which are implemented regularly. These include online training, simulations of fraud messages and news on intranet. In addition, targeted training is provided for selected target groups. This will be particularly emphasized in those roles where personal data are processed and data subjects' rights enforcement processes are implemented.

5.6 MONITORING AND CONTROL

Improving and maintaining the security level requires systematic and continuous automated monitoring of information systems' operation. The people who carry out the controls are bound by confidentiality obligations regarding the information they handle in their work.

The security situation is reported in the context of normal internal control and internal and external audits. Technical security is continuously assessed, and separate security audits are carried out in key environments.

Ilmatar's data protection and information security work is based on the continuous development of activities, technology, and skills in accordance with the data protection and information security management process described in the principles of continuous improvement:

PLANNING - In the planning phase, policies, principles, and plans are developed by management and security officers based on analysis and evaluation. This phase is required by legislation, risk management results, requirements (contracts, customers, and stakeholders) and operating conditions.

IMPLEMENTATION - The implementation phase is where the decisions and plans from the previous phase are implemented, communicated, and disseminated to staff, partners and customers.

MONITORING - This phase involves technical monitoring and reporting on data protection and information security and assessing whether the measures taken have resolved the identified security risks and reduced them to the planned level.

CHANGE MANAGEMENT - Change management activities are carried out in accordance with the change management process, based on the lessons learned from the monitoring phase.

5.7 DATA PROTECTION AND INFORMATION SECURITY INCIDENT HANDLING

Ilmatar's preparedness for incidents and emergencies is based on contingency planning. Together, these plans form an organizational contingency plan.

The principles of internal control and risk management of Ilmatar are approved by the Board of Directors. The principles describe the roles and responsibilities of the different actors in the ongoing process of internal control and risk management.

Ilmatar has defined an operational process and guidelines for the response to security and data protection breaches. This process will be followed in such situations.

Ilmatar, as the controller, must notify the supervisory authority of a data breach if it may pose a risk to the rights or freedoms of a natural person.

A personal data breach shall be notified to the supervisory authority without undue delay and, where possible, within 72 hours of the time when Ilmatar as controller becomes aware of the personal data breach.

A personal data breach shall be notified to the data subject if it is likely to result in a high risk to the rights and freedoms of natural persons. The data subject shall be informed without undue delay to allow him or her to protect him or herself. Notification of a personal data breach to the data subject may only be omitted in the circumstances specified in the GDPR.

5.8 SECURITY BREACHES

Data protection or information security breach is defined as an activity that is in breach of data protection and information security policies and guidelines. Ilmatar has defined procedures for dealing with breaches.

6 ORGANISATION AND RESPONSIBILITIES FOR INFORMATION SECURITY

Information security and data protection is managed and supervised by the Board of Directors of Ilmatar. The Management Board decides on the objectives, organization, resources, and powers for the development of the various aspects of overall security and Head of IT as responsible for Information Security and General Counsel as responsible for Data Protection.

The Chief Information Security Officer shall be responsible for the overall information security activities of Ilmatar within the resources and operational powers allocated to him/her by the management. He/she is also responsible for communicating security issues outside the company and within the company in general.

The Data Protection Officer is responsible for the protection and control of the personal data files of Ilmatar's customers, employees, and stakeholders.

Each information system has an owner and a person in charge. The responsibilities of the Information System Owner include defining the requirements for the operation and security of the information system (e.g., criticality, continuity planning, backup procedure) and granting and monitoring access rights.

The Head of Unit is responsible for providing guidance, information and supervision on security and data protection issues within his/her unit.

Each employee of Ilmatar, data processor, administrator of information systems or networks and user is responsible for implementing security and data protection and for complying with the guidelines. Each person is responsible for reporting threats and incidents related to information security and data protection to his or her manager, the Information Security Officer, or the Data Protection Officer.

Information security and data protection responsibilities for Ilmatar and key stakeholders and partners should be described and agreed in writing. Responsibilities should be agreed on by the people responsible for the services concerned in consultation with Operative Management Group.

Ilmatar's data protection and information security policy and any amendments thereto shall be approved by Ilmatar's Board of Directors. Individual security or data protection procedures that deviate from the policy are approved by the Data Protection Group. Information security and data protection standards and guidelines and any amendments thereto shall be approved by the Data Protection Group.

7 WHISTLEBLOWING

Ilmatar has implemented a whistleblowing channel, where you can report detected irresponsible activity or abuse. The reporting channel is intended for reporting suspected abuses related to Ilmatar. Notifications may concern, for example bribery, corruption, unfair competition, harassment, or working conditions.

Notifications are anonymous and encrypted to protect information. All notifications are treated confidentially, and it is not possible to trace the person who made the notification if he has not shared his personal information as part of the notification. The implementation of the reporting channel is based on the EU Whistleblower Directive.

Instructions for the use of electronic whistleblowing system can be found on the Ilmatar web site, under sustainability information.

ANNEX 1 - KEY CONCEPTS

Information security

Arrangements to ensure the availability, integrity, and confidentiality of information. Information security is risk management and part of corporate security.

Data protection

Data protection refers to measures designed to protect the privacy of individuals regarding the processing of personal data.

Data protection and information security policy

A management-approved vision of the goals, principles, and implementation of data protection and information security.

Information Security Planning

The planning process, including threat analysis, baseline security definition, recovery, and contingency planning, resulting in information security plans, policies, and guidelines.

Information Security

Information security activities aimed at maintaining the availability, integrity and confidentiality of documents, files, and other data media, through means such as the inventory and classification of data media and the management, handling, storage, and destruction of data media in accordance with guidelines.

Availability

The property that the information, information system or service is accessible and usable by those entitled to it at the desired time and in the required manner.

Integrity

The property that no unauthorized changes have been made to the information or message and that any changes can be verified from the audit trail.

Confidentiality

The processing of personal data in a manner that ensures appropriate security of personal data, including protection against unauthorized and unlawful processing

Personal data

Any information relating to an identified or identifiable natural person (e.g., name, personal identification number, photograph, biometric or genetic data). An identifiable person is one who can be identified, directly or indirectly, by reference to identifying information, such as name, location, online identifiers or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person.

Special categories of personal data, sensitive personal data

Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, genetic information, health information, or information concerning sexual behavior. The processing of special categories of data is subject to specific rules.

Processor of personal data

A natural or legal person, public authority, agency, or other body that processes personal data on behalf of a controller.

Processing of personal data

Any operation which is performed on personal data, whether by automatic or manual means. Processing includes, for example, the collection, recording, organization, structuring, storage, adaptation, retrieval, use, disclosure, dissemination or otherwise making available, alignment, combination, restriction, erasure, and destruction of personal data.

Breach of personal data security

A breach of data security resulting in unlawful processing of personal data. The breach results in the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored, or otherwise processed.

Obligation to demonstrate

Through accountability, an organization must be able to demonstrate that it has taken care of the following aspects of the processing of personal data:

- lawfulness, reasonableness, and transparency
- purpose limitation
- data minimization
- Accuracy, proportionality, fairness, proportionality, proportionality, fairness, proportionality, fairness, and accuracy
- limitation of retention; and
- integrity and confidentiality.

Controller

A natural or legal person, public authority, agency, or other body which, alone or in cooperation with others, determines the purposes and means of the processing of personal data.

The data subject

The person whose personal data is processed.

Data Protection Officer

A role as defined in the Data Protection Regulation to be designated by the controller and processor in situations laid down in the GDPR or voluntarily. s.

Administrative sanctions

Sanctions imposed by the supervisory authority for non-compliance with the requirements of the GDPR.

Anonymization

The removal of the identifiability of personal data so that it is no longer possible to link it to the data subject.

Pseudonymization

The processing of personal data in such a way that it can no longer be directly linked to a specific data subject without the use of additional information. Such additional data shall be kept separately and subject to technical and organizational measures to ensure that no such association with an identified or identifiable person occurs.

Impact assessment

Assessment of the impact of the envisaged personal data processing activities on data protection and individual freedoms. Where the processing is likely to present a high risk to the rights and freedoms of individuals, the controller must carry out a data protection impact assessment and identify measures to manage the risk before starting the processing operations.

ANNEX 2: AREAS OF INFORMATION SECURITY

Administrative security

Administrative security consists of management-approved policies, responsibilities, dedicated resources and risk assessment and control.

Software security

Activities on operating systems and other software, such as software identification, isolation, access control and verification procedures, monitoring and detection activities, logging procedures and quality assurance, as well as activities related to software maintenance and upgrades to improve information security.

Data security

Data security maintains the confidentiality of documents, records, and files and prevents the destruction or accidental alteration of data.

It is also essential that records are protected and properly stored.

Data security involves continuous backup, proper storage, and destruction of data.

Operational safety

Operational safety includes passwords, knowledge of the software in use and anti-malware. The access rights granted must be adapted to the job. Operational safety consists of secure use of systems, monitoring of data processing operations and ensuring continuity. Reliability of equipment is also about operational safety. A recovery plan is drawn up to ensure continuity of operations in the event of an unexpected situation.

Equipment safety

Measures relating to the availability, functionality, configuration and access control of computing and telecommunications equipment and facilities, as well as the availability of spare parts and supplies, to achieve information security.

Physical security

The protection of persons, equipment, materials, mail, premises and stores against damage and destruction. Physical security includes access and premises control, security, fire, water, electricity, ventilation and burglary prevention, and the security of couriers and consignments of data. Physical security consists of many different elements, but the foundations of security are laid at the construction stage.

Telecommunications security

Communication security aims to ensure the basic objectives of information security, i.e., the confidentiality, integrity and availability of the data transmitted over the network. A key objective is to ensure the authenticity, integrity, and confidentiality of messages. Information transport security refers to all those measures that ensure the security of information as it moves within a system or between organizations.

Personnel security

The aim of personnel security is to prevent an employee, through ignorance, lack of motivation or malicious intent, from altering or destroying information, or allowing an outsider to access it. The focus of personnel security is to avoid risks in advance and prevent them from arising.