AEREA S.p.A.

22078 TURATE (CO) ITALY · Via Cattaneo, 24

Tel. +39 02.33483.1 · Fax +39 02.33402676

AEREA SpA

Turate (CO) Via Cattaneo 24

General data protection policy

Code:	POL01
Revision:	01
Date of revision:	10.10.2024
Edited by:	Ecoconsult s.r.l.
Approved by:	AEREA SpA
Signature for approval of the legal representative of the data controller	

REVISION STATUS

Rev.	Date	Description of Changes
01	10.10.2024	Issue

Index

Purpose and scope

AEREA SpA, henceforth referred to as the "Organisation", undertakes to comply with the applicable laws and regulations concerning the protection of personal data in the countries where it operates.

This procedure defines the basic principles according to which the organisation processes the personal data of customers, suppliers, business partners, employees and other individuals, and indicates the responsibilities of its departments and employees in processing personal data.

This procedure applies to the organisation and its subsidiaries (directly or indirectly) that carry out their activities within the European Economic Area or process personal data of data subjects in that area.

The addressees of this procedure are all employees, temporary or permanent

1. Our principles

The data protection principles outline basic responsibilities for organisations that process personal data. Article 5(2) of the Regulation states that '*the data controller is responsible for compliance with these principles and must be able to demonstrate that its processing operations comply with them'.*

1.1. Lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and transparently in relation to the data subject.

1.2. Purpose limitation

Personal data must be collected for specific, explicit and legitimate purposes and not further processed in a way that is incompatible with these purposes.

1.3. Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. If possible, to reduce the risks for data subjects, the organisation must apply anonymisation or pseudonymisation to personal data.

1.4. Accuracy

Personal data must be accurate and, where necessary, kept up to date; reasonable steps must be taken to ensure that personal data that are inaccurate, in relation to the purposes for which they are processed, are deleted or rectified promptly.

1.5. Limitation of retention period

Personal data must be kept for no longer than is necessary for the purposes for which the data are processed.

1.6. Integrity and confidentiality

Considering the technology and other security measures available, the costs of implementation, and the likelihood and severity of risks to personal data, the organisation must use appropriate technical or organisational measures to process personal data in such a way as to ensure adequate security of personal data, including protection, by means of appropriate technical and organisational measures, against unauthorised or unlawful processing and accidental loss, destruction or damage.

1.7. Responsibility

The data controller is responsible for compliance with these principles and must be able to demonstrate that its processing operations comply with them.

1.8. Collection

The organisation must endeavour to collect as little personal data as possible. If personal data is collected by a third party, the controller must ensure that the personal data is collected in accordance with the law.

1.9. Use, storage and disposal

The organisation must maintain the accuracy, integrity, confidentiality and relevance of personal data according to the purpose of processing. Adequate security mechanisms must be used to protect personal data from being stolen or misused and to prevent personal data breaches. The Data Controller is responsible for compliance with the requirements listed in this section.

1.10. Disclosure to third parties

Whenever the organisation uses a third party provider or business partner to process personal data on its behalf, the Data Controller must ensure that this party provides adequate security measures to safeguard personal data in relation to the associated risks. For this purpose, a compliance questionnaire must be used.

The supplier or business partner shall process personal data only to fulfil its contractual obligations to the organisation or on the organisation's instructions and not for any other purpose. When the organisation processes personal data jointly with an independent third party, the organisation shall explicitly specify the respective responsibilities in the respective contract or in any other legally binding document, such as the supplier's Data Processing Agreement.

1.11. Cross-border transfer of personal data

Appropriate safeguards must be used before transferring personal data from the European Economic Area (EEA), including the signing of a data transfer agreement, as required by the

European Union and, if necessary, authorisation must be obtained from the data protection authority. The entity receiving the personal data must comply with the personal data processing principles set out in the Cross-Border Data Transfer Procedure.

1.12. Rights of access of data subjects

When acting as a data controller, the organisation is required to provide data subjects with a reasonable access mechanism that allows them to access their personal data and must allow them to update, correct, delete or transmit their personal data, if appropriate or required by law. The access mechanism will be further detailed in the Data Subject Access Request Procedure.

1.13. Data portability

Data subjects have the right to receive, upon request, a copy of the data they have provided, in a structured format, and to transmit such data to another data controller free of charge. the data controller is responsible for ensuring that such requests are processed within one month, are not excessive, and do not prejudice the personal data rights of other persons.

1.14. Right to be forgotten

Upon request, the data subject has the right to obtain from the organisation the deletion of his or her personal data. When the organisation acts as data controller, the data controller must take the necessary actions (including technical measures) to inform third parties who use or process that data to comply with the request.

2. Organisation and responsibility

The responsibility for ensuring proper processing of personal data rests with everyone who works within the organisation or on its behalf and has access to the personal data it processes.

The main areas of responsibility for the processing of personal data relate to the following organisational roles:

The Board of Directors or other competent decision-making body that makes decisions and approves the organisation's general data protection strategies.

The Data Protection Officer (DPO), or any other relevant employee, is responsible for the management of the data protection program and the development and promotion of end-to-end data protection procedures, as defined in the Data Protection Officer job description; Management and validity of the document.

The person responsible for the document is the data controller, who is responsible for checking it and, if necessary, updating it, at least annually.