Information Security Policy

Egon S.r.l. and Egon Data Quality SL consider the information that users entrust to them or process through the service made available to them to be a valuable asset. For this reason, the companies assume responsibility for protecting and enhancing this asset, committing to ensure that information can be used with due assurance of accuracy and completeness, and that it is adequately protected against misuse, unauthorized disclosure, and damage or loss.

This Information Security Policy therefore expresses our commitment to ensuring the security of information and of the physical, logical, and organizational tools used for processing information across all activities. It guarantees the requirements of confidentiality, integrity, and availability of the critical or sensitive information entrusted to the companies, carrying out appropriate controls to prevent breaches of these requirements.

The objectives of the information security policy are:

- To strengthen the company's image as a reliable and competent data manager;
- To protect its own information assets connected to the Egon services platform and the services associated with it;
- To gain a competitive advantage over other market players providing similar services by highlighting the value of information for the two companies;
- To avoid, as far as possible, service disruptions for users of the Egon services platform;
- To adopt measures aimed at ensuring staff retention and professionalism;
- To fully comply with the requirements of applicable and binding regulations in both Italian and Spanish territory;
- To raise the level of awareness and competence on security matters among its personnel;
- To protect information against data loss in terms of availability and integrity.

The objectives of the policy for cloud services are:

- To carry out continuous assessment of the risks inherent in privileged access by internal personnel, ensuring authorizations that are relevant to and not exceeding the scope of the activity, and tracking of activities;
- To provide, by design, the assurance of data isolation for each client through specific segregation at the logical level;
- To apply control procedures for administrative access to cloud services;
- To define specific communications to cloud service clients, notified by email with adequate advance notice, for the management of changes;
- To pay particular attention to the security of virtualization and to the access and protection of cloud service data;
- To apply procedures for managing the lifecycle of cloud service client accounts;
- To ensure that any security breaches are always reported and that the guidelines for exchanging information with the competent authorities are followed.

Milan, 11/05/2026

The Management