Integrated Quality and Information security Policy

© ESGeo
Do not duplicate without written permission

REVISION 02 – Update reference to ISO IEC 27001:2022 standard

WRITTEN BY:	date: 04/08/2025	Consultant
VERIFIED BY	date: 04/08/2025	Chiara Mantellini
APPROVED BY:	date: 04/08/2025	Fabrizio Fiocchi

Index

INTEGRATED QUALITY AND INFORMATION SECURITY POLICY 1

1. INTRODUZIONE 4
1.1. Premessa 4
1.2 Scopo 5
1.3 Area di Applicazione 5
1.4 Acronimi e abbreviazioni 5
1.5 Esclusioni 6

2. DESCRIZIONE POLITICA 6
2.1 Mission aziendale 7
2.2. La piattaforma 8
2.3 Risorse da salvaguardare 12
2.3 Obiettivi di ESGeo Srl 13
2.4 Leadership e commitment 16
2.5 Analisi dei rischi 18

3. RESPONSABILITÀ E VIOLAZIONI 19
3.1 Responsabilità 19
3.2 Violazioni 20

1. Introduction

1.1. Preface

The Integrated Management System of ESGeo Srl is developed in accordance with the following standards:

- ISO 9001:2015 - Quality Management System (QMS), which is a central element of the organization and business processes, focused on customer satisfaction
- ISO/IEC 27001: 2022 - Information Security Management System (ISMS), in order to ensure the confidentiality, integrity, and availability of the information used and managed at its Server Farm
- ISO/IEC 27017:2015 - Code of practice for security controls for cloud services based on ISO 27002
- ISO/IEC 27018:2019 - Code of practice for the protection of PII (Personally Identifiable Information) in public cloud services for cloud providers

The scope of application of the above-mentioned regulations is differentiated as follows:

SCHEMA	CAMPO DI APPLICAZIONE	SETTORE
ISO 9001	Design, planning, and provision of software services and IT solutions, including SaaS, and design and provision of training courses.	**EA33 EA37**
ISO/IEC 27001 ed estensioni	Design, planning, and delivery of software services and IT solutions, including SaaS	**EA33**

Where the EA code defines the Certification Sector:

- EA33: Information technology

- EA37: Education and training activities.

This document provides an overview of the policies adopted for the implementation of the company's Integrated Management System, with the aim of promoting its implementation and dissemination both internally and externally (publication on the website) and facilitating the achievement of its objectives.
In support of the contents of this document, the company's senior management has developed an integrated Quality and Information Security policy that sets out the principles, objectives, commitment, and leadership relating to the 9001 and 27001 integrated management system.

1.2 Scope

This policy is used as a tool to raise awareness throughout the organization of principles relating to quality, corporate information security, service management, and business continuity.

1.3 Area of Application

This policy applies, under the governance and support of Management, to all company personnel and to customers and suppliers involved in the scope of the Integrated Management System.

1.4 Acronyms and abbreviations

- **GDPR**: General Data Protection Regulation
- **RDA**: Risk Assessment Document
- **BCMS**: Business Continuity Management System
- **IMS**: Integrated Management System
- **QMS**: Quality Managment System
- **ISMS:** Information Security Managment

1.5 Exclusions

Due to the nature of its activities, the Company considers point 8.5.1 f of the UNI EN ISO 9001:2015 standard to be inapplicable and therefore excludes it from the scope of its system, as it does not carry out production processes and/or provide services whose final result cannot be verified by subsequent monitoring and measurement activities prior to delivery to the customer.

2. POLICY DESCRIPTION

This integrated company policy has been developed based on international standards that provide requirements for Quality Management Systems - ISO 9001:2015, Information Security - ISO/IEC 27001:2022, ISO/IEC 27107:2015, ISO/IEC 27018:2019,

This choice essentially corresponds to the following requirements:

- Define a system that allows for the implementation and governance of all organizational, physical, and logical measures necessary to guarantee service quality, the protection of company information, including personal data, and to ensure the security and availability of the services offered, in compliance with rules for the protection of the environment and the health and safety of personnel at work.
- Identify and include the different areas that make up an integrated management system.

The document outlines the strategic principles that ENGeo Srl intends to follow in order to achieve its objectives. These principles can be summarized as follows:

- Customer focus
- Leadership
- Active participation of people
- Process approach
- Continuous improvement
- Risk analysis
- Relationship management
- Guarantee of confidentiality, integrity, and availability of information
- Exercise of data subjects' rights in the area of privacy

- Continuity in providing products and services at predefined levels
- Sustainable environmental management
- Safeguarding the health and safety of human resources at work.

In detail, the main processes identified are:

- asset management
- human resources management, in particular organization
- communication management
- supplier management
- physical and environmental security
- operational management of IT resources
- access control
- acquisition, development, and maintenance of information systems
- design, development, control, review, production, and delivery of the product/service
- customer satisfaction
- security incident management
- business continuity management
- management of services provided
- change management
- compliance.

2.1 Mission

Founded in Milan in 2019, ESGeo is a company dedicated to managing ESG impact data governance. Founded by the Avvale group and manager Fabrizio Fiocchi, it has over 90 clients, mainly multinationals operating in various sectors. It has offices in Italy, Spain, Germany, and the United States.

ESGeo is a company that provides consulting and solutions dedicated to sustainability and supports companies in data management and reporting of direct impacts (DNF, Rating Reports, ESG Reports, ESG Ratings, impact investing, etc.) and indirect impacts

(value chain), reducing implementation times, ensuring the reliability of information, and improving the impacts generated.

2.2. The platform

Measuring and managing non-financial objectives is not only a regulatory obligation, but also a great **opportunity to enhance the value of initiatives, reduce reputational risks, and avoid sustainability-related disputes**.

ESGeo software is a SaaS (Software as a Service) application that uses the Microsoft Azure platform to deliver its services.

ESGeo is certified by the GRI Standards and is SASB inside. It also ensures alignment with the new European standards (ESRS).

ESGeo is an integrated technology solution for managing:

- the collection of qualitative and quantitative sustainability data (starter kit includes key KPIs required by the GRI Standards);
- the calculation, conversion, and consolidation of KPIs;
- the workflow and monitoring of KPIs;
- the reporting of sustainability-related content to support the preparation of the Non-Financial Statement or Sustainability Report;
- the traceability of the entire end-to-end process.

ESGeo is the main platform for integrated management of non-financial data, where KPIs are collected, processed, converted, and aggregated at every level of the organizational unit hierarchy, in order to produce the final output for the annual sustainability report. A structured workflow and intuitive interface allow for a guided process in which each user has a defined role and can perform their tasks in a user-friendly environment, compliant with internal and external audit requirements.

Thanks to the know-how developed over the years in supporting data collection and reporting processes for major groups and SMEs, we are able to offer clients a solution that enables a distinctive and tailored approach based on their specific needs.

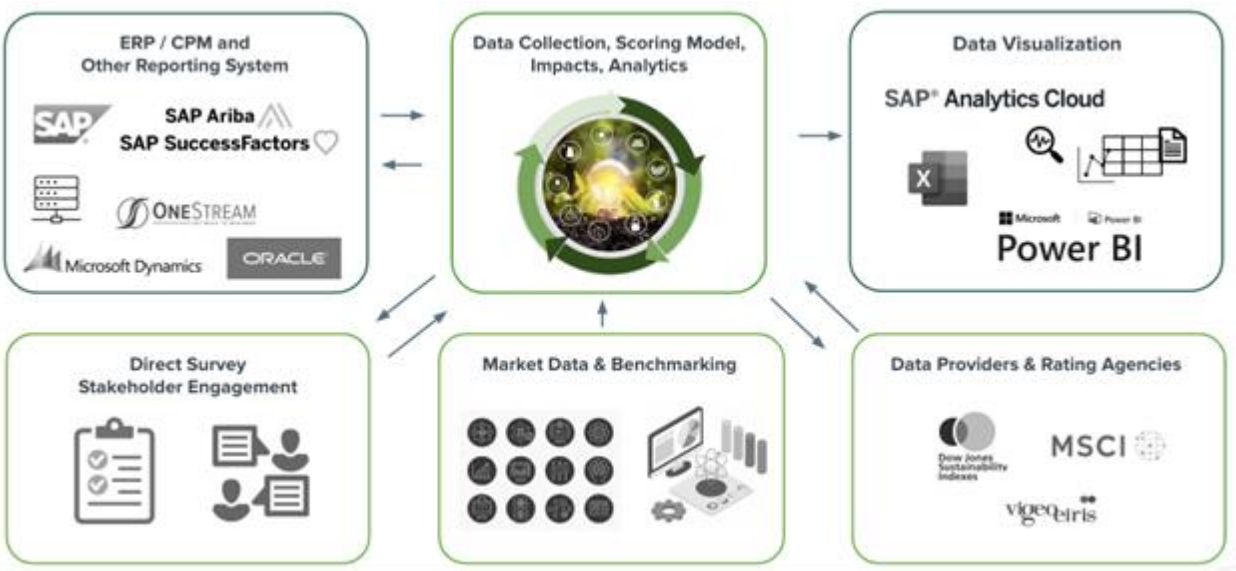
We therefore provide a consulting model based on the development of a vertical proposal that improves and simplifies the entire reporting process.

The proposed solution, based on the client's defined requirements, will be able to integrate future evolutions and/or updates from GRI Standards (or SASB), including directives issued by European regulations (new European Sustainability Reporting Standards (ESRS) developed by EFRAG under the CSRD); it complies with regulatory obligations and ESGeo best practices, covering all end-to-end functionalities of data

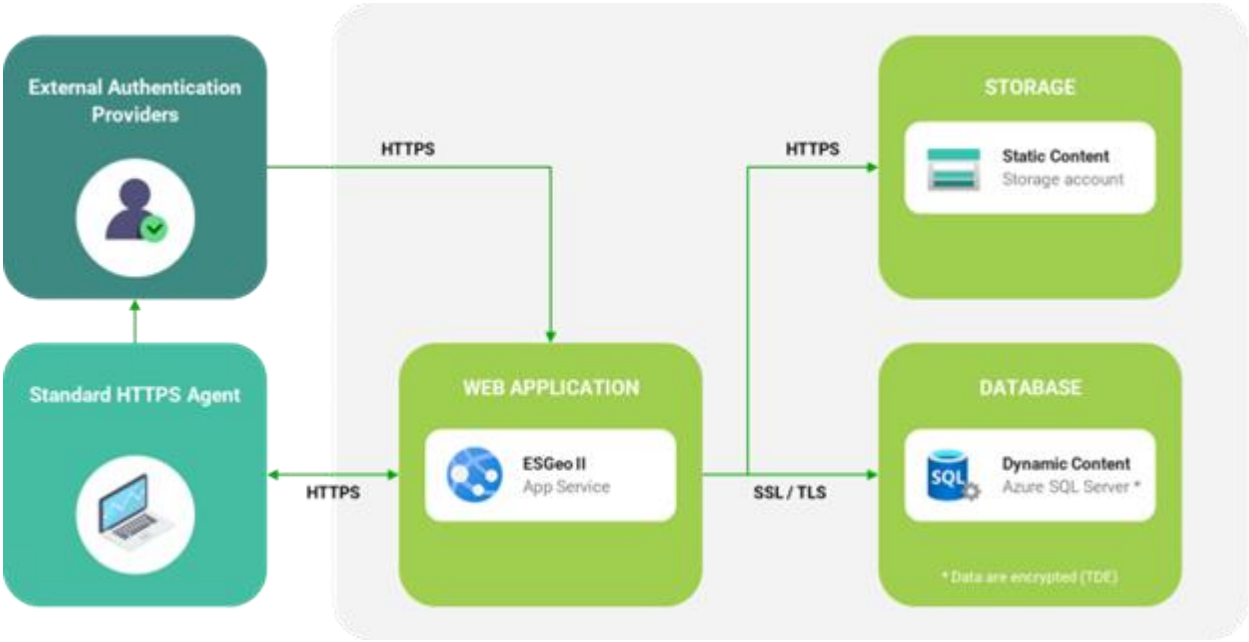
collection and reporting, and is integrable with corporate platforms and information providers.

ESGeo's architecture is designed to fully leverage the capabilities of the Microsoft Azure platform and is also equipped with an API layer to connect with various applications.

ESGeo can be integrated with major e-procurement platforms (SAP, ARIBA, JAGGAER, Ivalua, Coupa, etc.) and with information providers, as well as with other legacy systems of the client company. It can collect information from external contributors (stakeholder and supplier surveys), upload data from external providers, and is fully integrated with the Office suite and Power BI for dashboarding and reporting.



The architecture of ESGeo has been designed to make the most of the potential offered by the Microsoft Azure platform.

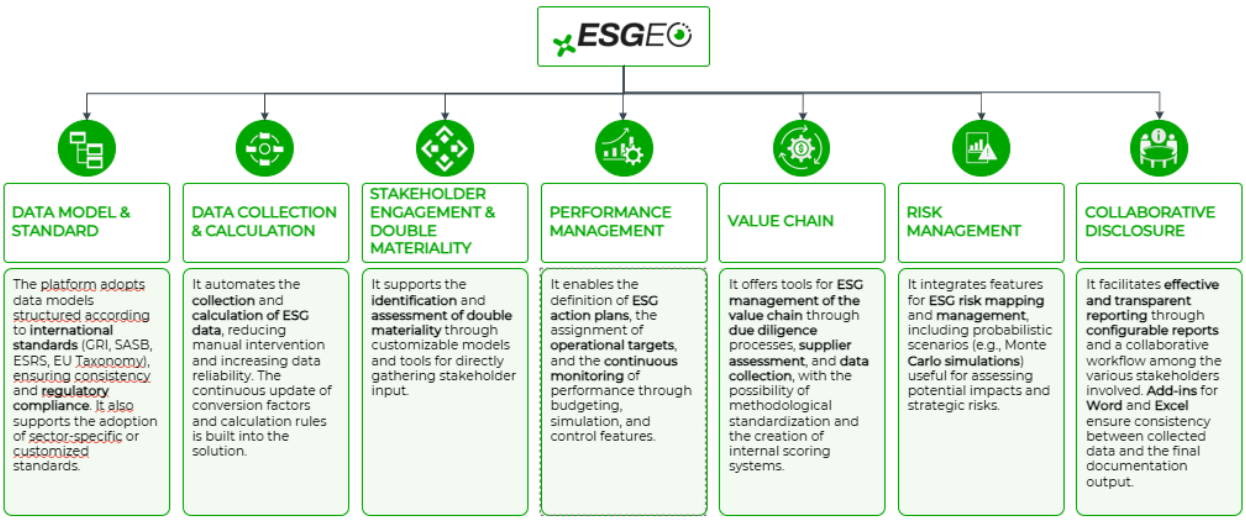


The aim of our proposal is to support the client in the process of managing and reporting non-financial data, i.e., to adopt a structured, traceable, and reconstructable workflow for the preparation of the sustainability report. In fact, to equip oneself with a Digital Governance tool for non-financial data.

- The methodological approach developed together with ESGeo will also enable the Group to achieve other important goals, which are key components and fundamental parts of such a data management process:
- Materiality assessment to prioritize the most important issues for the organization and its stakeholders and design the materiality matrix.
- Definition of ESG identity to outline a sustainability strategy aligned with the corporate vision and establish the most appropriate objectives.
- Development of a proprietary ESG scoring model to measure the company's ESG opportunities and risks, to measure corporate ESG performance across subsidiaries and managers, or to measure the impacts of external entities such as investments, loans, or suppliers.
- Transforming data into value by analyzing business results and comparing them with those of competitors.

- Supply chain analysis to guide the company in designing supply chain assessment, supply chain impact contributions (e.g., GHG Scope 3), and supplier mapping and scoring.

- Sustainability reporting to disclose environmental, social, and governance goals and progress toward achieving them, improving corporate reputation, transparency, stakeholder trust, and reducing risk.
- Communication strategy to convert communication risks into opportunities with a fully verifiable and traceable data framework.



2.3 Resources to be safeguarded

The resources that ESGeo Srl undertakes to safeguard are all those that underpin strategic processes and are carefully listed in the company's asset inventory. The main categories are:

- data/documents
- physical assets
- logical assets
- services
- personnel.

With regard to service delivery and in accordance with ISO/IEC 27001:2022 and its extensions ISO/IEC 27017:2015 and ISO/IEC 27018:2019, an annual analysis is conducted

of the risks to company assets and data processing. This analysis takes into account the strategic objectives set out in this policy, incidents that have occurred, and changes in business and technology that have taken place during the period.

2.3 Goals by ESGeo Srl

The basic principles that guide the actions of ESGeo Srl are:

- Achieving maximum customer satisfaction and that of other interested parties, such as citizens, in compliance with their expectations and needs, by providing high-quality services
- Offering an adequate level of security for the data and information processed during the management of service delivery processes, by identifying, assessing, and addressing the risks to which the services themselves may be subject
- Ensuring the protection of personal data in processing activities managed both as Data Controller and as Data Processor
- Ensuring that its services systematically comply with the SLAs (Service Level Agreements) agreed with the respective clients
- Ensuring service continuity through adequate allocation of resources to guarantee the identification and impact of potential losses, and the maintenance of recovery plans and strategies
- Providing safe and healthy workplaces, improving occupational health and safety, eliminating hazards and minimizing risks

With this policy, ESGeo Srl intends to formalize the following general objectives within the integrated management system:

- Regularly provide services that meet customer requirements and applicable mandatory and regulatory requirements
- Facilitate opportunities to increase customer satisfaction
- Address risks and opportunities associated with the context and its own objectives
- Demonstrate compliance with the requirements specified by the Integrated Management System
- Best preserve the company's image as a reliable and competent entity
- Provide full support and commitment to achieve compliance with mandatory requirements regarding personal data processing (GDPR)

- Protect its information assets so that:
    - Information is protected from unauthorized access through appropriate access policies based on security and business activity requirements
    - Information is not disclosed to unauthorized personnel due to deliberate actions or negligence
    - The integrity of information is protected and safeguarded from unauthorized modifications
    - Information support resources are adequately protected
- Ensure the protection of personal data by fulfilling the obligations set out by the General Data Protection Regulation (GDPR) and the related Italian legislation through:
    - Drafting the record of processing activities
    - Conducting data protection impact assessments, where applicable
    - Applying appropriate technical and organizational measures intended to ensure data security and guarantee accountability and compliance with the principles of privacy by design and by default, so that data is:
        - Processed lawfully, fairly, and transparently
        - Collected for specified, explicit, and legitimate purposes, and subsequently processed in a manner not incompatible with those purposes
        - Adequate, relevant, and not excessive
        - Accurate and kept up to date
        - Not retained longer than necessary
        - Processed in accordance with the rights of the data subject
        - Secure
        - Not transferred abroad without adequate protection
- Ensure business continuity so that information is available to authorized users when needed through:
- Implementation of uniformly managed and monitored information backup systems
- Drafting of service management plans, including continuity plans, constantly updated and monitored
- Drafting of business continuity plans, appropriately updated, monitored, and improved, in order to ensure the ability to respond to disastrous events, resilience, and service continuity

- Minimize damage resulting from external, internal, accidental, or intentional activities through:
- Appropriate controls for access to company information or assets by third parties
- Maintenance of the security of information and software exchanged within the company and with any external party
- Procedures for the necessary authorizations to take critical information, devices, and/or software outside the company
- Procedures for the security of devices outside the company by establishing access assignment methods
- Respond and react promptly to events that may reduce information security through:
    - Drafting procedures for timely communication and incident management in case of threats to information security, so that responsible parties and corrective actions to be taken are immediately identifiable
    - Timely communications to the appropriate parties regarding information security breaches
    - Fully comply with current and mandatory regulations.
    - Increase, within its organization, the level of awareness and competence on security issues through:
    - Updated communications and adequate training for all personnel regarding the implementation of the ISMS (Information Security Management System)
    - Detailed training programs on information security for all internal personnel and for all external personnel operating for extended periods within the company
- Provide opportunities for continuous improvement.
- Define and monitor, with regard to the provision of cloud services:
    - The methods of cloud service delivery: IaaS and PaaS
    - The management of access to services provided in cloud mode, according to ESGeo Srl's Logical Access Policy
    - Communications to customers in case of changes and to data subjects in case of data breaches, through a trouble ticketing system
    - The account lifecycle, defined in the operational notes related to services provided in cloud mode

- The inclusion in the risk analysis of additional risks arising from the provision of a cloud infrastructure: the ISO/IEC 27001 risk analysis is carried out including the assets related to cloud services
- The application of mandatory requirements derived from the European General Data Protection Regulation (GDPR)

2.4 Leadership e commitment

The senior management of ESGEo Srl, placing the ISM as a priority and strategic basis for achieving the identified general objectives, intends to demonstrate its leadership and concrete commitment.
The main actions in this regard are:

COMMITMENT	Implementation Methods
Ensure that ISM policies and objectives are properly established.	• Definition of the Integrated Management System Policy • Management review • Risk mitigation actions • Maintenance of adequate resources • Action in the event of a breach of the Integrated Management System Policies.
Ensure adequate integration of ISM processes into the organization's business processes.	• Training and awareness activities • Assignment of appropriate roles, responsibilities, and authority.
Make adequate resources available for the ISM	• Risk mitigation actions • ISM improvement plan
Communicate the importance of the effectiveness of ISMe in complying with the relevant requirements.	• Training and awareness activities.
Ensure that the ISM achieves its established objectives.	• Monitoring, measurement, and analysis of risk mitigation actions.

Lead and support staff in contributing to the effectiveness of the ISM.	• Training and awareness activities.
Promote continuous improvement.	• Training and awareness activities • ISM improvement plan
Support process managers in consolidating leadership in their relevant activities.	• Regular meetings for planning and communicating results.
Ensure that the ISM promotes and pursues full accountability.	• Compliance with legal requirements, regulations, and directives (local, national, and EU) applicable to the company, respecting all stakeholders and the needs they express during the provision of the service • Guarantee of the effectiveness and efficiency of company processes • Availability of this document to all interested parties, through appropriate internal and external communication channels • Constant monitoring and improvement of its Management Systems, defining objectives for improvement, verifying their achievement, and communicating them appropriately to all staff • Introduction and constant updating of • management and surveillance procedures for the constant monitoring of the safety of personnel, the environment, and energy performance, in order to plan appropriate interventions in the event of non-compliance, anomalies, or emergencies • Enhancing the information and training activities of all operators, ensuring their professional development as a strategic resource, making them aware of their individual obligations, the importance of

	their actions in achieving the expected results, and their responsibility in terms of the environment, social responsibility, and health and safety in the workplace • Considering customers as a fundamental element of our success, working to ensure their satisfaction, including with regard to social responsibility rules • Considering our suppliers as partners, not only for the implementation of activities but also with regard to social responsibility • Identification of risks, opportunities, and hazards arising from the performance of activities, through prior assessment of risks to personnel for existing activities and for any new activities and/or processes, in order to adopt solutions capable of preventing accidents, occupational diseases, environmental impacts, and energy waste, and to minimize, as far as possible, the occurrence and extent of such events • Conducting periodic internal audits; analyzing and monitoring any non-compliance

2.5 Risk Assessment

The Management has established and implements an approach based on the quantitative and qualitative assessment of the risks associated with the resources existing in the company, the processes and the objectives defined in the system, and the processing of personal data. This method makes it possible to determine objective values that allow the definition of the related countermeasures that must be adopted to reduce and make acceptable the value of the residual risk associated with the asset. In this sense, IT tools and deterministic methods are adopted which allow, in addition to implementing and managing the inventory of company assets, the register of personal data

processing activities, to measure the effectiveness of the application of actions and above all the replicability of the assessment, with a view to ensuring the improvement process. Furthermore, risk analysis constitutes a fundamental tool to support the organization's decisions, in order to avoid risks and seize opportunities.

Risk analyses and the related treatment plans are presented and evaluated at each Management Review in order to identify opportunities for improvement and define security measures. These security measures are intended to "counter," "prevent," "deter," "detect," "mitigate," "restore," or "correct" the threats that may affect the company's information systems. They must be implemented according to the methods described in specific operational procedures and/or operational instructions.

3. RESPONSIBILITY AND VIOLATIONS

3.1 Responsibility

This policy has been formulated by the Consultant in collaboration with the QMS and IMS Manager, who, on behalf of the Management, extends responsibility over all management systems.

It will be reviewed at least annually during each Management Review and in any case upon the occurrence of significant changes.

The persons responsible for the implementation of this policy are:

• The Management of ESGeo Srl, which establishes the acceptance criteria and the levels of risk acceptability and provides the necessary resources to ensure the correct application of the Integrated Management System processes, ensures the performance of internal audits and guarantees full support in the implementation of this policy, assigning to the various functions tasks of implementation, management and monitoring of the effectiveness and efficiency of the system, and assigns appropriate roles and responsibilities for

quality management, information security management, service management and business continuity.

• The Data Controller, in the person of the Sole Administrator, who is responsible for any processing of personal data carried out directly or by others on their behalf. In particular, they implement adequate and effective measures in order to be able to demonstrate the compliance of processing activities with the GDPR, including the effectiveness of the measures, which take into account the nature, scope, context and purposes of the processing, as well as the risk to the rights and freedoms of natural persons.

• The ISM Manager, who facilitates the implementation of this policy through appropriate rules and procedures.

• All ESGeo Srl personnel, to whom specific roles and responsibilities are assigned. They must have adequate competence to carry out the required tasks, and therefore must be properly informed and trained regarding the company's objectives in terms of quality, information security, personal data protection, service management, business continuity, occupational health and safety, and environmental management. Records on education, training, skills, experience and qualifications are defined and maintained. All personnel are responsible for reacting promptly to security incidents and/or product/service non-conformities and for reporting to Management any weaknesses identified in the system.

• Customers and Suppliers involved in the management of implemented products/services, which fall within the scope of the Integrated Management System. They are required to comply with the Integrated Policy of ESGeo Srl.

3.2 Violations

Senior management is personally involved in complying with and implementing these principles and is committed to ensuring that this policy is understood, shared, implemented, and enforced by all its employees and collaborators, while also sharing it with all stakeholders.

Considering the achievement of the set objectives to be of fundamental importance, the Integrated Management System is constantly monitored and it is acknowledged that any action that does not comply with this company policy will be examined and may give rise to the adoption of measures in accordance with the provisions of the law and with the applicable contractual regimes on a case-by-case basis.